El arte del engaño

Controlar el factor humano de la seguridad

Kevin D. Mitnick
Y William L. Simon
Prólogo de Steve Wozniak

Analizados por kineticstomp, revisada y ampliada por SWIFT

Para Reba Vartanian, Jaffe Shelly, Leventhal Chickie, y Mitchell Mitnick, y por la tarde Alan Mitnick, Mitnick Adán, y Biello Jack

Para Arynne, Victoria y David Sheldon, Vincent, y Elena.

Ingeniería social
Ingeniería social utiliza la influencia y la persuasión para engañar a la gente convenciéndolos de que el ingeniero social es alguien que no es, o por la manipulación. Como resultado, el ingeniero social es capaz de tomar aprovecharse de la gente para obtener información con o sin el uso de tecnología.

“Traducido con el traductor on-line de google por eso con las disculpas del caso, si alguien quiere consulte con el texto original en ingles.”
Herve Volpe

Contenido

Prefacio

Nosotros, los humanos nacemos con un impulso interno para explorar la naturaleza de nuestro alrededor. Como los jóvenes, tanto Kevin Mitnick y yo estábamos intensamente curiosos sobre el mundo y con ganas de probarnos a nosotros mismos. Fuimos premiados con frecuencia en nuestra los intentos de aprender cosas nuevas, resolver puzzles y ganar en los juegos. Pero al mismo tiempo tiempo, el mundo que nos rodea nos enseñó las reglas de comportamiento que limitaban nuestro interior impulso hacia la exploración libre. Para nuestros más audaces científicos y tecnológicos empresarios, así como para la gente como Kevin Mitnick, después de este impulso interior ofrece las más grandes emociones, permitiéndonos lograr cosas que otros creen que no pueden por hacer.

Kevin Mitnick es uno de las mejores personas que conozco. Pregunte a él, y él dirá: abiertamente que lo que solía hacer - ingeniería social - entrana la gente de órdenes de maniobra. Pero Kevin no es un ingeniero social. E incluso cuando estaba él, el motivo nunca fue a enriquecerse a sí mismo u otros daños. Eso no quiere decir que no hay delincuentes peligrosos y destructivos que hay que utilizar la ingeniería social para causar un daño real. De hecho, eso es exactamente por Kevin escribió este libro - para que le avise sobre ellos.

El arte del engaño muestra lo vulnerables que somos todos nosotros - gobiernos, empresas, y cada uno de nosotros personalmente - a las intrusiones de la ingeniería social. En este era consciente de la seguridad, que gastar grandes sumas en tecnología para proteger a nuestros redes y datos informáticos. Este libro destaca lo fácil que es engañar a los insiders y evitar toda esta protección tecnológica.

Ya sea que trabaje en los negocios o el gobierno, este libro ofrece un camino de gran alcance mapa para ayudarle a entender cómo el trabajo de los ingenieros sociales y lo que puede hacer para papel de ellos. Utilizando historias de ficción que son a la vez entretenido y revelador, Kevin y co-autor Bill Simon dar vida a las técnicas de lo social ingeniería inframundo. Después de cada historia, que ofrecen directrices prácticas para ayudar a protegerse contra las violaciones y las amenazas que están descritos.

Seguridad tecnológica deja grandes vacíos que la gente como Kevin nos puede ayudar cerca. Lee este libro y que finalmente se daran cuenta de que todos tenemos que recurrir a la Mitnick entre nosotros para recibir orientación.

Steve Wozniak

Prólogo

Algunos hackers destruir los archivos de las personas o unidades de disco duro entero, sino que son llamados crackers o vándalos. Algunos hackers novatos no se molestan en aprender la tecnología, sino que simplemente descargar herramientas de hacker para irrumpir en los sistemas informáticos, que son llamados script kiddies. Hackers más experimentados con conocimientos de programación desarrollar hacker programas y publicarlas en la Web y sistemas de boletines electrónicos. Y luego son personas que no tienen interés en la tecnología, sino utilizar el ordenador simplemente como una herramienta que les ayuda en el robo de dinero, bienes o servicios.
A pesar del mito creado por los medios de Kevin Mitnick, yo no soy un hacker malicioso. Pero me estoy adelantando.

INICIACIÓN
Mi camino se hizo probablemente temprano en la vida. Yo era un niño feliz y despreocupado, pero aburrido. Cuando mis padres se separaron yo tenía tres años, mi madre trabajaba como camarera Para ver conmigo entonces - un hijo único criado por una madre que puso en días largos, acosado en un horario a veces errático - habría sido ver a un joven en su propia casi todas las horas de vigilia. Yo era mi propia niñera.
Al crecer en una comunidad del Valle de San Fernando me dio la totalidad de Los Angeles para explorar, y por la edad de doce años que había descubierto una manera de viajar gratis a lo largo de toda la zona de mayor Los Ángeles. Me di cuenta un día en el autobús que la seguridad de la transferencia de autobuses que había comprado se basó en el patrón inusual de la perforadora de papel, que los controladores utilizados para conmemorar el día, hora y ruta en el hojas de transferencia. Un conductor amable, respondiendo a mi pregunta cuidadosamente plantados, me dijo dónde comprar ese tipo especial de ponche.
Las transferencias están destinadas a permitir cambiar de autobús y continuar un viaje a su destino, pero he trabajado la manera de utilizarlos para viajar a cualquier lugar que quería ir de forma gratuita. Realizar transferencias en blanco fue un paseo por el parque.
Los contenedores de basura en las terminales de autobuses estaban siempre llenos con los libros sólo en parte utilizados de las transferencias que los conductores arrojaban al final de los turnos. Con una almohadilla de espacios en blanco y el punzón, que podría marcar mi propio transferencias y viajar a cualquier parte que Los Ángeles fue autobuses. En poco tiempo, que casi había memorizado los horarios de los autobuses de todo el sistema. (Este fue un primer ejemplo de mi memoria sorprendente para algunos tipos de información, todavía puedo, hoy, recordar números de teléfono, contraseñas, y otros detalles aparentemente triviales, ya en mi infancia.)
Otro de los intereses personales que aparecieron en una edad temprana fue mi fascinación por hacer magia. Una vez que aprendí un nuevo truco funcionó, sería la práctica, la práctica, y practica un poco más hasta que lo dominaba. Hasta cierto punto, fue a través de magia que he descubierto el placer en la obtención de un conocimiento secreto.

Desde Phreak teléfono para Hacker.
Mi primer encuentro con lo que finalmente aprendí a llamar a la ingeniería social surgió durante mis años de secundaria cuando conocí a otro estudiante que fuimos atrapados en un pasatiempo llamado phreakin telefonico. Phreaking telefonicio es un tipo de piratería informática que le permite explorar la red telefónica mediante la explotación de los sistemas telefónicos y empleados de la compañía telefónica. Él me mostró truquitos que podía hacer con un teléfono, como la obtención de cualquier información de la compañía telefónica había en cualquier cliente, y el uso de un número de prueba secreta para hacer llamadas de larga distancia gratis.
(En realidad era gratis sólo para nosotros. Me enteré mucho más tarde que no era una prueba secreta número en absoluto. Las llamadas fueron, de hecho, se factura a alguna empresa MCI pobres cuenta).
Esa fue mi introducción a la ingeniería social de mi jardín de infantes, por así decirlo. Mi amigo y otro phreaker teléfonico conocí poco después que me escuche, ya que en cada pretexto hizo llamadas a la compañía telefónica. He oído lo que han dicho que suenen increíbles, he aprendido

acerca de las diferentes oficinas de la compañía telefónica, jerga, y los procedimientos. Pero que "la formación" no duró mucho tiempo, no tenía que hacerlo. Pronto lo estaba haciendo todo por mi cuenta, a medida que iba aprendiendo, haciendo que sea aún mejor que mis primeros profesores.

El curso de mi vida se había establecido y seguiría para los próximos quince años. De alto la escuela, una de mis bromas favoritas de todos los tiempos era el acceso no autorizado a los conmutadores telefónicos y el cambio de la clase de servicio de un compañeros phreaker. Cuando se hacia el intento de realizar una llamada desde su casa, se ponía un mensaje diciéndole que depositar una moneda de diez centavos, porque el interruptor de la compañía telefónica que había recibido de entrada indicó que estaba llamando desde un teléfono público. Yo se absorbí en todo lo relacionado con los teléfonos, no sólo de la electrónica, interruptores, y las computadoras, sino también la organización de la empresa, los procedimientos, y la terminología. Después de un tiempo, probablemente sabía más sobre el sistema telefónico que cualquier otro empleado. Y que había desarrollado mis habilidades de ingeniería social para el punto de que, a los diecisiete años, yo era capaz de hablar la mayoría de los empleados en telecomunicaciones casi cualquier cosa, si yo estaba hablando con ellos en persona o por teléfono.
Mi muy publicitada carrera de hacking en realidad comenzó cuando yo estaba en la secundaria. Aunque no puedo describir el detalle, basta decir que uno de los motores de las fuerzas de mi hacks a principios iba a ser aceptado por los chicos en el grupo de hackers.
En ese entonces se utilizó el término hacker para referirse a una persona que pasó una gran cantidad de pequeños ajustes de tiempo con el hardware y software, ya sea para el desarrollo más eficiente de programas o para evitar pasos innecesarios y hacer el trabajo más rápidamente. El plazo se ha convertido en algo peyorativo, que lleva el significado de "criminal malicioso". En estas páginas el término de la forma en que he usado siempre - en su más temprana y más sentido benigno.

Después de la secundaria, estudié las computadoras en el Centro de Aprendizaje de Computación en Los Angeles. En pocos meses, el gerente de la escuela de computación di cuenta que tenía encontró la vulnerabilidad en el sistema operativo y ganó completo privilegios administrativo en su minicomputadora IBM. El mejor equipo de expertos en su personal docente no podía entender cómo había hecho esto. En lo que podría haber sido uno de los primeros ejemplos de "contratar a los hacker", me dieron una oferta que no podía rechazar: ¿Es un proyecto de honores para mejorar la seguridad de la escuela de computación, o la cara suspensión para hackear el sistema. Por supuesto, he optado por hacer el proyecto honores, y terminé de graduarse con honores.
Convertirse en un ingeniero social. Algunas personas salir de la cama cada mañana temiendo su rutina de trabajo diario en las minas de sal proverbial. He tenido la suerte de disfrutar de mi trabajo. particular, no te puedes imaginar el desafío, la recompensa y el placer que tenía el tiempo que pasé como un investigador privado. Yo estaba afilando mis talentos en el arte de performance llamado social de ingeniería (que la gente haga cosas que normalmente no haría para un extranjero) y que se pagó por ella.
Para mí no fue difícil convertirse en experto en ingeniería social. Del lado de mi padre la familia había estado en el campo de las ventas por generaciones, por lo que el arte de la influencia y la persuasión podría haber sido un rasgo hereditario. Cuando se combinan ese rasgo con una inclinación de engañar a la gente, usted tiene el perfil de un ingeniero social típico.

Se podría decir que hay dos especialidades dentro de la clasificación del puesto de artista de la estafa. Alguien que estafa y engaña a la gente y su dinero pertenece a una sub-especialidad, el estafador. Alguien que utiliza el engaño, la influencia y persuasión frente a las empresas, por lo general dirigidas a la información, pertenece a la otros sub-especialidad, el ingeniero social.

Desde el momento de mi bus de transferencia de truco, cuando yo era demasiado joven para saber que había algo malo con lo que estaba haciendo, Yo había empezado a reconocer el talento para descubrir los secretos que no se suponía que tienen. He construido en ese talento

con el engaño, conociendo el idioma, y el desarrollo una habilidad bien ainado de manipulación. Una forma en que trabajó en el desarrollo de las habilidades de mi oficio, si se me permite llamarlo un oficio, fue a recoger a algún tipo de información que realmente no se preocupan de ver si es podía hablar a alguien en el otro extremo del teléfono en su prestación, sólo para mejorar mis habilidades. De la misma manera que solía practicar mis trucos de magia, practiqué pretextos. A través de estos ensayos, pronto me di cuenta que podía adquirir prácticamente cualquier información que objetivo.

Como describí en el testimonio ante el Congreso antes de que los senadores Lieberman y años más tarde Thompson:

He tenido acceso no autorizado a sistemas informáticos en algunas de las mayores las empresas en el planeta, y he penetrado con éxito algunos de los sistemas mas resistentes equipo se haya desarrollado. He utilizado dos técnicas y no técnicas medios para obtener el código fuente para varios sistemas operativos y dispositivos de telecomunicaciones para estudiar sus vulnerabilidades y su funcionamiento interior.

Toda esta actividad fue realmente para satisfacer mi propia curiosidad, para ver qué podía hacer; y obtener información secreta sobre los sistemas operativos, los teléfonos celulares, y cualquier otra cosa que agita mi curiosidad.

REFLEXIONES FINALES

He reconocido desde mi arresto que las acciones que tomé fueron ilegales, y que las invasiones de la privacidad comprometidos.

Mis delitos fueron motivados por la curiosidad. Yo quería saber todo lo que podía acerca de cómo las redes de teléfono funcionaba y la ins-y-outs de la seguridad informática. Yo pasé de ser un niño al que le encantaba realizar trucos de magia para convertirse en el hacker mundial más famoso, temido por las corporaciones y el gobierno. Al reflexionar hacia atrás en mi vida durante los últimos 30 años, admito que me hizo algunas extremadamente pobres decisiones, impulsado por la curiosidad, el deseo de aprender acerca de la tecnología, y la necesidad de un buen desafío intelectual.

Soy una persona diferente ahora. Estoy convirtiendo mis talentos y los amplios conocimientos He reunido información sobre las tácticas de ingeniería social y de seguridad para ayudar a gubernamentales, empresas e individuos para prevenir, detectar, y responder las amenazas de la seguridad de la información.

Este libro es una forma más que puedo utilizar mi experiencia para ayudar a otros a evitar los esfuerzos de los ladrones de información maliciosa del mundo. Creo que se encuentran las historias agradables, abro los ojos, y la educación.

Introducción:

Este libro contiene una gran cantidad de información sobre seguridad de la información y de ingeniería social. Para ayudarle a encontrar su camino, he aquí una breve explicación sobre cómo esta organizado este libro:

En la Parte 1 voy a revelar el eslabón más débil de la seguridad y mostrar por qué usted y su empresa están en riesgo de ataques de ingeniería social.

En la Parte 2 veremos cómo ingenieros sociales con su confianza, su deseo de ser útil, su simpatía y su credulidad humana son juguetes para conseguir lo que quieren.
Los cuentos de ficción de los ataques típicos se demostrará que los ingenieros sociales pueden llevar muchos sombreros y muchas caras. Si usted piensa que no ha encontrado nunca una, está probablemente equivocado. Se reconoce a un escenario que ha experimentado en estas historias y me pregunto si había un cepillo con la ingeniería social? Que muy bien podría. Pero una vez que haya leído los capítulos del 2 al 9, usted sabrá cómo obtener la ventaja cuando el ingeniero social viene después de la llamada.

En la Parte 3 es la parte del libro donde se ve cómo la apuesta de la alta ingenieria social, en historias inventadas que muestran cómo se puede pasar a sus instalaciones corporativas, robar el tipo de secreto que puede hacer o deshacer a su compañía, e impedir su hi-tech medidas de seguridad. Los escenarios en esta sección le hará consciente de las amenazas que van desde la venganza de un simple empleado hasta ciber-terrorismo. Si el valor de la información para mantener el negocio funcionando y la privacidad de sus datos, usted quiero leer los capítulos 10 al 14 de principio a fin.
Es importante tener en cuenta que a menos que se indique lo contrario, las anécdotas de este libro son pura ficción.

En la Parte 4 veremos que predicar con el ejemplo las empresas sobre cómo evitar el éxito en ingenieria social de los ataques contra su organización. El capítulo 15 ofrece un plan para un exitoso programa de entrenamiento de seguridad. Y el capítulo 16 sólo podría salvar su cuello - es una política de seguridad completa se puede personalizar para su organización e implementar de inmediato para mantener a su empresa y seguro de información.
Por último, he proporcionado un panorama de una seguridad en una sección, que incluye listas de control, tablas y gráficos que resumen la información clave que puede utilizar para ayudar a su los empleados de frustrar un ataque de ingeniería social en el trabajo. Estas herramientas también proporcionan información valiosa que puede utilizar en la elaboración de su propio programa de entrenamiento de seguridad.
A lo largo del libro encontrará también varios elementos útiles: cajas de Lingo proporcionar las definiciones de la ingeniería social y la terminología hacker; Mensajes Mitnick ofrecen breves palabras de sabiduría para ayudar a fortalecer su estrategia de seguridad, y las notas de fondo y barras laterales dan interesantes o más de la información.

Parte 1 Detrás de las escenas.

Capítulo 1
Eslabón más débil de Seguridad
Una empresa puede haber comprado las mejores tecnologías de seguridad que el dinero puede comprar, capacitando a sus miembros tan bien que se encierran todos los secretos antes de ir a casa por la noche, y los guardias contratados de mayor seguridad en el edificio de la empresa del negocio.

Que la empresa sigue siendo totalmente vulnerables.

Las personas pueden seguir todas las mejores prácticas de seguridad recomendadas por los expertos, servilmente instalar todos los productos de seguridad recomendadas, y estar atentos a fondo sobre la configuración adecuada del sistema y la aplicación de los parches de seguridad.

Esos individuos son todavía completamente vulnerable.

EL FACTOR HUMANO
Al testificar ante el Congreso no hace mucho, yo explique que muchas veces podía llegar a contraseñas y otras piezas de información sensible de su empresa fingiendo ser otra persona y sólo pedirla.
Es natural que se anhela una sensación de seguridad absoluta, lo que lleva a muchas personas a resolver por un falso sentido de seguridad. Considere la posibilidad de que el propietario responsable y amoroso que cuenta con un Médico, una cerradura del vaso que se conoce como pickproof, instalado en su puerta de frente para proteger a su esposa, sus hijos y su hogar. Ahora está cómodo que ha hecho su familia mucho más segura contra intrusos. Pero ¿qué pasa con el intruso que rompe una ventana, o descifra el código de la puerta del garaje? ¿Qué tal la instalación de un robusto sistema de seguridad? Mejor, pero todavía no hay garantía. Cerraduras caro o no, el dueño de casa sigue siendo vulnerable.

¿Por qué? Debido a que el factor humano es realmente el eslabón más débil de seguridad.
La seguridad es a menudo más que una ilusión, una ilusión a veces incluso peores cuando la credulidad, ingenuidad, ignorancia entran en juego. La mayor parte del mundo respetado científico del siglo XX, Albert Einstein, es citado diciendo, "Sólo dos cosas son infinitas, el universo y la estupidez humana, y no estoy seguro sobre el primero. "Al final, los ataques de ingeniería social puede tener éxito cuando la gente son tontos o, más comúnmente, simplemente ignorantes acerca de buenas prácticas de seguridad.

Con la misma actitud que nuestra seguridad consciente de dueño de casa, mucha información tecnología (IT) sostienen la idea errónea de que han hecho sus empresas en gran medida inmune a los ataques porque se han desplegado de seguridad estándar productos - firewalls, sistemas de detección de intrusos, o una autenticación más fuerte dispositivos tales como el tiempo basado en tokens biométricos o tarjetas inteligentes. Cualquiera que piense que los productos de seguridad sólo ofrecen la verdadera seguridad es la solución para. la ilusión de la seguridad. Es un caso de vivir en un mundo de fantasía: Inevitablemente, más adelante, si no antes, sufrir un incidente de seguridad.

Como se señaló el consultor de seguridad Bruce Schneier dice, "La seguridad no es un producto, es parte de un proceso" Por otra parte, la seguridad no es un problema de la tecnología - es un pueblo y gestión de problemas.
Como desarrolladores de inventar cada vez mejor las tecnologías de seguridad, por lo que es cada vez más difícil de explotar las vulnerabilidades técnicas, los atacantes se volverán más y más para explotar el elemento humano. Descifrando el firewall humano es a menudo fácil, no requiere ninguna inversión más allá del costo de una llamada telefónica, e implica un riesgo mínimo.

Un caso clásico de ENGAÑO

¿Cuál es la mayor amenaza para la seguridad de los activos de su empresa? Eso es fácil: la ingeniería social - un mago sin escrúpulos que tiene que ver con la mano izquierda mientras con la derecha roba sus secretos. Este personaje es a menudo tan amable, locuaz, y obliga a que se siente agradecido por haberlo encontrado.

Echa un vistazo a un ejemplo de ingeniería social. No mucha gente hoy en día todavía recuerdo el joven llamado Marcos Stanley Rifkin y su pequeña aventura con el ahora difunto Security Pacific National Bank de Los Angeles. Las cuentas de su escapada variar, y Rifkin (como yo) nunca ha dicho a su propia historia, por lo que el a continuación se basa en los informes publicados.

Rompiendo el código

Un día en 1978, Rifkin moseyed autorizó a la Seguridad del Pacífico a solo personal autorizado tirar un cable de transferencia a la habitación, donde el personal enviaba y recibía transferencias por un total de varios miles de millones de dólares todos los días.

Estaba trabajando para una empresa contratada para desarrollar un sistema de respaldo para la sala de datos, en caso de que su ordenador principal se cayera . Ese papel le dio el acceso a los procedimientos de transferencia, incluyendo cuando los funcionarios del Banco organizaban una transferencia para ser enviada. Se había enterado de que funcionarios de los bancos que fueron autorizados para las transferencias de seguridad se les asignaba un código todos los dias a la mañana, que estaban muy bien guardados, para utilizar la sala de seguridad .

En la sala de seguridad de los empleados se ahorró la molestia de tratar de memorizar el código de cada día: Ellos escribieron el código en una hoja de papel y se podía ver fácilmente. Este particular dia de noviembre Rifkin tuvo un motivo específico de su visita. Quería echar un vistazo a ese documento.

Al llegar a la sala de seguridad, tomó algunas notas sobre los procedimientos de operación, supuestamente para asegurarse de que el sistema de copia de seguridad estaba correctamente con el los sistemas regulares. Mientras tanto, superficialmente leia el código de seguridad de la hoja de papel publicada, y memorizarla. Unos minutos más tarde salió. Como él dijo después, se sentía como si hubiera ganado la lotería.

Hay, esta cuenta bancaria en Suiza .....

Salió de la habitación a las 3 de la tarde, se dirigió directamente al teléfono público en el vestíbulo de mármol del edificio, donde depositó una moneda y marcó el cuarto de seguridad de la transferencia. Luego cambió sombreros, transformándose de Stanley Rifkin, consultor del Banco, con Mike Hansen, un miembro del banco Departamento Internacional.

Según una fuente, la conversación fue algo como esto:

"Hola, este es Mike Hansen del internacional", dijo a la joven que contestó el teléfono.

Ella le preguntó por el número de la oficina. Que era un procedimiento estándar, y fue él preparado: "286", dijo.

La joven le preguntó: "Bueno, ¿cuál es el código?"

Rifkin ha dicho que su adrenalina potencia el latido del corazón "recogió su ritmo" en este punto. Él respondió sin problemas, "4789". Luego se procedió a dar instrucciones para la transferencia "Diez millones de dólares, con 200 mil dólares exactamente" a la Fundación Irving Compañía en Nueva York, para el crédito del Banco Wozchod Handels de Zurich, Suiza, donde había establecido ya una cuenta.

La joven dijo entonces: "Bueno, ya entendí. Y ahora necesito el número entre oficinas".

Rifkin rompió a sudar, lo que fue una pregunta que no había anticipado, algo que se había caído por las grietas de su investigación. Pero se las arregló para permanecer en carácter, actuó como si todo estaba bien, y sobre el terreno sin perder el ritmo de la respuesta, "Déjame ver, yo te llamo de vuelta". Cambió sombreros vez de nuevo a llamar a otro departamento en el banco, esta vez pretende ser un empleado de la sala de cable de transferencia. Obtuvo el número de asentamiento y llamó a la chica de nuevo.

Ella tomó el número y dijo: "Gracias." (Dadas las circunstancias, dándole las gracias él tiene que ser considerado muy irónico.)

Lograr el cierre
Pocos días después voló a Suiza Rifkin, cogió su dinero en efectivo, y entregó $ 8 millones a una agencia rusa de un montón de diamantes. Él voló de regreso, pasando a través de Aduanas de EE.UU. con las piedras ocultas en un cinturón de dinero. Se había realizado el robo de banco más grande de la historia - y hacerlo sin usar un arma de fuego, incluso sin un equipo. Curiosamente, su travesura finalmente lo hizo en las páginas del Guinness
Libro de los Récords en la categoría de "fraude más grande de equipo."

Stanley Rifkin ha utilizado el arte del engaño - las habilidades y técnicas que hoy se llama ingeniería social. La planificación minuciosa y un buen regalo del palique es todo lo que realmente tuvo.
Y eso es lo que trata este libro - las técnicas de ingeniería social (a la que su servidor es competente) y la forma de defenderse de ser utilizado en la empresa.

LA NATURALEZA DE LA AMENAZA
La historia Rifkin deja perfectamente claro lo engañoso que nuestro sentido de seguridad puede ser. Incidentes como este - bueno, tal vez no $ 10 millones robos, pero los incidentes perjudiciales sin embargo - están ocurriendo todos los días. Usted podría estar perdiendo dinero ahora mismo, o alguien puede robar los planes de nuevos productos, y que ni siquiera lo saben. Si no ha sucedido ya a su compañía, no es una cuestión de si va a pasar, pero cuando.

Una preocupación creciente
El Computer Security Institute, en su encuesta de 2001 de los delitos informáticos, informó que el 85 por ciento de las organizaciones encuestadas había detectado violaciones a la seguridad informática en los últimos doce meses. Eso es un número asombroso: sólo quince de cada cien organizaciones que respondieron fueron capaces de decir que no había tenido un fallo de seguridad durante el año. Igualmente sorprendente fue el número de organizaciones que informaron que habían sufrido pérdidas financieras debido a las infracciones equipo: el 64 por ciento. Más de la mitad de las organizaciones había problemas financieros. En un solo año.
Mi propia experiencia me lleva a creer que los números en los informes de este tipo es aumentar de forma errónea. Sospecho de la agenda de las personas que realizan la encuesta. Pero eso no quiere decir que el daño no es muy extensa. Los que no piensan planificar un incidente de seguridad está planeando el fracaso.
Los productos comerciales de seguridad desplegado en la mayoría de las empresas se dirigen principalmente a la protección contra los intrusos informáticos aficionados, como los jóvenes conocido como script kiddies. De hecho, estos hackers aspirante descargan software en su mayoría tan sólo son una molestia. Las mayores pérdidas, las amenazas reales, vienen de los atacantes sofisticados con objetivos bien definidos que están motivados por beneficio económico. Estas personas se centran en un objetivo a la vez en lugar de, como el aficionados, tratando de infiltrarse en tantos sistemas como sea posible. Mientras intrusos aficionados solo tiene equipo que van por la cantidad, el objetivo de los profesionales de la información van por calidad y valor. Tecnologías como dispositivos de autenticación (para probar la identidad), control de acceso (Para administrar el acceso a archivos y recursos del sistema), y detección de intrusos sistemas (el equivalente electrónico de alarmas contra robo) son necesarios para una empresa programa de seguridad. Sin embargo, es típico de hoy para que una empresa gastar más dinero en café que en el despliegue de medidas para evitar que la organización ataques a la seguridad. Así como la mente criminal no puede resistir la tentación, la mente hacker es conducida a encontrar formas de evitar medidas de seguridad potente tecnología. Y en muchos casos, que hacen que, al dirigirse a las personas que utilizan la tecnología.

Prácticas Engañosas
Hay un dicho popular de que un ordenador seguro es uno que está apagado. Inteligente, pero falsa: El pretexter simplemente alguien habla en ir a la oficina y convertir ese ordenador. Un adversario que desea que su información se puede obtener que, por lo general en una de varias

maneras diferentes. Es sólo una cuestión de tiempo, paciencia, personalidad, y la persistencia. Ahí es donde el arte del engaño entra en juego Para derrotar a las medidas de seguridad, un atacante, intruso, o un ingeniero social debe encontrar una manera de engañar a un usuario de confianza en la información que revela, o engañar a un desprevenido marca en que le proporcione el acceso. Cuando los empleados de confianza son engañados, influencia, o manipulados para que la información sensible que revela, o la realización de acciones que crean un agujero de seguridad para el atacante de deslizarse a través, no la tecnología en el mundo puede proteger a un negocio. Al igual que los criptoanalistas son a veces capaces de revelar el texto de un mensaje codificado por encontrar un punto débil que les permite pasar por alto la tecnología de encriptación, el engaño social practicada en el uso ingenieros a sus empleados para evitar la tecnología de seguridad.

Abuso de confianza

En la mayoría de los casos, el éxito de los ingenieros sociales tienen fuertes habilidades de la gente. Es encantador, amable y fácil como los rasgos sociales necesarios para el establecimiento de una rápida, relación de confianza. Un ingeniero social experimentado es capaz de acceder a prácticamente cualquier información específica mediante el uso de las estrategias y tácticas de su oficio.

Técnicos ingeniosos han desarrollado cuidadosamente seguridad de la información, las soluciones para minimizar los riesgos relacionados con el uso de las computadoras, sin embargo, no se abordan la vulnerabilidad más importante, el factor humano. A pesar de nuestro intelecto, que los seres humanos - usted, yo, y todos los demás - siguen siendo la amenaza más grave a cada otro de seguridad.

Nuestro carácter nacional

No somos conscientes de la amenaza, especialmente en el mundo occidental. En los Estados Unidos Estados, sobre todo, no estamos capacitados para sospechar de los demás. Se nos enseña "Amarás a tu prójimo" y tener confianza y fe en cada uno. Tenga en cuenta cómo difícil que es para las organizaciones de vigilancia de vecindario para que la gente a cerrar sus casas y automóviles. Este tipo de vulnerabilidad es evidente, y sin embargo parece ser ignorado por muchos de los que prefieren vivir en un mundo de ensueño - hasta que se queme. Sabemos que no todas las personas son amables y honestas, pero muchas veces vivimos como si. Esta encantadora inocencia ha sido el tejido de la vida de los estadounidenses y lo que es doloroso renunciar a él. Como una nación que hemos construido en nuestro concepto de libertad que los mejores lugares para vivir son aquellas en que las cerraduras y las llaves son lo menos necesarias.

La mayoría de la gente va en el supuesto de que no se deje engañar por otros, según en la creencia de que la probabilidad de ser engañado es muy baja, el atacante, la comprensión de esta creencia común, hace que el sonido de su petición tan razonable que no levanta ninguna sospecha, todo el tiempo la explotación de la confianza de la víctima.

La inocencia de la organización

Que la inocencia que es parte de nuestro carácter nacional se hizo evidente de nuevo cuando computadoras fueron los primeros en estar conectados de forma remota. Recordemos que el ARPANET (la Avanzada del Departamento de Defensa de Proyectos de la Red de Investigación de la Agencia), el antecesora de la Internet, fue diseñado como una forma de compartir la investigación información entre el gobierno, la investigación y las instituciones educativas. El objetivo
era la libertad de información, así como el avance tecnológico. Muchos
las instituciones educativas por lo tanto, establecer sistemas de computadora con muy poca o ninguna la seguridad. Uno de ellos observó software libertario, Richard Stallman, aunque se negó a proteger a su cuenta con una contraseña.

Pero con Internet se utiliza para el comercio electrónico, los peligros de la debilidad la seguridad en nuestro mundo interconectado han cambiado dramáticamente. El despliegue de más la tecnología no va a resolver el problema de la seguridad humana.

Basta con mirar a nuestros aeropuertos en la actualidad. La seguridad se ha convertido en algo fundamental, sin embargo, está alarmado por los informes de los medios de comunicación de los viajeros que han sido capaces de burlar la seguridad y portar armas potencial últimos puestos de control. ¿Cómo es posible durante un tiempo cuando nuestros aeropuertos se encuentran en un estado de alerta? Son los detectores de metales no? No. El problema no son las máquinas. El problema es el factor humano: la gente dotación de las máquinas. Las autoridades del aeropuerto puede encauzar la Guardia Nacional y instalar detectores de metales y sistemas de reconocimiento facial, pero la educación de la primera línea seguridad del personal de la manera correcta de pasajeros pantalla es mucho más probable que ayude.
El mismo problema existe en el gobierno, los negocios y la educación instituciones de todo el mundo. A pesar de los esfuerzos de los profesionales de la seguridad, información en todas partes sigue siendo vulnerable y seguirá siendo visto como una madura objetivo de los atacantes con conocimientos de ingeniería social, hasta que el eslabón más débil en el cadena de seguridad, el vínculo humano, se ha fortalecido.

Ahora más que nunca tenemos que aprender a dejar de pensar en un deseo y se vuelven más consciente de las técnicas que están siendo utilizados por aquellos que intentan atacar a los confidencialidad, integridad y disponibilidad de nuestros sistemas y redes.
Hemos llegado a aceptar la necesidad de conducir a la defensiva, es el momento de aceptar y aprender la práctica de la informática a la defensiva.
La amenaza de una ruptura en la que viola su privacidad, su mente, o el de tu empresa sistemas de información pueden no parecer real, hasta que sucede. Para evitar una costosa dosis de realidad, todos tenemos que ser conscientes, educados, atentos, y de manera agresiva protección de nuestros activos de información, nuestra información personal, y nuestra infraestructuras críticas del país. Y debemos poner en práctica las precauciones en la actualidad.

TERRORISTAS Y ENGAÑO
Por supuesto, el engaño no es una herramienta exclusiva de la ingeniería social. Físico el terrorismo hace que la noticia más importante, y nos hemos dado cuenta como nunca antes que el mundo es un lugar peligroso. La civilización es, después de todo, sólo una fina capa.
Los ataques contra Nueva York y Washington, DC, en septiembre de 2001 infundido tristeza y el miedo en los corazones de cada uno de nosotros - no sólo los estadounidenses, pero wellmeaning
personas de todas las naciones. Ahora estamos alertados del hecho de que hay terroristas obsesivo ubicado en todo el mundo, y - capacitación y espera poner en marcha ataques contra nosotros.
El esfuerzo intensificado recientemente por nuestro gobierno ha incrementado los niveles de nuestra
seguridad de la conciencia. Tenemos que estar alerta, en guardia contra toda forma de el terrorismo. Tenemos que entender cómo los terroristas traición crear falsas identidades, asumir roles como estudiantes y vecinos, y se funden en la multitud.
Ocultan sus verdaderas creencias, mientras que traman contra nosotros - la práctica de trucos de engaño similares a las que se lee en estas páginas.
Y mientras, a lo mejor de mi conocimiento, los terroristas aún no ha utilizado social ingeniería de artimañas para infiltrarse en las corporaciones, las plantas de tratamiento de agua, electricidad
instalaciones de generación, o de otros componentes vitales de nuestra infraestructura nacional, la
potencial está ahí. Es demasiado fácil. La toma de conciencia de seguridad y políticas de seguridad
que espero que se puso en marcha y ejecutadas por la alta dirección empresarial porque de este libro llegará justo a tiempo.
ACERCA DE ESTE LIBRO
Seguridad de la empresa es una cuestión de equilibrio. Demasiado poca seguridad sale de su compañía vulnerable, pero un énfasis excesivo en la seguridad se pone en el camino de la

asistir a los negocios, inhibiendo el crecimiento de la empresa y la prosperidad. La desafío es lograr un equilibrio entre seguridad y productividad.
Otros libros se centran en la seguridad de la empresa en tecnología de hardware y software, y no cubren adecuadamente la amenaza más grave de todos: el engaño humano. La propósito de este libro, en cambio, es para ayudarle a entender cómo usted, sus compañeros de trabajo,
y otros en su empresa están siendo manipulados, y el que las barreras puede erigir a dejar de ser víctimas. El libro se centra principalmente en la no-técnicos métodos que los intrusos hostiles utilizan para robar información, poner en peligro la integridad de información que se cree que es seguro, pero no lo es., o destruir la obra de la empresa del producto.
Mi tarea se ve dificultada por una simple verdad: todos los lectores han sido manipulada por los expertos de cola de todos los tiempos en la ingeniería social - sus padres. Ellos encontraron la manera de llegar - "por su propio bien" - para hacer lo que a ellos les parecía. Padres se convierten en grandes narradores de la misma manera que ingenieros sociales hábilmente desarrollan historias muy plausible, razones y justificaciones para el logro de sus objetivos. Sí, fuimos moldeados por todos nuestros padres: benevolente (ya veces no tan benévolo) los ingenieros sociales.
Condicionada por que la formación, nos hemos convertido en vulnerables a la manipulación. Nosotros
iba a vivir una vida difícil si tuviéramos que estar siempre en guardia, desconfiaba de otros, preocupados de que podría convertirse en víctima de alguien tratando de tomar aprovechan de nosotros. En un mundo perfecto implícitamente a confiar en los demás, seguro que las personas que se encuentran van a ser honesto y confiable. Pero lo que sí
No vivimos en un mundo perfecto, y lo que tenemos que ejercer un nivel de vigilancia para repeler a los esfuerzos engañosa de nuestros adversarios.
Las partes principales de este libro, partes 2 y 3, se compone de historias que muestran que los ingenieros sociales en acción. En estas secciones se podrá leer acerca de:
• ¿Qué phreakers descubrieron hace años: Un método para obtener una mancha de número de teléfono no de la compañía telefónica.
• Existen varios métodos diferentes usados por los atacantes para convencer incluso a alerta, sospechoso
los empleados a revelar sus nombres de usuario y contraseñas equipo.
• ¿Cómo un director de Centro de Operaciones colaborado en permitir a un atacante robar su información de la empresa de productos más secretos.
• Los métodos de un atacante que engañó a una mujer en la descarga de software que los espías en cada golpe de teclado que hace y mensajes de correo electrónico los detalles de él.
• ¿Cómo los investigadores privados obtener información sobre su empresa, y sobre usted personalmente, que prácticamente se puede garantizar que un escalofrío por la columna.
Se podría pensar al leer algunas de las historias en las partes 2 y 3 que no están posible, que nadie podía tener éxito en conseguir lejos con las mentiras, sucio trucos y esquemas de, se describe en estas páginas. La realidad es que en cada caso, estas historias describen los eventos que pueden suceder y suceden, muchos de ellos están pasando
todos los días en algún lugar del planeta, incluso a su negocio mientras usted lee esto libro.
El material de este libro será una verdadera revelación cuando se trata de proteger su negocio, sino también personalmente desviar los avances de un ingeniero social proteger la integridad de la información en su vida privada.
En la Parte 4 de este libro que cambiar de marcha. Mi objetivo aquí es ayudar a crear la las políticas necesarias de la empresa y la formación para la sensibilización para reducir al mínimo las posibilidades de
a sus empleados cada vez que se deje engañar por un ingeniero social. Comprensión de la estrategias, métodos y tácticas de la ingeniería social le ayudará a prepararse para

implementar controles razonables para proteger sus activos de TI, sin menoscabo de su
la productividad de la empresa.
En resumen, he escrito este libro para aumentar su conciencia sobre la grave amenaza
planteados por la ingeniería social, y que le ayudarán a asegurarse de que su compañía y su
los empleados tienen menos probabilidades de ser explotados de esta manera.
O tal vez debería decir, mucho menos probabilidades de ser explotados nunca más.

Parte 2: El arte del atacante

Capítulo 2
Cuando la información no es inocuo
¿Qué la mayoría de la gente piensa es la amenaza real de los ingenieros sociales? ¿Qué debe
que hacer para estar en guardia?
Si el objetivo es capturar un premio muy valioso - por ejemplo, un componente vital de la
capital intelectual de la compañía - tal vez entonces lo que se necesita es, en sentido figurado, a
un
fuerte bóveda y en mayor medida los guardias armados. ¿No?
Pero en la realidad penetra la seguridad de una empresa a menudo comienza con el malo
obtener alguna información o algún documento que parece tan inocente,
lo cotidiano y sin importancia, que la mayoría de personas de la organización no se ve
ninguna razón por la cual debe ser el elemento protegido y restringido
Valor oculto DE LA INFORMACIÓN
Mucha de la información aparentemente inocua en posesión de una empresa es
apreciado
por un atacante de ingeniería social, ya que puede jugar un papel vital en su esfuerzo por
vestirse con un manto de credibilidad.
A lo largo de estas páginas, me voy a mostrar cómo los ingenieros sociales no lo
lo hacen por lo que le permite "testigo" de los ataques por sí mismo - a veces la presentación de
la acción desde el punto de vista de la gente que es víctima, lo que le permite poner
Póngase en sus zapatos y medir cómo usted (o tal vez uno de sus
empleados o compañeros de trabajo) podrían haber respondido. En muchos casos, usted también
experiencia de los mismos hechos desde la perspectiva de la ingeniería social.
La primera historia que mira a una vulnerabilidad en el sector financiero.
CREDITCHEX
Durante mucho tiempo, los británicos dieron con un sistema bancario muy congestionada. Como
común, honrado ciudadano, que no podía caminar en la calle y abrir una cuenta bancaria
cuenta. No, el banco no la posibilidad de aceptar como cliente a menos que
persona que ya está bien establecida como un cliente le proporcionó una carta de
recomendación.
Una gran diferencia, por supuesto, en el mundo de la banca aparentemente igualitaria de
hoy en día. Y nuestra moderna facilidad de hacer negocios es nada más en evidencia que
en un amistoso, democrático de Estados Unidos, donde casi cualquier persona puede entrar en
un banco y
fácil abrir una cuenta corriente, ¿verdad? Bueno, no exactamente. La verdad es que los bancos
comprensiblemente tienen una reticencia natural a abrir. una cuenta de alguien que
sólo podría tener un historial de cheques sin fondos - que sería tan bienvenida
como una hoja de antecedentes penales del banco de cargos de robo o malversación de fondos.
Así que es una práctica habitual
en muchos bancos para obtener una rápida pulgar hacia arriba o pulgar abajo, en una nueva
perspectiva
de los clientes.
Una de las grandes empresas que contratan a los bancos para obtener esta información es un
equipo al que llamaremos CreditChex. Que proporcionan un valioso servicio a sus clientes, pero
Como muchas empresas, también pueden saberlo, ofrecer un servicio útil para saber
ingenieros sociales.

La primera llamada: Kim Andrews
"Banco Nacional, se trata de Kim. ¿Sabía usted desea abrir una cuenta hoy en día?"
"Hola, Kim. Tengo una pregunta para usted. ¿Ustedes utilizan CreditChex?"
"Sí".
"Cuando usted llama por teléfono a CreditChex, ¿cómo se llama el número que les da - se trata de una "identificación del comerciante?"
Una pausa, ella pesaba la cuestión, preguntándose de qué se trataba y si ella debe responder.
La persona que llama rápidamente continuó sin perder el ritmo:
"Porque, Kim, estoy trabajando en un libro. Se trata de investigaciones privadas".
"Sí", dijo, respondiendo a la pregunta con una nueva confianza, el placer de ser ayudar a un escritor.
"Así se llama una identificación del comerciante, ¿verdad?"
"Uh huh."
"Muy bien, muy bien. Porque quería masculina segura de que tenía la jerga de la derecha. Para el libro.
Gracias por su ayuda. Adiós, Kim. "
La segunda llamada: Chris Talbert
"National Bank, de nuevas cuentas, se trata de Chris."
"Hola, Chris. Se trata de Alex", dijo la persona que llama. "Soy un representante de servicio al cliente
CreditChex. Estamos haciendo una encuesta para mejorar nuestros servicios. ¿Puedes dedicarme un
par de minutos? "
Ella estaba contenta, y la persona que llama se encendió:
"Está bien - lo que es el horario de su oficina está abierta para los negocios?" Ella respondió, y continuó respondiendo a su serie de preguntas.
"¿Cuántos empleados en la sucursal de usar nuestro servicio?"
"¿Con qué frecuencia usted nos llama con una pregunta?"
"¿Cuál de los 800 números que nos ha asignado para que nos llama?"
"Tener a nuestros representantes siempre ha sido cortés?"
"¿Cómo es nuestro tiempo de respuesta?"
"¿Cuánto tiempo has estado en el banco?"
"¿Qué identificación del comerciante que se utiliza actualmente?"
"¿Te has encontrado alguna inexactitud en la información que he proporcionado usted? "
"Si usted tuviera alguna sugerencia para mejorar nuestro servicio, ¿cuáles serían?"
Y:
"¿Estaría usted dispuesto a llenar cuestionarios periódicos si se las envía a su rama? "
Ella estuvo de acuerdo, charlaron un poco, la llamada colgó y Chris volvió al trabajo.
La tercera convocatoria: Henry McKinsey
"CreditChex, esto es Henry McKinsey, ¿cómo puedo ayudarle?"
La persona que llamó dijo que era de Banco Nacional. Él dio la correcta identificación del comerciante y
luego dio el nombre y número de seguro social de la persona que estaba buscando información sobre. Henry pidió a la fecha de nacimiento, y la persona que le dio eso, también.
Después de unos momentos, Henry leer la lista de la pantalla de su ordenador.
"Wells Fargo informó NSF en 1998, una vez, la cantidad de 2.066 dólares." NSF - no fondos suficientes - es la jerga bancaria familiar para los controles que se han escrito cuando no hay suficiente dinero en la cuenta para cubrirlos.
"Cualquier actividad que desde entonces?"
"No hay actividades".
"¿Ha habido alguna otra pregunta?"
"Vamos a ver. Bueno, dos de ellos, tanto el mes pasado. Tercera de la Unión de Crédito de

Chicago. "Tropezó sobre el nombre de otro, las inversiones Schenectady Mutual,
y tenía que escribir. "Eso está en el estado de Nueva York", agregó.
Investigador privado en el Trabajo
Los tres de esas llamadas fueron hechas por la misma persona: un investigador privado que le
llamar a Oscar Gracia. Grace tenía un nuevo cliente, uno de sus primeros. Un policía hasta hace
unos pocos
meses antes, se encontró que parte de este nuevo trabajo era algo natural, pero algunos
ofrece un desafío a sus recursos e inventiva. Este vino abajo
firmemente en la categoría de desafío.
Los ojos duros privado de la ficción - las palas y el Sam Marlowes Felipe
- Pasar largas horas de la noche sentados en los coches a la espera de atrapar a un cónyuge
infiel.
De la vida real IP que hagan lo mismo. También hacen un menor por escrito acerca, pero no
menos importante
tipo de espionaje para los cónyuges en conflicto, un método que se apoya más en los social
habilidades de ingeniería que en la lucha contra el aburrimiento de las vigilias de la noche.
Nuevo cliente de Grace era una mujer que parecía como si tuviera un muy cómodo
presupuesto para ropa y joyas. Entró en su oficina un día y se sentó
en el sillón de cuero, la única que no tenía papeles apilados sobre el mismo. Se instaló
su gran bolso de Gucci en su escritorio con el logo se volvió hacia él y
anunció que planeaba decirle a su esposo que quería el divorcio, pero
admitió que "sólo un problema de muy poco."
Parecía que su marido estaba un paso por delante. Él ya se había retirado el dinero de
su cuenta de ahorros y una cantidad aún mayor de su cuenta de corretaje. Ella
quería saber dónde están sus activos habían sido buen recaudo, y su divorcio
abogado no fue ninguna ayuda en absoluto. Grace supuso el abogado fue uno de los
alta de la ciudad, de gran altura consejeros que no ensuciarse las manos en algo
sucio como de donde está el dinero.
Podría ayudar a Grace?
Él le aseguró que sería una brisa, citó a un cargo, los gastos facturados al costo, y
recogió un cheque por el primer pago.
Luego se enfrentó a su problema. ¿Qué hacer si usted nunca ha manejado un pedazo de
trabajo como esto antes y no se sabe muy bien cómo ir sobre la pista de un
dinero rastro? A avanzar por pasos de bebé. En este caso, de acuerdo mg a nuestra fuente, es
Historia de Grace.
Yo sabía de CreditChex y cómo los bancos utilizan el equipo - mi ex esposa solía
trabajar en un banco. Pero yo no sabía que el lenguaje y los procedimientos, y tratando de hacer
a mi
ex-sería una pérdida de tiempo.
Primer paso: Obtener la terminología recta y encontrar la manera de hacer la solicitud para
suena como yo sé lo que estoy hablando. En el banco me llama, el primer joven
mujer, Kim, era sospechosa cuando le pregunté sobre la forma en que se identifican
cuando CreditChex teléfono. Ella vaciló, no sabía si me dicen.
Se me desanime por eso? No un poco. De hecho, las dudas me dio una pista importante,
una señal de que tenía que suministrar una razón por la que iba a encontrar creíble. Cuando yo
trabajaba el Con
en ella acerca de hacer la investigación para un libro, que alivia sus sospechas. Usted dice que
está
un autor o un escritor de cine, y todo el mundo se abre.
Ella tenía otros conocimientos que han ayudado - cosas como la reforma
CreditChex requiere para identificar a la persona que está llamando, qué información
usted puede pedir, y el grande, lo que fue comerciante de Kim banco número de identificación. Yo
estaba dispuesto a hacer esas preguntas, pero su vacilación envió la bandera roja. Ella
compró la historia de la investigación libro, pero ella ya tenía una sospecha pocos insignificantes.
Si

que había estado más dispuestos manera correcta, yo le habría pedido que revelan más detalles sobre sus procedimientos.
LINGO
MARK: La víctima de una estafa.
QUEMA DE LA FUENTE: Un atacante se dice que quemó la fuente cuando
permite a la víctima a reconocer que el ataque ha tenido lugar. Una vez que la víctima
se da cuenta e informa a otros empleados o la gestión de la tentativa, que
llega a ser extremadamente difícil de explotar la misma fuente en futuros ataques.
Tienes que ir en su instinto, escuchar con atención lo que la marca está diciendo y cómo
lo está diciendo. Esta dama parecía lo suficientemente inteligente como para las campanas de alarma para empezar a irse
si me preguntas inusuales demasiados. Y aunque ella no sabía que yo
era o qué número estaba llamando, aún en este
negocio no quiere a nadie poner la palabra que en la búsqueda de
llamar a alguien para obtener información sobre el negocio. Eso es porque usted no
desea grabar la fuente - es posible que desee llamar a la oficina misma en otro momento.
Siempre estoy a la caza de pequeños signos que me da una lectura de cómo una cooperativa de persona, en una escala que va desde "Suena como una buena persona y creo que
todo lo que estás diciendo "a la" Llama a la policía, alerta a la Guardia Nacional, este tipo es para nada bueno. "
He leído Kim como un poco en el borde, por lo que acaba de llamar a alguien en una rama diferente.
En mi segunda convocatoria con Chris, el truco encuesta jugó a las mil maravillas. La táctica aquí es deslizar las cuestiones importantes de entre las consecuencias que se
utiliza para crear un sentido de credibilidad. Antes de que se me cayó la pregunta sobre el Número de identificación del comerciante con CreditChex, me encontré con un poco de última hora de prueba, pidiéndole
una pregunta personal acerca de cuánto tiempo había estado con el banco.
Una cuestión personal es como una mina terrestre - a algunas personas el paso por encima de ella y nunca
notificación, para otras personas, que explota y los envía corriendo por la seguridad. Así que si yo una pregunta personal y que responde a la pregunta y el tono de su voz
no cambia, lo que significa que probablemente no se muestra escéptico sobre la naturaleza de la solicitud. Puedo asegurar pedir el tratado después de la pregunta sin levantar su
sospechas, y probablemente me darán la respuesta que estoy buscando.
Una cosa más un IP bueno sabe: Nunca poner fin a la conversación después de recibir la información clave. Otra pregunta dos o tres, una pequeña charla, a continuación, que está bien decir adiós. Más tarde, cuando la víctima recuerda nada de lo que se le solicita,
probablemente será el último par de preguntas. El resto suele ser olvidado.
Así que Chris me dio su número de identificación del comerciante, y el número de teléfono que llaman a
hacer peticiones. Yo hubiera sido más feliz si hubiera llegado a hacer algunas preguntas sobre la cantidad de información que puede obtener a partir de CreditChex. Pero no fue mejor para empujar mi suerte.
Era como tener un cheque en blanco en CreditChex. Ahora podía llamar y obtener
información cada vez que quería. Ni siquiera tienen que pagar por el servicio. Ya que
Resultó que el representante CreditChex estaba feliz de compartir con exactitud la información que
quería: dos lugares marido de mi cliente había solicitado recientemente para abrir una cuenta.
Entonces, ¿dónde estaban los activos la que pronto será su ex esposa estaba buscando? Dónde, si no
en las instituciones bancarias el tipo de CreditChex en la lista?
Con el análisis de la
Este truco estaba basado en una de las tácticas fundamentales de la social
ingeniería: el acceso a la información de que un empleado de la compañía considera como

inocuos, cuando no lo es.
El empleado de banco confirmó por primera vez la terminología para describir la identificación de número que se utiliza al llamar CreditChex: la identificación del comerciante. El segundo siempre el número de teléfono para llamar CreditChex, y la pieza más importante de la información, del banco, número de identificación del comerciante. Toda esta información parece ser el secretario
inocuo. Después de todo, el empleado de banco pensó que estaba hablando con alguien de CreditChex-para lo que podría ser el daño al revelar el número?
Todo esto sentó las bases de la tercera convocatoria. Grace tenía todo lo necesario
al teléfono CreditChex, hacerse pasar por un representante de uno de los bancos con sus clientes,
Nacional, y simplemente para pedir la información que buscaba.
Con habilidad tanto en el robo de información como un estafador bien tiene en el robo de su dinero, Grace tenía bien afinado talento para la lectura de las personas. Sabía que el común táctica de enterrar a las cuestiones clave, entre los inocentes. Conocía a un personal cuestión prueba la voluntad del secretario segundo de cooperar, antes de inocencia preguntando por el número de identificación del comerciante.
El secretario del primer error en la confirmación de la terminología para la identificación de CreditChex
número sería casi imposible protegerse contra. La información es tan
ampliamente conocido en la industria bancaria que parece ser poco importante - la
muy modelo de la inocuidad. Sin embargo, el secretario segundo, Chris, no debería haber sido tan dispuesto a responder a las preguntas sin verificar positivamente que la persona que llama se realmente quien decía ser. Se debe, por lo menos, han tomado su nombre
y el número y llamó de nuevo, de esta manera, si alguna pregunta surgió más tarde, ella puede tener
mantener un registro de lo que el número de teléfono de la persona que había utilizado. En este caso, haciendo una
llamada así lo habría hecho mucho más difícil para el atacante
hacerse pasar por un representante de CreditChex.
Mitnick MENSAJE
Una identificación del comerciante en esta situación es similar a una contraseña. Si el personal del banco
lo trató como un PIN del cajero automático, pueden apreciar la naturaleza sensible de la
de la información. ¿Hay un código interno o número de su organización que la gente
no tratar con cuidado lo suficiente?
Mejor aún habría sido una llamada a CreditChex utilizando un banco de monja ya había en registro - no es un número proporcionado por la persona que llama - para verificar que la persona realmente
trabajaba allí, y que la empresa estaba haciendo una encuesta entre los clientes. Dado
los aspectos prácticos del mundo real y las presiones de tiempo que la mayoría de la gente trabaja
en la actualidad, sin embargo, este tipo de llamada de verificación por teléfono es mucho esperar, con la excepción
cuando un empleado es sospechoso de que algún tipo de ataque se está realizando.
LA TRAMPA DE INGENIERO
Es ampliamente conocido que los cazadores de cabeza las empresas utilizan la ingeniería social para reclutar
talento corporativo. He aquí un ejemplo de cómo puede ocurrir.
A finales de 1990, una agencia de empleo no es muy ético firmado un nuevo cliente, un
empresa en busca de ingenieros eléctricos con experiencia en el teléfono
de la industria. El mandamás en el proyecto era una mujer dotada de una voz gutural y
manera sexy que ella había aprendido a utilizar para desarrollar la confianza inicial y la relación más
el teléfono.

La señora decidió llevar a cabo una redada en un proveedor de servicios de telefonía celular para ver si ella
pudieron localizar algunos ingenieros que podrían verse tentados a cruzar la calle a un competidor. No exactamente podría llamar a la junta cambiar y decir: "Déjame hablar con cualquiera que tenga cinco años de experiencia en ingeniería. "En su lugar, por razones que se puesto de manifiesto en un momento, ella comenzó el asalto talento, buscando un pedazo de información que no parecía tener la sensibilidad a todos, la información que la empresa la gente da a casi todo el mundo que lo pida.

La primera llamada: La recepcionista

El atacante, con el nombre de Didi Sands, hizo una llamada a las oficinas corporativas de el servicio de telefonía celular. En parte, la conversación fue como sigue:

Recepcionista: Buenas tardes. Se trata de Marie, ¿en qué puedo ayudarle?
Didi: ¿Se puede conectar conmigo al Departamento de Transporte?
R: No estoy seguro de si tiene uno, voy a buscar en mi directorio. ¿Quién llama?
D: Es Didi.
R: ¿Está en el edificio, o ... ?
D: No, yo estoy fuera del edificio.
R: Didi quién?
D: Didi Sands. Tuve la extensión para el transporte, pero se me olvidó lo que era.
R: Un momento.

Para disipar las sospechas, en este punto Didi hizo una conversación casual, sólo hacer pregunta destinada a establecer que estaba en el "interior", familiarizado con instalaciones de la empresa.

D: ¿Qué edificio en que está - o Lakeview Plaza Mayor?
R: Plaza Principal. (Pausa) 805 555 6469.

Para proveer a sí misma con una copia de seguridad en caso de que la llamada a Transporte no proporcionó
lo que estaba buscando, Didi dijo que ella también quería hablar con Bienes Raíces. La recepcionista le dio a ese número, también. Cuando se le preguntó Didi estar conectado a el número de Transporte, el recepcionista intentó, pero la línea estaba ocupada.

En ese momento Didi pidió un número de teléfono en tercer lugar, las cuentas por cobrar, ubicado en un centro empresarial en Austin, Texas. La recepcionista le pidió que esperara un momento, y se salió de la línea. Informar a la Seguridad de que había un sospechoso llamada de teléfono y pensó que había algo sospechoso pasa? No, en absoluto, y Didi no tenía la más mínima preocupación. Ella estaba un poco molesto, pero a la recepcionista que todo era parte de un típico día de trabajo. Después de un minuto, el recepcionista volvió a la línea, busqué el número de cuentas por cobrar,
lo intentó, y poner a través de Didi.

La segunda llamada: Peggy

La siguiente conversación fue así:

Peggy: Cuentas por cobrar, Peggy.
Didi: Hola, Peggy. Se trata de Didi, en Thousand Oaks.
P: Hola, Didi.
D: ¿Cómo te va?
P: Bien.

Didi entonces se utiliza un término familiar en el mundo corporativo que describe la carga código de asignación de gastos con cargo al presupuesto de una organización específica o grupo de trabajo:

D: Excelente. Tengo una pregunta para usted. ¿Cómo puedo averiguar el centro de coste para un departamento en particular?
P: Usted tendría que obtener una bodega de la analista de presupuesto para el departamento.
D: ¿Sabe usted que sería el analista de presupuesto para
Thousand Oaks - sede? Estoy tratando de llenar un
forma y no sé el centro de coste adecuado.
P: Acabo de saber que todos ustedes necesitan un número de centro de costo, llame a su

presupuesto
analista.
D: ¿Usted tiene un centro de costos para su departamento hay en Texas?
P: Tenemos nuestro centro de costo, sino que no nos dan una lista completa de ellos.
D: ¿Cuántos dígitos es el centro de coste? Por ejemplo, ¿cuál es su centro de costos?
P: Bueno, como, usted está con 9WC o con el SAT?
Didi no tenía idea de lo que los departamentos o grupos de éstos se refiere, pero no materia. Ella respondió:
D: 9WC.
P: Entonces, es por lo general cuatro dígitos. ¿Quién dijiste que estabas?
D: Sede - Thousand Oaks.
P: Bueno, aquí está uno de Thousand Oaks. Es 1A5N, que es N como en Nancy.
Al pasar el rato con el tiempo suficiente a alguien dispuesto a ser útil, Didi había el número de centros de coste que necesitaba - una de esas piezas de información que no se piensa para proteger, ya que parece como algo que no podía ser de cualquier valor a un extraño.
La tercera convocatoria: un número equivocado útiles
Didi siguiente paso sería el de valerse de la cantidad de centros de coste en algo real valor utilizando como una ficha de póquer.
Ella comenzó a llamar al departamento de Bienes Raíces, fingiendo que había llegado a un número equivocado. A partir de un "Perdona que te moleste, pero ...." ella dijo que ella era un empleado que había perdido a su directorio de la empresa, y le pidió que le fueron que llamar para obtener una nueva copia. El hombre dijo que la copia impresa estaba fuera de fecha
ya que estaba disponible en el sitio intranet de la compañía.
Didi dijo que prefería utilizar una copia en papel, y el hombre le dijo que llamara Publicaciones, y luego, sin haber sido invitada - tal vez sólo para mantener el atractivo dama que suena en el teléfono un poco más - amablemente miró el número y la se lo dio a ella.
La Cuarta Convocatoria: Bart en Publicaciones
En Publicaciones, habló con un hombre llamado Bart. Didi dijo que estaba de Thousand Oaks, y que había un nuevo consultor que necesita una copia de la Directorio de la compañía. Ella le dijo que una copia impresa sería más apropiado para la consultor, aunque fuera un poco fuera de fecha. Bart le dijo que había que llenar un formulario de solicitud y enviar el formulario a él.
Didi dijo que estaba fuera de forma y fue una carrera, y podría ser una novia de Bart y rellene el siguiente formulario para ella? Estuvo de acuerdo con un entusiasmo demasiado, y Didi le dio los detalles. Para la dirección de la contratista de ficción, que arrastró las palabras el número de lo que los ingenieros sociales exigen una gota de correo, en este caso un Mail Boxes
Etc-tipo de actividad comercial donde su empresa alquiló cajas para situaciones de al igual que este.
El trabajo preliminar antes, ahora vino muy bien: No sería un cargo por el costo y el envío de la guía. Artes - Didi dio el centro de coste para Thousand Oaks: "IA5N, que es N como en Nancy".
Unos días más tarde, cuando el directorio de la empresa llegó, Didi encontró que era una aún mayor rentabilidad de lo que esperaba: no es sólo una lista de los nombres y números números, pero también mostró que trabajaba para los cuales - la estructura corporativa de la toda la organización.
La señora de la voz ronca estaba listo para comenzar a hacer su cazador de cabezas, peopleraiding
las llamadas telefónicas. Ella había estafado la información que necesitaba para lanzar su RAID con el don de la palabra afilada con un pulido de alto por todos los ingenieros sociales especializados.
Ahora estaba listo para el pago.

LINGO
GOTA MAIL: El mandato de la ingeniería social para un buzón de alquiler, generalmente alquilados
bajo un nombre falso, que son utilizados para entregar documentos o paquetes de la víctima ha sido engañado en el envío de
Mitnick MENSAJE
Al igual que piezas de un rompecabezas, cada pieza de información puede ser irrelevante sí mismo. Sin embargo, cuando las piezas se unen, surge una imagen clara. En este Me caso, la imagen de la ingeniería social se vio toda la estructura interna de la de la empresa.
Con el análisis de la
En este ataque de ingeniería social, Didi iniciadas por conseguir números de teléfono de tres los departamentos de la empresa objetivo. Esto fue fácil, porque los números que se pidiendo no eran ningún secreto, especialmente a los empleados. Un ingeniero social aprende a suena como una información privilegiada, y Didi era experto en este
juego. Uno de los números de teléfono de su lugar a una serie de centros de coste, que luego utiliza para obtener una copia de directorio de empleados de la empresa.
Las principales herramientas que necesitaba: sonido ambiente, utilizando la jerga de algunas empresas, y,
con la última víctima, tirar un poco las pestañas verbal-de bateo.
Y una herramienta más, un elemento esencial, no fácil de adquirir - el manipulador habilidades de la ingeniería social, refinado a través de la práctica extensa y no escritas de la lecciones de las generaciones pasadas de hombres de confianza.
MÁS "sin valor" INFO
Además de un número de centros de coste y las extensiones de teléfono internos, lo que otros información aparentemente inútil puede ser muy valioso a su enemigo?.
Llame a Peter Abel Teléfono
"Hola", la voz en el otro extremo de la línea, dice. "Se trata de Tom en el recorrido Parkhurst. Los billetes de San Francisco están listos. Qué quieren que les ofrecen, o
desea recogerlos? "
"San Francisco?" Pedro dice. "Yo no voy a San Francisco." "¿Es Peter
Abel? "
"Sí, pero yo no tengo ningún viaje por venir."
"Bueno," la persona que llama dice con una sonrisa amistosa "¿Seguro que no quieres ir a San Francisco? "
"Si usted piensa que usted puede hablar a mi jefe en ella ..." Pedro dice, jugando junto con el conversación amistosa.
"Suena como una confusión", la persona que llama dice. "En nuestro sistema, libro de viajes los acuerdos con el número de empleados. Tal vez alguien utiliza el mal
número. ¿Cuál es su número de empleado? "
Peter amablemente recita su número. Y ¿por qué no? Es evidente en casi todas las personal de forma que llena, mucha gente en la empresa tienen acceso a ella - recursos humanos, nómina, y, obviamente, la agencia de viajes del exterior. Nadie trata un número de empleado como una especie de secreto. ¿Qué diferencia podría hacer?
La respuesta no es difícil de entender. Dos o tres piezas de información podría ser todo lo necesario para preparar una respuesta eficaz suplantación - el encubrimiento ingeniero social
a sí mismo en identidad de otra persona. Hacerse con el nombre del empleado, su teléfono número, su número de empleado - y tal vez, en buena medida, de su manager nombre y número de teléfono - y de un ingeniero social a medio camino-competente está equipado
con la mayor parte de lo que es probable que necesita un sonido auténtico para el próximo objetivo que
llamadas.
Si alguien que dijo que era de otro departamento de su empresa había

llamó ayer, ha dado una razón plausible, y le pidió su número de empleado,
que usted ha tenido alguna reticencia en dar a él?
Y, por cierto, ¿cuál es su número de seguro social?
Mitnick MENSAJE
La moraleja de la historia es, no dar ninguna empresa o personal interno
información o identificadores para cualquier persona, a menos que su voz es reconocible y
el solicitante tiene la necesidad de saber.
PREVENCIÓN DE LA CON
Su empresa tiene la responsabilidad de hacer que los empleados tomen conciencia de cómo una seria
error puede ocurrir por mal manejo de información pública no. Un bien pensado
la política de seguridad de la información, junto con la educación y la capacitación adecuada, se
dramáticamente aumentar la conciencia de los empleados sobre el manejo adecuado de las empresas
negocio de la información. Una política de clasificación de datos le ayudará a poner en práctica
controles adecuados con respecto a la divulgación de información. Sin datos
política de clasificación, toda la información interna debe ser considerada confidencial,
a menos que se especifique lo contrario.
Siga estos pasos para proteger su empresa de la liberación de los aparentemente
información inocua:
El Departamento de Seguridad de la Información necesita para llevar a cabo formación sobre sensibilización
detalla los métodos utilizados por los ingenieros sociales. Un método, como se describió anteriormente,
es la obtención de información sensible, aparentemente no y lo utilizan como una ficha de póquer para ganar
a corto plazo la confianza. Cada empleado tiene que ser consciente de que cuando una persona
tiene conocimiento de procedimientos de la compañía, la jerga y los identificadores internos que se
no de cualquier manera, forma o forma autenticar al solicitante o autorizar que él o ella
que tienen una necesidad de saber. Una llamada podría ser un ex empleado o contratista con
la información privilegiada necesarios. Por lo tanto, cada empresa tiene una
responsabilidad de determinar el método de autenticación adecuado para ser utilizado
cuando los empleados interactúan con las personas que no reconocen en persona o por teléfono.
La persona o personas con el papel y la responsabilidad de elaborar una base de datos
política de clasificación debe examinar el tipo de detalles que se pueden utilizar para ganar
acceso para los empleados legítimos que parecen inofensivos, pero podría llevar a
información, es decir, sensible. A pesar de que nunca le daría a los códigos de acceso
su tarjeta de cajero automático, le diría a alguien lo que el servidor que se utiliza para desarrollar
productos de la empresa de software? ¿Podría ser que la información utilizada por una persona
pretendiendo ser alguien que tiene acceso legítimo a la red corporativa?
A veces el hecho de saber dentro de la terminología puede hacer la ingeniería social parece
autoridad y conocimiento. El atacante confía a menudo en este común
error para engañar a las víctimas en su cumplimiento. Por ejemplo, un
Identificación del comerciante es un identificador que la gente en el departamento de cuentas nuevas de un
banco casualmente usa todos los días. Sin embargo, dicho identificador exactamente lo mismo que un
contraseña. Si cada empleado comprenda la naturaleza de este identificador -
que se utiliza para autenticar a un solicitante de manera positiva - que se podría tratar con más respeto.
Mitnick MENSAJE
Como dice el viejo refrán - incluso los paranoicos tienen enemigos reales, probablemente.
Tenemos que

asumir que cada negocio tiene sus enemigos, también - los atacantes que se dirigen a la red infraestructura para comprometer secretos de negocios. No terminan siendo una estadística sobre delitos informáticos - es hora de reforzar las defensas necesarias por
la aplicación de controles adecuados a través de políticas de seguridad bien pensadas y procedimientos.
Ninguna empresa - así, muy pocos, por lo menos - dar a conocer los números de teléfono de línea directa
de su director general o presidente del consejo. La mayoría de las empresas, sin embargo, no tienen ninguna preocupación acerca de
dar números de teléfono a la mayoría de los departamentos y grupos de trabajo en el, organización - en especial a alguien que es o parece ser, a un empleado. A
posibles contramedidas: Implementar una política que prohíbe dar de teléfono interno número de empleados, contratistas, consultores y trabajadores temporales a los extranjeros. Más importante, desarrollar un procedimiento paso a paso para identificar con certeza si un persona que llama preguntando por el número de teléfono es en realidad un empleado.
Los códigos contables para grupos de trabajo y departamentos, así como copias de los directorio de la empresa (ya sea en papel, archivo de datos, o un libro electrónico en el teléfono intranet) son blanco frecuente de los ingenieros sociales. Toda empresa necesita un escrito, bien publicitada política de divulgación de este tipo de información. Las garantías
debe incluir el mantenimiento de un registro de auditoría que registra casos en los sensibles información sea divulgada a personas fuera de la empresa.
Información como un número de empleado, por sí mismo, no debe ser utilizado como cualquier tipo de autenticación. Todos los empleados deben ser entrenados para verificar no sólo la identidad de un solicitante, pero también es necesario que el solicitante a la información.
En el entrenamiento de seguridad, considere la enseñanza de los empleados de este enfoque: Siempre
una pregunta o pide un favor a un desconocido, aprender primero a declinar cortésmente hasta que la solicitud puede ser verificada. Entonces - antes de ceder al deseo natural de ser Sr. o Sra. útiles - Las políticas de la empresa y seguir los procedimientos con respecto a la verificación y divulgación de información no pública. Este estilo puede ir en contra
nuestra tendencia natural a ayudar a los demás, pero un poco de paranoia sana puede ser necesario
para evitar ser víctima junto al ingeniero social.
Como las historias de este capítulo se han mostrado, la información aparentemente inocua puede ser la llave a los secretos más preciados de su empresa.

Capítulo 3
El ataque directo: sólo pedimos que
Muchos ataques de ingeniería social son complejos, con un número de pasos y
elaborar la planificación, la combinación de una mezcla de manipulación y know-how tecnológico. Pero yo siempre les resulta sorprendente que un ingeniero social hábiles a menudo puede lograr su
gol con un simple ataque directo, directo. Sólo preguntaba abiertamente por el información puede ser todo lo que se necesita - como se verá.
UN QUICKIE MLAC
¿Quieres saber el número de teléfono de alguien no cotizan en bolsa? Un ingeniero social puede explicarle
media docena de formas (y usted encontrará algunos de ellos descritos en las historias de otros estas páginas), pero probablemente el caso más simple es aquella que utiliza un solo teléfono llamada, como éste.
Número, por favor
El atacante marcó el número de teléfono de la empresa privada para la MLAC, el
Centro de mecanizado Asignación de línea. A la mujer que respondió, dijo:
"Hey, este es Paul Anthony. Soy un empalmador de cables. Oye, una caja de terminales aquí se fritos en un fuego. Los policías creen que algunos arrastran trataron de quemar su propia casa por

el
de seguros. Me sacaron aquí solo tratando de volver a colocar la totalidad de los dos hundredpair terminal. Me vendría bien algo de ayuda en estos momentos. ¿Qué instalaciones deben ser de trabajo en 6723 South Main? "
En otras partes de la compañía telefónica, la persona que llama se sabe que invertir búsqueda de información sobre la publicación no (no publicado) el número se supone que ha de darse
MLAC a cabo sólo autorizado en el teléfono se supone que es conocida sólo por empleados de la compañía. Y mientras ellos nunca dar información al público, ¿quién querría rechazar un poco de ayuda a un hombre de la compañía para hacer frente a ese trabajo pesado
tarea?. Siente lástima por él, que ha tenido días malos en el trabajo ella misma, y ella
doblar las reglas un poco para ayudar a un compañero de trabajo con un problema. Ella le da él, el cable y los pares y cada número de trabajo asignado a la dirección.
Mitnick MENSAJE
Es la naturaleza humana a confiar en el prójimo, sobre todo cuando la solicitud cumpla con los prueba de ser razonable. Los ingenieros sociales utilizan este conocimiento para explotar sus las víctimas y para lograr sus objetivos.
Con el análisis de la
Como te darás cuenta en varias ocasiones en estas historias, el conocimiento de la jerga de la empresa, y
de su estructura corporativa - sus diversas oficinas y departamentos de lo que cada uno hace y la información que cada uno tiene - es parte de la bolsa de trucos esenciales del éxito ingeniero social.
HOMBRE JOVEN EN FUGA
Un hombre al que llamaremos Frank Parsons había estado prófugo durante años, sigue siendo buscado por la
gobierno federal por ser parte de un grupo contra la guerra subterránea en la década de 1960. En los restaurantes se sentó frente a la puerta y él tenía una manera de mirar por encima de su el hombro de vez en cuando de que otras personas encuentran desconcertante. Él se movió cada pocos años.
En un momento Frank aterrizó en una ciudad que no conocía, y se dedicó a la búsqueda de empleo. Para
alguien como Frank, con sus conocimientos de informática bien desarrollado (y social habilidades de ingeniería, así, incluso, aunque nunca figuran las de un puesto de trabajo aplicación), encontrar un buen trabajo por lo general no era un problema. Excepto en momentos en que
la economía es muy fuerte, las personas con un buen conocimiento técnico informático suelen encontrar sus talentos en alta demanda y tienen pocos problemas en el aterrizaje sus pies. Frank rápidamente encuentra un pozo - oportunidad de trabajo remunerado en una gran de lujo, cuidado a largo plazo instalación cerca de donde vivía.
Sólo el billete, pensó. Pero cuando empezó a andar con paso pesado su camino a través de la formularios de solicitud, se encontró con un uh-oh: El empleador está obligado el solicitante para proporcionar una copia de su registro de antecedentes penales del Estado, la cual tuvo que obtener
a sí mismo de la policía estatal. La pila de papeles de trabajo incluye un formulario para obtener este documento, y la forma tenía una pequeña caja de proporcionar una huella digital. A pesar de que estaban pidiendo una copia de tan sólo el dedo índice derecho, si igualó su mejor impresión con una base de datos del FBI, que probablemente pronto a trabajar en el servicio de comida en un centro turístico financiado con fondos federales.
Por otro lado, se le ocurrió a Frank que tal vez, sólo tal vez, todavía puede ser
capaz de salirse con la suya. Tal vez el estado no ha enviado las muestras de huellas digitales al FBI en absoluto. ¿Cómo podía saberlo?
¿Cómo? Él era un ingeniero social - ¿Cómo crees que se enteró? Colocó una

llamada telefónica a la patrulla estatal:. "Hola Estamos haciendo un estudio para el Departamento de Estado
de Justicia. Estamos investigando los requisitos para aplicar una nueva huella digital identificación del sistema. ¿Puedo hablar con alguien allí que es muy familiarizado con lo que estás haciendo lo mejor que nos puede ayudar? "
Y cuando el experto local se puso al teléfono, Frank le hizo una serie de preguntas acerca de lo que los sistemas que estaban usando, y la capacidad para buscar y almacenar de datos de huellas dactilares. Si hubieran tenido problemas con el equipo? Se ataron en el Delincuencia del Centro Nacional de Información (NCIC) Búsqueda de huellas dactilares o simplemente en el
Estado? Fue el equipo es bastante fácil para todo el mundo para aprender a usar? Disimuladamente, se coló la cuestión clave en los demás.
La respuesta fue música para sus oídos: No, no estaban atados en el NCIC, sólo compara con el Índice de Información Criminal (CII).
Mitnick MESSGAE
Estafadores expertos en información no tienen reparos en sonar a nivel federal, estatal o funcionarios del gobierno local para conocer los procedimientos de aplicación de la ley. Con esa información en mano, el ingeniero social puede ser capaz de eludir controles estándar de su empresa de seguridad.
Eso fue todo Frank necesitaba saber. Él no tenía ningún registro en ese estado, por lo que presentó su candidatura, fue contratado para el trabajo, y nadie se presentó en su escritorio un día con el saludo: "Estos señores, son del FBI y de que les gustaría tener una pequeña charla con usted. "
Y, de acuerdo con él, resultó ser un empleado modelo.
En el umbral
A pesar del mito de la oficina sin papeles, las empresas siguen para imprimir resmas de papel todos los días. Información impresa en su empresa puede ser vulnerable, incluso si se utiliza medidas de seguridad y el sello de confidencial.
He aquí una historia que muestra cómo los ingenieros sociales podrían obtener su mayoría de documentos secretos.
Loop-Alrededor de engaño
Cada año, la compañía de telefonía publica un volumen llamado el número de prueba Directorio (o al menos que antes, y porque todavía estoy en libertad condicional, No voy a preguntar si todavía lo hacen). Este documento fue muy apreciado por teléfono phreaks, ya que esta lleno de una lista de todos los teléfonos muy bien guardado números utilizados por los artesanos de la empresa, los técnicos, uno a otros por cosas como la trompa
pruebas o controles de los números que siempre suenan ocupados.
Uno de estos números de prueba, conocida en la jerga como un bucle alrededor, fue particularmente
útil. Phreakers lo utilizó como una manera de encontrar otros phreaks teléfono para charlar, sin costo alguno para ellos. Phreakers también se utiliza una forma de crear un número de devolución de llamada
para dar, por ejemplo, un banco. Un ingeniero social que decirle a alguien en el banco de la número de teléfono para llamar a llegar a su oficina. Cuando el banco llamó a la prueba número (loop-alrededor) del phreaker sería capaz de recibir la llamada, sin embargo, tenía la protección de haber usado un número de teléfono que no podía ser rastreada a él.
Un Directorio Número de prueba que una gran cantidad de información ordenada que podría ser utilizado
por cualquier hambrienta de información, Phreak testosteroned teléfono. Así que cuando el nuevo directorios se publican cada año, que eran codiciadas por muchos jóvenes cuyo pasatiempo era explorar la red telefónica.
Mitnick MENSAJE
De capacitación en seguridad con respecto a la política de la compañía diseñada para proteger la

información
activos debe ser para todos en la empresa, no sólo a cualquier empleado que tiene
acceso electrónico o físico a la empresa los activos de TI.
Estafa de Stevie
Naturalmente las compañías telefónicas no hacen estos libros fáciles de conseguir, así que teléfono
phreaks tienen que ser creativos para conseguir uno. ¿Cómo pueden hacer esto? Un joven impaciente
con una mente empeñado en adquirir el directorio podría aprobar un escenario como este.
Finales de un día, una noche suave en el otoño del sur de California, un hombre Voy a llamar a
le Stevie teléfonos una pequeña empresa de teléfono de la oficina central, que es el
la construcción de líneas telefónicas que ejecutar a todos los hogares y las empresas en el
estableció el área de servicio.
Cuando el guardagujas en servicio responde a la llamada, Stevie anuncia que él es de
la división de la compañía telefónica que publica y distribuye impresa
los materiales. "Tenemos el nuevo Directorio Número de prueba", dice. "Pero para la seguridad
razones, nosotros no podemos entregar la copia hasta que recoger el viejo. Y la entrega
tipo es tarde. Si usted quiere salir de su copia a las afueras de su puerta, se puede
swing, recoger el suyo, la caída de la nueva y estar en su camino. "
El guardagujas confiados parece pensar que parece razonable. Lo que hace
exactamente como se preguntó, sacando a las puertas del edificio de la copia de la
directorio, su cubierta claramente marcada en grandes letras rojas con la empresa "
CONFIDENCIAL - CUANDO YA NO NECESITA ESTE DOCUMENTO
DEBE ser triturados. "
Stevie unidades por y mira a su alrededor con cuidado para detectar cualquier policía o empresa telefónica
seguridad de las personas que podrían estar al acecho detrás de los árboles o mirando para él de
vehículos estacionados. Nadie a la vista. Casualmente recoge el directorio deseado y
se aleja.
He aquí un ejemplo más de lo fácil que puede ser para un ingeniero social para obtener
lo que quiere, siguiendo el principio simple de "sólo pregunta por ella."
Ataque con gas
No sólo los activos de la compañía están en riesgo en un escenario de ingeniería social. A veces
a sus clientes de una empresa que son las víctimas.
Trabajo como empleado de servicio al cliente trae su cuota de frustraciones, su participación en
se ríe, y su cuota de errores inocentes - algunos de los cuales puede tener infeliz
consecuencias para los clientes de una empresa.
Janie historia de Acton
Janie Acton había sido la dotación de un cubículo como un representante de servicio al cliente
Procedencia f
Energía Eléctrica, en Washington, DC, a poco más de tres años. Ella fue
considerado como uno de los empleados mejor, inteligente y consciente
Fue la semana de Acción de Gracias, cuando este llamado un particular entró la persona que
llama, dijo,
"Se trata de Eduardo en el departamento de facturación. Tengo una mujer en espera, es una
secretaria en las oficinas del ejecutivo que trabaja para uno de los vicepresidentes, y
ella está pidiendo alguna información y no puedo usar mi computadora tengo un e-mail
de esta chica en Recursos Humanos que dice "ILOVEYOU". y cuando abrí
el archivo adjunto, que no podía usar mi máquina más. Un virus. Me vi atrapado por un
virus de la estupidez. En cualquier caso, podría buscar alguna información del cliente para mí? "
"Claro", respondió Janie. "Se estrelló su computadora? Eso es terrible."
"Sí".
"¿Cómo puedo ayudar?" Janie le preguntó.
Aquí el atacante llamó a la información de su avance de la investigación para hacer
a sí mismo un sonido auténtico. Había aprendido que la información que, quería era

almacenados en algo llamado el Sistema de Información de facturación al cliente, y si hubiera descubierto cómo los empleados a que se refiere al sistema. -Le preguntó, "¿Puede abrir un cuenta en CBIS? "
"Sí, ¿cuál es el número de cuenta.?"
"No tengo el número, te necesito para que aparezca su nombre."
"Está bien, ¿cuál es el nombre?"
"Es Marning Heather". Se escribe el nombre, y Janie ha escrito in
"Está bien, lo tengo arriba."
"Gran. Es la cuenta corriente?"
"Uh huh, es actual."
"¿Cuál es el número de cuenta?" -le preguntó.
"¿Tienes un lápiz?"
"Está listo para escribir."
"Cuenta BAZ6573NR27Q número."
Leyó el número de la espalda y luego dijo: "Y lo que es la dirección de servicio?"
Ella le dio la dirección.
"Y lo que es el teléfono?"
Janie amablemente leer esa información, también.
La persona que llamó le dio las gracias, se despidió y colgó. Janie se fue a la siguiente llamada, sin pensar más en ello.
Proyecto de Investigación de Arte Sealy
Arte Sealy había dejado de trabajar como editor freelance para pequeñas editoriales cuando se enteró de que podía ganar más dinero haciendo una investigación para escritores y las empresas. Pronto se descubrió que los honorarios que pueden cobrar aumentaron en proporción a la proximidad de la asignación lo llevó a la línea a veces confusa entre lo legal y lo ilegal. Sin siquiera darse cuenta, sin duda darle un nombre, el arte se convirtió en un ingeniero social, utilizando técnicas familiares para todos los información del corredor. Se volvió a tener un talento innato para los negocios, averiguar por sí mismo las técnicas que los ingenieros sociales más tenía que aprender de otros. Después de un tiempo, cruzó la meta sin el menor asomo de culpabilidad.
Un hombre puso en contacto conmigo que estaba escribiendo un libro sobre el Consejo de Ministros en el gobierno de Nixon años, y fue en busca de un investigador que pudo enterarse de los detalles en William E. Simon, que había sido secretario del Tesoro de Nixon. El Sr. Simon había murió, pero el autor tenía el nombre de una mujer que había estado en su equipo. Fue bastante seguro de que aún vivía en Washington DC, pero no había sido capaz de obtener una dirección. Ella no tenía un teléfono en su nombre, o al menos ninguno que se enumeran. Así que eso es cuando me llamó. Yo le dije, claro, no hay problema.
Este es el tipo de trabajo que por lo general puede llevar fuera de una llamada telefónica o dos, si Sé lo que estás haciendo. Cada compañía local de servicios en general, se puede contar con para dar la información de distancia. Por supuesto, usted tiene que BS un poco. Pero lo que es un mentira piadosa de vez en cuando - a la derecha?
Me gusta usar un enfoque diferente cada vez, sólo para mantener las cosas interesantes. "Este es así-y-lo que en las oficinas ejecutivas "siempre ha funcionado bien para mí. Así que ha" He tiene a alguien en la línea de la oficina del vicepresidente Alguien Presidente ", que trabajó esta vez, también.
Mitnick MENSAJE
No creo que todos los ataques de ingeniería social deben ser elaborados ardides tan complejo que es probable que sea reconocida antes de que se puede completar. Algunos son iNAND-a cabo, la huelga y desaparecer, los ataques muy simples que no son más que .., bueno, sólo que lo soliciten.
Usted tiene que desarrollar una especie de instinto de la ingeniería social, el tener una idea de cómo

cooperación de la persona en el otro extremo va a estar con ustedes. Esta vez
suerte con una señora amable y servicial. En una sola llamada telefónica, que tenía la dirección y número de teléfono. Misión cumplida.
Con el análisis de la
Ciertamente, Janie sabía que la información del cliente es sensible. Ella
Nunca discutir la cuenta de un cliente con otro cliente, o dar a conocer
información privada a la pública.
Pero, naturalmente, por la persona que llama desde el interior de la empresa, se aplican reglas diferentes. Para una
compañero de trabajo que trata de ser un jugador de equipo y ayudar unos a otros a la
realizar su trabajo. El hombre de la facturación podría haber mirado los datos sí mismo si su equipo no había sido por un virus, y que estaba contenta de poder ayudar a un compañero de trabajo.
Arte desarrolla gradualmente a la información clave que fue muy tarde, pidiendo
preguntas en el camino de las cosas que realmente no necesita, como la
número de cuenta. Sin embargo, al mismo tiempo, la información del número de cuenta
siempre un plan alternativo: Si el empleado se había convertido en sospechoso, que había llamado por segunda vez
y tienen una mejor oportunidad de éxito, porque sabiendo el número de cuenta
lo haría el sonido aún más auténtico a la siguiente empleado llegó.
Nunca se les ocurrió a Janie que alguien realmente puede mentir acerca de algunos
algo como esto, que la persona que llama no puede ser en realidad en el departamento de facturación en
todos. Por supuesto, la culpa no está a los pies de Janie. Ella no estaba muy versado en la regla de asegurarse de que usted sabe con quién está hablando antes de hablar
información en el archivo de un cliente. Nadie había jamás le habló del peligro de una llamada de teléfono como el de Arte. No estaba en la política de la empresa, que no era parte de su formación, y su supervisor no lo había mencionado.
PREVENCIÓN DE LA CON
Un punto a incluir en su formación en seguridad: El hecho de que la persona que llama o visitante conoce
los nombres de algunas personas de la empresa, o sabe algo de la jerga corporativa
o procedimientos, no significa que él es quien dice ser. Y definitivamente no
establecer él como alguien autorizado a dar información interna, o el acceso a
su sistema informático o red.
Formación en seguridad tiene que destacan: En caso de duda, verificar, comprobar, verificar.
En épocas anteriores, el acceso a la información dentro de una empresa era una marca de rango y
privilegio. Trabajadores alimentado a los hornos, corrió las máquinas, escribe las letras, y presentado los informes. El capataz o jefe les dijo qué hacer, cuándo y cómo. Lo
era el capataz o el jefe que supo widgets que cada trabajador debe ser
producir en un turno, cuántos y en qué colores y tamaños de la fábrica es necesario
a su vez, esta semana, la próxima semana, y al final del mes.
Los trabajadores manejan máquinas y herramientas y materiales, y maneja los jefes
de la información. Trabajadores que se necesitan sólo la información específica a sus tareas específicas.
La imagen de hoy es un poco diferente, ¿no? Muchos trabajadores de la fábrica utilizar algunos forma de equipo o máquina por ordenador. Para una gran parte de la fuerza laboral,
información crítica se empuja hacia abajo a los escritorios de los usuarios para que puedan cumplir
su responsabilidad de hacer su trabajo. En el entorno actual, casi
todo lo que hacen los empleados implica el manejo de la información.
Es por eso que la política de seguridad de una compañía debe ser distribuido en toda la empresa, independientemente de la posición. Todo el mundo debe entender que no se trata sólo de los patrones y

ejecutivos que tienen la información que un atacante podría ser después. Hoy en día, los trabajadores en todos los niveles, incluso aquellos que no usan una computadora, son susceptibles de ser dirigidos. El representante de nuevo ingreso en el grupo de servicio al cliente puede ser sólo el débil enlace que se rompe un ingeniero social para lograr su objetivo.
Capacitación en seguridad y políticas de seguridad corporativas necesidad de fortalecer ese enlace.

Capítulo 4
Construyendo Confianza
Algunas de estas historias podrían llevar a pensar que yo creo que todos los empresarios es un completo idiota, listo, incluso ansioso, para regalar todos los secretos de su la posesión. El ingeniero social sabe que no es cierto. ¿Por qué son la ingeniería social ataques tanto éxito? No es porque la gente es tonta o la falta de sentido común.
Pero nosotros, como seres humanos son vulnerables a ser engañados porque la gente puede perder su confianza si se manipula en cierta manera.
El ingeniero social anticipa la sospecha y la resistencia, y está dispuesto siempre a su vez, la desconfianza en confianza. Un ingeniero social bien sus planes de ataque como un juego de ajedrez juego, anticipando las preguntas que su objetivo podría preguntar por lo que puede estar listo con la respuestas adecuadas.
Una de sus técnicas más comunes consiste en la construcción de un sentido de confianza por parte de los sus víctimas. ¿Cómo es un estafador que usted confía en él? Confía en mí, él puede.
CONFIANZA: LA CLAVE DEL ENGAÑO
Cuanto más un ingeniero social puede hacer que su contacto parecer lo de siempre, el más se disipa la sospecha. Cuando la gente no tiene una razón para sospechar, es fácil para un ingeniero social para ganarse su confianza.
Una vez que tiene su confianza, el puente levadizo se reduce y echado la puerta del castillo abierta para que pueda entrar y tener toda la información que quiere.
NOTA
Usted puede notar que me refiero a los ingenieros sociales, phreakers, y en contra de juego los operadores como "él" a través de la mayor parte de estas historias Esto no es chauvinismo;. simplemente refleja la verdad que la mayoría de los profesionales en estos campos son hombres. Sin embargo, aunque hay no son muchas mujeres ingenieros sociales, el número está creciendo. Hay suficientes mujeres ingenieros sociales por ahí que no se debe bajar la guardia sólo porque escuchar la voz de una mujer. De hecho, las mujeres ingenieros sociales tienen un clara ventaja, ya que pueden usar su sexualidad para obtener cooperación.
Encontrarás un pequeño número de llamado sexo suave representados en estas páginas
La primera llamada: Andrea López
Andrea López contestó el teléfono en la tienda de alquiler de vídeo en la que trabajaba, y en un momento estaba sonriendo: Siempre es un placer cuando un cliente toma la problemas para decir que está contento con el servicio. Esta persona dijo que había tenido una muy buena experiencia tratar con la tienda, y que quería enviar el gerente de una carta al respecto.
-Le preguntó el nombre del gerente y la dirección de correo, y ella le dijo que era Tommy Allison, y le dio la dirección. Cuando estaba a punto de colgar, que había otra idea y dijo: "Puede ser que desee escribir en su sede de la empresa, también. ¿Cuál es tu número de la tienda? "Ella le dio esa información, también. Dijo gracias, añadió algo agradable acerca de lo útil que había sido, y dijo:

adiós.
"Una llamada así", pensó, "siempre parece que el cambio vaya más rápido. ¿Cómo
bueno sería si la gente lo que más a menudo. "
La segunda llamada: Ginny
"Gracias por llamar al Video Studio. Esta es Ginny, ¿cómo puedo ayudarle?"
"Hola, Ginny", dijo la persona que llama con entusiasmo, que suena como si hablaba con Ginny
cada semana o así. "Es Tommy Allison, director de Forest Park, tienda 863. Nos
tiene un cliente de aquí que quiere alquilar Rocosas 5 y todos estamos de copias.
¿Se puede comprobar en lo que tienes? "
Ella volvió a la línea después de unos momentos y dijo: "Sí, tenemos
tres copias. "
"Bueno, voy a ver si él quiere conducir por ahí. Escucha, gracias. Si alguna vez necesita
la ayuda de nuestra tienda, solo llame y pregunte por Tommy. Estaré encantado de hacer lo que pueda
para usted. "
Tres o cuatro veces durante el próximo par de semanas, Ginny recibió llamadas de Tommy
ayuda con una cosa u otra. Se les solicita aparentemente legítimas, y
siempre fue muy amable, sin sonar como si estuviera tratando de llegar a
ella. Era un conversador poco en el camino, y - "¿Has oído acerca de los grandes
fuego en Oak Park? Manojo de calles cerradas por allá ", y similares. Las llamadas se
un pequeño descanso de la rutina del día, y Ginny siempre estaba contento de tener noticias de
él.
Un día, Tommy llamada que suena subrayó. Él preguntó: "¿Han sido
teniendo problemas con sus computadoras? "
"No," respondió Ginny. "¿Por qué?"
"Un tipo estrelló su vehículo contra un poste de teléfono, y la compañía telefónica
reparador dice toda una parte de la ciudad perderá su teléfono e Internet
conexión hasta que arreglar esto. "
"Oh, no. Era el hombre herido?"
"Se lo llevaron en una ambulancia. De todos modos, me vendría bien un poco de ayuda. Tengo
un cliente suyo aquí que quiere alquilar Padrino II y no tiene su
tarjeta con él. ¿Podría verificar su información para mí? "
"Sí, claro."
Tommy le dio el nombre del cliente y la dirección, y Ginny le hallaron en el
equipo. Ella dio a Tommy el número de cuenta.
"Todo vuelve tarde o saldo adeudado?" Tommy le preguntó.
"Nada de lo que muestra."
"Muy bien, muy bien. Voy a firmar con la mano para una cuenta aquí y lo puso en nuestro
base de datos más adelante, cuando los equipos vienen de nuevo. Y que quiere poner
este cargo en la tarjeta Visa que utiliza en su tienda, y él no lo tiene con él.
¿Cuál es el número de tarjeta y fecha de caducidad? "
Ella se lo dio, junto con la fecha de vencimiento. Tommy dijo: "Oye, gracias por
la ayuda. Hablaremos pronto ", y colgó.
Historia de Doyle Lonnegan
Lonnegan no es un hombre joven que se quiere encontrar la espera cuando se abre
puerta de su casa. Un hombre de una sola vez la colección de deudas de juego mal, todavía no
un favor ocasional, si no se lo puso fuera mucho. En este caso, fue
ofrece un paquete considerable de dinero en efectivo para poco más que hacer algunas llamadas telefónicas a
una tienda de videos. Suena fácil. Es sólo que ninguno de sus "clientes" sabía
cómo ejecutar este contexto, ellos necesitaban a alguien con el talento y el saber hacer de Lonnegan.
La gente no emitir cheques para cubrir sus apuestas cuando se tiene la mala suerte o estúpido en el
mesa de póquer. Todo el mundo sabe eso. ¿Por qué estos amigos míos seguir

jugando con un tramposo que no tenía a cabo verde en la mesa? No lo hacen. Tal vez son un poco de luz en el departamento de inteligencia. Pero son mis amigos - lo que puede que haces?
Este tipo no tiene el dinero, así que tomaron un cheque. Les pido! En caso de coche lo llevaron a un cajero automático, es lo que deberían de hacer. Pero no, un cheque. Para 3.230 dólares.
Naturalmente, se recuperó. ¿Qué esperas? Así que me llaman, puedo ayudar?
No cerrar las puertas en los nudillos de las personas más. Además, hay mejores maneras hoy en día. Yo les dije, el 30 por ciento de comisión, que vería qué podía hacer. Por lo que dame su nombre y dirección, y me voy para arriba en el ordenador para ver cuál es el más tiendas de video de él. Yo no estaba en un gran apuro. Cuatro llamadas telefónicas para adular a
el gerente de la tienda, y después, bingo, tengo el número de la trampa de la tarjeta Visa.
Otro amigo mío es dueño de un bar topless. Por cincuenta dólares, se puso de poker del tío dinero a través de un cargo de Visa en el bar. Vamos a explicar el truco que a su esposa. ¿Crees que podría intentar decir Visa no es su cargo? Piense otra vez. Él sabe que sabe quién es. Y si podemos conseguir su número de Visa, él que figura podría obtener mucho más además. No se preocupe sobre el particular.
Con el análisis de la
Llamadas iniciales de Tommy a Ginny eran simplemente para construir la confianza. Cuando llegó el momento
el ataque real, ella bajó la guardia y aceptado Tommy por lo que él
decía ser, el gerente de otra tienda de la cadena.
¿Y por qué no iba a aceptarlo - que ya lo conocía. Ella sólo lo había conocido por teléfono, por supuesto, pero que habían establecido una amistad de negocios que es la base para la confianza. Una vez que ella lo había aceptado como una figura de autoridad, un gerente
en la misma empresa, la confianza que se había establecido y el resto fue un paseo por el parque.
Mitnick MENSAJE
La técnica de la picadura de la construcción de confianza es uno de los interlocutores sociales más eficaces
tácticas de ingeniería. Usted tiene que pensar si realmente conoces a la persona que está hablando. En algunos casos raros, la persona puede no ser quien dice ser.
En consecuencia, todos tenemos que aprender a observar, pensar y cuestionar la autoridad.
Variación de un tema: tarjeta de captura
La construcción de un sentido de confianza no necesariamente demanda una serie de llamadas telefónicas con
la víctima, según lo sugerido por la historia anterior. Recuerdo un incidente que presencié en cinco minutos fue todo lo que.
Sorpresa, papá
Una vez sentado en una mesa en un restaurante con Henry y su padre. En el curso de conversación, Henry reprendió a su padre para dar a su número de tarjeta de crédito como si fuera su número de teléfono. "Claro, usted tiene que dar su número de tarjeta cuando usted comprar algo ", dijo." Pero le da a una tienda que los archivos de su número en su registros - que es real tonta ".
El único lugar donde hacerlo es en Video Studio ", dijo Conklin, nombrando a los mismos cadena de tiendas de video. "Pero yo voy a mi cuenta de Visa cada mes. Si empiezan a corriendo los cargos, lo sabría.
Seguro ", dijo Henry," pero una vez que su número, que es tan fácil que alguien roban "
¿Quieres decir que un empleado de torcido. "
No, a nadie - no sólo un empleado ".
Usted está hablando a través de su sombrero ", dijo Conklin.
Me puede llamar ahora mismo y hacer que me diga su número de Visa, "tiro de Henry

espalda.
No, no se puede ", dijo su padre.
"Yo puedo hacerlo en cinco minutos, aquí delante de usted sin tener que abandonar
la mesa ".
Sr. Conklin parecía apretado alrededor de los ojos, la mirada de alguien que siente de
sí mismo, sino que no quieren mostrarlo. "Yo digo que no saben que usted está hablando
sobre ", le gritó, sacando su cartera y bofetadas cincuenta billete de un dólar hacia abajo en el
mesa. "Si usted puede hacer lo que usted dice, eso es
la suya.
"Yo no quiero su dinero, papá", dijo Henry.
Sacó su teléfono celular, le pidió a su padre que la rama que utiliza, y llamó a
Asistencia de Directorio para el número de teléfono, así como el número de la tienda
Cerca de Sherman Oaks.
Luego llamó a la tienda de Sherman Oaks. El uso más o menos el mismo enfoque
se describe en el artículo anterior, se puso rápidamente el nombre del director y almacenar los
número.
Luego llamó a la tienda donde su padre tenía una cuenta. Tiró de la vieja
hacerse pasar por el gestor de truco, utilizando el nombre del director como suyos, y dando
el número de la tienda que acababa de obtener. Luego se usa el engaño mismo: "¿Están sus
equipos de trabajo ¿de acuerdo? Nuestros han estado arriba y abajo. "Escuchaba a su respuesta
y luego dijo: "Bueno, mira, yo tengo uno de sus clientes aquí que quiere alquilar
un vídeo, pero nuestras computadoras se han reducido en estos momentos. Necesito que buscar
la
cuentas de los clientes y asegúrese de que es un cliente en su sucursal ".
Henry le dio el nombre de su padre. Luego, usando sólo una ligera variación en
técnica, se hizo la petición al leer la información de la cuenta: dirección,
número de teléfono y fecha de apertura de la cuenta. Y entonces él dijo: "Oye, escucha,
Estoy sosteniendo una larga lista de clientes aquí. ¿Cuál es el número de tarjeta de crédito y
fecha de caducidad? "
Henry puso el teléfono celular a la oreja con una mano mientras le escribió en una
papel servilleta con la otra. Al terminar la llamada, se deslizó en la servilleta
delante de su padre, quien lo miró con la boca abierta. El pobre tipo a
pareció sorprendido totalmente, como si todo su sistema de confianza acababa de bajar la
drenaje.
Con el análisis de la
Piense en su propia actitud cuando alguien que no conoces te pide
algo. Si un extraño mal llega a su puerta, no es probable que lo dejó
en, si un extraño llega a su puerta muy bien vestido, zapatos lustrados, el cabello perfecto,
con buenas maneras y una sonrisa, es muy probable que sea mucho menos sospechoso. Tal vez
en realidad es Jason de las películas de Viernes 13, pero que está dispuesto a comenzar
confiar en esa persona, siempre y cuando se ve normal y no tiene un cuchillo en
su mano.
Lo que es menos obvio es que juzgar a las personas en el teléfono de la misma manera. Se
Suena esto como persona que está tratando de venderme algo? ¿Es amigable y
salientes o que tengo la sensación de algún tipo de hostilidad o la presión? ¿Él o ella tienen la
habla de una persona educada? Juzgamos estas cosas y otras tal vez una docena de
inconscientemente, en un instante, a menudo en los primeros momentos de la conversación.
Mitnick MENSAJE
Es la naturaleza humana a pensar que es poco probable que usted está siendo engañado en
alguna particular
transacción, por lo menos hasta que haya alguna razón para creer lo contrario. Pesamos
los riesgos y entonces, la mayoría de las veces, dar a la gente el beneficio de la duda. Eso es
el comportamiento natural de la gente civilizada .., al menos la gente civilizada que nunca han
sido engañado o manipulado o engañado por una gran cantidad de dinero.
Como los hijos de nuestros padres nos enseñaron a no confiar en extraños. Tal vez todos

deberíamos prestar atención a
este antiguo principio en el lugar de trabajo de hoy.
En el trabajo, la gente hace peticiones de nosotros todo el tiempo. ¿Tiene una dirección de correo electrónico
de este tipo? ¿Dónde está la versión más reciente de la lista de clientes? ¿Quién es el subcontratista en esta parte del proyecto? Por favor, envíenme la última actualización del proyecto.
Necesito la nueva versión del código fuente.
Y adivinen qué: A veces la gente que hace esas peticiones son las personas de su
no conozco personalmente, personas que trabajan para alguna otra parte de la empresa, o reclamo que hacen. Pero si la información que dan los cheques, y ellos parecen ser
en el saber ("Marianne dijo...", "Es en el servidor de K-16 ...";" ... la revisión de 26
los planes de nuevos productos "), extendemos nuestro círculo de confianza para incluirlos, y alegremente darles lo que están pidiendo.
Claro, que puede tropezar un poco, nos preguntamos "¿Por qué alguien en la
Planta de Dallas que ver los planes de nuevos productos? "O" Qué daño podía hacer nada para dar a conocer el nombre del servidor que pasa? "Así que otra pregunta o dos. Si el
respuestas parecen razonables y forma de la persona es tranquilizador, dejamos caer
la guardia, vuelve a nuestra inclinación natural a confiar en el prójimo o la mujer, y
hacer (dentro de lo razonable) lo que sea que nos está pidiendo que hagan.
Y no creo que por un momento que el atacante sólo se centrará en el uso de las personas ho sistemas de la compañía informática. ¿Qué pasa con el hombre en la sala de correo? "¿Quieres hacer
Hazme un favor rápido? Caída de este en la bolsa de la empresa de correo dentro? "¿El mail recepcionista sabe que contiene un disquete con un programa especial para los pequeños
Secretario del CEO? Ahora el atacante obtiene su propia copia personal de la CEO
de correo electrónico. Wow! ¿Podría realmente ocurrir en su empresa? La respuesta es, absolutamente.
EL CENT-MÓVIL
Mucha gente mire a su alrededor hasta que el), encontrar una oferta mejor, los ingenieros sociales no se ven
para un mejor trato, que encuentran una manera de hacer un mejor trato. Por ejemplo, a veces un compañía lanza una campaña de marketing que es lo que no puede soportar la idea de pasar arriba, mientras que el ingeniero social se ve en la oferta y se pregunta cómo puede endulzar el trato.
No hace mucho, una compañía de telefonía móvil en todo el país tenía una gran promoción en marcha
que ofrece un teléfono nuevo para un solo centavo cuando se inscribió en uno de sus
los planes de llamadas.
Como muchas personas han descubierto demasiado tarde, hay muchas preguntas que un buen comprador prudente debe hacer antes de inscribirse en un plan de llamadas de teléfono celular si el servicio es analógico, digital, o una combinación, el número de en cualquier momento minutos se puede utilizar en un mes, si las tarifas de roaming están incluidos .., y,
y otra vez. Especialmente importante entender desde el principio es el plazo del contrato de compromiso - ¿Cuántos meses o años va a tener que comprometerse a?
Imagen de un ingeniero social en Filadelfia que se siente atraída por un modelo de teléfono barato ofrecidos por una empresa de telefonía celular en el registro, pero odia el plan de llamadas que va con él. No es un problema. He aquí una forma que podría manejar la situación.
La primera llamada: Ted
En primer lugar, el ingeniero social marca una tienda de electrónica de la cadena en el oeste de Girard.
"Electron ciudad. Se trata de Ted".
«Hola, Ted-. Este es Adán. Escuche, yo estaba en la otra noche hablando con un tipo de ventas sobre un teléfono móvil. Le dije que le vuelva a llamar cuando me decidí por el plan que yo quería, y se me olvidó su nombre. ¿Quién es el chico que trabaja en ese departamento en la noche

cambio?
"Hay más de uno. Fue William?"
"No estoy seguro. Tal vez fue William. ¿Qué aspecto tiene?" "Tall tipo. Tipo de
flaco. "
"Creo que ese es él. ¿Cuál es su apellido, una vez más?
". Hadley H - A - D - L - E - Y."
"Sí, eso suena bien. ¿Cuándo fue que él va a estar?"
"No sé su horario de esta semana, pero la gente la noche vienen en unos cinco años."
"Bien. Voy a intentar esta noche, entonces. Gracias, Ted".
La segunda llamada: Katie
La siguiente llamada es a una tienda de la misma cadena en el norte de la calle Broad.
"Hola, Ciudad de electrones. Katie hablando, ¿cómo puedo ayudarle?"
"Katie, hola. Esto es William Hadley, más en la tienda de West Girard. ¿Cómo te
hoy en día? "
"Poco lento, ¿qué pasa?"
"Tengo un cliente que entraba en la celda para que el programa de un centavo teléfono.
saben a cuál me refiero? "
"De acuerdo. Vendí un par de esos la semana pasada."
"Todavía hay algunos de los teléfonos que van con ese plan?"
"Tengo un montón de ellos".
"Gran Porque me acaba de vender uno a un cliente El tipo pasó de crédito;.. Firmamos
él arriba en el contrato. Revisé el inventario condenados y no tenemos ningún
teléfonos izquierda. Estoy tan avergonzada. ¿Puedes hacerme un favor? Le voy a enviar a
su tienda a recoger un teléfono. ¿Se puede vender lo que el teléfono de un centavo y escribir
él un recibo? Y se supone que me devuelva la llamada una vez que tiene el teléfono, así que
puede hablar él a través de la forma de programa ".
"Sí, claro. Envíale más."
"Está bien. Su nombre es Ted. Yancy Ted".
Cuando el chico que se llama Ted Yancy se presenta en la
Norte Broad St. tienda, Katie escribe de una factura y le vende
el teléfono celular de un centavo, tal como ella había pedido que se
por su "compañero de trabajo." Se enamoró de el gancho en contra, la línea, y el plomo.
Cuando llegue el momento de pagar, el cliente no tiene monedas de un centavo en el bolsillo, por lo que
mete la mano en el plato pequeño de monedas en el mostrador de la caja, toma uno, y
se lo da a la niña en la caja registradora. Se pone el teléfono sin tener que pagar hasta el
ciento de la misma.
Él es entonces libre para ir a otra compañía de telefonía móvil que utiliza el mismo modelo de
teléfono, y elegir cualquier plan de servicio que le gusta. Preferiblemente uno en un mes a mes
base, sin el compromiso necesarios.
Con el análisis de la
Es natural que las personas tengan un mayor grado de aceptación para cualquier persona que
pretende ser un compañero de trabajo, y que conoce los procedimientos de la empresa, d jerga.
El ingeniero social en esta historia tomó ventaja de que al descubrir los detalles
de una promoción, que se identificó como una empresa
empleado, y pedirle un favor a otra rama. Esto sucede
entre las ramas de las tiendas y entre los departamentos de una empresa, las personas
están separadas físicamente y hacer frente a sus compañeros de trabajo que nunca se han
días reunió a día.
PIRATERÍA EN LA FEDS
La gente a menudo no nos detenemos a pensar en lo que los materiales de su organización está haciendo
disponible en la Web. Para mi programa semanal en la radio la FKI en Los Angeles,
el productor hizo una búsqueda en línea y encontró una copia de un manual de instrucciones para
-acceso a la base de datos del Centro Nacional de Información Criminal. Más tarde se encontró

el manual actual NCIC sí mismo en la línea, un documento sensible que da toda la instrucciones para recuperar información de bases de datos nacionales sobre la delincuencia del FBI.

El manual es una guía para las agencias de aplicación de la ley que le da el formato y los códigos para recuperar información sobre los criminales y los crímenes de los nacionales base de datos. Agencias en todo el país pueden buscar en la misma base de datos de información para ayudar a resolver crímenes en su propia jurisdicción. El manual contiene los códigos utilizados en la base de datos para la designación de todo, desde los diferentes tipos de tatuajes, hasta cascos de embarcaciones diferentes, a las denominaciones de dinero robado y bonos.

Cualquiera con acceso al manual puede buscar la sintaxis y los comandos para extraer información de la base de datos nacional. Luego, siguiendo instrucciones del la guía de procedimientos, con un nervio poco, cualquiera puede extraer información de los base de datos. El manual también ofrece números de teléfono para pedir ayuda en el uso de la del sistema. Es posible que haya manuales similares en sus códigos de producto de la empresa que ofrece o los códigos de recuperación de información sensible.

El FBI casi seguro que nunca se ha descubierto que su manual sensible y instrucciones de procedimiento están disponibles a cualquier persona en línea, y no creo que sería muy contento con él si lo supieran. Una copia fue publicada por un gobierno departamento de Oregon, y el otro por una agencia de aplicación de la ley en Texas. ¿Por qué? En cada caso, alguien probablemente pensó que la información no tenía ningún valor y publicación que no podía hacer ningún daño. Tal vez alguien lo publicaron en sus intranet sólo como una conveniencia para sus propios empleados, nunca darse cuenta de que lo hizo la información a disposición de todos en Internet que tiene acceso a una buena búsqueda motor, tales como Google - incluyendo los justos-llano-curioso, el policía aspirantes, el hacker, y el jefe del crimen organizado.

Aprovechando el sistema

El principio de utilizar esa información para engañar a alguien en el gobierno o una ambiente de negocios es la misma: Debido a que un ingeniero social sabe cómo acceder a bases de datos o aplicaciones específicas, o conoce los nombres de equipo de una empresa servidores, o similares, se gana credibilidad. La credibilidad lleva a la confianza. Una vez que el social ingeniero tiene esos códigos, obtener la información que necesita es un proceso fácil. En este ejemplo, se podría comenzar por llamar a un vendedor en un local Teletipo de la policía estatal de oficinas, y una pregunta de uno de los códigos en el manual - por ejemplo, el código de delito. Se podría decir algo como, "Cuando yo una investigación OFF en el NCIC, me estoy poniendo de un sistema "se ha reducido" de error. ¿Está usted conseguir lo mismo cuando haces un OFF? Sería que lo pruebes para mí? "O tal vez diría que estaba tratando de buscar un wpf - hablar de la policía de una persona quería archivo.

El secretario de teletipo en el otro extremo del teléfono que recoger la señal que la persona que llama estaba familiarizado con los procedimientos operativos y los comandos para consulta la base de datos del NCIC. ¿Quién más que no sea una persona capacitada en el uso de NCIC sabría estos procedimientos?

Después de que el empleado ha confirmado que su sistema está funcionando bien, la conversación podría ser algo como esto:

"Me vendría bien un poco de ayuda." "¿Qué estás buscando?"

"Yo necesito que hagas una orden de descuento en Reardon, Martin. DOB 10118/66".
"¿Cuál es la sosh?" (Agentes de la ley a veces se refieren a la
número de seguro social como el sosh.)
"700-14-7435".
Después de buscar la lista, que podría volver con algo así como:
"Él tiene un 2602."
El atacante sólo tendría que buscar en el NCIC en línea para encontrar el significado de
el número: El hombre tiene un caso de estafa en su historial.
Con el análisis de la
Un ingeniero social no se logra detener por un momento para reflexionar sobre las formas de irrumpir en la base de datos del NCIC. ¿Por qué se debe, cuando una simple llamada a su local departamento de policía, y algunos hablando suave por lo que suena convincente como un información privilegiada, es todo lo que necesita para obtener la información que él quiere? Y la próxima vez, sólo
llama a una agencia de policía diferentes y utiliza el mismo pretexto.
LINGO
SOSH: Ley de la jerga de ejecución de un número de seguro social
Usted podría preguntarse, ¿no es riesgoso para llamar a un departamento de policía, estación del alguacil, o
una oficina de la patrulla de caminos? No el atacante correr un riesgo tan grande?
La respuesta es no. . . y por una razón específica. La gente en la legislación aplica-ción, como personas en las fuerzas armadas, han arraigado en ellos desde el primer día en la academia un el respeto por el rango. Siempre y cuando el ingeniero social se hace pasar por un sargento o teniente - una categoría superior a la persona que está hablando con - la víctima se
regido por la lección bien aprendida que dice que no pongo en duda las personas que están en una posición de autoridad sobre ti. Grado, en otras palabras, tiene sus privilegios, en particular el privilegio de no ser impugnada por las personas de rango inferior.
Pero no creo que la policía y los militares son los únicos lugares donde esta
el respeto por el rango puede ser explotada por el ingeniero social. Los ingenieros sociales a menudo
utilizar la autoridad o rango en la jerarquía corporativa como un arma en sus ataques contra empresas - como una serie de historias en estas páginas demuestran.
PREVENCIÓN DE LA CON
¿Cuáles son algunas medidas que su organización puede tomar para reducir la probabilidad de que
ingenieros sociales se aprovechan del instinto de sus empleados natural a confiar en
la gente? He aquí algunas sugerencias.
Proteja a sus clientes
En esta era electrónica muchas compañías que venden al consumidor mantener las tarjetas de crédito
en el archivo. Hay razones para ello: Se ahorra al cliente la molestia de tener que proporcionar la información de su tarjeta de crédito cada vez que visita la tienda o el sitio Web hacer una compra. Sin embargo, la práctica debe ser desalentado.
Si usted tiene que mantener los números de tarjetas de crédito en el archivo, este proceso tiene que ser
acompañadas de disposiciones de seguridad que van más allá de cifrado o usando el acceso para de control. Los empleados deben ser entrenados para reconocer las estafas de ingeniería social como
los que están en este capítulo. Compañero de trabajo que usted nunca ha conocido en persona, pero
que se ha convertido en un amigo por teléfono no puede ser que él o ella dice ser. Él
pueden no tener la "necesidad de saber" para acceder a información confidencial de clientes, porque en realidad no puede trabajar para la compañía en todo.
Mitnick MENSAJE
Todo el mundo debe ser consciente del modus operandi de la ingeniería social es: Colecciona

todos los
mucha información sobre el objetivo como sea posible, y utilizar esa información para obtener la confianza como un allegado. A continuación, saltar a la yugular!
Confianza con prudencia
No se trata sólo de las personas que tienen acceso a la información claramente sensible - el ingenieros de software, la gente de I + D, y así sucesivamente - que necesitan para estar en el defensa contra las intrusiones. Casi todos en su organización las necesidades de formación para proteger a la empresa de espías industriales y los ladrones de información.
Sentando las bases para esto debe comenzar con un estudio de toda la empresa los activos de información, buscando por separado en cada uno de los activos sensibles, críticos, o de valor,
y pedir lo que los métodos de un atacante podría utilizar para comprometer los activos mediante el uso de tácticas de ingeniería social. La formación adecuada para las personas que tienen acceso confiable a esa información debería ser diseñado en torno a las respuestas a estas preguntas.
Cuando alguien que usted no conoce personalmente las peticiones alguna información o material, o le pide que realice cualquier tarea en el equipo, que sus empleados se pida sí algunos. preguntas. Si me dio esta información a mi peor enemigo, podría ser utilizado para herir a mí oa mi empresa? ¿Debo entender completamente el potencial efecto de los comandos se me pide para entrar en mi ordenador?
No queremos ir por la vida sospechar de cada nueva persona que encuentro. Sin embargo, la mayor confianza que estamos, es más probable que la próxima social ingeniero en llegar a la ciudad será capaz de engañarnos a renunciar a nuestra empresa información confidencial.
Lo que le pertenece en su intranet?
Partes de su intranet pueden estar abiertos al mundo exterior, otras partes restringido a los empleados. ¿Cómo es cuidadosa de su empresa en la toma de la información que no publicado, donde es accesible al público que la intención de protegerlo de la? Cuando es la última vez que alguien en su organización revisa para ver si cualquier información sensible información en la intranet de su compañía había sido sin querer ponerse a disposición a través de las áreas de acceso público de su sitio Web?
Si su empresa ha implementado servidores proxy como intermediarios para proteger a los empresa de las amenazas de seguridad electrónica, han sido revisados los servidores recientemente para asegurarse de que está configurado correctamente?
De hecho, ¿alguien ha comprobado la seguridad de su intranet?

Capítulo 5
"Let Me Help You"
Estamos muy agradecidos cuando estamos plagados de un problema y alguien con la conocimiento, la habilidad y la disposición viene ofreciendo a echarnos una mano. La ingeniero social entiende que, y sabe cómo sacar provecho de ella.
También sabe cómo hacer que un problema para usted .., y luego hacer que agradecidos cuando resuelve el problema .., y, finalmente, jugar en su agradecimiento a extraer algunos información o un pequeño favor de usted, que dejará su empresa (o tal vez que, de forma individual) mucho peor para el encuentro. Y es posible que nunca siquiera sabe que ha perdido algo de valor. He aquí algunas maneras típicas que social ingenieros paso adelante para "ayudar".
Del problema de red
Día / Hora: Lunes, 12 de febrero, 15:25
Lugar: Oficinas de estribor la construcción naval
La primera llamada: Tom Delay
"Tom DeLay, Contabilidad".
"Oye, Tom, se trata de Eddie Martin de la Mesa de Ayuda. Estamos tratando de solucionar un problema de redes de computadoras. ¿Sabe si algún miembro de su grupo ha estado teniendo problemas para mantenerse en la línea? "

"Uh, no, que yo sepa."
"Y usted no está teniendo problemas a ti mismo."
"No, parece estar bien."
"Bueno, eso es bueno. Oye, estamos llamando a las personas que podrían verse afectados" ITLS causa
importantes que vamos a saber de inmediato si pierde su conexión de red. "
"Eso no suena bien. ¿Crees que podría pasar?"
"Esperamos que no, pero vas a llamar si lo hace, ¿verdad?"
"Ya lo creo."
"Escucha, suena como que la conexión de red bajar sería una
problema para usted ... "
"Por supuesto que lo haría."
"... Así que estamos trabajando en esto, te voy a dar mi número de teléfono celular. Entonces puede ponerse en contacto conmigo directamente si es necesario. "
"Eso sería genial. Adelante."
"Es 555 867 5309."
"555 867 5309. Lo tengo. Hey, gracias. ¿Cuál era tu nombre?"
"Es Eddie Oye, otra cosa -. Tengo que comprobar que el puerto el equipo está
conectado. Echa un vistazo en su equipo y ver si hay una etiqueta
en alguna parte que dice algo así como "Número de puerto".
"Espera No, no veo nada de eso."
"Bien, entonces en la parte posterior del ordenador, se puede reconocer el cable de red."
"Sí".
"Que se remontan a donde está enchufado ver si hay una etiqueta en la toma es
conectado a ".
"Espera un segundo Sí, espera un momento -. He aquí que agacharse para que pueda obtener lo suficientemente cerca como para leerlo. Bueno - dice Puerto 6 tablero de 47 ".
"Bueno - eso es lo que usted tenía a medida, simplemente asegurarse".
La segunda llamada: El hombre lo
Dos días después, llegó una llamada a través de operaciones de red de la misma compañía Centro.
"Hola, esto es Bob, estoy en la oficina de Tom DeLay en Contabilidad Estamos tratando. solucionar un problema de cableado. Necesito que inhabilitar el puerto 6-47. "
El chico de TI dijo que se llevaría a cabo en pocos minutos, y para hacerles saber
cuando él estaba listo para tenerlo habilitado.
La tercera convocatoria: Obtener ayuda de su enemigo
Una hora más tarde, el hombre que se hacía llamar Eddie Martin estaba de compras en Circuit City, cuando sonó su teléfono móvil. Miró el identificador de llamadas, vio que la llamada fue
de la empresa de construcción naval, y corrió a un lugar tranquilo antes de contestar.
"Atención al cliente, Eddie".
"Oh, hey, Eddie. Tienes un eco, ¿dónde estás?"
"Estoy, eh, en un armario de cableado. ¿Quién es?
"Es Tom DeLay. Chico, me alegro de que se en contacto contigo. Tal vez usted recuerde
me llamó el otro día? Mi conexión a la red sólo cayó como usted lo dijo
puede, y yo estoy aquí un poco de pánico. "
"Sí, tenemos un montón de gente hasta ahora. Tendríamos que haber tomado
cuidado de la final de la jornada. ¿Te parece bien? "
"¡NO! Maldita sea, me pondré muy por detrás de si estoy abajo tanto tiempo. ¿Qué es lo mejor que puede hacer
para mí? "
"¿Cómo está presionado?"
"Pude hacer algunas otras cosas por ahora. Alguna posibilidad de que pudiera hacerse cargo de ella
en media hora? "

"Media hora! Usted no quiere mucho. Bueno, mira, voy a dejar lo que estoy haciendo y ver si puedo hacerle frente a usted. "
"Oye, te agradezco que, Eddie".
La Cuarta Convocatoria: Gotcha!
Cuarenta y cinco minutos más tarde ...
"Tom? Es Eddie. Vaya por delante e intentar la conexión de red."
Después de un par de momentos:
"Oh, bueno, está funcionando. Eso es genial."
"Bueno, me alegro que podía cuidar de él para usted."
"Sí, muchas gracias."
"Oye, si quieres asegurarte de que tu conexión no volver a bajar, no hay algunos programas que deberías estar en ejecución. Basta con echar un par de minutos. "
"Ahora no es el mejor momento".
"Entiendo ... Se nos podría ahorrar grandes dolores de cabeza la próxima vez que esta red problema que ocurre ".
"Bueno... Si se trata de sólo unos pocos minutos".
"Esto es lo que haces ..."
Eddie se llevó a Tom a través de los pasos de descargar una pequeña aplicación de un Web site. Después de que el programa se había descargado, Eddie le dijo a Tom que hacer doble clic en que. Lo intentó, pero informó:
"No está funcionando. No está haciendo nada."
"¡Oh, qué dolor. Algo debe andar mal con el programa. Vamos a deshacerse de la misma, podemos intentarlo de nuevo en otro momento. "Y habló Tom través de los pasos de eliminar el programa de manera que no se pudo recuperar.
Tiempo total transcurrido, doce minutos.
El atacante de la historia
Bobby Wallace siempre pensé que era de risa cuando él tomó una buena asignación como éste y su cliente en todo el pussyfooted sin respuesta, pero pregunta obvia de por qué querían la información. En este caso, sólo podría pensar en dos razones. Tal vez representa un poco de equipo que estaba interesado en la compra de la empresa objetivo, la construcción naval de estribor, y quería saber lo que tipo de condiciones financieras que estaban realmente en - especialmente todas las cosas el objetivo posible que desee mantener ocultas de un comprador potencial. O tal vez representaba los inversionistas que pensaban que había algo sospechoso en la forma en que el dinero era ser manipulados y quería saber si algunos de los ejecutivos había un caso de las manos en la cookie-jar.
Y tal vez también su cliente no quería decirle la verdadera razón porque, si Bobby sabía lo valioso que la información era, probablemente querrá más dinero para hacer el trabajo.
Hay un montón de maneras de crack en los archivos más secretos de la empresa. Bobby pasó un unos días dándole vueltas a las opciones y hacer un control poco antes de que todo decidió por un plan. Se decidió por el que pidió un enfoque que sobre todo le gustaba, cuando el objetivo está configurado de modo que le pide al atacante en busca de ayuda.
Para empezar, Bobby tomó un teléfono celular 39,95 dólares en una tienda de conveniencia. Él hizo una llamada al hombre que había elegido como objetivo, se hizo pasar como de la mesa de ayuda de la empresa, y poner las cosas por lo que el hombre se llama Bobby teléfono móvil en cualquier momento se encontró con un problema con su conexión de red. Dejó una pausa de dos días para no ser demasiado obvio, y luego hizo un llamado a el Network Operations Center (NOC) en la empresa. Él decía que era la solución de problemas un problema para Tom, el blanco, y pidió que la red de Tom conexión con discapacidad. Bobby sabía que esta era la parte más delicada de todo el aventura - en muchas empresas, la gente del mostrador ayudar a trabajar en estrecha

colaboración con el CON;
de hecho, él conocía la mesa de ayuda es a menudo parte de la organización de TI. Sin embargo, el
hombre indiferente NOC habló con el llamado tratado de forma rutinaria, no pregunte por el nombre de la persona del mostrador de ayuda que supuestamente estaba trabajando en la red problema, y estuvo de acuerdo para desactivar el puerto de destino de red. Cuando haya terminado, Tom
estar totalmente aislado de la intranet de la empresa, no puede recuperar los archivos de la servidor, archivos de intercambio con sus compañeros de trabajo, descarga su correo electrónico, o incluso enviar un
página de datos a la impresora. En el mundo actual, que es como vivir en una cueva.
Cuando Bobby se esperaba, no pasó mucho tiempo antes de que su teléfono celular sonó. Por supuesto que lo hizo
el mismo sonido deseoso de ayudar a este pobre "compañero de trabajo" en peligro. Luego se llamado el NOC y que la conexión del hombre de la red se vuelve a encender. Por último, llamó al hombre y le manipula una vez más, esta vez haciendo que se sienta
culpable por decir que no después de Bobby le había hecho un favor. Tom accedió a la petición que descargar un software en su computadora.
Por supuesto, lo que estuvo de acuerdo en que no era exactamente lo que parece. El software que
Tom le dijo que mantener su conexión a la red de descender, era en realidad una
Caballo de Troya, una aplicación de software que se hizo por ordenador Tom es lo que el engaño original hecho por los troyanos: Se llevó el enemigo dentro del campo. Tom informó que no pasó nada cuando se hace doble clic en el icono del software, el hecho es que, por diseño, no podía ver que pase nada, a pesar de que la pequeña aplicación se instala un programa secreto que le permitiría al infiltrado acceso encubierto al equipo de Tom.
Con el funcionamiento del software, Bobby se le proporcionó un control completo sobre Equipo de Tom, un acuerdo conocido como un shell de comandos remoto. Cuando Bobby acceder a equipo de Tom, que podrían buscar los archivos de contabilidad que pueden ser de interés y copiarlos. Luego, en sus ratos de ocio, los había de examinar la información que dan a sus clientes lo que ellos estaban buscando.
LINGO
Caballo de Troya: un programa que contiene código malicioso o dañino, diseñado para dañar la computadora de la víctima o los archivos, u obtener información de la víctima computadora o red. Algunos troyanos están diseñados para ocultar dentro de la computadora de instrucciones del sistema operativo y espiar a cada golpe de teclado o de la acción, o aceptar más una conexión de red para realizar alguna función, todo ello sin que la víctima sea consciente de su presencia.
Y eso no fue todo. Él podría volver en cualquier momento para buscar a través del correo electrónico
mensajes y notas privadas de los ejecutivos de la empresa, realizar una búsqueda de texto de palabras que podrían revelar cualquier cositas interesantes de la información.
Tarde en la noche que estafó a su objetivo de instalar en el Caballo de Troya
software, Bobby tiró el teléfono celular en un contenedor de basura. Por supuesto, él tuvo el cuidado
para borrar la memoria primero y tire de la batería antes de que lo lanzó - la última
Lo que quería era que alguien llame al número del teléfono móvil por error y
tiene el toque empezar teléfono!
Con el análisis de la
El atacante teje una red de convencer a la meta que tiene un problema que, de hecho, no existe realmente - o, como en este caso, un problema que no ha sucedido todavía, pero que el atacante sabe que va a suceder porque él lo va a hacer. A continuación, se presenta como la persona que puede proporcionar la solución.
La configuración de este tipo de ataque es especialmente jugosa para el atacante:

Debido a la semilla plantada por adelantado, cuando el objetivo descubre que tiene
un problema, se hace la llamada telefónica para pedir ayuda. El atacante
simplemente se sienta y espera a que suene el teléfono, una táctica conocida cariñosamente en el comercio
como revertir la ingeniería social. Un atacante que puede hacer que el blanco le llaman
gana credibilidad instantánea: Si hago una llamada a alguien que creo que es en la mesa de ayuda,
Yo no voy a empezar a pedirle que probar su identidad. Fue entonces cuando el atacante
lo ha hecho.
LINGO
DISTANCIA shell de comandos: Una interfaz gráfica no que acepte texto
comandos de base para realizar ciertas funciones o ejecutar programas. Un atacante que
explota las vulnerabilidades técnicas o es capaz de instalar un programa caballo de Troya en el
el equipo de las víctimas puede ser capaz de obtener acceso remoto a un shell de comandos
MANIPULACIÓN SOCIAL: Un ataque de ingeniería social en la que el
atacante configura una situación en la que la víctima se encuentra con un problema y contactos
el atacante en busca de ayuda. Otra forma de ingeniería social inversa da la vuelta
sobre el atacante. El objetivo reconoce el ataque, y utiliza psicológica
principios de la influencia de extraer tanta información como sea posible de la
atacante para que la empresa puede proteger los activos específicos.
Mitnick MENSAJE
Si un extraño te hace un favor, y luego le pide un favor, no sin reciprocidad
pensar cuidadosamente acerca de lo que está pidiendo.
En una estafa como esta, el ingeniero social trata de elegir un objetivo que es probable que
tienen un conocimiento limitado de computadoras. Cuanto más se sabe, es más probable que
que va a sospechar, o sólo la figura simple que está siendo manipulado. Lo que
a veces llamar a la computadora reto de los trabajadores, que está menos informado
acerca de la tecnología y los procedimientos, es más probable que cumplan. Que es aún más
probabilidades de caer en una trampa como "Sólo tienes que descargar este pequeño programa,"
porque no tiene
idea del daño potencial de un programa de software puede causar. Lo que es más, hay
una probabilidad mucho menor que va a entender el valor de la información sobre la
equipo de red que está poniendo en riesgo.
UNA PEQUEÑA AYUDA PARA EL NUEVO GAL
Los nuevos empleados son un blanco propicio para los atacantes. No conozco a mucha gente, sin embargo,
que no conocen los procedimientos o los dos y no hacer de la empresa. Y, en el
nombre de hacer una buena primera impresión, que están ansiosos por mostrar cómo cooperativo y
respondió rápidamente que pueden ser.
Andrea útil
"Recursos Humanos, Andrea Calhoun."
"Andrea, hola, este es Alex, con la seguridad corporativa."
"¿Sí?"
"¿Cómo te va hoy?"
"Está bien. ¿Qué puedo ayudarte?"
"Mira, estamos desarrollando un seminario de seguridad para los nuevos empleados y tenemos que
reunir a algunas personas para probarlo en el. Quiero obtener el nombre y número de teléfono
de todas las nuevas contrataciones en el último mes. ¿Me pueden ayudar con eso? "
"No voy a ser capaz de llegar a ella 'hasta esta tarde. ¿Está bien?
"¿Cuál es su extensión?"
"Claro, está bien, es 52... Oh, uh, pero voy a estar en las reuniones de la mayor parte de hoy. Te llamo
cuando estoy en mi oficina, probablemente después de cuatro años. "

Cuando Alex llamó alrededor de las 4:30, Andrea tenía la lista, y le leyó los nombres y las extensiones.

Un mensaje de Romero

Romero Morgan se mostró encantado con su nuevo trabajo. Ella nunca había trabajado para una revista antes y fue encontrar a las personas mucho más amigable de lo que esperaba, un sorpresa debido a la presión incesante la mayoría del personal estaba siempre bajo para obtener un nuevo tema terminado antes del plazo mensual. La llamada que recibió Un jueves por la mañana volvió a confirmar esa impresión de amistad.

"¿Es que Rosemary Morgan?"

"Sí".

"Hola, Rosemary. Este es Bill Jorday, con el grupo de seguridad de la información."

"¿Sí?"

"¿Alguien ha discutido en la sección de las mejores prácticas de seguridad con usted?"

"Yo no lo creo."

"Bueno, vamos a ver. Para empezar, no se permite a nadie para instalar el software trajo desde fuera de la empresa. Eso es porque no queremos que de cualquier responsabilidad derivada uso sin licencia de software. Y para evitar cualquier problema con el software que pueda tener un gusano o un virus. "

"De acuerdo".

"¿Estás al tanto de nuestras políticas de correo electrónico?"

"No."

"¿Cuál es tu dirección de correo electrónico actual?" "Rosemary@ttrzine.net".

"¿Te acceder con el nombre de usuario Romero?"

"No, es R subrayado Morgan."

"De acuerdo. Nos gusta que todos nuestros nuevos empleados consciente de que puede ser peligroso para abra ningún archivo adjunto de correo electrónico que no se esperaba. Gran cantidad de virus y gusanos se enviado alrededor y vienen en los correos electrónicos que parecen ser de personas que conoce. Así que si usted recibe un correo electrónico con un archivo adjunto que no esperaba que siempre debe verifique que la persona que aparece como remitente realmente se envía el mensaje. Usted entender? "

"Sí, he oído hablar de eso."

"Bien. Y nuestra política es que usted cambie su contraseña cada noventa días. ¿Cuándo fue la última vez que cambie su contraseña? "

"Sólo he estado aquí tres semanas, todavía estoy usando la primera vez que establece."

"Está bien, está bien. Usted puede esperar el resto de los noventa días. Pero tenemos que ser seguro que la gente está utilizando contraseñas que no son demasiado fáciles de adivinar. ¿Está utilizando un contraseña que se compone de letras y números? "

"No."

Tenemos que arreglar eso. ¿Qué contraseña está usando ahora? "

"Es el nombre de mi hija - Annette".

"Eso en realidad no es una contraseña segura. Nunca se debe elegir una contraseña que es sobre la base de información de la familia. Bueno, vamos a ver .., usted podría hacer lo mismo que yo.

Está bien usar lo que está utilizando ahora como la primera parte de la contraseña, pero luego cada vez que lo cambie, añade un número del mes en curso. "

"Así que si lo hacía ahora, en marzo, se debe utilizar tres, o tres-oh".

"Eso depende de usted. ¿Qué estaría usted más cómodo?"

"Creo que Annette y tres."

"Está bien. ¿Quieres que te acompañe a través de cómo hacer el cambio?"

"No, yo sé cómo hacerlo".
"Bien. Y una cosa más que tenemos que hablar. Usted tiene software anti-virus en el equipo y que es importante para mantenerse al día. Nunca se debe desactivar la actualización automática, incluso si el equipo se ralentiza de vez en al mismo tiempo. ¿De acuerdo? "
"Seguro".
"Muy bien. ¿Y tiene nuestro número de teléfono por aquí, lo que nos puede llamar si usted tiene algún problema informático? "
No lo hizo. Le dio el número, lo escribió con cuidado, y volvió para trabajar, una vez más, contento por lo bien cuidado que se sentía.
Con el análisis de la
Esta historia refuerza un tema subyacente encontrará en este libro: El información más común que un ingeniero social que quiere de un empleado, independientemente de su objetivo final, son las credenciales de autenticación de la meta. Con una nombre de cuenta y contraseña de la mano de un solo empleado en el área de derecho de la empresa, el atacante tiene lo que necesita para entrar y localizar cualquier la información que busca. Tener esta información es como encontrar las llaves de la reino, y con ellos en la mano, se puede mover libremente por todo el panorama empresarial y encontrar el tesoro que busca.
Mitnick MENSAJE
Antes de que los nuevos empleados se les permite el acceso a los sistemas de la compañía informática, deben estar capacitados para seguir las buenas prácticas de seguridad, especialmente las políticas sobre no revelar sus contraseñas.
No es tan seguro como PIENSA
"La empresa que no hace un esfuerzo por proteger su información sensible está simplemente por negligencia. "Mucha gente estaría de acuerdo con esa afirmación. Y el mundo sería un lugar mejor si la vida fuera tan obvio y tan simple. La verdad es que incluso aquellas empresas que hacen un esfuerzo por proteger la información confidencial información puede estar en serio riesgo.
He aquí una historia que ilustra una vez más cómo las empresas se engañan todos los día en el pensamiento de sus prácticas de seguridad, diseñado por el competente y con experiencia, profesionales, no puede eludirse.
Historia de Steve Cramer
No era un jardín grande, no uno de esos diferenciales caro cabeza de serie. Se obtuvo ninguna la envidia. Y ciertamente no era lo suficientemente grande para darle una excusa para comprar una de brazos caídos cortadora de césped, que estaba bien porque no se han utilizado de todos modos. Steve disfrutado de cortar el césped con una cortadora de césped a mano, ya que tomó más tiempo, y el tarea siempre una buena excusa para centrarse en sus propios pensamientos en vez de escuchar a Anna contándole historias sobre la gente en el banco donde ella trabajado o explicar las diligencias para que él haga. Odiaba las listas de miel que se se había convertido en una parte integral de sus fines de semana. Que brilló, aunque su mente que el 12 - años de edad, Pete fue maldito inteligente para unirse al equipo de natación. Ahora tendría que estar en práctica o cumplir con todos los sábados para que no se queden con las tareas del sábado.
Algunas personas podrían pensar trabajo de Steve diseño de nuevos dispositivos para GeminiMed Productos Médicos fue aburrido, Steve sabía que era salvar vidas. Steve pensó en a sí mismo como estar en una línea creativa de la obra. Artista, compositor, ingeniero -, en Punto de vista de Steve todos enfrentan el mismo tipo de desafío que él hizo: Crearon

algo que nadie había hecho antes. Y su último trabajo, un intrigante astuto
nuevo tipo de stent cardíaco, sería su mayor logro todavía.
Eran casi las 11:30 de este sábado en particular, y Steve molesto porque
Casi había terminado de cortar el césped y que no había hecho ningún progreso real en la encontrar la manera de reducir la demanda de potencia en el stent del corazón, los últimos obstáculos restantes. Un problema perfecta para reflexionar sobre durante la siega, pero no la solución
había llegado.
Anna apareció en la puerta, su pelo cubierto en el pañuelo vaquero rojo Paisley ella
siempre llevaba en polvo. "Llamada telefónica", le gritó a él. "Alguien de
trabajo ".
"¿Quién?" Steve gritó.
"Ralph algo. Creo."
Ralph? Steve no podía recordar a nadie en GeminiMed llamado Ralph, que
podría ser llamado a un fin de semana. Pero Anna probablemente tenía el nombre equivocado.
"Steve, se trata de Ramón Pérez de Soporte Técnico". Ramon - cómo en el mundo se
Anna obtener de un nombre hispano a Ralph, Steve se preguntó.
"Esto es sólo una visita de cortesía, Ramón estaba diciendo." Tres de los servidores están inactivos,
pensamos que tal vez un gusano, y tenemos que limpiar los discos y restaurar la copia de seguridad.
Debemos ser capaces de tener sus archivos en marcha el miércoles o el
Jueves. Si tenemos suerte. "
"Absolutamente inaceptable", dijo Steve con firmeza, tratando de no dejar que su frustración tomar
más. ¿Cómo pudo esta gente ser tan estúpido? ¿De verdad cree que puede
manejar sin acceso a sus archivos todos los fines de semana y la mayor parte de la próxima semana? "De ninguna manera.
Voy a sentarme en mi casa, en la terminal casi dos horas y tengo que
el acceso a mis archivos. ¿Estoy haciendo esto claro? "
"Sí, bueno, todo el mundo me ha llamado hasta ahora quiere estar en la parte superior de la lista.
Renuncié a mi fin de semana para venir y trabajar en esto y no es divertido tener
todo el mundo me habla para conseguir enojado conmigo. "
"Estoy en un plazo breve, la empresa cuenta con esto, tengo que conseguir un trabajo
hecho esta tarde. ¿Qué parte de esto ¿no lo entiendes? "
"Todavía tengo un montón de gente para llamar antes de que pueda comenzar", establece Ramón.
"¿Qué tal si dice que va a tener sus archivos para el martes?"
"No martes no, miércoles, en la actualidad. NOW!" Steve dijo, preguntándose quién
Se va a llamar si no podía conseguir su punto a través del cráneo grueso de este tipo.
"Bueno, bueno", dijo Ramón, y Steve le podía oír un suspiro de
molestia. "Déjame ver qué puedo hacer para que te va. Utilice el RM22
servidor, ¿verdad? "
"RM22 y el GM16. Las dos cosas."
. "En este acuerdo, puedo cortar algunas esquinas, ahorrar algo de tiempo - I'll necesita su nombre de usuario
y una contraseña. "
Uh oh, pensó Steve. ¿Qué está pasando aquí? ¿Por qué iba a necesitar mi contraseña?
¿Por qué sería, de todas las personas, pregunte por él?
"¿Qué has dicho tu apellido era y quién es su supervisor?" "Ramón
Perez. Mira, te diré algo, cuando lo contrataron, había una forma que había que
llenar para obtener su cuenta de usuario, y había que poner una contraseña. Podría
mira eso y demostrar que lo tenemos en el archivo aquí. ¿De acuerdo? "
Steve caliente que durante unos instantes, y luego estuvo de acuerdo. Colgó con cada vez mayor impaciencia, mientras que Ramón iba a recuperar documentos de un archivador. Finalmente

De regreso al teléfono, Steve le oía arrastrando los pies a través de una pila de papeles.
"Ah, aquí está", dijo Ramón, por fin. "Usted pone abajo" Janice ". La contraseña" Janice,
Steve pensó. Era el nombre de su madre, y él había hecho, a veces se utiliza como
una contraseña. Él muy bien podría haber puesto hacia abajo para que su contraseña cuando se llena
a cabo sus nuevas contrataciones papeles.
"Sí, es cierto", reconoció.
"Bueno, estamos perdiendo el tiempo aquí. Tú sabes que yo soy de verdad, quieres que el uso
el acceso directo y obtener archivos de nuevo a toda prisa, que vas a tener que ayudarme
aquí ".
"Mi ID es s, d, subrayado, Cramer -. Cramer La contraseña es" un pelícano ".
"Voy a hacerlo bien en él", dijo Ramón, que suena útil al fin. "Dame un par de
horas. "
Steve terminó el césped, había comida, y cuando llegó a su ordenador que se encuentra
que sus archivos se habían hecho restaurado. Estaba satisfecho de sí mismo para el manejo de
que no cooperan IT hombre con tanta fuerza, y esperanza de Anna había oído hablar de la firmeza
que era. Sería bueno para dar al hombre o su jefe un attaboy, pero él lo sabía
Era una de esas cosas que nunca había moverse a hacer.
Historia de Craig Cogburne
Craig Cogburne había sido un vendedor de una empresa de alta tecnología, y hace bien en
que. Después de un tiempo empezó a darse cuenta de que tenía una habilidad para la lectura de un cliente,
entender que la persona era resistente y el reconocimiento de
alguna debilidad o vulnerabilidad que hace que sea fácil de cerrar la venta. Comenzó a
pensar en otras maneras de utilizar este talento, y el camino le llevó a una
campo mucho más lucrativo: el espionaje corporativo.
Este fue un trabajo en caliente. No se veía a llevarme mucho tiempo y vale la pena
suficiente para pagar un viaje a Hawai. O tal vez Tahití.
El tipo que me contrató, él no me dijo el cliente, por supuesto, pero pensé que se
alguna empresa que quería ponerse al día con la competencia en el rápido, grande,
salto fácil. Todo lo que tendría que hacer es conseguir los diseños y especificaciones de producto para un nuevo
dispositivo llamado un stent cardíaco, lo que era. La empresa se llamaba
GeminiMed. Nunca he oído hablar de él, pero era un traje de Fortune 500 con sede en la mitad
una docena de lugares - que hace el trabajo más fácil que una empresa más pequeña, donde
hay una posibilidad razonable del hombre con quien estás hablando con el chico sabe que está reclamando que se
y sabe que no lo son. Este, como los pilotos decir de un choque en el aire, puede arruinar
el día entero.
Mi cliente me ha enviado un fax, un poco de la revista un médico que dijo GeminiMed
estaba trabajando en un stent con un nuevo diseño radical y sería llamado el STHIO0.
Por el amor de Dios, algún periodista ya ha hecho un gran pedazo de la
trabajo de campo para mí. Yo tenía una cosa que necesitaba, incluso antes de que se inició, el nuevo
nombre del producto.
Primer problema: Obtenga los nombres de las personas en la empresa que trabajó en el STH-100
o que tenga que ver los diseños. Así que llamé a la operadora y le dijo: "Yo
prometió una de las personas en su grupo de ingeniería me ponía en contacto con él
y no recuerdo su apellido, pero su nombre comenzó con una S. "Y
dijo: "Tenemos un arquero Scott Davidson y Sam." Me tomó un largo tiempo. "¿Qué
se trabaja en el grupo STH100? "Ella no lo sabía, así que acaba de recoger Scott Archer
al azar, y ella llamó a su teléfono.
Cuando respondió, me dijo: "Hey, este es Mike, en la sala de correo. Tenemos un
FedEx aquí que es para el corazón stent STH-100 del equipo del proyecto. Cualquier idea de

quién
debe ir? "Él me dio el nombre del líder del proyecto, Jerry Mendel. Incluso
lo puso a buscar el número de teléfono para mí.
Que se llama. Mendel no estaba allí, pero su mensaje de voz dijo que estaría de vacaciones hasta el decimotercero, lo que significaba que tenía otra semana para esquiar o lo que sea, y todo aquel que necesitaba algo, mientras tanto, debe llamar a Michelle en
9137. Muy útil, a estas personas. Muy útil.
Colgué el teléfono y llamó a Michelle, tiene ella por teléfono y le dijo: "Este es Bill Thomas. Jerry me dijo que debería llamar cuando tuve la especificación de lista que quería que los chicos de su equipo para su revisión. Usted está trabajando en el stent del corazón, ¿verdad? "
Ella dijo que eran.
Ahora estábamos llegando a la parte sudoroso de la estafa. Si ella empezó a sonar sospechoso, que estaba listo para jugar la carta acerca de cómo yo estaba tratando de hacer un favor a Jerry me había pedido. Le dije: "¿Qué sistema está usted?"
"Sistema?"
"¿Qué equipo servidor tiene en su grupo?"
"Oh," ella dijo, "RM22. Y algunos de los grupos también utilizan GM16." Buena. Que necesitaba eso, y fue una pieza de información que pude conseguir de ella sin su
sospechoso. Que le ablandó el siguiente fragmento, hecho con tanta naturalidad como pudiera manejar. "Jerry dijo que me podía dar una lista de direcciones de correo electrónico para las personas en el
equipo de desarrollo, "dije, y contuve la respiración.
"Por supuesto. La lista de distribución es demasiado largo para leer, puedo enviar por correo electrónico?"
Lo sentimos. Cualquier dirección de correo electrónico que no terminó en GeminiMed.com sería una enorme bandera roja. "¿Y tú por fax a mí?" Me dijo.
Ella no tenía ningún problema en hacer eso.
"Nuestra máquina está en un abrir y cerrar. Voy a tener que obtener el número de otro. Llame de vuelta en un poco ", le dije, y colgué.
Ahora, usted puede pensar que tenía que cargar con un problema pegajosa aquí, pero es sólo Otro truco habitual del comercio. Esperé un rato para que mi voz no sonara
familiar a la recepcionista, a continuación, la llamó y le dijo: "Hola, soy Bill Thomas, nuestro fax máquina no está trabajando aquí, puedo tener un fax enviado a su máquina? ", dijo ella seguro, y me dio el número.
Luego simplemente entrar y recoger el fax, ¿verdad? Por supuesto que no. Primera regla: Nunca visitar las instalaciones a menos que sea absolutamente necesario. Que tienen dificultades para identificar si usted es sólo una voz en el teléfono. Y si no puede identificar
usted, no lo puede arrestar. Es difícil poner las esposas en torno a una voz. Así que llamé a la recepcionista de vuelta después de un rato y le preguntó qué mi fax vienen? "Sí,"
dijo.
"Mire", le dije, "tengo que llegar a un consultor que estamos usando. ¿Podría
? enviarlo para mí "ella estuvo de acuerdo y por qué no -. ¿cómo podría ser cualquier recepcionista
espera que reconozcan los datos sensibles? Mientras que envió el fax a la
"Consultor", tenía mi ejercicio para el día caminando a una tienda de papelería cerca yo, el que tiene el cartel de fuera "faxes enviados / Rcvd". El fax se suponía que
llegar antes que yo, y como se esperaba, que estaba allí esperando para mí cuando entré Seis páginas de $ 1.75. Por un billete de $ 10 y el cambio, tenía toda la lista del grupo de nombres y direcciones de correo electrónico.
Conseguir el interior
Muy bien, así que ahora había hablado con tres o cuatro personas diferentes en sólo unas pocas horas
y ya era un gran paso más cerca de conseguir dentro de las computadoras de la compañía. Pero que iba a necesitar un par de piezas más antes de que yo estaba en casa.

El número uno es el número de teléfono de marcación en el servidor de Ingeniería de exterior. Llamé de nuevo GeminiMed y pidió a la telefonista de la IT Departamento, y pidió al hombre que respondió a alguien que me pudiera dar alguna ayuda de la computadora. Él me trasladaron, y me pongo un acto de ser confundido y el tipo de estupideces sobre todo técnica. "Estoy en casa, acaba de comprar una nueva portátil, y tengo que configurar o que puedo marcar desde fuera ".

El procedimiento fue evidente, pero con paciencia dejar que me hable a través de ella hasta que se el número de marcación telefónica. Me dio el número como si fuera sólo otra pieza habitual de la información. Entonces le hizo esperar mientras que lo intenté. Perfecta. Así que ahora me había pasado el obstáculo de la conexión a la red. Marqué y descubrieron que se crearon con un servidor de terminal que le permitiría a una persona que llama conectarse a cualquier computadora en su red interna. Después de un montón de intentos me encontré con computadora de alguien que tenía una cuenta de invitado sin contraseña. Algunos sistemas operativos, cuando se instala por primera vez, dirigen al usuario a establecer una identificación y contraseña, sino que también proporcionan una cuenta de invitado. El usuario debe programar su propia contraseña para la cuenta de invitado o desactivarlo, pero la mayoría de los hombres no saben sobre esto, o simplemente no se molestan. Este sistema fue probablemente acaba de crear y propietario no se había molestado en deshabilitar la cuenta de invitado.

LINGO

HASH PASSWOPRD: Una serie de galimatías que resulta de un proceso contraseña a través de un proceso unidireccional de encriptación. El proceso se supone que irreversible, es decir, su cree que no es posible reconstruir la contraseña a partir del hash

Gracias a la cuenta de invitado, que ahora tienen acceso a una computadora, que resultó que se ejecuta una versión anterior del sistema operativo UNIX. Bajo Unix, el sistema operativo mantiene un archivo de contraseñas, que con-las lluvias cifrados contraseñas de todas las personas autorizadas para acceder a ese equipo. El archivo de contraseñas contiene el hash de un solo sentido (es decir, una forma de cifrado que es irreversible) de cada usuario una contraseña. Con un hash de una vía una contraseña real, como, por ejemplo, "JUSTDOIT" estaría representada por una almohadilla en forma encriptada, en este caso el hash se convertiría en UNIX a trece caracteres alfanuméricos.

Cuando Billy Bob en el pasillo quiere transferir algunos archivos a una computadora, es requiere que se identifique proporcionando un nombre de usuario y contraseña. El sistema programa que "revisa su autorización cifra la contraseña que entra, y luego compara el resultado con el password encriptado (hash) que figura en el contraseña del archivo, si ambas coinciden, que le ha dado acceso.

Debido a que las contraseñas en el archivo se cifran, el archivo mismo se hizo disponibles para cualquier usuario en la teoría de que no hay manera conocida para descifrar el contraseñas. Eso es una risa - He descargado el archivo, corrió un ataque de diccionario en él (Véase el Capítulo 12 para más información sobre este método) y encontró que uno de los ingenieros en el equipo de desarrollo, un hombre llamado Steven Cramer, en la actualidad tenía una cuenta en el equipo con la contraseña "Janice". Sólo en la oportunidad, traté de entrar en su cuenta con la contraseña de uno de los servidores de desarrollo, si se hubiera trabajado, me habría ahorrado mucho tiempo y un poco de riesgo. No lo hizo.

Eso significaba que tendría que engañar al hombre a decirme su nombre de usuario y contraseña. Por eso, yo esperaría hasta el fin de semana. 70 Ya sabes el resto. El sábado llamado Cramer y lo acompañó a través de un ardid de un gusano y los servidores tener que ser restaurados de copia de seguridad para superar sus sospechas.

¿Qué pasa con la historia que le contó, la de la inclusión de una contraseña cuando se llena

los papeles de su empleado? Yo contaba con él, no recuerdo que nunca se había
que pasó. Un empleado de nuevo llena de tantas formas que, años más tarde, que se
¿te acuerdas? Y de todos modos, si me había dado con él, yo aún tenía esa larga lista de
otros nombres.
Con su nombre de usuario y contraseña, me metí en el servidor, pesca de alrededor de un poco
tiempo, y luego encuentra los archivos de diseño para la STH-100. Yo no estaba muy seguro
cuáles fueron la clave, por lo que acaba de transferir todos los archivos a una caída de muerto, un
FTP gratuito
sitio en China, donde podrían ser almacenados sin que nadie se empezaban a sospechar. Dejar
el tipo de clientes a través de la basura y encontrar lo que quiere.
LINGO
MUERTOS Escribir un lugar para dejar la información en que es improbable que se encuentran
por
otros. En el mundo de los espías tradicionales, esto podría estar detrás de una piedra suelta en un
pared, en el mundo de los hacker, que es comúnmente un sitio de Internet en un
país remoto.
Con el análisis de la
Para el hombre que está llamando a Craig Cogburne, o alguien como él mismo un experto en
las artes ladrona-pero-no-siempre-ilegal de la ingeniería social, el reto
que aquí se presenta casi de rutina. Su objetivo era localizar y descargar archivos
almacenados en un equipo corporativo seguro, protegido por un cortafuegos y todos los
habituales de la
tecnologías de seguridad.
La mayor parte de su trabajo fue tan fácil como atrapar el agua de lluvia en un barril. Comenzó
haciéndose pasar por alguien de la sala de correo y amueblado añade una sensación de
urgencia, alegando que había un paquete de FedEx a la espera de ser entregados. Este
engaño producido el nombre del líder del equipo para la ingeniería de corazón stent
grupo, que estaba de vacaciones, pero - conveniente para cualquier ingeniero social tratando de
robar información - que había dejado amablemente el nombre y número de teléfono de su
asistente. Llamándola, Craig desactivó cualquier sospecha al afirmar que él era
respondiendo a una solicitud del jefe de equipo. Con el líder del equipo fuera de la ciudad,
Michelle no tenía manera de comprobar su afirmación. Ella lo aceptó como la verdad y no tenía
problema de proporcionar una lista de personas en el grupo - por Craig, una necesaria y
altamente
conjunto estimado de la información.
Ni siquiera a sospechar cuando Craig quería que la lista enviada por fax en vez de
por correo electrónico, habitualmente más conveniente en ambos extremos. ¿Por qué estaba tan
ingenuos?
Al igual que muchos empleados, que no quería a su jefe para volver a la ciudad y encontrar que
había
trabas a una llamada de alguien que sólo estaba tratando de hacer algo que el jefe le había
pedido
para. Además, la persona que llamó dijo que el jefe no había autorizado recientemente la
solicitud, pero
le pidió su ayuda. Una vez más, he aquí un ejemplo de alguien que muestra la
fuerte deseo de ser un jugador de equipo, lo que hace que la mayoría de las personas
susceptibles a
engaño.
Craig evitar el riesgo de entrar en el edificio físico simplemente por tener la
fax enviado a la recepcionista, a sabiendas de que era probable que sea útil. Recepcionistas
Después de todo, generalmente elegidos por su personalidad encantadora y su capacidad para
dar una buena impresión. Haciendo pequeños favores como recibir un fax y enviarlo
viene con el territorio de la recepcionista, un hecho que Craig fue capaz de tomar
ventaja. Lo que ella estaba terminando a pasado a ser la información que pueda
han hecho sonar la alarma con que nadie lo sepa el valor de la información - pero

¿cómo podría recepcionista esperar para saber qué información es benigna y
que sensible?
El uso de un estilo diferente de la manipulación, Craig actuó confuso e ingenuo
convencer al hombre en las operaciones de computadora que le proporcione el acceso dial-up
número de servidor de terminal de la empresa, el hardware que se utiliza como una conexión
punto a otros sistemas informáticos dentro de la red interna.
Mitnick MENSAJE
Primera prioridad de todos en el trabajo es hacer el trabajo. Bajo esa presión,
prácticas de seguridad a menudo a un segundo plano y se pasan por alto o ignoradas. Social
los ingenieros confían en esto cuando la práctica de su oficio.
Craig fue capaz de conectar fácilmente al intentar una contraseña por defecto que no se había
cambiado, uno de los evidentes, abiertas las brechas que existen en muchos internos
redes que se basan en la seguridad del cortafuegos. De hecho, las contraseñas por defecto para
muchos
sistemas operativos, routers, y otros tipos de productos, incluyendo PBXs, se
disponible en línea. Cualquier ingeniero social, hacker, o un espía industrial, así como
la curiosidad simplemente, puede encontrar la lista en http://www.phenoelit.de/dpl/dpl.html.
(Es absolutamente increíble lo fácil que Internet hace la vida para los que saben
dónde buscar. Y ahora usted sabe, también.)
Cogburne luego se las arregló para convencer a un hombre prudente, sospechoso
("¿Qué has dicho tu apellido era ¿Quién es su supervisor?") Para divulgar sus
nombre de usuario y contraseña para poder acceder a los servidores utilizados por el corazón-
stent
desarrollo del equipo. Esto fue como salir de Craig con una puerta abierta para navegar por la
empresa la mayoría de los secretos celosamente guardados y descargar los planos para el nuevo
del producto.
¿Qué pasa si Steve Cramer había seguido a sospechar acerca de la llamada de Craig? Fue
poco probable que iba a hacer nada sobre el informe de sus sospechas, hasta que apareció
en el trabajo en la mañana del lunes, que habría sido demasiado tarde para prevenir la
ataque.
Una de las claves para la última parte de la treta: Craig en un primer momento se hizo el sonido
apática y desinteresada en las preocupaciones de Steve, y luego cambió de parecer y
Sonaba como si estuviera tratando de ayudar a que Steve podía hacer su trabajo. La mayoría de
los
tiempo, si la víctima cree que estamos tratando de ayudar o no le de algún tipo de
favor, que se parte de la información confidencial que de otro modo habría
cuidadosamente protegidos.
PREVENCIÓN DE LA CON
Uno de los trucos más poderosos de la ingeniería social consiste en convertir las tablas.
Eso es lo que he visto en este capítulo. El ingeniero social que crea el problema,
y luego por arte de magia resuelve el problema, engañar a la víctima en el abastecimiento de
el acceso a los secretos mejor guardados de la compañía. ¿Sus empleados se encuentran en
este
tipo de artimaña? ¿Ha tomado la molestia de redactar y distribuir las normas específicas de
seguridad que
podría ayudar a evitar?
Educar, educar y educar ...
Hay una vieja historia sobre un visitante de Nueva York que se detiene a un hombre en la calle
y pregunta: "¿Cómo puedo llegar al Carnegie Hall?" El hombre contesta, "Práctica, práctica,
la práctica. "Todo el mundo es tan vulnerable a los ataques de ingeniería social que un
empresa única defensa eficaz es educar y capacitar a su gente, dándoles
la práctica que necesitan para detectar un ingeniero social. Y luego seguir recordando a la gente
sobre una base consistente de lo que han aprendido en el entrenamiento, pero son muy
propensos a
olvidar.

Todos en la organización deben estar capacitados para ejercer un grado apropiado de desconfianza y cautela cuando fue contactado por alguien que él o ella no relacionada con saber, especialmente cuando ese alguien está pidiendo ningún tipo de acceso a una computadora o red. Es la naturaleza humana a querer confiar en los demás, sino como el Japoneses dicen, el negocio es la guerra. Su negocio no puede permitirse el lujo de bajar la guardia.

La política de seguridad de la empresa debe definir claramente apropiados e inapropiados comportamiento.

La seguridad no es una talla única para todos. Personal de la empresa por lo general tienen roles diferentes

y las responsabilidades y la posición que cada uno tiene asociado vulnerabilidades. Hay debe ser un nivel básico de formación que todos en la empresa está obligada a personas completas, a continuación, también deben ser entrenados de acuerdo a su perfil de trabajo de

se adhieren a ciertos procedimientos que reduzcan la posibilidad de que se conviertan en parte del problema. Las personas que trabajan con información sensible o se colocan en puestos de confianza se debe dar capacitación especializada adicional.

Mantener la información más delicada

Cuando la gente se les acerca un extraño que ofrecen a ayudar, como se ve en las historias en este capítulo, tienen que recurrir a la política de seguridad corporativa que se adapte adecuada a las necesidades de la empresa, el tamaño y la cultura de su empresa.

NOTA

Personalmente, no creo que cualquier negocio debe permitir que cualquier cambio de las contraseñas.

Es mucho más fácil establecer una regla que prohíbe al personal de nunca compartir o el intercambio de claves de acceso confidenciales. Su más seguro. Sin embargo, cada empresa debe evaluar

su propia cultura y los problemas de seguridad en la toma de esta decisión

No cooperar con un desconocido que le pide a buscar información, ingrese comandos desconocidos en una computadora, realizar cambios en la configuración del software o -

potencialmente más desastroso de todos - abrir un archivo adjunto de correo electrónico o descargar

software sin marcar. Cualquier programa de software - incluso uno que parece no hacer nada en todo - no puede ser tan inocente como parece ser.

Hay ciertos procedimientos que, no importa lo bueno que nuestra formación, que tienden a crecen descuidados en el tiempo. Entonces nos olvidamos de que la formación en el momento de crisis,

sólo cuando lo necesitamos. Se podría pensar que no dar su nombre de cuenta y la contraseña es algo que casi todo el mundo sabe (o debería saber) y no necesita que le digan: es simple sentido común. Pero, en realidad, todos los empleados es necesario recordar con frecuencia que dar el nombre de usuario y contraseña a su computadora de oficina, computadora de su casa, o incluso la máquina de franqueo en el sala de correos es equivalente a dar el número PIN de su tarjeta de cajero automático.

Hay ocasiones - muy de vez en cuando - una circunstancia muy válida cuando es es necesario, incluso importantes, para dar a alguien más confidenciales de la información. Por esa razón, no es apropiado para hacer una regla absoluta acerca "Nunca". Sin embargo, sus políticas y procedimientos de seguridad tiene que ser muy específico sobre las circunstancias bajo las cuales un empleado puede dar a conocer su contraseña y - más importante - que está autorizado para solicitar la información.

Considere la fuente

En la mayoría de las organizaciones, la regla debe ser que cualquier información que sea posible causar daño a la empresa o de a. compañero de trabajo sólo podrá ser otorgada a alguien que se sabe sobre una base cara a cara, o cuya voz es tan familiar que usted lo reconoce sin lugar a dudas.

En situaciones de alta seguridad, las únicas solicitudes que deben otorgarse son los
entregada en persona o con una forma de autenticación fuerte - por ejemplo, dos
elementos separados, como un secreto compartido y una muestra basada en el tiempo.
Procedimientos de clasificación de datos debe indicar que no se facilite información
de una parte de la organización implicadas en el trabajo sensible a cualquier persona que no
conocido personalmente o avalado de alguna manera.
NOTA
Increíblemente, incluso buscando el nombre y número de teléfono del llamante en la
base de datos de la empresa de los empleados y lo llamaba de nuevo no es una garantía absoluta
ingenieros sociales conocen los nombres de las formas de plantación en una base de datos
corporativa o
redirigir las llamadas telefónicas.
Entonces, ¿cómo manejar una petición legítima de sonido para obtener información de
otro empleado de la compañía, tales como la lista de nombres y direcciones de correo electrónico
de
personas en su grupo? De hecho, ¿cómo dar a conocer a fin de que un artículo como
esto, que es claramente menos valiosa que, por ejemplo, una hoja de especificaciones de un
producto
desarrollo, se reconoce como algo sólo para uso interno? Una parte importante de
la solución: Designar los empleados en cada departamento que se encargará de todos los
las solicitudes de información que se envía fuera del grupo. Un securitytraining avanzada
programa se debe proporcionar para que estos empleados designados
conocimiento de los procedimientos especiales de verificación que deben seguir.
Nadie olvida
Cualquiera puede recitar de un tirón la identidad de las organizaciones dentro de su empresa
que necesitan un alto grado de protección contra ataques maliciosos. Pero a menudo
pasar por alto otros lugares que son menos obvios, pero muy vulnerable. En uno de estos
historias, la solicitud de un fax que se enviará a un número de teléfono dentro de la empresa
parecía inocente y lo suficientemente seguro, sin embargo, el atacante se aprovechó de esta
seguridad laguna. La lección aquí: Todo el mundo de las secretarias y
auxiliares administrativos a los ejecutivos de la empresa y los administradores de alto nivel tiene
que
tener una formación especial de seguridad para que puedan estar atentos a este tipo de trucos.
Y no se olvide de guardia de la puerta principal: Recepcionistas, también, a menudo son primos
objetivos de los ingenieros sociales, y también deben ser conscientes de la engañosa
técnicas utilizadas por algunos visitantes y personas que llaman.
Seguridad de la empresa debe establecer un único punto de contacto como una especie de
central
cámara de compensación para los empleados que piensan que puede haber sido el blanco de
una social
ingeniería artimaña. Tener un lugar único para reportar incidentes de seguridad los
un eficaz sistema de alerta temprana que hará que sea querido en forma coordinada
ataque está en marcha, por lo que cualquier daño puede ser controlado de inmediato.

Capítulo 6
"Usted me puede ayudar?"
Ha visto cómo los ingenieros sociales engañar a la gente, ofreciendo a help.Another
enfoque preferido da la vuelta: El ingeniero social manipula haciéndose pasar por
que necesita de la otra persona para ayudarle. Todos podemos simpatizar con la gente de
situación difícil, y el enfoque resulta eficaz una y otra vez para permitir que un
ingeniería social para conseguir su objetivo.
El fuera de Towner
Una historia en el capítulo 3 muestra cómo un atacante puede hablar de una víctima para que
revele su
número de empleado. Éste utiliza un enfoque diferente para la consecución de los mismos

resultado de ello, y luego muestra cómo el atacante puede hacer uso de esa
Mantenerse al día con los vecinos
En Silicon Valley hay una cierta compañía global que no nombraré. La
oficinas de ventas dispersos y otras instalaciones de campo en todo el worldare todos
conectado a la sede de esa compañía a través de WAN, una red de área amplia. La
intruso, un hombre inteligente, luchadora llamado Brian Atterby, sabía que era casi siempre
más fácil entrar en una red en uno de los sitios remotos donde la seguridad es
prácticamente garantizado para ser más laxos que en la sede.
El intruso llamó por teléfono a la oficina de Chicago y pidió hablar con el Sr. Jones.
La recepcionista me preguntó si conocía a nombre del señor Jones, respondió:
"Yo tenía aquí, yo estoy buscando. ¿Cómo Jones tiene usted?" Ella dijo:
"Tres. ¿Qué departamento iba a estar?"
Él dijo, "Si me leen los nombres, tal vez lo reconocen." Y así lo hizo:
"Barry, José, y Gordon."
"Joe. Estoy bastante seguro de que era", dijo. "Y él estaba en lo que ..
departamento? "
"Development Business".
"Está bien. Que se puede conectar, por favor?"
Ella puso la llamada. Cuando Jones respondió, el atacante dijo: "Sr.
Jones? Hola, esto es Tony en la nómina. Acabamos de poner a través de su solicitud para que su
cheque depositado directamente a su cuenta de ahorro y crédito ".
"¿QUÉ ???!!! Tienes que estar bromeando. No me hizo ninguna petición de esa manera. I
ni siquiera tienen una cuenta en una cooperativa de crédito. "
"Oh, maldita sea, yo ya lo hice pasar."
Jones fue más que un poco molesto ante la idea de que su cheque de pago puede ser
va a cuenta de otra persona, y él estaba empezando a pensar que el tipo de la
otro extremo del teléfono debe ser un poco lento. Antes de que pudiera responder, la
atacante dijo: "Yo mejor lo que pasó. cambios de nómina se introducen por
número de empleado. ¿Cuál es su número de empleado? "
Jones dio el número. La persona que llamó dijo: "No, tienes razón, la solicitud no era de
usted, entonces. "Reciben más estúpido todos los años, Jones pensamiento.
"Mira, voy a ver que es atendido voy a poner en una corrección en este momento lo tanto, no se
preocupe.. -
obtendrá su próximo cheque de pago está bien ", dijo el hombre tranquilizador.
Un viaje de negocios
No mucho tiempo después, el administrador del sistema en la empresa Austin, Texas, las ventas
oficina recibió una llamada telefónica. "Se trata de Joseph Jones," anunció la persona que llama.
"Estoy en
Desarrollo de Negocio de la empresa. Voy a estar en que, para la semana, en el Driskill
Hotel. Me gustaría que me has configurado con una cuenta temporal para que pueda acceder a
mi
correo electrónico sin realizar una llamada de larga distancia. "
"A ver si ese nombre otra vez, y me dan su número de empleado," el sistema de administración
, dijo. El falso Jones dio el número y continuó, "¿Tiene usted alguna de alta velocidad
números de acceso telefónico.
"Un momento, amigo. Tengo que verificar en la base de datos." Después de un rato, dijo: "Bueno,
Joe. Dime, ¿cuál es tu número de la casa? "El atacante había hecho su
tarea y tenía la respuesta preparada
Mitnick MENSAJE
No se fíe de las garantías de la red y firewalls para proteger su información. Ver
a su punto más vulnerable. Por lo general, encontrará que la vulnerabilidad se encuentra en su
personas.
"Está bien", el administrador del sistema le dijo: "me has convencido."
Era tan simple como eso. El administrador del sistema ha verificado el nombre de Joseph Jones,
de la

departamento, y el número de empleados, y "Joe" le había dado la respuesta correcta a la pregunta de la prueba. "Su nombre de usuario va a ser la misma que la una empresa, jbjones ", dijo el administrador del sistema", y yo voy a dar una contraseña inicial de "Cámbiame".

Con el análisis de la

Con un par de llamadas telefónicas y quince minutos de tiempo, el atacante había ganado el acceso a la red de la compañía de área amplia. Esta era una empresa que, como muchos, tenía lo que se refieren a la seguridad de caramelo, después de una primera descripción utilizada por dos Bell

Laboratorios de los investigadores, Steve Bellovin y Cheswick Steven. Se describe como la seguridad como "una cáscara crujiente duro con un centro masticable a menudo" - como un caramelo de M & M.

La capa exterior, el firewall, Bellovin y Cheswick argumentó, no es suficiente protección, porque una vez que un intruso es capaz de eludir la interna los sistemas informáticos tienen la seguridad suave y masticable. La mayoría de las veces, son no estén protegidos adecuadamente.

Esta historia se ajusta a la definición. Con un número telefónico y una cuenta, el atacante ni siquiera tienen que molestarse en intentar derrotar a un firewall de Internet, y, una vez dentro, que era fácilmente capaz de comprometer la mayor parte de los sistemas de la red interna.

A través de mis fuentes, entiendo que esta artimaña exacta en que se trabajó en uno de los mayores fabricantes de programas informáticos en el mundo. Se podría pensar que el los administradores de sistemas en una empresa serían entrenados para detectar este tipo de artimaña. Pero en mi experiencia, nadie está completamente seguro si es un ingeniero social inteligente y lo suficientemente persuasivo.

LINGO

SEGURIDAD CANDY Un término acuñado por Bellovin y Cheswick de Bell Labs para describir un escenario de seguridad en el perímetro exterior, tales como firewall, es fuerte, pero la infraestructura que hay detrás es débil. El término se refiere a los dulces M & M, que tiene una cáscara exterior dura y centro blando.

LINGO

Seguridad La seguridad SPEAKEASY que se basa en saber donde se desee información, y el uso de una palabra o un nombre para tener acceso a esa información o sistema informático.

SPEAKEASY SEGURIDAD

En los viejos tiempos de clandestinos - los clubes era de la prohibición-en los llamados gin bañera fluido - un posible cliente fue admitido por presentarse en el puerta y llamar. Después de unos momentos, un pequeño colgajo en la puerta le swing abierta y una cara dura e intimidante que se asoman. Si el visitante se encontraba en el sabe, iba a hablar el nombre de algún patrón frecuente del lugar ("Joe enviado me ", fue lo suficiente), con lo cual el portero se destrabe el interior de la puerta y lo dejaron entrar

El verdadero truco estaba en saber la ubicación de la taberna porque la puerta estaba sin marcar, y los propietarios no exactamente el rato luces de neón para marcar su presencia. En su mayor parte, sólo a aparecer en el lugar correcto era todo lo que llevó a entrar el mismo grado de custodia, por desgracia, una práctica generalizada en el mundo empresarial, proporcionando un nivel de protección no que yo llamo clandestino la seguridad.

Lo vi en el cine

He aquí una ilustración de una película favorita que mucha gente va a recordar. En Los tres días del Cóndor, el personaje principal, Turner (interpretado por Robert Redford), trabaja para una pequeña firma de investigación contratado por la CIA. Un día regresa de un almuerzo de ejecutar para encontrar que todos sus compañeros de trabajo han sido asesinados

hacia abajo. Que ha dejado de averiguar quién ha hecho esto y por qué, sabiendo todo el tiempo que los chicos malos, sean quienes sean, lo están buscando.

A finales de la historia, Turner se las arregla para obtener el número de teléfono de uno de los chicos malos.
Pero, ¿quién es esta persona, y cómo puede Turner precisar su ubicación? Está de suerte:
El guionista, David Rayfiel, ha dado felizmente Turner un fondo que
incluye la formación como un instalador de líneas de teléfono con el Cuerpo de Señales del Ejército, por lo que
lo bien informado acerca de las técnicas y prácticas de la compañía telefónica. Con
número del chico malo de teléfono en la mano, Turner sabe exactamente qué hacer. En el guión, la escena se lee así:
TURNER vuelve a conectar y MACHOS DESDE OTRO NUMERO.
RING! RING! Entonces:
VOZ DE MUJER (FILTRO) CNA, la señora Coleman habla.
TURNER (en conjunto de pruebas)
Se trata de Harold Thomas, la señora Coleman. Servicio al Cliente.
CNA en el 202-555-7389, por favor.
VOZ DE MUJER (FILTRO) Un momento, por favor. (Casi a la vez)
Leonard Atwood, 765 Mackensie Lane, Chevy Chase, Maryland.
Ignorando el hecho de que el guionista error utiliza un área de Washington, DC,
código para una dirección de Maryland, puede detectar lo que ha pasado aquí?
Turner, debido a su formación como instalador de líneas de teléfono, sabía a qué número llamar con el fin de llegar a una oficina de la compañía de teléfono llamado CNA, el nombre del cliente y Dirección de la oficina. CNA está configurado para la comodidad de los instaladores y otros personal autorizado de la compañía telefónica. Un instalador puede llamar a la CNA, y dar ellos un número de teléfono. El secretario CNA wouldrespond proporcionando el nombre de la persona que el teléfono pertenece a la dirección andhis.
Engañando a la compañía telefónica
En el mundo real, el número de teléfono de la CNA es un secreto muy bien guardado.
Aunque las compañías telefónicas, finalmente tuvo éxito y en estos días son menos generoso en la entrega de información tan fácilmente, a la vez que opera
en una variación de la seguridad clandestino que los profesionales de seguridad llamado seguridad
través de la oscuridad. Se presume que todo aquel que llama la CNA y sabía que el jerga adecuada ("El servicio al cliente. CNA en el 555-1234, por favor, por ejemplo) era un persona autorizada para disponer de la información.
LINGO
La seguridad por oscuridad un método ineficaz de equipo
de seguridad que se basa en mantener en secreto los detalles de cómo funciona el sistema (Protocolos, algoritmos y los sistemas internos). La seguridad por oscuridad se basa en la falsa suposición de que nadie fuera de un grupo de confianza de la gente será capaz de burlar el sistema.
Mitnick MESSGAE
La seguridad por oscuridad no tiene ningún efecto en el bloqueo social
ingeniería de los ataques. Todos los sistemas de computadora en el mundo tiene al menos un humano
que lo utilizan. Por lo tanto, si el atacante es capaz de manipular a las personas que utilizan los sistemas,
la oscuridad del sistema es irrelevante.
No había necesidad de verificar o identificar a sí mismo, sin necesidad de dar a un empleado número, sin necesidad de una contraseña que se cambian a diario. Si supieras la cantidad para llamar y que sonaba auténtica, debe tener derecho a la información.
Que no era una hipótesis muy sólida por parte de la compañía telefónica. Sus
único esfuerzo de la seguridad iba a cambiar el número de teléfono en forma periódica l, en por lo menos una vez al año. Aún así, el número actual en un momento determinado fue muy ampliamente conocido entre los phreakers, que se deleitaban en el aprovechamiento de este fuente útil de información y de compartir el cómo-a-hacer-con sus

phreaks compañeros. El CN, fue engañar a la Oficina una de las primeras cosas que aprendí cuando me
fue para la afición de phone phreaking cuando era adolescente.
En todo el mundo de los negocios y el gobierno, la seguridad clandestino. sigue siendo frecuente. Es probable que alrededor de los departamentos de su empresa, la gente, y la jerga. A veces les a que: a veces un número de teléfono interno es todo lo que necesita.

EL GERENTE DE ORDENADOR CARELESS

A pesar de que muchos empleados en las organizaciones son negligentes, indiferentes, o no sabe de peligros de seguridad, lo que espera a alguien con el administrador de título en el equipo centro de una corporación Fortune 500 para estar completamente informado acerca de las mejores
prácticas de seguridad, ¿verdad?
Uno no esperaría que un gerente de centro de cómputo - alguien que es parte de su empresa del departamento de tecnología de la información - que son víctimas de una visión simplista y
obvio ingeniería social estafa. Sobre todo, no el ingeniero social no es
más de un niño, acababa de salir de su adolescencia. Pero a veces las expectativas pueden ser mal.

En sintonía

Hace años era un pasatiempo divertido para muchas personas para mantener una radio sintonizada a la
policía local o las frecuencias del cuerpo de bomberos, escuchando la muy ocasional conversaciones acusado de un robo a un banco en curso, un edificio de oficinas incendio o una persecución a alta velocidad como el evento se desarrolló. Las frecuencias de radio utilizadas por
los organismos policiales y de bomberos solía estar disponible en los libros de
la librería de la esquina, hoy en día están previstas en los listados en la web, y de una libro se puede comprar en las frecuencias de Radio Shack por local, regional, estatal, y, en algunos casos, incluso las agencias federales.
Por supuesto, no fue sólo a los curiosos que estaban escuchando in ladrones robar en una tienda en el medio de la noche puede sintonizar para saber si un coche de policía estaba siendo enviado a la ubicación. Traficantes de drogas podrían mantener un control sobre las actividades de la
local de drogas los agentes de la Agencia. Un pirómano podría mejorar su enfermedad
el placer de encender un fuego y luego de escuchar todo el tráfico de radio, mientras que los bomberos luchaban por apagar.
En los últimos años la evolución de la tecnología informática han hecho posible encriptar mensajes de voz. Como ingenieros encontraron la manera de meter más y más poder de cómputo en un solo microchip, comenzaron a construir pequeñas cifrada, radios de la policía que mantuvo a los malos y los curiosos de la escucha
in

Danny el espía

Un entusiasta del escáner y hacker experto que llamaremos Danny decidió ver si él
No podía encontrar una manera de tener en sus manos el software de cifrado super-secreto - la código fuente - de uno de los principales fabricantes de sistemas de radio seguro. Fue con la esperanza de un estudio del código le permitiría aprender a escuchar en la ley ejecución, y posiblemente también el uso de la tecnología de manera que incluso los más poderosos
agencias gubernamentales tendrían dificultades para controlar sus conversaciones con su los amigos.
El Dannys del oscuro mundo de los piratas pertenecen a una categoría especial
que se ubica entre los más que curiosos, pero totalmente benigna y el
peligroso. Dannys tener el conocimiento de los expertos, junto con la
hacker malicioso es el deseo de entrar en sistemas y redes de la
desafío intelectual y en el placer de ganar conocimiento como la tecnología

funciona. Sin embargo, su ruptura y entrar electrónicos acrobacias son sólo eso - acrobacias. Estas personas, estos hackers benignos, entran ilegalmente en los sitios para la diversión pura y emoción de la prueba de que pueden hacerlo. Ellos no roban nada, no hacen dinero de sus hazañas, no destruyen los archivos, alterar cualquier red conexiones, o accidente de cualquier sistema informático. El mero hecho de estar allí, atrapar copias de los archivos y la búsqueda de mensajes de correo electrónico para las contraseñas detrás de las espaldas de los ridad y los administradores de red, ajustes de las narices de los responsables de mantener alejados a los intrusos como ellos. La rivalidad es una gran parte de la satisfacción.

De acuerdo con este perfil, nuestra Danny quería examinar los detalles de su objetivo producto más celosamente guardado compañía sólo para satisfacer su ardiente curiosidad propia y admirar lo innovaciones inteligentes del fabricante podría haber llegado hasta con.

Los diseños de los productos eran, huelga decirlo, cuidadosamente guardado los secretos comerciales, como preciosa y protegida como cualquier cosa en posesión de la empresa. Danny lo sabía. Y que no le importaba un poco. Después de todo, era sólo un grande, sin nombre de la empresa.

Pero, ¿cómo obtener el código fuente del software? Al final resultó que, tomando la corona joyas del Grupo de Seguridad de la empresa de comunicaciones resultó ser muy fácil, a pesar de que la empresa fue una de las que utiliza autenticación de dos factores, un acuerdo en virtud del cual las personas están obligados a utilizar no uno, sino dos separadas identificadores para probar su identidad.

He aquí un ejemplo que probablemente ya está familiarizado. Cuando su renovación tarjeta de crédito llega, se le pedirá al teléfono de la empresa emisora para que sepan que la tarjeta está en posesión del cliente previsto, y que no a alguien robó el sobre del correo electrónico. Las instrucciones con la tarjeta en estos días por lo general le dicen que llame desde su casa. Cuando llame, el software de la tarjeta de crédito empresa analiza la ANI, la identificación automática de número, que es proporcionada por la central telefónica de llamadas gratuitas que la compañía de tarjetas de crédito está pagando.

Un equipo de la compañía de tarjeta de crédito utiliza el número de la persona que llama siempre por la ANI, y el número de partidos que contra la base de datos de la compañía de los titulares de tarjetas. Por el momento el secretario viene en la línea, ella o su pantalla muestra información de la base de datos con detalles sobre el cliente. Así que el secretario ya sabe la llamada proviene de la casa de un cliente, que es una forma de autenticación.

LINGO

Autenticación de dos factores el uso de dos tipos diferentes de autenticación para verificar la identidad. Por ejemplo, una persona podría tener para identificar a sí mismo llamando desde un lugar determinado y saber identificar una contraseña.

El empleado elige un elemento de la información que aparece acerca de usted - la mayoría de los muchas veces número de seguro social, fecha de nacimiento, o el nombre de soltera de la madre - y le pide por esta parte de la información. Si usted le da la respuesta correcta, que es un segundo forma de autenticación - basado en la información que usted debe saber.

En la empresa de fabricación de los sistemas de radio seguros de nuestra historia, cada los empleados con acceso a computadoras tenían su nombre de cuenta y su contraseña habituales, pero además se le facilitó un pequeño dispositivo electrónico llamado Secure ID. Es lo que se denomina una muestra basada en el tiempo. Estos dispositivos vienen en dos tipos: Uno es sobre la mitad del tamaño de una tarjeta de crédito, pero un poco más gruesa, y otra es lo

suficientemente pequeño que
la gente simplemente se adhieren a sus llaveros.
Derivado del mundo de la criptografía, este gadget en concreto tiene una pequeña
ventana que muestra una serie de seis dígitos. Cada sesenta segundos, la pantalla
cambia para mostrar un diferente número de seis dígitos. Cuando una persona autorizada
necesita
para acceder a la red desde fuera del sitio, primero debe identificarse a sí misma como una
autorización
usuario, simplemente introduciendo su PIN secreto y los dígitos que aparece en su dispositivo
token.
Una vez verificado por el sistema interno, que se autentica con su cuenta
nombre y una contraseña.
Para el joven hacker Danny para obtener el código fuente que tan codiciado, que se
que no sólo comprometen el nombre de algún empleado de la cuenta y la contraseña (no
un gran reto para el ingeniero con experiencia social), sino también conseguir alrededor de la
basada en el tiempo simbólico.
La derrota de la autenticación de dos factores de una muestra basada en el tiempo combinado
con un
código PIN secreto de usuario suena como un desafío a la derecha de Misión Imposible.
Pero para los ingenieros sociales, el desafío es similar al que lució por un jugador de poker
que tiene más de la habilidad de costumbre en la lectura a sus oponentes. Con un poco de suerte,
cuando se sienta en una mesa que él sabe que es probable que a pie con una gran pila
de dinero de otras personas.
El asalto a la fortaleza
Danny comenzó a hacer su tarea. En poco tiempo se las había arreglado para poner
juntas las piezas suficientes para hacerse pasar por un empleado real. Que había de un empleado
nombre, departamento, número de teléfono y número de empleado, así como la
nombre del director y número de teléfono.
Ahora era la calma antes de la tormenta. Literalmente. Pasando por el plan que había elaborado
a cabo, Danny necesita una cosa más antes de que pudiera dar el siguiente paso, y así fue
algo que él no tenía control sobre: necesitaba una tormenta de nieve. Danny necesitaba un
poca ayuda de la madre naturaleza en forma de tiempo tan malo que mantendrá
los trabajadores de entrar en la oficina. En el invierno de Dakota del Sur, donde el
planta de fabricación en cuestión se encuentra, cualquiera que espere para el mal tiempo hizo
No queda mucho tiempo para esperar. El viernes por la noche, una tormenta llegó. Lo que
empezó como
la nieve se convirtió rápidamente en lluvia helada, para que, por la mañana, las calles estaban
cubiertas
con una sábana resbaladiza y peligrosa de hielo. Para Danny, esta era una oportunidad perfecta.
Telefoneó a la planta, pidió-la sala de ordenadores y alcanzó uno de los
las obreras de las TI, un operador que se anunció como Roger
Kowalski.
Dando el nombre del empleado real que había obtenido, Danny dijo: "Este es Bob
Billings. Yo trabajo en el seguro del Grupo de Comunicaciones. Estoy en casa ahora mismo y
No puedo conducir en debido a la tormenta. Y el problema es que necesito para acceder a mi
estación de trabajo y el servidor de casa, y salí de mi ID seguro en mi escritorio. Puede
que ir a buscarla para mí? ¿O puede alguien? Y luego leer el código cuando
necesitan para entrar? Debido a que mi equipo tiene un plazo crítico y no hay manera de que
pueda
hacer mi trabajo. Y no hay manera de que pueda llegar a la oficina - las carreteras son mucho
más
muy peligroso a mi manera.
El operador del equipo dijo: "No puedo dejar el Centro de Cómputo". Danny saltó
derecho: "¿Tiene usted una identificación segura a ti mismo?".
"No hay nadie aquí en el Centro de Cómputo", dijo. "Mantenemos una para el

los operadores en caso de una emergencia. "
"Escucha", dijo Danny. "¿Puedes hacerme un gran favor? Cuando debo marcar
en la red, puedes dejar que me preste su ID seguro? Sólo hasta que sea seguro para
disco in "
"¿Quién eres tú otra vez?" Kowalski preguntó.
"¿Quién dice que usted trabaja.
"Por Ed Trenton".
"Oh, sí, lo conozco."
Cuando es obligado a enfrentarse a difíciles trineo, un ingeniero de bien social se
más de la cantidad usual de la investigación. "Estoy en el segundo piso", fue Danny
sobre. "Junto a Roy Tucker."
Sabía que el nombre, también. Danny volvió a trabajar en él. "Sería mucho más
más fácil sólo para ir a buscar a mi escritorio y mi ID seguro para mí. "
Danny estaba convencido de que el chico no iba a comprar a este. En primer lugar, habría
No quiero dejar en el centro de su turno para ir penosamente por los pasillos y hasta
escaleras a alguna parte lejana del edificio. No sería también quiero tener que
pata a través de otro servicio, violando el espacio personal de alguien. No,
era una apuesta segura que no quiero hacer eso.
Kowalski no quiere decir que no a un tipo que necesitaba ayuda, pero no
quiere decir que sí y se meten en problemas, ya sea. Así que dejó de lado la decisión: voy a tener
pedir a mi jefe. Salir adelante. "Él colgó el teléfono, y Danny le oía
recoger a otro teléfono, poner en la convocatoria, y explicar la solicitud. Kowalski entonces
algo inexplicable: En realidad avalada por el hombre con el nombre de Bob
Billings. "Yo le conozco", le dijo a su manager. "Él trabaja para Ed Trenton. Podemos
Que use el ID seguro de Danny el Centro de Cómputo ", aferrándose a la
teléfono, se sorprendió al escuchar este apoyo extraordinario e inesperado por su
causa. No podía creer lo que escuchaba o su suerte.
Después de un par de momentos, Kowalski volvió a la línea y le dijo: "Mi
gerente quiere hablar con usted a sí mismo ", y le dio el nombre del hombre y de células
número de teléfono.
Danny se llama el director y se fue a través de toda la historia una vez más,
añadiendo detalles sobre el proyecto que estaba trabajando o, y por qué su equipo de producción
necesarios para cumplir con una fecha límite crítico. "Sería más fácil si alguien va solo y
obtiene la tarjeta ", dijo." No creo que el escritorio está bloqueado, debería estar allí en
mi cajón superior izquierdo. "
"Bueno", dijo el gerente, "sólo por el fin de semana, creo que podemos dejar que se utiliza el
uno en el Centro de Cómputo. Le diré a los chicos de turno que cuando usted llama, que
debe leer el código de acceso aleatorio para usted ", y le dio el PIN
número para utilizarlo con él.
Para el fin de semana, cada vez Danny quería entrar en la empresa
sistema informático, sólo tenía que llamar al Centro de Informática y pedirles que lean
de los seis dígitos que aparece en la ficha Identificación de seguridad.
Un trabajo interno
Una vez que él estaba dentro del sistema informático de la empresa, entonces ¿qué? ¿Cómo
Danny encontrar su camino en el servidor con el software que quería? Ya había
preparado para esto.
Muchos usuarios están familiarizados con los grupos de noticias, que la amplia serie de
boletines electrónicos donde la gente puede hacer preguntas que otras personas
respuesta, o buscar compañeros virtuales que comparten un interés en la música, las
computadoras, o
cualquiera de los cientos de otros temas.
Lo que pocas personas se dan cuenta cuando publicar cualquier mensaje en un sitio de noticias
es que
su mensaje permanece en línea y disponible desde hace años. Google, por ejemplo, ahora
mantiene un archivo de 700 millones de mensajes, algunos que datan de nuevo

veinte años! Danny comenzó por ir a la dirección Web
http://groups.google.com.
Como los términos de búsqueda, Danny entró en "las comunicaciones de radio de cifrado" y la nombre de la empresa, y encontró un mensaje de años sobre el tema de una
de los empleados. Se trataba de una publicación que se habían hecho de nuevo cuando la compañía fue la primera
desarrollo del producto, probablemente, mucho antes de que los departamentos de policía y federales
organismos habían considerado codificación de señales de radio.
El mensaje contenía la firma del remitente, lo que no sólo el nombre del hombre,
Scott prensa, pero su número de teléfono e incluso el nombre de su grupo de trabajo, la Seguros del Grupo de Comunicaciones.
Danny tomó el teléfono y marcó el número. Parecía una posibilidad remota -
¿Seguiría siendo de trabajo en los años de la organización misma tarde? ¿Estaría en
trabajar en un fin de semana de tormenta? El teléfono sonó una, dos, tres veces, y
Entonces vino una voz en la línea. "Se trata de Scott", dijo.
Que dice ser de IT de la compañía del Departamento de Prensa Danny manipulado (en
una de las formas ya familiares a usted de los capítulos anteriores) para que revelen la nombres de los servidores que utilizan para el trabajo de desarrollo. Estos eran los servidores que podría esperarse para mantener el código fuente que contiene la encriptación propietario algoritmo y el firmware utilizado en productos de la compañía de radio seguro.
Danny fue acercando más y más, y su entusiasmo edificio. Fue
anticipándose a las prisas, el gran sumo que siempre se sintió cuando sucedió a
algo que sabía que sólo un número muy limitado de personas podía lograr.
Sin embargo, no estaba en casa sin embargo. Para el resto del fin de semana que sería capaz de entrar en
red de la compañía cada vez que quería, gracias a la cooperación
equipo responsable del centro. Y él sabía que los servidores que querían acceder. Pero
cuando marcó en el servidor de terminal que inició sesión en que no le permitía
conectarse a sistemas de comunicación seguros para el Desarrollo. Tiene que
haber sido un servidor de seguridad interno o router proteger los sistemas informáticos de que grupo. Tendría que encontrar otra forma de in
El siguiente paso tuvo nervios: Danny volvió a llamar a Kowalski en Informática
Operaciones y se quejó de "Mi servidor no me deja conectar", y dijo a la IT
tipo: "Yo necesito que me creó con una cuenta en uno de los equipos de la
departamento, así que puede usar Telnet para conectar con el sistema ".
El gerente ya había aprobado la divulgación del código de acceso que aparece en la basada en el tiempo token, por lo que esta nueva solicitud no parece razonable. Kowalski establecido
una cuenta temporal y contraseña en una de las computadoras del Centro de Operación,
y le dijo a Danny que "me vuelva a llamar cuando usted no lo necesita más y yo le quite se. "
Una vez registrado en la cuenta temporal, Danny fue capaz de conectarse a través de la red de los sistemas informáticos del Grupo de Comunicaciones de seguro. Después de una hora de la búsqueda en línea para una vulnerabilidad de técnicas que le permitan el acceso a una servidor principal de desarrollo, se sacó la lotería. Al parecer, el sistema o red
administrador no estaba alerta para mantenerse al día con las últimas noticias sobre fallos de seguridad
en el sistema operativo que permite el acceso remoto. Pero Danny.
En poco tiempo se había localizado los archivos de código fuente que estaba después y fue transferir de forma remota a un sitio de comercio electrónico que ofrece espacio de almacenamiento gratuito.
En este sitio, incluso si los archivos fueron descubiertos nunca, nunca se remontan
de espaldas a él.
Había un último paso antes de firmar: el metódico proceso de borrado de su

pistas. Terminó antes de que el programa de Jay Leno se había ido fuera del aire por la noche. Danny cuenta de esto había sido un fin de semana de trabajo muy bien. Y él nunca había tuvo que ponerse personalmente en peligro. Fue una emoción embriagadora, incluso mejor que el snowboard o el paracaidismo.

Danny se emborrachó esa noche, no en whisky, ginebra, cerveza, o bien, sino en su sentido de la el poder y los logros que se vierte a través de los archivos que había robado, el cierre de en el software difícil de alcanzar, radio en extremo secreto.

Con el análisis de la

Como en la historia anterior, este truco sólo funcionó porque los empleados de una empresa era demasiado dispuestos a aceptar sin más que una llamada fue realmente el empleado que decía ser. Ese afán de ayudar a un compañero de trabajo con un problema es, en el por un lado, parte de lo que engrasa las ruedas de la industria, y parte de lo que hace que el los empleados de algunas empresas más agradable que trabajar con los empleados de otros. Pero por otro lado, esta utilidad puede ser una vulnerabilidad importante que un ingeniero social que intentar aprovechar.

Un poco de manipulación Danny utilizado fue deliciosa: Cuando se hizo la solicitud que alguien obtener su ID seguro de su escritorio, él siempre decía que quería alguien a "buscar" para él. Fetch es un comando que usted dé a su perro. Nadie quiere que le digan a buscar algo. Con esa sola palabra, Danny hizo que todo el más segura la solicitud sería denegada y aceptado alguna otra solución en cambio, que era exactamente lo que quería.

El operador del Centro de Cómputo, "Kowalski, fue recogida por Danny dejar caer el nombres de las personas Kowalski pasó a conocer. Pero ¿por qué Kowalski director - gerente de TI, no menos - permitir algún tipo de acceso ajeno a la compañía red interna? Simplemente porque la petición de ayuda puede ser una poderosa persuasión, herramienta en el arsenal de la ingeniería social.

Mitnick MENSAJE

Esta historia viene a demostrar que las formas basadas en el tiempo y fichas similares de autenticación no son una defensa contra la ingeniería social astuto. El único la defensa es un empleado de conciencia que sigue las políticas de seguridad y entiende cómo otros maliciosamente puede influir en su comportamiento.

¿Podría algo así alguna vez sucede en su empresa? Tiene ya?

PREVENCIÓN DE LA CON

Parece ser un elemento a menudo repetido en estas historias que un atacante dispone para llamar a una red de ordenadores fuera de la empresa, sin que la persona que le ayuda a tomar las medidas suficientes para verificar que la persona que llama es realmente una

los empleados y el derecho al acceso. ¿Por qué vuelvo a este tema tan a menudo?

Porque realmente es un factor en los ataques de ingeniería social para muchos. Para el desarrollo social

ingeniero, es la forma más fácil de alcanzar su meta. ¿Por qué debería pasar a un atacante horas tratando de entrar, cuando puede hacerlo en su lugar con una simple llamada telefónica?

Uno de los métodos más poderosos para la ingeniería social para llevar a cabo este tipo de ataque es la táctica simple de pretender necesita ayuda - un enfoque con frecuencia utilizado por los atacantes. Usted no quiere dejar a sus empleados de ser útil a los compañeros de trabajo o clientes, por lo que necesita para el brazo con la verificación específica procedimientos para el uso con cualquier persona hacer una solicitud de acceso a una computadora o

información confidencial. De esa manera puede ser útil para aquellos que merecen ser ayudó, pero al mismo tiempo, proteger los activos de la organización de la información y los sistemas informáticos.

Procedimientos de la compañía de seguridad tienen que explicar en detalle qué tipo de verificación

mecanismos deben ser utilizados en diversas circunstancias. El capítulo 17 ofrece una lista detallada de los procedimientos, pero aquí hay algunas pautas a tener en cuenta:

Una buena manera de verificar la identidad de una persona que haga una solicitud para llamar a la
número de teléfono que figuran en el directorio de la empresa para esa persona. Si la persona que hace la solicitud es en realidad un atacante, la llamada de verificación sea lo que hablar con la persona real en el teléfono mientras el impostor está en espera, o le llegar a correo de voz del empleado para que pueda escuchar el sonido de su voz, y lo comparan con thespeech del atacante.
Si el número de empleados se utilizan en su empresa para verificar la identidad, entonces los números tienen que ser tratados como información confidencial, cuidadosamente guardado y no entregado a los extraños. Lo mismo ocurre con todos los otros tipos de identificadores internos, como los números de teléfono interno, los identificadores de los departamentos de facturación, e incluso
direcciones de correo electrónico.
Formación empresarial debe llamar la atención de todos a la práctica común de aceptar a las personas desconocidas que los empleados legítimos de la base de que sonido de autoridad o conocimiento. El hecho de que alguien sabe de una empresa prácticas o usos internos terminología no es razón para suponer que su identidad no tiene que ser verificada por otros medios.
Los oficiales de seguridad y administradores de sistemas no debe reducir su enfoque a fin de que sólo están atentos a la forma consciente de la seguridad a todos los demás es ser. También necesidad de asegurarse de que se están siguiendo las mismas reglas, procedimientos y prácticas.
Contraseñas, etc, por supuesto, nunca será compartida, pero la restricción en contra de compartir es aún más importante con el tiempo basado en tokens de seguridad y otros
formas de autenticación. Debe ser una cuestión de sentido común que el intercambio de cualquier de estos artículos violan el punto central de la empresa de haber instalado el sistemas. Compartir significa que no puede haber rendición de cuentas. Si un incidente de seguridad
se lleva a cabo o algo va mal, usted no será capaz de determinar quién es el parte responsable.
Como repito a lo largo de este libro, los empleados deben estar familiarizados con el social estrategias de ingeniería y métodos para analizar cuidadosamente las solicitudes que reciben. Considere el uso de juegos de rol como una parte estándar de formación en seguridad, por lo que los empleados pueden llegar a una mejor comprensión de cómo el ingeniero de obras sociales.

Capítulo 7
Sitios falsos y archivos adjuntos potencialmente peligrosos
Hay un viejo refrán que nunca obtener algo por nada,
Sin embargo, la táctica de ofrecer algo gratis sigue siendo un gran atractivo tanto para los legítima ("Pero espera - hay más llamadas en este momento y vamos a lanzar en un conjunto de! cuchillos y un popper de las palomitas! ") y no tan legítimos (" Comprar un acre de pantanos de la Florida y obtener un acre segundo libre! ") las empresas.
Y la mayoría de nosotros estamos tan ansiosos de conseguir algo gratis que nos pueden distraer de la
pensar con claridad acerca de la oferta o la promesa que se hizo.
Sabemos que la advertencia familiar, "el comprador tenga cuidado", pero es hora de prestar atención a otro
Advertencia: Tenga cuidado de venir-en los archivos adjuntos de correo electrónico y el software libre. El experto
atacante usará casi cualquier medio para entrar en la red corporativa, incluyendo apelando a nuestro deseo natural de conseguir un regalo gratis. Aquí están algunos ejemplos.
¿No le gustaría un país libre (en blanco)? "
Al igual que los virus han sido una maldición para los profesionales de la humanidad y de atención médica ya que el

principio de los tiempos, por lo que el virus de la computadora bien llamada representa una maldición similar
a los usuarios de la tecnología. Los virus informáticos que obtienen la mayoría de la atención y terminar en el centro de atención, no por casualidad, hacer el mayor daño. Estos son los producto de vándalos informáticos.
Nerds ordenador encendido malicioso, vandalismo equipo se esfuerzan por demostrar lo inteligentes que son. A veces, sus actos son como un rito de iniciación, destinado a impresionar a los hackers más viejos y experimentados. Estas personas están motivadas para crear un gusano o un virus tuvo intención de infligir daño. Si su trabajo destruye los archivos, destroza todo el disco duro, y correos electrónicos en sí a miles de personas inocentes, vándalos hojaldre con orgullo en sus logros. Si el virus causa el caos suficiente
que los periódicos escriben sobre ella y la difusión de noticias de la red en guardia contra él, tanto mejor.
Mucho se ha escrito acerca de los vándalos y sus virus, libros, software
programas, y las empresas de todo ha sido creado para ofrecer protección, y
No trataremos aquí con las defensas contra los ataques técnica. Nuestro interés en
el momento es menor en los actos destructivos de los actos vandálicos que en el más específico los esfuerzos de su primo lejano, el ingeniero social.
Llegó en el correo electrónico
Es probable que reciba correos electrónicos no solicitados todos los días que llevan publicidad mensajes y ofrecer un libre algo-o-otros que ni necesitan ni quieren. Usted
sabe el tipo. Prometen asesoramiento de inversión, descuentos en los equipos, televisores, cámaras, vitaminas, o de viajes, ofertas de tarjetas de crédito no es necesario, un dispositivo que le permitirá recibir canales de televisión de pago libre, las formas de mejorar su salud o su vida sexual, y así sucesivamente.
Pero de vez en cuando una oferta aparece en su buzón de correo electrónico para
algo que llame la atención. Tal vez es un juego gratuito, una oferta de fotos de
tu estrella favorita, un programa de calendario libre, o compartir barato "software que se proteger su equipo contra los virus. Cualquiera que sea la oferta, el correo electrónico que usted dirige
para descargar el archivo con las golosinas que el mensaje ha convencido de que usted intente.
O tal vez usted recibirá un mensaje con una línea de asunto que dice don, te echo de menos ", o "Ana, ¿por qué no me has escrito", o "Hola, Tim, aquí está la foto sexy me
prometiste. "Esto no puede ser el correo basura de publicidad, que piensa, porque tiene su propio nombre en él y suena tan personal. Por lo que abrir el archivo adjunto para ver la foto o leer el mensaje.
Todas estas acciones - la descarga de software que ha aprendido acerca de un
correo electrónico de publicidad, al hacer clic en un enlace que te lleva a un sitio que no han oído hablar de
antes, abrir un archivo adjunto de alguien que no sabe muy bien - se
invitaciones a los problemas. Claro, la mayoría de las veces lo que se obtiene es exactamente lo que
espera, o en el peor, algo decepcionante u ofensivo, pero inofensivos. Pero
a veces lo que se obtiene es la obra de un vándalo.
El envío de código malicioso en su equipo es sólo una pequeña parte del ataque. La atacante necesita para persuadir a descargar el archivo adjunto para que el ataque éxito.
NOTA
Un tipo de programa conocido en el underground informático como una rata, o del control remoto Troya de acceso, le da al atacante acceso completo a su ordenador, como si fuera
sentado en su teclado.
Las formas más dañinas de código malicioso - gusanos con nombres como El amor Carta, SirCam, y Kournikiva Anna, por nombrar algunos - han confiado en social
técnicas de ingeniería del engaño y el aprovechamiento de nuestro deseo de obtener
algo de la nada para ser extendido. El gusano llega como archivo adjunto

a un correo electrónico que ofrece algo tentador, como información confidencial, gratuito
la pornografía, o - un truco muy ingenioso - un mensaje que dice que el archivo adjunto es el
recibo de algún artículo caro que supuestamente ordenó. Esta estratagema última vez que lleva
abrir el archivo adjunto por temor a su tarjeta de crédito ha sido acusado de un elemento que
no el fin.
Es asombroso cómo muchas personas caen en estos trucos, incluso después de ser dicho y
dijo de nuevo sobre los peligros de la apertura de adjuntos de correo electrónico, la conciencia de la
se desvanece el peligro en el tiempo, dejando a cada uno de nosotros vulnerables.
Detectar software malintencionado
Otro tipo de malware - abreviatura de software malicioso - pone un programa en
su computadora que funciona sin su conocimiento o consentimiento, o realiza una
tarea sin su conocimiento. Malware puede parecer bastante inocente, puede ser incluso un
Documento de Word o una presentación de PowerPoint, o cualquier programa que tenga macro
la funcionalidad, pero en secreto se instala un programa no autorizado. Por ejemplo,
malware puede ser una versión del caballo de Troya se habla en el capítulo 6. Una vez
este software está instalado en su máquina, puede alimentar a cada golpe de teclado que escriba
al atacante, incluyendo todas sus contraseñas y números de tarjetas de crédito.
Hay otros dos tipos de software malicioso que puede encontrar chocante.
Se puede alimentar al atacante cada palabra que dices dentro del alcance del equipo
micrófono, incluso cuando usted piensa que el micrófono está apagado. Peor aún, si
tiene una cámara web conectada a su computadora, un atacante con una variación de este
técnica puede ser capaz de capturar todo lo que ocurre delante de su
terminal, incluso cuando usted piensa que la cámara está apagada, día o noche.
LINGO
MALWARE argot de software malicioso, un programa de ordenador, como por ejemplo un virus,
Caballo gusano o caballo de Troya, que realiza tareas perjudiciales.
Mitnick MENSAJE
Cuidado con los frikis con los regalos, de lo contrario la empresa puede soportar el mismo
como destino la ciudad de Troya. En caso de duda, para evitar una infección, usar protección.
Un hacker con un sentido del humor malicioso podría tratar de plantar un pequeño programa
diseñado para ser perversamente molesto en su ordenador. Por ejemplo, podría tener
la bandeja de la unidad de CD están apareciendo constantemente abierto, o el archivo que está
trabajando en mantener
minimizar. O que pueda causar un archivo de audio para reproducir un grito a todo volumen en el
medio de la noche. Ninguno de estos es mucho más divertido cuando estás tratando de dormir o
realizar su trabajo .., pero al menos no hacen ningún daño duradero.
Mensaje de un amigo
Los escenarios pueden empeorar aún más, a pesar de las precauciones. Imagine: Usted ha
decidió no correr ningún riesgo. Ya no descargar ningún archivo, excepto
de sitios seguros que usted conoce y confía, como SecurityFocus.com o
Amazon.com. Que ya no haga clic en enlaces de correo electrónico
de fuentes desconocidas. Ya no abrir archivos adjuntos en cualquier correo electrónico que usted
no esperaba. Y revisar su página del navegador para asegurarse de que es un
símbolo sitio seguro en cada sitio que visita para las transacciones de comercio electrónico o
intercambio de información confidencial.
Hasta que un día recibe un correo electrónico de un amigo o empresa que realiza
un archivo adjunto. No podía ser nada malo si se trata de alguien que
conoce bien, ¿verdad? Sobre todo porque usted sabe que la culpa de que su
datos de la computadora fueron dañados.
Abrir el archivo adjunto, y ... BOOM! Usted acaba de golpe con un gusano o caballo de Troya
Caballo. ¿Por qué alguien que usted conoce hacer esto para usted? Porque algunas cosas son
no como aparecen. Usted ha leído acerca de esto: el gusano que llega a una persona
equipo, y luego se emails a todo el mundo en el libro de dirección de esa persona. Cada
de estas personas recibe un correo electrónico de alguien que conoce y confía, y cada uno de

los correos electrónicos de confianza contiene el gusano, que se propaga como las ondas a partir de una piedra arrojada a un estanque tranquilo.
La razón de esta técnica es tan eficaz es que se sigue la teoría de la muerte de dos pájaros de un tiro: La capacidad de propagarse a otras víctimas inocentes, y la apariencia de que se originó a partir de una persona de confianza.
Mitnick MENSAJE
El hombre ha inventado muchas cosas maravillosas que han cambiado el mundo y nuestra forma de vida. Pero por cada buen uso de la tecnología, ya sea un ordenador, teléfono o Internet, siempre habrá alguien que encontrar una forma de abusar de ella o por su sus propios fines.
Es un hecho triste de la vida en el estado actual de la tecnología que usted puede conseguir un e-mail
de alguien cercano a usted y todavía tiene que preguntarse si es seguro abrir.
Variaciones sobre un tema
En esta era de la Internet, hay un tipo de fraude que implica que desviando a un sitio web que no es lo que usted espera. Esto sucede con regularidad, y se necesita una variedad de formas. Este ejemplo, que se basa en una estafa perpetrada en la actual Internet, es representativo.
Feliz Navidad. . .
Un vendedor de seguros jubilado llamado Edgar recibió un e-mail un día de PayPal, una empresa que ofrece una manera rápida y conveniente de hacer en línea los pagos. Este tipo de servicio es especialmente útil cuando una persona en una parte del el país (o del mundo, para esa materia) es la compra de un artículo de una persona que no lo sabe. PayPal cobra la tarjeta de crédito del comprador y las transferencias de dinero directamente a la cuenta del vendedor. Como un coleccionista de antigüedades Edgar frascos de vidrio hizo mucho
de negocio a través de eBay de subastas en línea de la compañía. Se utiliza PayPal, a menudo, a veces varias veces a la semana. Así que Edgar estaba interesado, cuando recibió un de correo electrónico en la temporada de fiestas de 2001 que parecía ser de PayPal, ofreciéndole una recompensa para la actualización de su cuenta PayPal. El mensaje decía:
Feliz Navidad y Año Valor al Cliente de PayPal;
Cuando se acerca el año nuevo y como todos se preparan para pasar un año antes, PayPal le gustaría darle un crédito de $ 5 en tu cuenta!
Todo lo que tienes que hacer para reclamar su regalo de $ 5 de nosotros es actualizar su información en
nuestro Pay Pal sitio seguro por el 01 de enero 2002. Un año trae un montón de cambios, por actualizar su información con nosotros que nos permitirá seguir proporcionando usted y nuestro servicio de valor al cliente con un servicio excelente y al mismo tiempo, mantener registros de derecho!
Para actualizar su información ahora y recibirá $ 5 en su cuenta PayPal al instante, haga clic en este enlace:
http://www, paypal, seguro. com / cgi-bin
Gracias por utilizar PayPal.com y ayudarnos a crecer para ser el más grande de nuestra tipo! Sinceramente les deseo un muy "Feliz Navidad y Feliz Año Nuevo"
PayPal equipo
Una nota sobre E.commerce Sitios Web
Probablemente conozca a personas que se resisten a comprar productos en línea, incluso de las empresas de marca tales como Amazon y eBay, o los sitios web de Old Navy, Objetivo, o Nike. En cierto modo, tienen razón para sospechar. Si el navegador utiliza hoy en día estándar de cifrado de 128 bits, la información que envía a cualquier seguro sitio sale de su computadora encriptada. Estos datos pueden ser cifrados con un gran esfuerzo, pero probablemente no se puede romper en un período razonable de tiempo, excepto tal vez por la Agencia de Seguridad Nacional (NSA y el, hasta ahora 98, que sabemos, no ha mostrado ningún interés en el robo de números de tarjetas de crédito de American

los ciudadanos o tratar de averiguar quién está ordenando cintas de video sexy o rizado ropa interior).

Estos archivos cifrados en realidad podría ser roto por cualquiera con el tiempo y los recursos. Pero realmente, ¿qué tonto ir a todo el esfuerzo para robar una tarjeta de crédito número cuando muchas empresas de comercio electrónico en el error de almacenar todas sus información financiera del cliente sin cifrar en sus bases de datos? Peor aún, un número de empresas de comercio electrónico que utilizan un determinado software base de datos SQL mal agravan el problema: Ellos nunca han cambiado el sistema por defecto contraseña de administrador para el programa. Cuando se llevaron a cabo el programa de la casilla, la contraseña era "nulo", y sigue siendo "nula" en la actualidad. Por lo tanto el contenido de la base de datos están disponibles para cualquier usuario de Internet que decide tratar de conectarse a el servidor de base de datos. Estos sitios están bajo ataque en todo momento y que la información roban, sin que nadie lo supiera,

Por otro lado, la misma gente que no va a comprar en Internet, porque son miedo de tener información de sus tarjetas de crédito robadas no tienen ningún problema comprar con la misma tarjeta de crédito en una tienda de ladrillo y mortero, o pagar por el almuerzo, la cena o las bebidas con la tarjeta incluso en un bar de atrás de la calle o un restaurante que no se llevaría a su madre. Crédito recibos de las tarjetas roban de estos lugares todo el tiempo, o sacó de los contenedores de basura en el callejón. Y cualquier empleado sin escrúpulos o un camarero puede anotar su nombre y la información de la tarjeta, o usar un gadget fácilmente disponibles en Internet, una tarjeta de deslizar-dispositivo que almacena los datos de cualquier tarjeta de crédito pasa a través de ella, para su posterior recuperación.

Hay algunos riesgos para las compras en línea, pero es probable que sea tan seguro como ir de compras en una tienda de ladrillos y mortero. Y las compañías de tarjetas de crédito que ofrecen las mismas protección al usar su tarjeta en línea - si cualquier cargo fraudulento hecho llegar a la cuenta, usted es único responsable de los primeros $ 50.

Así que en mi opinión, el miedo a las compras en línea es más que otro fuera de lugar preocupación.

Edgar no se dio cuenta de los varios signos reveladores de que algo andaba mal con este correo electrónico (por ejemplo, el punto y coma después de la línea de saludo, y el texto ilegible sobre "nuestro servicio al cliente valorado con un servicio excelente"). Él clic en el enlace, entró en la información que se solicita - Nombre, dirección, teléfono el número y la información de su tarjeta de crédito - y se sentó. de nuevo a esperar a los cinco millones de dólares de crédito a aparecer en su próxima factura de la tarjeta de crédito. Lo que se presentó en cambio, fue una lista de cargos por artículos que nunca compró.

Con el análisis de la Edgar había sido engañado por una estafa de Internet comunes. Es una estafa que viene en una variedad de formas. Uno de ellos (que se detallan en el capítulo 9) consiste en un nombre de usuario señuelo pantalla creada por el atacante que parece idéntico a la cosa real. La diferencia es que la pantalla falsa no da acceso al sistema informático que el usuario está tratando de alcanzar, sino que alimenta a su nombre de usuario y contraseña al hacker.

Edgar había sido engañado por una estafa en la que los ladrones se habían inscrito un sitio Web con el nombre de "paypal-secure.com" - que suena como si debiera haber sido un página segura en el sitio de PayPal legítimo, pero no lo es. Cuando entró en

información en ese sitio, los atacantes se justo lo que querían.
Mitnick MENSAJE
Si bien no es infalible (no es de seguridad), cada vez que visite un sitio que las solicitudes información que considera privado, asegúrese siempre de que la conexión se autenticado y encriptado. Y aún más importante, no de forma automática haga clic en Sí en cualquier cuadro de diálogo que puede indicar un problema de seguridad, como un inválido, expirado, o revocado el certificado digital.
VARIACIONES EN LA VARIACIÓN
¿De cuántas maneras hay otros para engañar a los usuarios de computadoras a ir a un falso Sitio web donde ofrecen información confidencial? No creo que nadie tiene una respuesta válida, precisa, pero "mucho, mucho", servirá al propósito.
El eslabón perdido
Un truco aparece regularmente: El envío de un correo electrónico que ofrece un motivo tentador visitar un sitio, y proporciona un vínculo para ir directamente a ella. Excepto que el enlace no te llevará al sitio que crees que vas, porque el enlace en realidad sólo se asemeja a un enlace de ese sitio. He aquí otro ejemplo de pastel que se ha utilizado realmente en Internet, una vez más la participación de la mala utilización de PayPal nombre:
www. PayPai. com
A simple vista, esto parece como si se dice PayPal. Incluso si la víctima avisos, que puede pensar que es sólo un ligero defecto en el texto que hace que el "yo" de Pal parecer un "I." Y que se daría cuenta a simple vista que:
www. PayPal. com
utiliza el número 1 en lugar de una letra L minúscula? Hay bastante gente que aceptar faltas de ortografía y mala dirección para hacer de esta táctica continuamente popular con los bandidos de tarjeta de crédito. Cuando la gente vaya al sitio falso, parece que el sitio que esperaban para ir a, y alegremente entrar en su tarjeta de crédito de la información. Para configurar una de estas alertas, un atacante sólo tiene que registrar el nombre de dominio falso, enviar sus correos electrónicos, y esperar a que los retoños que aparecen, listo ser engañado.
A mediados de 2002, recibí un correo electrónico, al parecer parte de un envío masivo de correo que se marcada como de "Ebay@ebay.com". El mensaje se muestra en la Figura 8.1.
Figura 8.1. El enlace en este o cualquier otro correo electrónico debe ser utilizado con precaución.
---------- ----------
---
msg: Estimado usuario de eBay,
Se ha vuelto muy sensible que otra parte ha ido corrompiendo su eBay cuenta y ha violado nuestra política de las Condiciones de uso en la lista:
4. De licitación y compra de
Usted está obligado a completar la transacción con el vendedor si adquiere un artículo a través de uno de nuestros formatos de precio fijo o al mejor postor como se describe a continuación. Si usted es el mejor postor al final de una subasta (el cumplimiento de los mínimo de puja o los requisitos de reserva) y su oferta es aceptada por el vendedor, usted está obligado a completar la transacción con el vendedor, o el transacción está prohibida por la ley o el presente Acuerdo.
Ha recibido esta notificación por parte de eBay, ya que ha llegado a nuestra atención que su cuenta corriente ha causado interrupciones con otros usuarios de eBay y eBay requiere la verificación inmediata de su cuenta. Por favor, verifique su cuenta o la cuenta puede ser desactivada. Haga clic aquí para verificar su cuenta - http://error ebay.tripod.com
Las marcas comerciales y marcas mencionadas son propiedad de sus respectivos propietarios, eBay y el logotipo de eBay son marcas comerciales de eBay Inc.
---------- ----------

Víctimas que han hecho clic en el enlace fue a una página Web que se parecía mucho a una página de eBay. De hecho, la página está bien diseñado, con el logotipo de eBay auténticos, y "Buscar", "Venta" y otros vínculos de navegación que, si se hace clic, se que el visitante el sitio de eBay real. También había un logo de seguridad en la esquina inferior derecha. A disuadir a la víctima inteligente, el diseñador ha utilizado incluso el cifrado HTML para enmascarar donde la información proporcionada por el usuario se está enviando.
Fue un excelente ejemplo de un equipo malintencionado de ingeniería con sede social ataque. Sin embargo, no estuvo exenta de varios defectos.
El mensaje de correo electrónico no estaba bien escrito, en particular, el párrafo que comienza "Usted ha recibido este aviso" es torpe e inepto (los responsables de estos engaños no contratar a un profesional para editar su copia, y eso se nota siempre). Por otra parte, alguien que estaba prestando mucha atención se habría convertido en sospechoso eBay PayPal pidiendo información de los visitantes, no hay razón que eBay solicitar a un cliente para obtener esta información privada con la participación de una empresa diferente.
Y nadie bien informado sobre el Internet es probable que reconocer que el hipervínculo no se conecta al dominio de eBay, pero a tripod.com, que es un país libre Servicio de alojamiento web. Este fue un claro indicativo de que el correo electrónico no es legítimo.
Aún así, apuesto a que mucha gente entró en su información, incluyendo una tarjeta de crédito número, en esta página.
NOTA
¿Por qué hay personas que pueden registrar nombres de dominio engañosos o inapproprate?. Porque bajo la ley actual y la política en línea, cualquier persona puede registrar ningún nombre de sitio que "no está ya en uso.
Las empresas tratan de luchar contra este uso de las direcciones de imitación, pero tenga en cuenta lo que están haciendo en contra. General Motors presentó una demanda contra una compañía que registró f ** kgeneralmotors.com (pero sin los asteriscos) y señaló la dirección de Sitio Web de General Motors. GM perdió.
Esté alerta
Como los usuarios individuales de Internet, todos tenemos que estar alerta, haciendo un esfuerzo consciente decisión acerca de cuándo puede volver a introducir información personal, contraseñas, cuentas números, números PIN, etc.
¿Cuántas personas conoce usted que podría decir que si un particular Internet página que están viendo cumple con los requisitos de una página segura? ¿Cuántos empleados de su empresa sabe qué buscar?
Todos los que usan la Internet debe saber sobre el pequeño símbolo que a menudo aparece en algún lugar en una página Web y se parece a un dibujo de un candado. Ellos debe saber que cuando el cerrojo está cerrado, el sitio ha sido certificado como seguro. Cuando el cerrojo abierto o el icono del candado que falta es, el sitio web no es autenticado de efectivo, y cualquier información transmitida se encuentra en el claro - es decir, sin encriptar.
Sin embargo, un atacante que consigue poner en peligro los privilegios administrativos en una informático de la empresa puede ser capaz de modificar o reparar el código del sistema operativo para cambiar la percepción del usuario de lo que realmente está sucediendo. Por ejemplo, la instrucciones de programación en el software de navegación que indican que un sitio Web de certificado digital es válido puede ser modificado para omitir la comprobación. O el sistema puede ser modificado con algo llamado rootkit, la instalación de uno o más atrás puertas a nivel del sistema operativo, que son más difíciles de detectar.
Una conexión segura autentica el sitio como genuino, y cifra el

información que se comunica, de modo que un atacante no puede hacer uso de cualquier dato que
es interceptado. ¿Puedes confiar en cualquier otro sitio Web, incluso una que utiliza una conexión segura
conexión? No, porque el propietario del sitio no puede ser vigilantes sobre la aplicación de todas las
parches de seguridad necesarios, o forzar a los usuarios o administradores a respetar buena prácticas contraseña. Por lo que no se puede asumir que cualquier sitio supuestamente seguro es invulnerable a los ataques.

LINGO

BACK DOOR Un punto de partida secreta que proporciona una forma secreta a un usuario de equipo que es desconocido para el usuario. También es utilizado por los programadores mientras que el desarrollo
un programa de software para que puedan entrar en el programa para solucionar problemas

Secure HTTP (Hypertext Transfer Protocol) o SSL (Secure Sockets Layer) proporciona
un mecanismo automático que utiliza certificados digitales no sólo para cifrar
información que se envía al sitio distante, sino también para proporcionar servicios de autenticación (un
seguridad de que usted se está comunicando con el sitio Web real). Sin embargo, este mecanismo de protección no funciona para los usuarios que no prestar atención a
si el nombre del sitio aparece en la barra de direcciones es de hecho la dirección correcta de el sitio que está intentando acceder.

Otra de las cuestiones de seguridad, en su mayoría ignorados, aparece como un mensaje de advertencia que dice
algo así como "Este sitio no es seguro o el certificado de seguridad ha caducado. Do
quiere ir al sitio de todos modos? "Muchos usuarios de Internet no entienden el
mensaje, y cuando aparece, simplemente haz clic en Aceptar o Sí y continuar con
su trabajo, sin saber que pueden estar en arenas movedizas. Tenga cuidado: En un sitio Web que no utiliza un protocolo seguro, nunca se debe ingresar ninguna información confidencial información tal como su dirección o número de teléfono, tarjeta de crédito o cuenta bancaria números, o cualquier cosa que desea mantener en privado.

Thomas Jefferson dijo que mantener nuestra libertad requiere "vigilancia eterna."
Privacidad y el mantenimiento de la seguridad en una sociedad que utiliza la información como moneda de cambio
requiere no menos.

Convertirse en Savvy Virus

Una nota especial sobre el software de virus: Es esencial para la intranet corporativa, pero también es esencial para cada empleado que usa una computadora. Más allá de tener contra software antivirus instalado en sus máquinas, los usuarios, obviamente, deben tener la software de encendido (que muchas personas no les gusta, ya que inevitablemente retrasa por algunas de las funciones de ordenador).

Con el software anti-virus no hay otro procedimiento importante a tener en
mente, así: Mantener las definiciones de virus actualizadas. A menos que su compañía está establecidos para distribuir software o actualizaciones a través de la red a todos los usuarios, cada uno
cada usuario debe llevar la responsabilidad de la descarga de la última serie de virus definiciones por su cuenta. Mi recomendación personal es que todo el mundo establecer el las preferencias de software antivirus para que nuevas definiciones de virus se actualizan automáticamente
todos los días.

LINGO

Secure Sockets Layer Protocolo desarrollado por Netscape que ofrece
autenticación de cliente y servidor en una comunicación segura en el
internet.

En pocas palabras, usted es vulnerable a menos que las definiciones de virus se actualizan

periódicamente.
Y aun así, usted todavía no está completamente a salvo de virus o gusanos que la lucha contra la las compañías de software antivirus aún no conocen o no han publicado todavía una archivo de patrones para la detección.
Todos los empleados con privilegios de acceso remoto desde sus ordenadores portátiles o en el hogar
equipos deben tener actualizado el software antivirus y un firewall personal en los máquinas como mínimo. Un atacante sofisticado se verá en el cuadro grande de buscar el eslabón más débil, y ahí es donde te atacará. Recordando a las personas con equipos remotos con regularidad sobre la necesidad de firewalls personales y actualizada, software antivirus activo es una responsabilidad, porque no se puede esperar que trabajadores, directivos, personal de ventas, y otros a distancia de una TI departamento recordar los peligros de dejar a sus computadoras sin protección.
Más allá de estos pasos, te recomiendo el uso de las menos comunes, pero no menos importante, los paquetes de software que protegen contra los ataques de caballo de Troya, los llamados
anti-Troyanos software. En el momento de escribir estas líneas, dos de los más conocidos programas son los más Limpia (www.moosoft.com), y barrido de Defensa de Troya (Www.diamondcs.com.au).
Finalmente, lo que probablemente es el mensaje de seguridad más importante de todos para empresas que no buscar correos electrónicos peligrosos en el gateway corporativo: Desde todos tendemos a ser olvidadizo o negligente en las cosas que parecen periféricos conseguir nuestros trabajos realizados, los empleados necesitan que se les recuerde una y otra vez, en
de diferentes maneras, de no abrir archivos adjuntos de correo electrónico a menos que esté seguro de que
la fuente es una persona u organización que pueden confiar. Y la gestión también es necesario para recordar a los empleados que deben utilizar el software de virus activo y anti-troyanos software que proporciona una protección invaluable contra el parecer de confianza correo electrónico que puede contener una carga destructiva.

Capítulo 8
Utilizando Simpatía, la culpa y la intimidación
Como se discutió en el capítulo 15, un ingeniero social utiliza la psicología de la influencia de llevar a su objetivo de cumplir con su petición. Expertos ingenieros sociales son muy hábiles en el desarrollo de un ardid que estimula las emociones, como miedo, excitación o de culpa. Lo hacen mediante el uso de disparadores psicológicos - mecanismos automáticos que conducen la gente a responder a las solicitudes, sin un análisis en profundidad de todos los disponibles de la información.
Todos queremos evitar situaciones difíciles para nosotros y para los demás. Con base en esta impulso positivo, el atacante puede jugar en la simpatía de una persona, que a su víctima se sienten culpables, o usar la intimidación como arma.
Aquí hay algunas lecciones de la escuela de posgrado en las tácticas populares que juegan en el emociones.
Una visita al estudio
¿Has notado cómo algunas personas pueden caminar hasta la guardia en la puerta de, por ejemplo, un salón de un hotel en alguna reunión, fiesta privada, o un libro de lanzamiento función está en marcha, y sólo pasar por delante de esa persona sin que se le pidió su boleto o pase?
De la misma manera, un ingeniero social puede hablar a su manera en los lugares que No hubiera creído posible - como la siguiente historia acerca de la industria del cine deja en claro.
La llamada telefónica
"Oficina de Ron Hillyard, se trata de Dorothy."
"Dorothy, hola. Mi nombre es Kyle Bellamy. Acabo de subir a bordo para trabajar en

Animación de Desarrollo en el personal Brian Glassman. Ustedes seguro de hacer las cosas diferentes por aquí. "
"Creo que. Nunca he trabajado en cualquier otra película mucho, así que no lo sé. ¿Qué se puede Puedo hacer por ti? "
"A decir verdad, me siento una especie de estúpido. Tengo un escritor que viene sobre esta por la tarde para una sesión de paso y no sé que se supone que debo hablar acerca de Su incorporación a la suerte. La gente aquí en la oficina de Brian es muy agradable, pero Odio tener que preocuparse, ¿cómo puedo hacer esto, ¿cómo puedo hacer eso. Es como si acabara de
comenzó la secundaria y no puedo encontrar mi camino al baño. ¿Sabes lo que
decir? "
Dorothy se echó a reír.
"Usted quiere hablar con seguridad. Dial 7, y luego 6138. Si
obtener Lauren, dígale a su Dorothy dijo que debería tomar buena
el cuidado de usted. "
"Gracias, Dorothy. Y si no puede encontrar el baño de hombres, puede que le devuelva la llamada!"
Se echó a reír a más de la idea, y colgó.
La historia de David Harold
Me encantan las películas y cuando me mudé a Los Ángeles, pensé que iba a llegar a satisfacer todo tipo de personas en el negocio del cine y que me llevará a lo largo de partes y me tienen más a comer a los estudios. Bueno, yo estaba allí por un año, se estaba convirtiendo veintiséis años de edad, y lo más cercano que se iba en el Universal Studios Tour con toda la buena gente de Phoenix y Cleveland.
Así que finalmente llegué a un punto en que pensé que, si no me invitan, yo voy a invitar a mí mismo. ¿Qué es lo que hice.
Compré una copia de Los Angeles Times y leer la columna de entretenimiento por un par de días, y escribió los nombres de algunos productores en diferentes estudios. Decidí intentar golpear a uno de los grandes estudios de primero. Así que llamé a la centralita y pidió a la oficina del productor que había leído en la
papel. El secretario respondió que sonaba como el tipo de madre, así que me imaginé había tenido suerte, si era una chica joven que estaba allí con la esperanza de que ella estaría descubierto, probablemente no me habría dado la hora del día.
Pero esto Dorothy, que sonaba como si alguien que hubiera adoptado en un gato callejero, alguien que me siento por el chico nuevo que se sentía un poco abrumado
en el nuevo trabajo. Y estoy segura que tiene el toque justo con ella. No es todos los días tratan de engañar a alguien y te dan mucho más de lo que usted pidió. Fuera de lástima, que no sólo me dio el nombre de una de las personas en materia de seguridad, pero dijo que
debe decirle a la señora que Dorothy quería que me ayudara.
Por supuesto que yo había planeado usar el nombre de Dorothy de todos modos. Esto lo hizo aún mejor.
Lauren abrió la derecha y ni siquiera se molestó en buscar el nombre que le di a ver si realmente estaba en la base de datos de los empleados.
Cuando llegué a la puerta de la tarde, que no sólo tenía mi nombre en el lista de visitantes, que incluso tenía una plaza de aparcamiento para mí. Tuve un almuerzo tardío en el
comisario, y vagó por la suerte hasta el final del día. Incluso se coló en una par de estudios de sonido y los miraba películas. No se fue hasta el 7 de en punto. Fue uno de mis días más emocionantes.
Con el análisis de la
Todo el mundo era un empleado nuevo una vez. Todos tenemos recuerdos de lo que primero día era como, sobre todo cuando eran jóvenes e inexpertos. Por eso, cuando una nueva empleado le pide ayuda, se puede esperar que muchas personas - sobre todo de nivel de entrada personas - se acordará de su propio nuevo chico en el bloque de los sentimientos y salir de

su manera de echar una mano. El ingeniero social lo sabe, y entiende el que
se puede utilizar para jugar en las simpatías de sus víctimas.
Te lo ponemos muy fácil para los de afuera Con su camino en nuestra empresa
plantas y oficinas. Incluso con guardias en las entradas y de inicio de sesión para los
procedimientos
cualquiera que no sea un empleado, cualquiera de las múltiples versiones sobre el engaño
utilizado en
esta historia permitir a un intruso obtener un gafete de visitante y caminar a la derecha adentro y
Si su empresa requiere que los visitantes serán escoltados? Esa es una buena regla, pero es
sólo es eficaz si sus empleados son realmente conscientes de detener a nadie
con o sin un pase de visitante que es por sí mismo, y hacerle preguntas. Y
entonces, si las respuestas no son satisfactorias, sus empleados tienen que estar dispuestos a
contacto de seguridad.
Por lo que es demasiado fácil para los de afuera para hablar a su manera en sus instalaciones
pone en peligro
información confidencial de su empresa. En el clima actual, con la amenaza de
ataques terroristas se cierne sobre nuestra sociedad, es algo más que la información que
podría estar en riesgo.
"Hazlo ahora"
No todo el que utiliza tácticas de ingeniería social es un ingeniero social pulido.
Cualquiera con un conocimiento íntimo de una empresa particular puede a su vez
peligroso. El riesgo es aún mayor para cualquier empresa que tiene en sus archivos y
bases de datos de información personal sobre sus empleados, que, por supuesto, la mayoría de
los
las empresas hacen.
Cuando los trabajadores no están educados o capacitados para reconocer los ataques de
ingeniería social,
determinadas personas como la señora plantado en la siguiente historia puede hacer cosas que
la gente más honesta sería que imposible.
Historia de Doug
Las cosas no habían ido tan bien con Linda de todos modos, y yo sabía que tan pronto como sea
Conocí a Erin que ella era la única para mí. Linda es, al igual que, un poco ... así, una especie de
no
exactamente inestable pero puede especie de ir por las paredes cuando ella se enoja.
Le dije que lo más suave que podía que tenía que salir, y me ayudó a empacar y
aunque dejó un par de CDs Queensryche que en realidad eran míos. Tan pronto
como ella se fue me fui a la ferretería de un nuevo bloqueo de Medico para poner en el
puerta principal y lo puso en esa misma noche. A la mañana siguiente llamé por teléfono
empresa y les cambio mi número de teléfono, y lo hizo sin publicar.
Que me dejó libre para perseguir Erin.
Historia de Linda
Yo estaba listo para salir, de todos modos, yo no había decidido cuando. Pero a nadie le gusta
sentirse
rechazada. Por lo que era sólo una cuestión de, ¿qué podía hacer para hacerle saber lo que es un
idiota
era?
No pasó mucho tiempo para averiguar. Tenía que haber otra chica, de lo contrario
no me enviaron de embalaje con tanta prisa. Por lo que acababa de esperar un poco y luego
empezar a
llamándolo tarde en la noche. Ya sabes, todo el tiempo que se lo quiere
para ser llamado.
Esperé hasta el próximo fin de semana y llamó alrededor de las 11 de la noche del sábado.
Sólo había cambiado su número de teléfono. Y el número nuevo no cotizan en bolsa. Que
sólo muestra qué clase de hijo de puta el tipo era.
No era tan grande de un revés. Empecé a hurgar en los papeles que había

logró llevarse a casa justo antes de que dejé mi trabajo en la compañía telefónica. Y hay era - yo había guardado un billete de reparación de una vez, cuando había un problema con la de la línea telefónica a Doug, y la impresión de listados
el cable y par de su teléfono. Vea, usted puede cambiar su número de teléfono de todos los que quiera, pero usted todavía tiene el mismo par de cables de cobre que va desde su casa a la oficina de la compañía de conmutación telefónica, llamada Central Oficina, o CO El conjunto de cables de cobre de cada casa y apartamento identificados por estos números, llamados el cable y par. Y si sabes cómo la compañía telefónica hace las cosas, que voy a hacer, a sabiendas de cable del objetivo y el par es
todo lo que necesita saber el número de teléfono.
Yo tenía una lista dando a todos los objetores de conciencia en la ciudad, con sus direcciones y teléfonos
números. Miré el número de la CO en el barrio donde yo
vivía con Doug el tirón, y llamó, pero, naturalmente, no había nadie.
¿Dónde está el guardavías cuando realmente lo necesitamos? Me llevó a todos de una veintena de
segundos para llegar a un plan. Comencé a llamar a los objetores de conciencia en torno a sí y Finalmente encuentra a un chico. Pero él era millas de distancia y probablemente estaba sentado con los pies. Yo sabía que él no quiere hacer lo que yo necesitaba. Yo estaba dispuesto a mi plan.
"Esta es Linda, Centro de Reparación", le dije. "Tenemos un servicio de emergencia. Por un unidad de paramédicos se ha reducido. Tenemos un técnico de campo tratando de restaurar servicio pero no puede encontrar el problema. Es necesario que usted conduzca a la Webster CO inmediatamente y ver si tiene tono salir de la oficina central. "
Y entonces yo le dije, 'Te llamaré cuando llegue allí ", porque por supuesto que no habría podido llamar al Centro de Reparación y preguntando por mí.
Yo sabía que él no quiere dejar la comodidad de la oficina central para abrigarse
y sobre hielo raspar el parabrisas y la unidad a través de los sobornos a altas horas de la noche. Pero
que era una emergencia, por lo que no podía decir con exactitud que estaba muy ocupado.
Cuando le llegó a cuarenta y cinco minutos más tarde, en la CO Webster, le dije que Compruebe el cable de 29 pares 2481, y se acercó a la llama y comprobado, y dijo:
Sí, hay tono de marcado. Que por supuesto yo ya sabía.
Entonces me dijo: "Bueno, yo necesito que hagas una LV," lo que significa que la verificación de línea,
que le pide que identifique el número de teléfono. Lo hace mediante la marcación de un número especial que lee el número que es llamado desde. Él no sabe
nada acerca de si se trata de un número privado o que es justbeen cambiado, por lo que hizo lo que he pedido y he oído el número que se anunció en su conjunto de pruebas de liniero.
Hermoso. Todo había funcionado a las mil maravillas.
Yo le dije: "Bueno, el problema debe estar en el campo", como yo sabía, la, sombra
todo el tiempo. Le agradecí y le dije que habíamos seguir trabajando en ello, y se despidió por la noche.
Mitnick MENSAJE
Una vez que un ingeniero social sabe cómo funcionan las cosas dentro de la empresa objetivo, que
se convierte en fácil de utilizar ese conocimiento para desarrollar una buena relación con los legítimos
los empleados. Las empresas tienen que prepararse para los ataques de ingeniería social de empleados actuales o anteriores que pudieran tener un interés personal. Verificación de antecedentes
Puede ser útil para eliminar a las perspectivas que pueden tener una propensión hacia el este tipo de comportamiento. Pero en la mayoría de los casos, estas personas será muy difícil detectar. La única garantía razonable en estos casos es hacer cumplir y de auditoría

procedimientos para la verificación de la identidad, incluida la situación laboral de la persona, antes de
de revelar cualquier información a cualquiera que no conozca personalmente el silencio junto a la de la empresa.
Esto en cuanto a que Doug y tratando de esconderse de mí a un número privado.
La diversión estaba a punto de comenzar.
Con el análisis de la
La joven de esta historia fue capaz de obtener la información que quería llevar a
a cabo su venganza, porque había en el interior del conocimiento: los números de teléfono, procedimientos, y la jerga de la compañía telefónica. Con él no sólo era capaz de
encontrar un nuevo número, teléfono de uso restringido, pero fue capaz de hacerlo en medio de un
noche de invierno, el envío de un guardagujas teléfono persiguiendo a través de la ciudad para ella.
"MR. BIGG quiere esto"
Una forma popular y altamente eficaz de intimidación - popular, en gran medida
porque es muy simple - se basa en que influyen en el comportamiento humano mediante el uso de la autoridad.
Sólo el nombre del asistente en la oficina del director general puede ser valiosa. Privado investigadores y hasta la cabeza los cazadores-hacer esto todo el tiempo. Van a llamar a la telefonista y dicen que quieren estar conectados a la oficina del CEO.
Cuando la secretaria o asistente ejecutiva respuestas, ellos dicen que tienen un
documento o paquete para el CEO, o si se envía un archivo adjunto de correo electrónico, se que se imprima? O si no, le pregunto, ¿cuál es el número de fax? Y, por cierto,
¿Cuál es tu nombre?
Luego llame a la siguiente, y decir: "Jeannie en la oficina de Mr. Bigg me dijo que
llamar a usted para que usted me puede ayudar con algo. "
La técnica se denomina nombre-que caen, y por lo general es utilizado como un método para rápidamente establecer una buena relación, influyendo en el destino para creer que el atacante es conectado con alguien de autoridad. Un objetivo es más probable que hagan un favor a
alguien que conoce a alguien que sabe.
Si el atacante tiene sus ojos puestos en la información altamente sensible, puede utilizar este tipo de enfoque para despertar emociones útiles para la víctima, tales como el miedo de conseguir en problemas con sus superiores. He aquí un ejemplo.
Historia de Scott
"Scott Abrams."
"Scott, se trata de Christopher Dalbridge. Acabo de hablar por teléfono con el Sr. Biggley,
y es más que un poco triste. Él dice que él envió una nota hace diez días que
personas para obtener copias de toda su investigación sobre la penetración de mercado a nosotros para
análisis. Nunca nos dieron nada. "
"La investigación penetración en el mercado? Nadie me dijo nada al respecto.
¿Qué departamento se encuentra usted? "
"Somos una firma consultora que contrató, y ya estamos retrasados". "Escucha,
Estoy en mi camino a una reunión. Déjame tu número de teléfono
y. . . "
El atacante ahora sonaba poco menos de una verdadera frustración: "¿Es eso lo
Qué quieres que diga el señor Biggley? Escucha, que espera que el análisis para mañana por la mañana y tenemos que trabajar en ello esta noche. Ahora, ¿quiere que le diga que no podía hacerlo porque no pudimos conseguir el informe de usted, o quiere decir
lo que a ti mismo? ".
Un CEO enojo puede arruinar su semana. El objetivo es probable que decida que tal vez este es algo que mejor tener cuidado de antes de ir a esa reunión. Una vez más,
el ingeniero social se ha presionado el botón derecho para obtener la respuesta que quería.
Con el análisis de la

La astucia de la intimidación por parte de la autoridad de referencia funciona especialmente bien si el
otra persona está a un nivel bastante bajo en la empresa. El uso de un importante
nombre de la persona no sólo supera resistencia normal o la sospecha, pero a menudo
hace que la persona con ganas de agradar, el instinto natural del deseo de ser útil es
multiplica cuando se piensa que la persona que está ayudando a que es importante o
influyentes.
El ingeniero social sabe, sin embargo, que es lo mejor cuando se ejecuta este particular
engaño a utilizar el nombre de alguien en un nivel superior al propio jefe de la persona.
Y esta táctica es difícil de usar en una organización pequeña: el atacante no
desea a su víctima con un comentario oportunidad el vicepresidente de marketing. "Me envió a los
plan de marketing de producto que tenía ese hombre me llama sobre "pueden fácilmente producir una
respuesta de "¿Qué plan de marketing? ¿Qué tipo?" Y que podría llevar a la
descubrimiento de que la empresa ha sido víctima.
MITNICKS MENSAJE
La intimidación puede crear un temor al castigo, influenciar a la gente a cooperar.
La intimidación también pueden aumentar el miedo al ridículo o de ser descalificado
de que la nueva promoción.
Las personas deben ser entrenados que no es sólo aceptable, pero espera que el reto
autoridad cuando la seguridad está en juego. Formación en seguridad debe incluir
enseñar a la gente a desafiar a la autoridad en un amistoso al cliente formas, sin
dañar las relaciones. Por otra parte, esta expectativa tiene que ser sostenidos por el
de arriba hacia abajo. Si un empleado no va a ser una copia de seguridad para las personas difíciles
independientemente de su situación, la reacción normal es dejar un desafío - sólo el
lo contrario de lo que usted desea.
LO QUE LA ADMINISTRACIÓN DEL SEGURO SOCIAL SABE
USTED
Nos gusta pensar que las agencias gubernamentales con LES en nosotros mantener la información
encerrados bajo llave y lejos de la gente sin una auténtica necesidad de saber. La realidad es
que incluso el gobierno federal no es tan inmune a la penetración como nos gustaría
imaginar.
Llame al teléfono de mayo de Linn
Lugar: una oficina regional de la Administración del Seguro Social
Tiempo: 1 0:1 8 a.m., jueves por la mañana
"Mod tres. Esto es de mayo de Linn Wang".
La voz al otro lado del teléfono sonó de disculpa, casi tímido.
"La Sra. Wang, se trata de Arthur Arondale, en la Oficina del Inspector General. ¿Puedo
te llaman 'Mayo'?
"Es 'de mayo de Linn"', dijo.
"Bueno, es así, de mayo de Linn. Tenemos un nuevo tipo de aquí que no hay
equipo de ahora, y ahora él tiene un proyecto prioritario y que está usando la mía.
Somos el gobierno de los Estados Unidos, para salir llorando fuerte, y ellos dicen
no tiene suficiente dinero en el presupuesto para comprar un equipo para que este tipo de uso.
Y ahora mi jefe piensa que me estoy cayendo por detrás y no quiero oír excusas,
¿sabes? "
"Yo sé lo que quieres decir, está bien."
"¿Me puedes ayudar con una investigación rápida sobre la SQM?" -preguntó, usando el nombre de
el sistema informático para buscar información sobre los contribuyentes.
"Claro, What'cha necesita?"
"Lo primero que necesito hacer es un ALPHADENT de Joseph Johnson, fecha de nacimiento
7/4/69. "(ALPHADENT significa tener la búsqueda electrónica de una cuenta

alfabéticamente por el nombre del contribuyente, más identificados por fecha de nacimiento.)
Tras una breve pausa, preguntó:
"¿Qué necesitamos saber?"
"¿Cuál es su número de cuenta?" dijo, con el de información privilegiada
la abreviatura del número de seguro social. Ella lo leyó.
"Bueno, yo necesito que hagas una numident en que el número de cuenta"
la persona que llamó dijo.
Esa fue una solicitud para que ella lea la información del contribuyente básico, y Linn mayo respondió dando lugar del contribuyente de nacimiento, nombre de soltera de su madre, y el nombre del padre. La persona que llama escuchó pacientemente mientras ella también le dio el mes y
año de la tarjeta fue emitida, y la oficina del distrito que fue emitido por.
El siguiente pedido un DEQY. (Se pronuncia "Deck-wee", que es corto
para "consulta de los ingresos detallados.")
La solicitud DEQY trajo la respuesta: "¿Para qué año?"
La persona que llamó dijo: "Año 2001".
De mayo de Linn dijo: "La cantidad fue $ 190,286, el pagador era Johnson Micro Tech".
"Los salarios de otros?"
"No."
"Gracias", dijo. "Ha sido muy amable."
Luego trató de organizar a su llamada en cualquier momento la información que necesitaba y no podía
llegar a su computadora, utilizando de nuevo el truco favorito de los ingenieros sociales de siempre
tratando de establecer una conexión para que pueda seguir yendo a la misma
persona, evitando las molestias de tener que encontrar una nueva marca en cada ocasión.
"No la próxima semana", le dijo, porque ella iba a Kentucky por su hermana
boda. En cualquier otro momento, que haría lo que pudiera.
Cuando colgó el teléfono, de mayo de Linn sentí bien de que ella había sido capaz de ofrecer un poco de ayuda a un compañero servidor público apreciado.
Historia de Keith Carter
A juzgar por las películas y novelas policíacas de gran éxito, una empresa privada
investigador es corto y largo plazo sobre la ética en el conocimiento de cómo hacer que los hechos jugosa
en las personas. Lo hacen mediante el uso de métodos totalmente ilegales, mientras que apenas la gestión para evitar ser arrestado. La verdad, por supuesto, es que la mayoría de ejecutar IP totalmente los negocios legítimos. Dado que muchos de ellos comenzaron su vida laboral como jurados oficiales de la ley, ellos saben perfectamente lo que es legal y qué
no es, y la mayoría no se sienten tentados a cruzar la línea.
Hay, sin embargo, excepciones. Algunos Pis - más de unos pocos - de hecho la forma
molde de los chicos en las historias de crimen. Estos chicos son conocidos en el comercio como agentes de información, un término amable para las personas que están dispuestos a romper las reglas.
Ellos saben que pueden conseguir cualquier trabajo hecho mucho más rápido y una buena
más fácil si se toma algunos atajos. Que estos atajos de pasar a ser potencial
delitos que pudieran tierra tras las rejas por unos pocos años no parece disuadir a
los más inescrupulosos.
Mientras tanto, los inhibidores de la proteasa de lujo - los que trabajan fuera de una suite de oficina de lujo en un
de alta renta parte de la ciudad - no hacer este tipo de trabajo ellos mismos. Simplemente alquilar algunos broker de información que lo haga por ellos.
El chico al que llamaremos Keith Carter era el tipo de detective privado sin el estorbo de
la ética.
Fue un caso típico de "¿Dónde está escondiendo el dinero?" O a veces es
"¿Dónde se ha escondido el dinero?" A veces era una mujer rica que quería

sabe donde su marido había escondido su dinero (aunque por qué una mujer con el dinero nunca se casa con un hombre sin un enigma Keith Carter se preguntó acerca de ahora y entonces, pero nunca había encontrado una buena respuesta para).

En este caso el marido, cuyo nombre era Joe Johnson, fue el mantenimiento de la dinero en el hielo. Él "era un tipo muy inteligente que había creado una empresa de alta tecnología con diez mil dólares que le prestó la familia de su esposa y construido en un cien millones de dólares la empresa. De acuerdo con su abogado de divorcio, que había hecho un impresionante trabajo de ocultar su patrimonio, y el abogado quería un resumen completo.

Keith se imaginaba que su punto de partida sería la Administración del Seguro Social, dirigidos a sus archivos de Johnson, que se llena de gran utilidad información para una situación como esta. Armado con su información, Keith podía pretender ser el objetivo y obtener de los bancos, casas de bolsa e instituciones offshore para contar lo todo.

Su primera llamada telefónica fue a una oficina de distrito local, utilizando el mismo número 800 que cualquier miembro de los usos públicos, el número que aparece en la guía telefónica local. Cuando un empleado entró en la línea, Keith pidió ser conectado a una persona en las reivindicaciones.

Otra espera, y luego una voz. Ahora Keith cambió de marcha, "Hola", comenzó. "Esto es Gregory Adams, la Oficina de Distrito 329. Oye, estoy tratando de llegar a un ajustador de reclamos que maneja un número de cuenta que termina en 6363, y el número que va a tener una máquina de fax. "

"Eso es Mod 2," dijo el hombre. Levantó la vista del número y se lo dio a Keith.

A continuación llamó Mod 2. Cuando de mayo de Linn respondió él cambió los sombreros y se fue a través de la rutina de ser de la Oficina del Inspector General, y el problema de otra persona tener que utilizar su ordenador. Ella le dio el la información que estaba buscando, y acordaron hacer todo lo que podía cuando necesitaba ayuda en el futuro.

Con el análisis de la

¿Qué hizo que este enfoque fue efectivo el juego de la simpatía de los empleados con la historia de otra persona utilizando su ordenador y "mi jefe no está contento con . me "La gente no mostrar sus emociones en el trabajo muy a menudo, y cuando lo hacen, puede rollo de la derecha sobre la defensa de alguien más comunes contra la ingeniería social ataques. El truco emocional de "estoy en problemas, no me puedes ayudar?" fue todo lo que llevó a ganar el día.

La inseguridad social

Aunque parezca increíble, la Administración del Seguro Social ha publicado una copia de la totalidad de su Programa de Operaciones Manual en la Web, repleta de información que es útil para su pueblo, pero también es increíblemente valioso para los ingenieros sociales. Contiene abreviaturas, jerga, y las instrucciones de cómo solicitar lo que desee, se describe en esta historia.

¿Quieres saber más información sobre el interior de la Administración del Seguro Social? Sólo tienes que buscar en Google o introduzca la siguiente dirección en su navegador: http://policy.ssa.gov/poms.nsf/. A menos que la agencia ya ha leído esta historia y eliminado el manual para el momento en que usted lea esto, que usted encontrará en línea las instrucciones que incluso dan información detallada sobre los datos de un empleado de SSA se permite dar a las fuerzas del orden. En términos prácticos, esto incluye a cualquier comunidad ingeniero social que puede convencer a un empleado de SSA que es de una aplicación de la ley la organización. El atacante no podría haber tenido éxito en la obtención de este información de uno de los empleados que se encarga de las llamadas telefónicas de la general público. El tipo de ataque Keith utiliza sólo funciona cuando la persona en el

el extremo receptor de la llamada es a alguien cuyo número de teléfono no está disponible para la público, y que por lo tanto tiene la expectativa de que llamar a nadie debe ser alguien en el interior - otro ejemplo de la seguridad clandestino ". Los elementos que ayudó a este ataque a trabajar fueron:

Conocer el número de teléfono al Ministerio de Defensa.

Conocer la terminología que utiliza - numident, ALPHADENT y DEQY.

Haciéndose pasar por la Oficina del Inspector General, que todos los federales empleado del gobierno conoce como una agencia de investigación de todo el gobierno con amplios poderes. Esto le da al atacante un aura de autoridad.

Un detalle interesante: Los ingenieros sociales parecen saber cómo hacer peticiones por lo que casi nadie piensa, "¿Por qué me llamas" -. aun cuando, lógicamente, tendría más sentido si la llamada se había ido a algún otro persona en algún departamento completamente diferente. Tal vez simplemente ofrece una ruptura de la monotonía de la rutina diaria para ayudar a la persona que llama que la víctima descuentos lo inusual de la llamada parece.

Por último, el atacante en este incidente, no contentos con conseguir la información que acaba para el caso que nos ocupa, quería establecer un contacto que podríamos llamar con regularidad. Él de lo contrario podría haber sido capaz de usar una táctica común para el ataque simpatía - "Se me cayó el café sobre el teclado." Que no era bueno aquí, sin embargo, debido a que un teclado puede ser reemplazado en un día.

Por lo tanto se utiliza la historia de otra persona utilizando su equipo, que podría razonablemente cadena a partir de semana: "Sí, pensé que tendría su propio ordenador ayer, pero un vino y otro tipo sacó algún tipo de acuerdo y lo consiguió en su lugar. Así que este payaso es todavía aparece en mi cubículo. "Y así sucesivamente. Pobre de mí, necesito ayuda. Funciona como un encanto.

Una simple llamada

Uno de los principales obstáculos a un atacante es hacer que el sonido de su petición razonable algo típico de las solicitudes que se presentan en la jornada de trabajo de la víctima, algo que no ponga a la víctima de forma exagerada. Al igual que con muchas otras cosas en la vida, hacer una petición lógica de sonido puede ser un desafío, un día, pero el siguiente, que puede ser un pedazo de la torta.

Llame a Mary H. Teléfono

Fecha / hora: lunes, 23 de noviembre de 7:49 A.M.

Lugar: Mauersby y Storch de Contabilidad, de Nueva York

Para la mayoría de la gente, el trabajo de contabilidad es el crujido de número y conteo de frijol, generalmente considerado como un de lo más agradable tener un tratamiento de conducto. Afortunadamente, no todos ven el trabajo de esa manera. Mary Harris, por ejemplo, que se encuentra su trabajo como contador principal absorbente, parte de la razón por la que fue uno de los más empleados dedicados a su contabilidad firme.

Sobre el particular lunes, María llegó temprano para conseguir una ventaja en lo que espera que sea un día largo, y se sorprendió al encontrar a su teléfono sonando. Ella lo cogió y le dio su nombre.

"Hola, esto es Peter Sheppard. Estoy con apoyo Arbuclde, la empresa que hace soporte técnico para su empresa. Hemos registrado un par de quejas sobre el fin de semana de personas que tienen problemas con las computadoras allí. Pensé que podría solucionar los problemas antes de que todo el mundo viene al trabajo esta mañana. ¿Tiene cualquier problema con el ordenador o la conexión a la red? "

Ella le dijo que no sabía todavía. Volvió la computadora y al mismo tiempo que se el arranque, explicó lo que quería hacer.

"Me gustaría hacer un par de pruebas con usted, él dijo." Yo soy capaz de ver en la pantalla las pulsaciones de teclas que escribe, y quiere asegurarse de que van a través de la red correctamente. Así que cada vez que escribe un derrame cerebral, quiero que me digas lo que es,

y me voy
ver si la misma letra o número que aparece aquí. ¿De acuerdo? "
Con no visiones de pesadilla de su equipo de trabajo y un día frustrante de no
ser capaz de conseguir cualquier trabajo hecho, estaba más que feliz de ayudar a este hombre
ella. Después de unos momentos, ella le dijo: "Tengo la pantalla de inicio de sesión, y yo voy a
tipo en mi ID. Lo estoy escribiendo ahora - M ... A. .. R. .. Y. .. D. "
"Muy bien hasta ahora", dijo. "Estoy viendo que aquí. Ahora, seguir adelante y escriba su
contraseña, pero no me digas lo que es. Nunca nadie debe decirle a su
contraseña, ni siquiera de soporte técnico. Voy a ver asteriscos aquí - la contraseña es
protegidos por lo que no se puede ver:. Nada de esto era cierto, pero que tiene sentido a María. Y
luego dijo: "Dime una vez que su equipo ha puesto en marcha".
Cuando ella dijo que estaba en funcionamiento, le había abierto dos de sus aplicaciones, y
informó que se puso en marcha "muy bien".
María se sintió aliviado al ver que todo parecía estar funcionando con normalidad. Peter
dijo: "Me alegro de haber podido asegurarse de que usted será capaz de utilizar su equipo está
bien. Y
escuchar ", continuó," que acaba de instalar una actualización que permiten a las personas a
cambiar sus
contraseñas. ¿Estaría usted dispuesto a tomar un par de minutos conmigo, así que puedo
ver si conseguimos que funcione bien?
Ella estaba agradecida por la ayuda que le había dado y acordado con facilidad. Pedro habló
ella a través de los pasos de poner en marcha la aplicación que permite al usuario cambiar
contraseñas, un elemento estándar del sistema operativo Windows 2000. "Ir
por delante e introduzca su contraseña ", le dijo." Pero recuerda que no debes decirlo en
voz alta. "
Cuando hubo hecho esto, Pedro dijo: "Solo por esta prueba rápida, cuando se le pide su
nueva contraseña, introduzca "test123. Vuelva a escribirla en el cuadro de verificación, y
haga clic en Enter ".
Él la acompañó a través del proceso de desconexión del servidor. Él le había
esperar un par de minutos, a continuación, conecte de nuevo, esta vez tratando de conectarse
con su
nueva contraseña. Funcionó a las mil maravillas, Peter parecía muy contento, y habló de su
a través del cambio de vuelta a su clave original o elegir uno nuevo - una vez
más advirtiendo sobre su no decir la contraseña en voz alta.
"Bueno, María," Pedro le dijo. "No se encontró ningún problema, y eso es genial. Oye,
si hay algún problema no llegar, no dude en llamar aquí a Arbuckle. Estoy por lo general en
proyectos especiales, pero nadie aquí que las respuestas le pueden ayudar. "Ella se lo agradeció
y se despidieron.
La historia de Pedro
La palabra había tenido tiempo de Peter - un número de las personas en su
comunidad que habían ido a la escuela con él había oído que se convirtió en una especie
de un genio de las computadoras, que a menudo puede encontrar información útil que otras
personas
no podría conseguir. Cuando Alicia Conrad acudían a él para pedirle un favor, me dijo que no al
principio.
¿Por qué debería ayudarte? Cuando se encontró con ella una vez y trató de pedir una cita, ella
se había convertido él por frío.
Pero su negativa a ayudar a no parecía darle una sorpresa. Ella dijo que no creía que fuera
algo que podía hacer de todos modos. Que era como un reto, porque, por supuesto,
estaba seguro de poder. Y así fue como llegó a
de acuerdo.
Alice le había ofrecido un contrato para un trabajo de consultoría para una comercialización
empresa, pero los términos del contrato no parecía muy bueno. Antes de volver a
pedir un mejor trato, que ella quería saber qué términos había otros consultores en
sus contratos.

Así es como Pedro le dice a la historia.
Yo no le diría a Alice, pero me bajé en la gente que quiere que yo haga algo que
no creo que pueda, cuando yo sabía que iba a ser fácil. Bueno, no es fácil, precisamente, no
este momento. Haría falta un poco de hacer. Pero que estaba bien.
Que yo pudiera mostrar lo inteligente era realmente.
Un poco después de las 7:30 lunes por la mañana, llamé a las oficinas de la empresa de marketing y
tiene la recepcionista, le dije que estaba con la compañía que maneja su pensión
planes y necesito hablar con alguien en contabilidad. Si hubiera dado cuenta si alguno de los
Las personas de contabilidad habían llegado todavía? Ella dijo: "Creo que vi a María venir en unos pocos
minutos, voy a tratar de su para usted. "
Cuando María cogió el teléfono, le conté mi pequeña historia sobre el equipo
problemas, que fue diseñado para darle el nerviosismo por lo que estaría encantado de colaborar.
Tan pronto como yo le había hablado a través de cambiar su contraseña, entonces rápidamente sesión
en el sistema con la contraseña temporal mismo que yo le había pedido que el uso,
test123.
Aquí es donde entra en el dominio - He instalado un pequeño programa que
me permitió el acceso al sistema informático de la compañía cuando yo quisiera, con un
contraseña secreta de mi cuenta. Después de colgar con María, mi primer paso fue eliminar
la pista de auditoría para que nadie ni siquiera sabía que yo había estado en su sistema. Fue
fácil. Después de elevar mis privilegios del sistema, tuve la oportunidad de descargar una
programa que se llama clearlogs que he encontrado en un sitio Web relacionado con la seguridad en
www.ntsecurity.nu.
Tiempo para el trabajo real. Hice una búsqueda de cualquier documento con el contrato de palabra "en
el nombre del archivo, y descargar los archivos. Luego busqué un poco más y entró en
la veta madre - el directorio que contiene todos los informes de pago de consultores. Así que
juntar todos los expedientes de los contratos y una lista de pagos.
Alicia pudo poros a través de los contratos y ver cuánto están pagando otros
consultores. Vamos a hacer lo donkeywork de estudiar minuciosamente a través de todos esos archivos. Tuve
hecho lo que me pidió.
De los discos que poner los datos en, imprimí algunos de los archivos, así que
podía mostrar la evidencia. Me hizo verme a comprar la cena. Usted debe
he visto su cara cuando ella hojeó la pila de papeles. "No hay manera",
, dijo. "De ninguna manera".
No he traído el disco conmigo. Ellos fueron el cebo. Me dijo que tenía que venir
a conseguir, con la esperanza de que había tal vez quiere mostrar su agradecimiento por el favor que
como ella lo hizo.
Mitnick MENSAJE
Es increíble lo fácil que es para un ingeniero social para que la gente de hacer las cosas basado en
en la forma en que las estructuras de la solicitud. La premisa es provocar una respuesta automática
basado en principios psicológicos, y confiar en la gente toma atajos mentales
cuando perciben que la persona que llama como un aliado.
Con el análisis de la
La llamada de Pedro de teléfono a la empresa de marketing representa la forma más básica de ingeniería social - un simple intento que necesita poca preparación, trabajó en el
primer intento, y sólo tomó unos minutos para que fuera.
Mejor aún, María, la víctima, no tenía ninguna razón para pensar que cualquier tipo de truco o

artimaña
había sido jugado en ella, no hay razón para presentar una denuncia o levantar un alboroto.
El esquema de trabajo a través del uso de Peter de tres tácticas de ingeniería social. Primero
obtuvo la cooperación inicial de María mediante la generación de miedo - haciéndole pensar que
su
equipo no se pueda utilizar. Luego tomó el tiempo para tener su apertura de dos de sus
aplicaciones para que pudiera estar seguro de que estaban funcionando bien, el fortalecimiento
de la
relación entre los dos de ellos, un sentido de ser aliados. Finalmente, consiguió su
una mayor cooperación de la parte esencial de su tarea, jugando con su gratitud
por la ayuda que había proporcionado en asegurarse de que su equipo estaba bien.
Diciéndole que ella nunca debe revelar su contraseña, no debe revelarse ni siquiera al
él, Pedro hizo un trabajo minucioso y sutil de convencerla de que le preocupaba
sobre la seguridad de los archivos de su compañía. Esto incrementó su confianza en que él
debe ser legítimo porque estaba protegiendo a ella y la empresa.
La operación policial
Imagen de esta escena: El gobierno ha estado tratando de tender una trampa a un hombre
llamado
Arturo Sánchez, quien ha estado distribuyendo películas gratuitas a través de Internet. La
Los estudios de Hollywood dicen que está violando sus derechos de autor, él dice que está
tratando de
empujón a reconocer un mercado tan inevitable que van a empezar a hacer algo
sobre la fabricación de nuevas películas disponibles para descargar. Señala (correctamente) que
esto podría ser una enorme fuente de ingresos para los estudios que parecen ser
ignorando por completo.
Orden de registro, por favor
De vuelta a casa una noche, comprueba las ventanas de su apartamento de
lado de la calle y las comunicaciones las luces están apagadas, a pesar de que siempre deja un
en cuando sale.
Golpea y golpea a la puerta de un vecino hasta que se despierte el hombre, y aprende
que había hecho una redada policial en el edificio. Pero hicieron los vecinos
permanecer abajo, y todavía no está seguro de lo que entró en apartamento. Sólo
sabe que la izquierda llevar cosas pesadas, sólo que estaban envueltos y
No podría decir lo que eran. Y no tener a nadie y esposado.
Arturo mira su apartamento. La mala noticia es que hay un documento de la policía
exigir que se llame de inmediato y hacer una cita para una entrevista
plazo de tres días. La peor noticia es que sus computadoras están desaparecidos.
Arturo se pierde en la noche, va a quedar con un amigo. Pero la incertidumbre
roe en él. ¿Cuánto sabe la policía? Han cogido con él en
pasado, pero le dejó una oportunidad de huir? ¿O se trata de algo completamente distinto,
algo que puede aclarar, sin tener que salir de la ciudad?
Antes de seguir leyendo, deténgase y piense por un momento: ¿Puede usted imaginar que
cualquier forma de
podría descubrir lo que la policía sepa de ti? Suponiendo que usted no tiene ningún
contactos políticos o amigos en el departamento de policía o la fiscalía s, se
Puedes imaginar que haya ninguna manera de que usted, como ciudadano de a pie, podría
conseguir este
información? O que incluso alguien con habilidades de ingeniería social puede?
Estafa de la Policía
Arturo satisfecha su necesidad de saber de esta manera: En primer lugar, se puso el teléfono
número de una tienda de fotocopias cercana, los llamó y les pidió su número de fax.
Entonces él llamó a la oficina del fiscal de distrito, y pidió para los expedientes. Cuando se le
conectado con la oficina de registros, se presentó como un investigador de la
Condado de Lake, y dijo que necesitaba hablar con el empleado que los archivos de la activa
órdenes de allanamiento.

"Yo", dijo la señora. "Oh, muy bien", respondió. "Debido a que irrumpieron en una sospechoso la noche anterior y estoy tratando de localizar a la declaración jurada. "
"Los archivos de la dirección," le dijo ella.
Él dio su dirección y su voz sonaba casi emocionado. "Oh, sí", que con burbujas "que saber acerca de eso. "El derecho de autor Caper".
"Ese es el uno," dijo. "Estoy buscando a la declaración jurada y copia de la orden.
"Oh, lo tengo aquí mismo."
"Gran", dijo. "Oye, estoy en el campo y tengo una reunión con el secreto Servicio en este caso si yo quince minutos. He estado tan distraído últimamente, me fui el archivo en su casa, y nunca voy a hacer allí y volver en el tiempo. ¿Puedo obtener copias de usted? "
"Claro, no hay problema voy a hacer copias;.. Usted puede venir a la derecha una y recogerlos"
"Gran", dijo. "Eso está muy bien. Pero, oiga, yo estoy en el otro lado de la ciudad. Es posible que usted podría enviarlos por fax a mí? "
Que creó un pequeño problema, pero no insuperables. "No tenemos un fax a aquí en los registros ", dijo." Pero tienen una planta baja en la oficina del Secretario que podría dejarme usar. "
Él dijo: "Voy a llamar a la oficina del secretario y la levantó".
La señora en la oficina del secretario dijo que estaría encantado de cuidar de él, pero quería saber "¿Quién va a pagar por él?" Ella necesitaba un código contable.
"Voy a por el código y te llamo de vuelta", le dijo.
Luego llamó a la oficina del fiscal, una vez más se identificó como un oficial de policía y simplemente le pidió a la recepcionista: "¿Qué es el código de contabilidad de la oficina del fiscal?"
Sin dudarlo, le dijo.
Volver a llamar a la oficina del secretario de proporcionar el número de contabilidad le dio la excusa para manipular a la señora un poco más: Él le habló a caminar piso de arriba para obtener las copias de los documentos a enviar por fax.
NOTA
¿Cómo un ingeniero social conocer los detalles de la operación tantas - la policía departamentos, oficinas fiscales, las prácticas de la compañía telefónica, la organización de empresas que están en los campos de utilidad en sus ataques, tales como telecomunicaciones y la informática? Porque es su negocio para averiguarlo. Este el conocimiento es una acción de los ingenieros sociales en el comercio, porque la información puede ayudar a
él en sus esfuerzos para engañar.
Borrar sus huellas
Arturo todavía tenía un par de pasos a seguir. Siempre había una posibilidad que alguien huele algo raro, y que podría llegar a la tienda de fotocopias para encontrar una pareja de detectives, vestido de manera informal y tratando de parecer ocupado hasta
alguien se presentó pidiendo que el fax particular. Esperó un rato, y luego llamó a la oficina del secretario de vuelta para comprobar que la señora había enviado el fax. Bien hasta ahora.
Llamó a otro almacén de copia de la misma cadena en la ciudad y utiliza el engaño sobre la forma que estaba "complacido con su manejo de un trabajo y desea escribir la gerente de una carta de felicitación, ¿cómo se llama? "Con esa pieza esencial de la información, llamó a la tienda de la primera copia de nuevo y dijo que quería hablar con el gerente. Cuando el hombre cogió el teléfono, Arturo dijo: "Hola, esto es Edward en la tienda 628 en Hartfield. Mi manager, Anna, me dijo que te llame. Tenemos un cliente que es muy molesto - alguien le dio el número de fax de la tienda equivocada. Ya está aquí la espera de un fax importante, sólo el número que se le dio es para su tienda ". El director prometió que una de sus personas a encontrar el fax y enviarlo en el almacén de Hartfield inmediatamente.
Arturo ya estaba esperando en la tienda de segunda cuando el fax llegó allí. Una vez

que lo tenía en la mano, volvió a llamar a la oficina del secretario de decir la señora, gracias, y "No es necesario para llevar a los ejemplares al piso de arriba, sólo puede tirar lejos ahora. "Entonces llamó el gerente de la primera tienda y le dijo, también, para tirar su copia del fax. De esta manera, no habría ningún registro de lo que había tenido lugar, en caso de que alguien más tarde llegó a hacer preguntas.
Los ingenieros sociales sabe que nunca puede ser demasiado cuidadoso.
Dispuestos de esta manera, Arturo ni siquiera tener que pagar cargos en la tienda de la primera copia para la recepción de fax y enviarlo de nuevo a la tienda de segunda. Y si se Resultó que la policía se presentó en la primera tienda, Arturo ya se tener su fax y mucho tiempo desaparecido en el momento en que podría arreglar para que la gente a la segunda ubicación.
El final de la historia: La declaración jurada y garantiza mostró que la policía había bien documentado evidencia de la copia de películas de Arturo actividades. Eso era lo que necesitaba saber. Antes de la medianoche, había cruzado la línea de estado. Arturo estaba en el paso a una nueva vida, en otro lugar con una nueva identidad, listo para comenzar de nuevo en su campaña.
Con el análisis de la
Las personas que trabajan en cualquier oficina del fiscal de distrito, en cualquier lugar, están en constante contacto con los agentes del orden - responder a las preguntas, lo que hace los acuerdos, tomar mensajes. Cualquier persona con agallas suficientes para llamar y decir que es un oficial de la policía, alguacil, o cualquiera que sea probable que se tomarán la palabra.
A menos que sea obvio que él no conoce la terminología, o si él es nervioso y tropieza con sus palabras, o de alguna otra manera no suena auténtica, puede ni siquiera se hizo una sola pregunta para verificar su afirmación. Eso es exactamente lo que pasó aquí, con dos diferentes los trabajadores.
Mitnick MENSAJE
La verdad del asunto es que nadie es inmune a ser engañados por un bien social ingeniero. Debido al ritmo de vida normal, no siempre se toman el tiempo para decisiones bien pensadas, incluso en asuntos que son importantes para nosotros. Complicado situaciones, la falta de tiempo, el estado emocional o la fatiga mental puede distraernos. Así que tomamos un atajo mental, tomar nuestras decisiones sin analizar los información cuidadosa y completamente, un proceso mental conocido como automático de responder. Esto es cierto incluso para los federales, estatales, y la policía local los funcionarios. Todos somos humanos.
La obtención de un código de carga necesaria se maneja con una sola llamada telefónica. Entonces Arturo jugado la carta de solidaridad con la historia de "una reunión con el secreto Servicio en quince minutos, he estado distraído y dejó el archivo en su casa. "Ella naturalmente, sentía pena por él, y salió de su manera de ayudar.
A continuación, mediante el uso de no uno sino dos tiendas de copiado, Arturo se hizo extremar las precauciones cuando él fue a recoger el fax. Una variante de este que hace que el fax aún más difícil seguir la pista: En lugar de tener el documento enviado a otra tienda de copia, el atacante puede dar lo que parece ser un número de fax, pero en realidad es una dirección en un servicio de Internet gratuito que se recibe un fax de forma automática para usted y lo remitirá al su dirección de correo electrónico. De esta manera se puede descargar directamente a la del atacante equipo, y nunca tiene que mostrar su rostro en cualquier lugar donde alguien podría más tarde ser capaz de identificar. Y la dirección de correo electrónico y número de fax electrónico se puede

abandonó tan pronto como la misión ha sido cumplida.
Vuelta a las tablas
Un joven al que llamaremos Michael Parker fue una de esas personas que descubrió una
poco más tarde que los trabajos mejor pagados en su mayoría destinados a personas con títulos
universitarios. Él
tenido la oportunidad de asistir a una universidad local, con una beca parcial y la educación
préstamos, pero eso significaba trabajar en las noches y fines de semana para pagar el alquiler,
comida, gas, y
seguros de automóviles. Michael, que siempre me ha gustado encontrar atajos, pensé que tal vez
no
era otra manera, que dio sus frutos rápidamente y con menos esfuerzo. Debido a que había
estado aprendiendo acerca de las computadoras desde el momento en que llegó a jugar con uno
a diez años de edad
y quedó fascinado con saber cómo funcionaban, decidió ver si él
podría "crear" su licenciatura propia acelerado en ciencias de la computación.
Graduarse - Sin honores
Podía haber entrado en los sistemas informáticos de la universidad estatal, que se encuentra la
registro de alguien que se había graduado con un agradable B + o A media-, copió el
registro, puso su propio nombre en él, y añadió que los registros de que el año
clase de graduación. Pensando en esto a través, de alguna manera sentirse incómodos con la
idea,
se dio cuenta de que debe haber otros registros de un estudiante de haber sido en el campus -
registros de pago de matrícula, la oficina de vivienda, y quién sabe qué más. La creación de
sólo el registro de los cursos y grados se deja demasiadas lagunas.
Trazado más, a tientas, se le ocurrió que podía llegar a su
objetivo de ver si la escuela se había graduado con el mismo nombre que el suyo, que había
obtuvo un grado de la informática en cualquier momento durante un lapso apropiado de años. Si
Por lo tanto, él podría dejar el otro Michael Parker, número de seguro social
formas de solicitud de empleo, cualquier empresa que comprobar el nombre y social
número de seguro con la universidad se le dijo que sí, que tenía la
afirmó grado. (No sería obvio para la mayoría de la gente, pero era obvio para él
que podía poner un número de seguro social en la solicitud de empleo y, si
contratado, puso su número real propia de las formas de nuevos empleados. La mayoría de las
empresas
nunca se le ocurriría para comprobar si un nuevo empleado había utilizado un número diferente
anteriormente en el proceso de contratación.)
Inicio de sesión en problemas
¿Cómo encontrar un Michael Parker en los registros de la universidad? Se fue de él como
lo siguiente:
Ir a la biblioteca principal del campus universitario, se sentó frente a una computadora
terminal, se levantó a través de Internet, y acceder a sitios Web de la universidad. A continuación,
llamó a la oficina del Registrador. Con la persona que contestó, se dirigió a través de un
de las rutinas de la ingeniería por ahora familiar social: "Estoy llamando desde el
Centro de Cómputo, estamos haciendo algunos cambios en la configuración de red y
queremos asegurarnos de que no
interrumpir el acceso del usuario. Qué servidor se conecta a? "
"¿Qué quieres decir, un servidor, se le preguntó.
"¿Qué equipo se conecta a cuando usted necesita para buscar académico de los estudiantes
de la información.
La respuesta, admin.rnu.edu, le dio el nombre del equipo en el estudiante
registros fueron almacenados. Esta fue la primera pieza del rompecabezas: ahora sabía que su
objetivo de la máquina.
LINGO
Terminal tonto Un terminal que no contiene su propio microprocesador.
Terminales tontas sólo puede aceptar comandos simples y caracteres de visualización de texto

y los números.
Escribió que la URL en el equipo y no obtuvo respuesta - como se esperaba, no hubo
un firewall que bloquea el acceso. Y corriendo un programa para ver si podía conectar a cualquier
de los servicios que se ejecutan en ese equipo, y encontrar un puerto abierto con Telnet
funcionamiento del servicio, que permite a un ordenador para conectarse remotamente a otro
ordenador y acceder a ella, como si directamente conectado con un terminal tonto. Todo lo que
tendría que tener acceso sería el ID de usuario y una contraseña estándar.
Él hizo otra llamada a la oficina de registro, esta vez de escuchar con atención para
asegurarse de que estaba hablando con una persona diferente. Se levantó una señora, una y otra vez que decía
ser del Centro de Computación de la universidad. Ellos fueron la instalación de una nueva producción
sistema de registros administrativos, le dijo. Como un favor, que le gustaría conectar su
al nuevo sistema, aún en modo de prueba, para ver si podía acceder académico de los estudiantes
registros bien. Le dio la dirección IP para conectarse a, y habló ella a través del
proceso.
De hecho, la dirección IP la llevó al equipo Michael estaba sentado en el
biblioteca del campus. Usando el mismo proceso descrito en el capítulo 8, que había creado una
Ingresar simulador - un signo en la trampa de pantalla - que buscan al igual que el que ella se
acostumbrados a ver cuando se va en el sistema de archivos del estudiante. "No es
de trabajo ", le dijo." Se sigue diciendo que "Login incorrect.
Por ahora el simulador de inicio de sesión se había alimentado las pulsaciones de su nombre de cuenta y
contraseña a la terminal de Michael, misión cumplida. Él le dijo, "Oh, algunos de los
las cuentas no han sido traídos sin embargo, a esta máquina. Vamos a poner a su
cuenta, y yo te llamaré. "cuidadoso acerca de atar cabos sueltos, como cualquier
ingeniero social competente tiene que ser, que sería un punto de llamar más tarde para
decir que el sistema de prueba no funcionaba bien, sin embargo, y, si estaba bien con ella
que yo llamaría de nuevo a ella oa una de las otras personas que cuando se había dado cuenta de
lo que estaba causando el problema.
El Secretario útiles
Ahora Michael sabía lo que necesitaba sistema informático de acceso, y tenía una
ID de usuario y contraseña. Pero, ¿qué órdenes iba a necesitar a fin de buscar la
archivos para obtener información sobre un graduado de ciencias de la computación con el nombre correcto y
fecha de la graduación? La base de datos de los estudiantes sería una propiedad, creado en
la escuela para satisfacer las necesidades específicas de la universidad y el Registro de
oficina, y que tienen una forma única de acceder a la información en la base de datos.
El primer paso en la limpieza de este último obstáculo: Averigüe quién podría guiarlo a través de la
misterios de la búsqueda de la base de datos de los estudiantes. Llamó a la oficina del Secretario
de nuevo, esta vez llegando a una persona diferente. Él era de la oficina del Decano
de Ingeniería, dijo a la señora, y le preguntó: "¿Quién se supone que vamos a pedir
ayuda cuando estamos teniendo problemas para acceder a los académicos de los estudiantes rues.
Minutos más tarde estaba hablando por teléfono con el administrador de la base de la universidad,
tirando de la Ley de simpatía:. "Estoy Mark Sellers, en la oficina de registro Uno se siente como
haber tenido compasión de un hombre nuevo? Perdón por ser te está llamando, pero todos están en una reunión de este
por la tarde y no hay nadie cerca para ayudarme. Tengo que recuperar una lista de todos los
se gradúa con un grado de la informática, entre 1990 y 2000. Ellos lo necesitan
al final del día y si no lo tiene, no puede tener este trabajo por mucho tiempo. Usted

dispuestos a ayudar a un chico en problemas? "Ayudar a la gente se parte de lo que esta administrador de la base, así también era paciente extra mientras hablaba por el paso de Michael paso en el proceso.
En el momento de colgar, Michael se había descargado la lista completa de equipo los graduados en ciencias de los años. A los pocos minutos que había corrido una búsqueda, ubicado a dos Parkers Michael, elegido uno de ellos, y obtuvo la de tipo social número de seguro social, así como otra información pertinente almacenada en la base de datos. Él acababa de convertirse en "Michael Parker, Licenciatura en Ciencias de la Computación, graduado con honores, 1998. "En este caso, el" BS "era únicamente apropiado.
Con el análisis de la
Este ataque utiliza un truco que no he hablado antes: el atacante pidiendo a la administrador de la organización de base de datos le guiará por los pasos de la realización a cabo un proceso informático que no sabía cómo hacer. Un potente y eficaz de giro de las tablas, este es el equivalente a pedirle a la dueña de una tienda para ayudar a lleva una caja que contiene los elementos que ya se robaron de sus estantes a su coche.
Mitnick MENSAJE
Los usuarios de computadoras a veces ni idea de las amenazas y vulnerabilidades asociados con la ingeniería social que existen en el mundo de la tecnología. Ellos tienen acceso a la información, sin embargo, carecen de un conocimiento detallado de lo que pueda ser a ser una amenaza a la seguridad. Un ingeniero social se dirigirá a un empleado que tiene poco comprensión del valor que tiene la información que se busca es, por lo que el objetivo es más probabilidades de acceder a la solicitud del extranjero.
PREVENCIÓN DE LA CON
Simpatía, la culpa, y la intimidación son tres factores desencadenantes psicológicos muy popular utilizado por el ingeniero social, y estas historias han demostrado las tácticas de la acción. Pero, ¿qué pueden hacer usted y su empresa para evitar este tipo de ataques?
Protección de datos
Algunas de las historias en este capítulo hincapié en el peligro de enviar un archivo a alguien no lo sé, aun cuando esa persona es (o parece ser) un empleado, y el archivo se envía internamente, a una dirección de correo electrónico o la máquina de impuestos en el de la empresa.
Política de la empresa de seguridad tiene que ser muy específico acerca de las garantías para entrega de los datos de valor a alguien que no conoce personalmente al remitente. Exigente procedimientos deben ser establecidos para la transferencia de archivos con información sensible. Cuando la solicitud es de alguien que no conozco personalmente, debe ser claro los pasos a seguir para la verificación, con diferentes niveles de autenticación en función de la sensibilidad de la información.
Aquí están algunas técnicas a considerar:
Establecer la necesidad de saber (que puede requerir la obtención de la autorización de la información designada propietario).
Mantener un registro personal o departamental de estas transacciones.
Mantener una lista de personas que han sido especialmente entrenados en los procedimientos y que son de confianza para autorizar el envío de información sensible. Requerir que sólo estas personas serán autorizadas para enviar la información a nadie fuera del grupo de trabajo.
Si la solicitud de los datos se hace por escrito (correo electrónico, fax o correo electrónico) adopte medidas adicionales seguridad de los pasos para verificar que la solicitud en realidad procedían de la persona que aparece que han venido.
Acerca de las contraseñas
Todos los empleados que pueden acceder a información sensible - y que hoy

significa que prácticamente todos los trabajadores que usa una computadora - tienen que entender que
actos simples como cambiar la contraseña, ni siquiera por unos momentos, puede llevar a una violación de seguridad importante.
Formación en seguridad tiene que tratar el tema de las contraseñas, y que tiene que centrarse en parte sobre cuándo y cómo cambiar tu contraseña, lo que constituye un nivel aceptable contraseña, y los peligros de dejar que alguien más se involucran en el proceso.
La capacitación especial debe transmitir a todos los empleados que deben ser
Sospeche de cualquier solicitud que involucra sus contraseñas.
En la superficie parece ser un simple mensaje a transmitir a los empleados. Es
No, porque para apreciar esta idea requiere que los empleados comprender cómo una simple actuar como el cambio de contraseña puede llevar a un compromiso de seguridad. Usted puede decir
niño "Mire a ambos lados antes de cruzar la calle", pero hasta que el niño entiende
Por eso es importante, usted está confiando en la obediencia ciega. Y reglas que obliguen a ciegas
la obediencia son generalmente ignorados u olvidados.
NOTA
Las contraseñas son como un foco central de los ataques de ingeniería social que le dedicamos un
sección aparte para el tema en el capítulo 16, donde se encuentra específicos
las políticas recomendadas en la gestión de contraseñas.
Un Punto de Información Central
Su política de seguridad debe proporcionar a una persona o un grupo designado como central punto de partida para informar sobre actividades sospechosas que parecen ser intentos de infiltración
su organización. Todos los empleados necesitan saber a quién llamar en cualquier momento se sospecha
un intento de intrusión electrónica o física. El número de teléfono del lugar de
que estos informes debe estar siempre a la mano para que los empleados no tienen que cavar ya que si se sospecha que el ataque se lleva a cabo.
Proteja su red
Los empleados tienen que entender que el nombre de un servidor de la computadora o red no trivial de información, sino que puede dar un conocimiento esencial atacante que
le ayuda a ganarse la confianza o encontrar la ubicación de la información que desea.
En particular, la gente, como los administradores de bases de datos que trabajan con software pertenecen a esa categoría de personas con conocimientos de tecnología, y que necesitan para operan bajo reglas especiales y muy restrictivos sobre la verificación de la identidad de
las personas que los llaman de información o asesoramiento.
Las personas que regularmente proporciona ninguna. tipo de ayuda de la computadora deben estar bien entrenados
¿En qué tipo de solicitudes deben ser banderas rojas, lo que sugiere que la persona que llama puede ser
intentar un ataque de ingeniería social.
Vale la pena señalar, sin embargo, que desde la perspectiva del administrador de la base de datos
en la última historia de este capítulo, la persona que llama se reunieron los criterios para ser legítimo: El
se llama desde el campus, y era evidente que estaba en un sitio que requiere un
nombre de cuenta y contraseña. Esto sólo pone de manifiesto una vez más la importancia de contar con procedimientos estandarizados para la verificación de la identidad de cualquier persona solicitar
información, especialmente en un caso como este, donde la llamada fue para pedir ayuda en obtener acceso a los registros confidenciales.
Todos estos consejos el doble para los colegios y universidades. No es noticia que

piratería informática es un pasatiempo favorito de muchos estudiantes universitarios, y en caso de que
También no es de extrañar que los registros de los estudiantes - y en ocasiones los registros profesores, así -
son un blanco tentador. Este abuso está tan extendida de que algunas empresas realmente considerar las escuelas en un ambiente hostil, y crear reglas de firewall que bloquean el acceso de las instituciones educativas con las direcciones que terminan en. edu.
El largo y el corto de él es que todos los expedientes de los estudiantes y el personal de cualquier tipo
debe ser visto como los principales objetivos de ataque, y deben estar bien protegidos como información confidencial.
Consejos de Formación
La mayoría de los ataques de ingeniería social son ridículamente fácil de defender contra el ... para
Cualquiera que sepa lo que en la búsqueda de.
Desde el punto de vista corporativo, existe una necesidad fundamental para una buena formación. Pero también hay una necesidad de algo más: una variedad de maneras de recordar a la gente lo que han aprendido.
Use pantallas de inicio que aparece cuando el ordenador del usuario está activada, con un de seguridad de mensajes diferentes cada día. El mensaje debe ser diseñado de manera que no desaparece automáticamente, pero requiere que el usuario haga clic en algún tipo de reconocimiento de que él / ella ha leído.
Otro enfoque que yo recomiendo es comenzar una serie de recordatorios de seguridad. Frecuente mensajes de aviso son importantes, un programa de sensibilización debe ser continuo y de nunca acabar. En la entrega de contenido, los recordatorios no deberían redactarse el mismo en cada caso. Los estudios han demostrado que estos mensajes son más eficacia recibió cuando varían en su redacción o cuando se utiliza en diferentes ejemplos.
Un excelente enfoque es utilizar blurbs corto en el boletín de la empresa. Este no debe ser una columna completa sobre el tema, a pesar de una columna de Seguridad sin duda muy valiosa. En su lugar, el diseño de un inserto de dos o tres columnas de ancho, algo así como un anuncio pequeña pantalla en su periódico local. En cada número de la boletín de noticias, presente un recordatorio de seguridad nuevo en este corto, llamativos camino.

Capítulo 9
El golpe inversa
El aguijón, que se menciona en este libro (y en mi opinión, probablemente el mejor película que s siempre han hecho acerca de una operación en contra), expone su argumento complicado en
fascinantes detalles. La operación encubierta en la película es una representación exacta de cómo
timadores superior ejecutar "el cable", refiere uno de los tres tipos de estafas importantes como "Contras grande". Si usted quiere saber cómo un equipo de profesionales se quita una estafa rastrillar en una gran cantidad de dinero en una sola noche, no hay libro de texto mejor.
Pero los inconvenientes tradicionales, cualquiera que sea su truco particular, ejecute de acuerdo a un
patrón. A veces una estratagema se trabaja en la dirección opuesta, lo que se denomina revertir la picadura. Este es un giro interesante en el que el atacante configura la situación para que las llamadas a la víctima de que el atacante en busca de ayuda, o un compañero de trabajo ha hecho un
solicitud, que el atacante está respondiendo.
¿Cómo funciona esto? Estás a punto de descubrir.
LINGO
REVERSE STING una estafa en la que la persona que está siendo atacado pide al atacante para ayudar a
EL ARTE DE Friendly Persuasion

Cuando la persona media evoca la imagen de un pirata informático, lo que
por lo general viene a la mente es la imagen de un halagüeño introvertido solitario,
nerd cuyo mejor amigo es su equipo y que tiene dificultades para llevar a
conversación, sino por la mensajería instantánea. El ingeniero social, que a menudo ha
habilidades de hacker, también tiene habilidades de la gente en el extremo opuesto del espectro - bien desarrollada
habilidades para usar y manipular a la gente que le permiten hablar de su
en conseguir la información de maneras que nunca hubiera creído posible.
Llamadas de Angela
Lugar: Valle de la rama, el Banco Industrial Federal.
Hora: 11:27 A.M.
Angela Wisnowski respondió a una llamada telefónica de un hombre que dijo que estaba a punto de
para recibir una herencia importante y que quería información sobre los diferentes tipos
de cuentas de ahorro, certificados de depósito, y las inversiones que cualquier otro
podría sugerir que estaría a salvo, pero ganan interés decente. Ella
explicó que había un buen número de opciones y le preguntó si le gustaría venir
y sentarse con ella para hablar de ellos. Él se iba en un viaje tan pronto como el
dinero llegó, dijo, y había un montón de arreglos que hacer. Así que empezó a
sugiere algunas de las posibilidades y darle los detalles de los tipos de interés,
¿qué pasa si usted vende un CD a principios, y así sucesivamente, al tratar de precisar su objetivos de inversión.
Parecía estar haciendo progresos cuando dijo: "Oh, lo siento, tengo que aprovechar esta
otra llamada. ¿A qué hora puedo terminar esta conversación con usted para que yo pueda hacer algo
las decisiones? ¿Cuándo te vas a comer? "Ella le dijo a 12:30 y me dijo que iba a tratar
para volver a llamar antes de esa fecha o al día siguiente.
Llamada de Luis
Los grandes bancos utilizan códigos de seguridad interna que cambian todos los días. Cuando alguien
de una rama de las necesidades de información de otra rama, que demuestre que tiene derecho
a la información mediante la demostración de que conoce el código del día. Para añadir un
grado de seguridad y flexibilidad, algunos de los principales bancos múltiples códigos de cada tema
día. En un traje de la Costa Oeste Voy a llamar a Banco Industrial Federal, cada empleado se encuentra
una lista de los cinco códigos para el día, identificada como la A a la E, en su ordenador
todas las mañanas.
Lugar: El mismo.
Tiempo:. 12:48 "M., el mismo día.
Louis Halpburn no creo que nada de ello cuando recibió una llamada en la tarde, una
llame al igual que otros que manejan regularmente varias veces por semana.
"Hola", dijo la persona que llama. "Este es Neil Webster. Voy a llamar a partir de 3182 en la rama Boston. Angela Wisnowski, por favor. "
"Ella está en el almuerzo. ¿Puedo ayudarte?"
"Bueno, ella dejó un mensaje que solicita a fax alguna información sobre uno de nuestros los clientes. "
La persona que llama sonaba como si hubiera sido un mal día.
"La persona que normalmente se ocupa de las peticiones está enfermo", dijo. "Tengo un
pila de éstos a hacer, es casi cuatro aquí y se supone que debo estar fuera de este
lugar para ir a una cita médica en media hora. "
La manipulación - dando todas las razones por la otra persona debe sentir pena
para él - era parte de ablandamiento de la marca. Continuó: "El que llevó a su
mensaje telefónico, el número de fax es ilegible. Es 213-algo. ¿Cuál es la
resto? "

Louis le dio el número de fax y la persona que llama, dijo, "Está bien, gracias.
Antes de que pueda enviar por fax este, tengo que pedirle Código B. "
"Pero usted me llamó", dijo con simplemente relajarse lo suficiente para que el hombre de Boston recibirían el mensaje.
Esto es bueno, la persona que llama pensamiento. Es tan cool cuando la gente no caiga en la primera
suave empujón. Si el, no resisten un poco, el trabajo es demasiado fácil y que podría empezar a recibir
perezoso.
Para Louis, dijo, "Tengo un gerente de la sucursal que acaba de cumplir paranoico
conseguir la verificación antes de enviar nada, es todo. Pero escucha, si no
nos necesitan para enviar por fax la información, está bien. No hay necesidad de verificar ".
"Mira", dijo Luis, "Angela estará de regreso en media hora o así. Puedo tener su llamada
de vuelta. "
"Voy a decirle que no podía enviar la información de hoy, porque no se
identificar esto como un reclamo legítimo por darme el código. Si no estoy de baja por enfermedad mañana, voy a llamarla en aquel entonces. "
"El mensaje dice:" Urgente ". No importa, sin verificación de mis manos están atadas.
Te voy a decir que traté de enviar, pero no le daría el código, ¿de acuerdo? "
Luis renunció bajo la presión. Un suspiro de fastidio vino volando
su camino por la línea telefónica.
"Bueno", dijo, "espere un minuto;. Tengo que ir a mi ordenador ¿Qué código se
que quieres? "
"B", dijo la persona que llama.
Él puso la llamada en espera y luego de un poco tomó la línea de nuevo. "Es 3184."
"Ese no es el código correcto."
"Sí, lo es - B es 3184."
"Yo no he dicho B, me dijo E."
"Oh, maldita sea. Espera un minuto".
Otra pausa mientras él volvió a mirar a los códigos.
"E 9697".
"9697 -. Derecha voy a tener el fax en el camino bien.?"
"Por supuesto. Gracias."
Llame a Walter
"Industrial Federal, esto es Walter."
"Oye, Walter, es Bob Grabowski en Studio City, sucursal 38," la persona que llamó dijo. "Yo
Necesito que tirar de una tarjeta de SIG en la cuenta del cliente y enviarlo por fax a mí. "La tarjeta de firmas,
o la tarjeta de firma, tiene algo más que la firma del cliente en él, sino que también ha
la identificación de la información, los elementos conocidos, como el número de seguro social, fecha de
nacimiento, nombre de soltera de su madre, e incluso a veces el número de licencia de conducir. Muy
útil para un ingeniero social.
"Claro que nada. ¿Cuál es el Código C?"
"Otro cajero está usando mi computadora en este momento", dijo la persona que llama. "Pero acabo de utilizar
B y E, y me acuerdo de aquellos. Me pregunta uno de ellos. "
"Bueno, ¿qué evaluación?"
"E 9697".
Unos minutos más tarde, Walter enviado por fax la tarjeta de SIG a lo solicitado.
Solla Donna de llamadas
"Hola, esto es el Sr. Anselmo".
"¿Cómo puedo ayudarle?"
"¿Cuál es ese número 800 se supone que debo llamar cuando quiera para ver si tiene un depósito

ha acreditado todavía? "
"Usted es un cliente del banco?"
"Sí, y yo no he usado el número en un tiempo y ahora no sé dónde
lo escribió. "
"El número es 800-555-8600."
"Está bien, gracias."
Cuento Vince Capelli
El hijo de un policía de Spokane calle, Vince sabía desde muy temprana edad que no estaba
va a pasar su vida como esclavos durante largas horas y arriesgando su cuello para un mínimo de
los salarios. Sus dos principales objetivos en la vida se hizo para salir de Spokane, y entrar en
negocio por sí mismo. La risa de sus matones en el instituto sólo
despidieron a todos los más - que pensaban que era divertido que fue arrestado etc
de iniciar su propio negocio, pero no tenía idea de lo que las empresas que podría ser.
Secreto Vince sabía que tenían razón. Lo único que se le daba bien era jugar
receptor en el equipo de béisbol de alta. Pero no lo suficiente para capturar un
becas universitarias, de ninguna manera lo suficientemente bueno para el béisbol profesional.
Entonces, ¿qué
negocio iba a ser capaz de empezar?
Una de las cosas a los chicos en el grupo de Vince nunca imaginado: Cualquier cosa
uno de ellos --- una navaja nueva, un par de guantes ingenioso caliente, un sexy
la nueva novia de Vince si lo admiraba, en poco tiempo el tema era suyo. No se lo roban,
o furtivamente a espaldas de nadie, no tenía que hacerlo. El tipo que había que
renunciar a ella voluntariamente, y luego nos preguntamos luego cómo había sucedido. Incluso
pidiendo Vince no le habría llegado a ninguna parte: no conocía a sí mismo.
La gente parecía que le permitiera tener lo que quisiera.
Vince Capelli fue un ingeniero social desde una edad temprana, a pesar de que nunca había
oído el término.
Sus amigos dejaron de reír, una vez que todos tenían diploma de escuela superior en la mano.
Mientras que los otros slogged por la ciudad en busca de trabajo en el que no tenía que
dicen: "¿Quieres patatas fritas con eso?" Vince padre lo envió a hablar con un policía de la vieja
amigo que había salido de la fuerza para empezar su propio negocio de investigación privada en
San
Francisco. Rápidamente se vio el talento de Vince para el trabajo, y lo llevó adelante.
Eso fue hace seis años. Odiaba la parte de conseguir los bienes de infieles
cónyuges, que implicaba horas dolorosamente aburrida de sentarse y mirar, pero me sentí
continuamente desafiado por las tareas de desenterrar la información de activos para los
abogados
tratando de averiguar si alguna rigidez miserable era lo suficientemente rico como para ser digno
de una demanda.
Estos trabajos le dieron muchas oportunidades de usar su ingenio.
Al igual que el tiempo que tuvo que buscar en las cuentas bancarias de un hombre llamado Joe
Markowitz. Joe había trabajado tal vez un acuerdo de sombra con una amiga de una sola vez de
la suya,
que ahora amigo quería saber si él demandó, fue Markowitz ras suficiente como para que
el amigo puede ser que consiga algo de su dinero de vuelta?
Vince primer paso sería el de encontrar al menos uno, pero de preferencia dos, de la
códigos de seguridad del banco para el día. Eso suena como un desafío casi imposible:
¿Qué diablos podría inducir a un empleado del banco para golpear un punto débil en su propio
sistema de seguridad? Pregúntate a ti mismo - si usted quería hacer esto, ¿tienes alguna idea
de cómo hacerlo?
Para gente como Vince, es muy fácil.
Personas de su confianza si conoce el idioma dentro de su trabajo y su empresa. Es
como mostrar que pertenecen a su círculo cercano. Es como un apretón de manos secreto.
No necesitaba mucho de esto por un trabajo como este. Definitivamente no es cirugía cerebral.
Todo lo que es

necesarios para empezar un número de la sucursal. Cuando marqué el Beacon Street
de oficinas en Buffalo, el tipo que contestó sonaba como un cajero.
"Este es Tim Ackerman," le dije. Cualquier nombre que hacer, no lo iba a escribir
hacia abajo. "¿Cuál es el número de la sucursal no?"
"El número de teléfono o el número de sucursales, lo que quería saber, que era bastante
estúpido porque me había marcado sólo el número de teléfono, si no es así? "Número de
sucursal".
"3182", dijo. Así como así. No, "Whad'ya quieres saber?" o cualquier otra cosa.
Porque no es información confidencial, que está escrito en la pieza de casi todos los de papel
que utilizan.
Paso dos, llame a la sucursal donde mi objetivo fue la banca, obtener el nombre de una
de su pueblo, y saber cuando la persona se fuera para el almuerzo. Angela.
Sale a las 12:30. Hasta ahora, todo bien.
Paso tres, volver a llamar a la misma rama durante el almuerzo de Angela, dicen que soy
llamando desde el número de ramas tal y como en Boston, Angela necesita este
información por fax, dame un código para el día. Esta es la parte difícil, es donde la
momento de la verdad. Si yo estaba haciendo una prueba para ser un ingeniero social, pondría
algo como esto en ella, donde la víctima empieza a sospechar - por una buena razón -
y que aún se apegan a ella hasta que lo rompen y obtener la información que
necesitan. No se puede hacer que al recitar las líneas de un guión o el aprendizaje de una rutina,
Tiene que ser capaz de leer su víctima, recuperar el estado de ánimo, el juego le gusta el
aterrizaje de un pez
en la que dejó escapar una pequeña línea y el carrete en, dejó escapar y el carrete pulg Hasta
que ponerlo en
la red y en el flop él en el barco, ¡plaf!
Así que lo llevó y tuvo uno de los códigos para el día. Un gran paso. Con la mayoría de
los bancos, uno es todo lo que uso, por lo que habría sido huir de su hogar. Industrial Federal
utiliza cinco, por lo que sólo uno de cada cinco está probabilidades de largo. Con dos de cada
cinco, me
tienen una probabilidad mucho mayor de que a través del siguiente acto de este pequeño drama.
Yo
amor que parte de "yo no he dicho B, dije E." Cuando funciona, es hermoso. Y
trabaja la mayor parte del tiempo.
Conseguir una tercera habría sido aún mejor. De hecho, he conseguido
tres en una sola llamada - "B", "D" y "sonido E" tan parecidos que puede reclamar
te entendido mal otra vez. Pero hay que estar hablando con alguien que es un
pushover real. Este hombre no estaba. Me quedo con dos.
Los códigos de los días iba a ser mi triunfo para obtener la tarjeta de firma. Que yo llamo, y el tipo
pide un código. C que quiere, y sólo tengo B y E. Pero no es el final de la
mundo. Tienes que mantener la calma en un momento como este, el sonido seguro, manténgase
a la derecha en
va, muy suave, le tocó con el sobre, "Alguien está usando mi
equipo, me pregunta uno de estos otros ".
Estamos todos los empleados de la misma empresa, todos estamos juntos en esto, que sea fácil
en el hombre - que es lo que está esperando que la víctima está pensando en un momento como
este.
Y se ajustó precisamente por el guión. Tomó una de las opciones que se ofrecen, me dio
él la respuesta correcta, envió el fax de la tarjeta de sig.
Casi en casa. Una llamada más me dio el número 800 que los clientes utilizan para la
servicio automatizado, donde una voz electrónica que lee la información que
pedir. De la tarjeta de firmas, que tenía todos los números de cuenta de mi objetivo y su PIN
número, ya que el banco utiliza los cinco primeros o los últimos cuatro dígitos de la social
número de seguro social. Pluma en la mano, llamé al número 800 y después de unos minutos de
pulsar los botones, que tenía el último balance de los cuatro de las cuentas del tío, y sólo
en buena medida, sus depósitos y retiros más recientes en cada uno.

Todo lo que mi cliente había pedido y más. Siempre me gusta dar un poco más de una buena medida. Mantener los clientes contentos. Después de todo, la repetición de negocios es lo que mantiene una operación en marcha, ¿no?

Con el análisis de la

La clave de todo este episodio fue la obtención de los códigos día tan importante, y hacer que el atacante, Vince, que se utiliza varias técnicas diferentes.

Comenzó con un pequeño forcejeo verbal cuando Luis se mostró reacio a dar él un código. Louis tenía razón de ser sospechosos - los códigos están diseñados para ser utilizados en la dirección opuesta. Sabía que en el flujo normal de las cosas, a lo desconocido persona que llama se le da un código de seguridad. Este fue el momento crítico para Vince, que dependerá de lo que todo el éxito dependía de su esfuerzo.

Frente a la sospecha de Luis, Vince simplemente lo puso sobre la manipulación, el uso una apelación a la compasión ("ir al médico"), y la presión ("Tengo un montón de hacer, es casi cuatro "), y la manipulación (" Dile que no me daría la . código ") Astutamente, Vince en realidad no hacen una amenaza, sólo implica una: Si no me dan el código de seguridad, no voy a enviar la información al cliente que su las necesidades de un compañero de trabajo, y yo le digo que lo habría enviado, pero que no cooperaría.

Sin embargo, no hay que ser demasiado apresurado en culpar a Louis. Después de todo, la persona en el teléfono sabía (o al menos parecía saber) que un compañero de trabajo Angela había solicitado un fax. La persona que llama sabía acerca de los códigos de seguridad, y sabía que no fueron identificados por carta designación. La persona que llamó dijo que su gerente de la sucursal fue que requieren una mayor la seguridad. Hay realmente no parecía ninguna razón para no darle la verificación que estaba pidiendo.

Luis no está solo. Los empleados del Banco renunciar a los códigos de seguridad social a los ingenieros todos los días. Increíble pero cierto.

Hay una línea en la arena donde las técnicas de un investigador privado de dejar de ser legal y empezar a ser ilegal. Vince permaneció legal, cuando obtuvo el poder número. Él incluso se quedó legal cuando estafó a Louis para que le diera dos de los códigos de seguridad de día. Cruzó la línea cuando él tenía información confidencial sobre un cliente del banco por fax a él.

Sin embargo, para Vince y su empleador, es un crimen de bajo riesgo. Al robar el dinero o bienes, alguien se dará cuenta de que se ha ido. Al robar la información, la mayoría de los tiempo nadie se dará cuenta porque la información se encuentra todavía en su poder.

Mitnick MENSAJE

Códigos verbales de seguridad son equivalentes a las contraseñas en la prestación de un cómodo y medio fiable de protección de datos. Sin embargo, los empleados tienen que estar bien informado sobre los trucos que los ingenieros sociales utilizan, y entrenados para no dejar las llaves de la reino.

Los policías como incautos

Para un investigador privado con sombra o un ingeniero social, hay ocasiones en las frecuentes cuando sería útil para saber el número de controladores de alguien de la licencia - por ejemplo, si quiere asumir la identidad de otra persona para obtener información sobre los saldos de su banco.

A falta de levantamiento de la cartera de la persona o mirando por encima del hombro a un oportuno momento, conocer el número de la licencia de conducir debe ser casi imposible.

Pero para cualquier persona con conocimientos de ingeniería social, aunque sean modestas, es apenas un desafío.
Un ingeniero social particular - Eric Mantini, lo llamaré, necesario para obtener de conducir licencia y los números de registro de vehículos sobre una base regular. Eric pensó que era incrementar innecesariamente el riesgo de llamar al Departamento de Vehículos Motorizados (DMV) y pasar por el mismo tiempo de engaño una y otra vez cada vez que necesitaba que de la información. Se preguntó si no había alguna manera de simplificar el proceso.
Probablemente nadie había pensado en ello antes, pero él encontró una manera para obtener la información en un abrir y cerrar, cada vez que él quería. Lo hizo mediante la adopción de
ventaja de un servicio proporcionado por el Departamento de su estado de Vehículos de Motor. DMV muchos estados (o lo que el departamento puede ser llamado en su estado) hacer información privilegiada acerca de otro modo-a disposición de los ciudadanos de las compañías de seguros,
investigadores privados, y otros grupos que la legislatura estatal ha considere con derecho a compartirlo por el bien del comercio y de la sociedad en general.
El DMV, por supuesto, tiene limitaciones apropiadas a los tipos de datos se entregado. La industria de seguros pueden obtener ciertos tipos de información de la archivos, pero no en otros. Un conjunto diferente de limitaciones se aplica a los inhibidores de la proteasa, y así sucesivamente.
Para los oficiales de cumplimiento de la ley, una regla diferente se aplica en general: El DMV facilitará toda la información en los registros de cualquier oficial de policía bajo juramento a quienes corresponda
identifica a sí mismo. En el estado de Eric vivía entonces en la identificación requiere un Código solicitante emitido por el DMV, junto con la licencia de conducir del oficial de número. El empleado del DMV siempre comprobar comparando el de oficial nombre junto al número de su licencia de conducir y una pieza de información - por lo general la fecha de nacimiento - antes de dar cualquier información.
¿Qué ingeniero Eric social que quería hacer era nada menos que a sí mismo en la capa identidad de una agente de la ley. ¿Cómo logró eso? Mediante la ejecución de un revertir la picadura de la policía!
Sting Eric
Primero llamó a información telefónica y le pidió el número telefónico del DMV sede en la capital del estado. Se le dio el número 503555-5000, que, de
Por supuesto, es el número de llamadas del público en general. Entonces llamó a uno cercano la estación del alguacil y le pidió teletipo - la oficina donde las comunicaciones son mandar y recibir información de otras agencias de aplicación de la ley, la delincuencia nacional base de datos, órdenes de local, y así sucesivamente. Cuando llegó teletipo, me dijo que estaba buscando el número de teléfono para hacer cumplir la ley para llamar al DMV Estado de la sede.
"¿Quién eres tú?" el oficial de policía le preguntó teletipo.
"Se trata de Al. Me estaba llamando a 503-555-5753", dijo. Esto fue en parte una suposición, y en parte una serie que sacó de la nada, sin duda el conjunto especial de la oficina del DMV para tomar las llamadas fuerzas del orden estaría en el mismo código de área como el número gtyen a cabo para que el público llame y era casi como la certeza de que los próximos tres dígitos, el prefijo, sería el mismo. también. Todo lo que realmente necesitaba saber era los últimos cuatro años.
El sitio de un alguacil de teletipo no recibe llamadas del público. Y la persona que llama ya tenía la mayor parte de la serie. Obviamente, era legítimo.
"Es 503-555-6127", dijo el funcionario.
Así que Eric tenía ahora el número de teléfono especial para los agentes del orden para llamar el DMV. Sin embargo, sólo el número uno no era suficiente para satisfacer, de la oficina tienen un buen número de más de la línea telefónica, y Eric necesitaba saber cómo muchas líneas no fueron, y el número de teléfono de cada uno.

El Switch

Para llevar a cabo su plan, necesario para acceder a la central telefónica que maneja las líneas de aplicación de la ley de teléfono en el DMV. Hizo un llamamiento al Estado Departamento de Telecomunicaciones y afirmó que era de Nortel, la fabricante de la DMS-100, uno de los comerciales más utilizados conmutadores telefónicos. Él dijo: "¿Puedes por favor me traslado a uno de los switch técnicos que trabaja en el DMS-100? "

Cuando llegó el técnico, que decía ser el técnico de Nortel Centro de Asistencia de Apoyo en Texas, y explicó que se estaban creando una base de datos principal para actualizar todos los interruptores con las últimas actualizaciones de software. Sería todo se hace a distancia - no hay necesidad para cualquier técnico de cambiar a participar. Pero necesario el número telefónico al cambiar de modo que pudieran realizar las actualizaciones directamente desde el Centro de Soporte.

Sonaba completamente plausible, y el técnico dio Eric el número de teléfono. Ahora podía llamar directamente a una de las centrales telefónicas del Estado.

Para defenderse de los intrusos, los conmutadores comerciales de este tipo son protegido por contraseña, al igual que todas las redes de computadoras corporativas. Ningún bien social ingeniero con un fondo de teléfono phreaking sabe que los conmutadores de Nortel proporcionan un nombre de cuenta por defecto para las actualizaciones de software: NTAS (la abreviatura de Nortel Apoyar la asistencia técnica, no muy sutil). Pero ¿qué pasa con una contraseña? Eric marcado en varias ocasiones, cada vez que intenta una de las obvias y de uso común opciones. Entrar en el mismo que el nombre de la cuenta, NTAS, no funcionó. Tampoco "Ayudante". Tampoco "parche".

Luego trató de "actualizar". . . y fue in típicos. El uso de un evidente, fácilmente contraseña adivinado es muy poco mejor que no tener una contraseña.

Que ayuda a estar al día en su campo, Eric probablemente sabía tanto que interruptor y la forma de programar y solucionar problemas como el técnico. Una vez que se poder acceder al conmutador como un usuario autorizado, que podría obtener el control total sobre las líneas telefónicas que eran su objetivo. De su equipo, preguntó el interruptor el número de teléfono que le habían dado para las llamadas fuerzas del orden para que el DMV, 555-6127. Se encontró que había otros diecinueve líneas telefónicas en el mismo departamento. Es obvio que manejan un alto volumen de llamadas.

Para cada llamada entrante, el switch se ha programado para "cazar" a través de los veinte líneas hasta encontrar uno que no estaba ocupado.

Tomó dieciocho número de línea en la secuencia, y entró en el código que añade el desvío de llamadas a esa línea. Para el número de reenvío de llamadas, entró en el teléfono número de su nuevo teléfono barato, celulares de prepago, el tipo que los narcotraficantes son tan cariño porque son lo suficientemente económico para tirar después de que el trabajo esté terminado.

Con el desvío de llamadas ahora se activa en la línea XVIII, tan pronto como la oficina se puso a trabajar lo suficiente para tener diecisiete llamadas en curso, la siguiente llamada a entrar en no sonaba en la oficina del DMV, sino que sería enviado a la celda de Eric teléfono. Se sentó y esperó.

Un llamado a la DMV

Poco antes de las 8 de la mañana, el teléfono sonó. Esta parte fue la mejor, la más deliciosa. Aquí estaba Eric, el ingeniero social, hablando con un policía, alguien con la autoridad para venir a arrestarlo, u obtener una orden de registro y realizar un allanamiento para obtener pruebas contra él.

Y no sólo un policía se llama, pero una serie de ellos, uno tras otro. Por un ocasión, Eric estaba sentado en un restaurante comiendo con amigos, sobre el terreno una

llamada
cada cinco minutos o así, escribir la información en una servilleta de papel con un
prestada la pluma. Todavía se encuentra esta hilarante.
Pero hablar con los agentes de policía no perturba un ingeniero de bien social en lo más mínimo. En
De hecho, la emoción de engañar a las agencias de aplicación de la ley probablemente añadida a Disfrute Eric s del acto.
De acuerdo con Eric, la llama fue algo como esto:
"DMV, qué puedo ayudarle?"
"Este es el detective Andrew Cole".
"Hola, soy detective. ¿Qué puedo hacer por usted hoy?"
"Necesito un Soundex en la licencia 005602789," se podría decir, usando el término
familiar en la aplicación de la ley para pedir una foto - útil, por ejemplo, cuando los agentes van a arrestar a un sospechoso y quiere saber qué aspecto tiene.
"Claro, que yo lleve el registro," Eric iba a decir. "Y, el detective Cole, lo que
su agencia? "
"Condado de Jefferson". Y luego Eric haría las preguntas calientes:
"Detective, ¿cuál es su código de solicitante?
¿Cuál es el número de su licencia de conducir. "¿Cuál es tu fecha de nacimiento"
La persona que llamó le daría a su información de identificación personal. Eric iría
a través de algún pretexto de verificar la información, y luego decirle a la persona que llama que la información de identificación ha sido confirmada, y pregunte por los detalles de lo
la persona que llama quería saber de la DMV. Había pretenden empezar a buscar el
nombre, con la persona capaz de escuchar el ruido de las teclas, y luego decir algo
como, "Oh, maldita sea, mi equipo acaba de ir de nuevo. Lo sentimos, detective, mi
equipo ha estado en un abrir y cerrar, toda la semana. ¿Te importaría volver a llamar y conseguir otro empleado que le ayude? "
De esta manera se terminaría la llamada atar los cabos sueltos sin despertar ninguna sospecha de por qué no fue capaz de ayudar al oficial con su petición. Mientras tanto, Eric
había un robo de identidad - los detalles que él podría utilizar para obtener confidencial DMV información siempre que lo necesitaba.
Después de recibir llamadas de un par de horas y la obtención de decenas de códigos de solicitante, Eric
marcado en el interruptor y se desactiva el desvío de llamadas.
Durante meses después de que había llevar a cabo las tareas jobbed a él por
empresas legítimas PI que no quería saber cómo estaba su información.
Cada vez que necesitaba, que había marcado de nuevo en el interruptor, a su vez en el desvío de llamadas,
y reunir otra serie de credenciales de agente de la policía.
Con el análisis de la
Vamos a realizar una reproducción en el artimañas Eric se puso una serie de personas para hacer este
el engaño de trabajo. En el primer paso exitoso, llegó un agente del alguacil en un teletipo
espacio para dar a conocer un número confidencial DMV teléfono a un completo desconocido, aceptar al hombre como un diputado sin solicitar ningún tipo de verificación.
Entonces, alguien en el Departamento de Estado de Telecomunicaciones hizo lo mismo, la aceptación de
Reclamación de Eric que estaba con un fabricante de equipo, y proporcionar los
extranjero con un número de teléfono para llamar a la central telefónica al servicio de la DMV.
Eric fue capaz de entrar en el interruptor, en gran medida debido a la poca seguridad
prácticas por parte del fabricante del interruptor en el uso del mismo nombre de cuenta
en todos los switches. Que el descuido hizo un paseo por el parque para el desarrollo social ingeniero de adivinar la contraseña, sabiendo una vez más que los técnicos de cambiar, sólo como casi todos los demás, elegir contraseñas que será muy fácil para ellos

recordar.
Con el acceso al switch, estableció el desvío de llamadas desde un teléfono del DMV
líneas para la aplicación de la ley a su propio teléfono celular.
Y luego, la parte taponadora y más flagrante, que estafó a una aplicación de la ley
oficial tras otro a revelar no sólo sus códigos de solicitante, sino su propia
información de identificación personal, lo que Eric la capacidad de hacerse pasar por ellos.
Si bien no fue sin duda el conocimiento técnico necesario para llevar a cabo este truco, que
no podría haber funcionado sin la ayuda de una serie de personas que no tenían ni idea de que
estaban hablando con un impostor.
Esta historia fue otro ejemplo del fenómeno de por qué la gente no pregunta
"¿Por qué yo?" ¿Por qué el oficial de teletipo dar esta información a algunos
ayudante del sheriff de que no sabía - o, en este caso, un desconocido hacía pasar por
un ayudante del sheriff - en vez de sugerir que obtener la información de un compañero
diputado o su propio sargento? Una vez más, la única respuesta que puedo ofrecer es que la
gente
rara vez se hacen esta pregunta. No se les ocurre preguntar? No quiero sonar
desafiante e inútil? Tal vez. Ninguna otra explicación no sería más que
conjeturas. Pero los ingenieros sociales no les importa la razón, sino que sólo se preocupan de
que este hecho poco
hace que sea fácil de obtener información que de otro modo podría ser un reto a conseguir.
Mitnick MENSAJE
Si usted tiene una central telefónica en las instalaciones de su empresa, lo que la persona
a su cargo hacer si recibió una llamada del proveedor, solicitando el número telefónico?
Y, por cierto, tiene esa persona nunca cambia la contraseña por defecto para la
switch? Es que la contraseña de una forma fácil de adivinar la palabra en ningún diccionario?
PREVENCIÓN DE LA CON
Un código de seguridad, se utilizan adecuadamente, añade una capa de protección valiosa. A la
seguridad
el código no se utiliza correctamente puede ser peor que no hacer nada, ya que da la ilusión
de la seguridad en las que no existe realmente. ¿De qué sirven los códigos de si sus empleados
no las guarde. secreto?
Cualquier empresa con una necesidad de los códigos de seguridad verbal tiene que definir con
claridad para
sus empleados cuándo y cómo se utilizan los códigos. Una formación adecuada, el carácter de
la primera historia en este capítulo no se han tenido que confiar en sus instintos, fácilmente
superar, cuando se le preguntó a dar un código de seguridad a un extraño. Sintió que
No se debe pedir esta información bajo las circunstancias, pero que carecen de una
la política de seguridad clara - y el buen sentido común - que rápidamente dio pulg
Procedimientos de seguridad también debe establecer los pasos a seguir cuando un empleado de
los campos
una petición inapropiada para un código de seguridad. Todos los empleados deben ser
entrenados para
informe inmediatamente cualquier solicitud de credenciales de autenticación, como un diario
código o contraseña, hecha bajo circunstancias sospechosas. También debe informar
cuando se intenta verificar la identidad de un solicitante no ver.
Por lo menos, el empleado debe registrar el nombre del llamante, número de teléfono,
y la oficina o departamento, y luego cuelga. Antes de llamar de nuevo que debe verificar
que la organización realmente tiene un empleado de ese nombre, y que la llamada
número nuevo de teléfono coincide con el número de teléfono en el on-line o en papel
Directorio de la compañía. La mayoría de las veces, esta simple táctica será todo lo que se
necesita para
verificar que la persona que llama es quien dice ser.
Verificación se vuelve un poco más difícil cuando la compañía ha publicado un teléfono
directorio en lugar de una versión on-line. La gente se contrató, la gente sale, la gente
los departamentos de cambio, puestos de trabajo, y el teléfono. El directorio en papel ya está

de la fecha del día después de que se publicó, incluso antes de ser distribuidos. Incluso en línea directorios no siempre se puede confiar, porque los ingenieros sociales saben
modificarlos. Si un empleado no puede verificar el número de teléfono de una organización independiente
fuente, que deben ser instruidos para comprobar por otros medios, tales como
ponerse en contacto con el gerente del empleado.

Parte 3: Alerta de intruso

Capítulo 10
Entrar en los locales
¿Por qué es tan fácil para una persona ajena a asumir la identidad de un empleado de la compañía
y llevar una imitación tan convincente que incluso las personas que son altamente
conscientes de la seguridad se toman en? ¿Por qué es tan fácil engañar a las personas que pueden
ser plenamente conscientes de los procedimientos de seguridad, que desconfiaba de la gente que personalmente no
saber, y de protección de los intereses de su empresa?
Reflexionar sobre estas cuestiones a medida que lee las historias en este capítulo.
LA GUARDIA DE SEGURIDAD VERGÜENZA
Fecha / hora: martes, 17 de octubre de 2:16 A.M.
Lugar: Skywatcher Aviation, Inc. planta de fabricación en las afueras de Tucson,
Arizona.
Historia de la Guardia de Seguridad
Escuchar sus tacones de cuero, haga clic en el suelo en los pasillos de la casi desierta
planta hizo Leroy Greene se sienten mucho mejor que pasar las horas de la noche de su
ver frente a los monitores de vídeo en la oficina de seguridad. Allí no se
permite hacer otra cosa que mirar a las pantallas, ni siquiera leer una revista o su
encuadernado en cuero Biblia. Sólo había que sentarse allí mirando las pantallas de los todavía imágenes en las que nada se movía.
Sin embargo, caminando por los pasillos, al menos fue estirando las piernas, y cuando
Recordó a tirar los brazos y los hombros en el paseo, le puse un poco
hacer ejercicio. A pesar de que en realidad no cuenta mucho como ejercicio para un hombre que había jugado el tackle derecho en el equipo All-City campeón de fútbol de la escuela. Sin embargo,
pensó, un trabajo es un trabajo.
Se dio la vuelta de la esquina suroeste y comenzó a lo largo de la galería con vistas al Halfmile-planta de producción de largo. Bajó la mirada y vio a dos personas caminando pasado
la línea de helicópteros en parte construido. La pareja se detuvo y pareció estar apuntando las cosas
unos a otros. Una extraña visión en este momento de la noche. "Es mejor ver", pensó.
Leroy se dirigió a una escalera que lo llevaría a la planta de producción en línea
detrás de la pareja, y no sentir su acercamiento hasta que dio un paso al costado.
"Buenos días. ¿Puedo ver su tarjetas de seguridad, por favor", dijo. Leroy siempre trató de mantener su voz suave y en momentos como éste, que sabía que el tamaño de él podría parece amenazante.
"Hola, Leroy", dijo uno de ellos, al leer el nombre de su placa. "Soy Tom Stilton,
de la oficina de marketing de las empresas en Phoenix. Estoy en la ciudad para las reuniones y Quería mostrar mi amigo lo más helicópteros del mundo, se construyen ".
"Sí, señor. Su tarjeta de identificación, por favor", dijo Leroy. No podía dejar de notar cómo los jóvenes
que parecían. El tipo de marketing parecía recién salido de la escuela secundaria, el otro
tenía el pelo hasta los hombros y miró unos quince años.
El uno con el corte de pelo mano en el bolsillo de su placa, luego comenzó a

palmaditas en los bolsillos. Leroy fue de repente comienza a tener un mal
este. "Maldita sea", dijo el chico. "Debe haber dejado en el coche lo puedo conseguir -. Llévame diez
minutos para salir del estacionamiento y la espalda. "
Leroy tenía su libreta por el momento. "¿Qué dijiste que te llamabas, sr. Preguntó:
y cuidadosamente escribió la respuesta. Luego se les pidió que lo acompañara a la
Oficina de Seguridad. En el ascensor hasta el tercer piso, Tom hablaron de haber sido
con la empresa por sólo seis meses y esperaba que él no iba a llegar en cualquier
problemas por esto.
En la sala de control de seguridad, los otros dos en el turno de noche, con Leroy
se unió a él en el cuestionamiento de la pareja. Stilton dio su número de teléfono, y dijo:
su jefe era Judy Underwood y dio su número de teléfono, y la
toda la información protegido en el equipo. Leroy tomó los otros dos de seguridad
la gente a un lado y hablaron acerca de qué hacer. Nadie quería conseguir este mal;
Los tres coinciden en que más llaman jefe del tío a pesar de que significa despertar
ella en el medio de la noche.
Leroy llamó la señora Underwood sí mismo, explicó quién era y lo hizo un
El Sr. Tom Stilton trabajando para ella? Sonaba como si estuviera aún medio dormido.
"Sí", dijo.
"Bueno, lo encontramos abajo en la línea de producción a las 2:30 de la mañana sin
Tarjeta de identificación. "
La señora Underwood, dijo: "Déjame hablar con él."
Stilton se puso al teléfono y le dijo: "Judy, lo siento mucho sobre estos tipos de vigilia
que en medio de la noche. Espero que no vamos a
esto contra mí. "
Me escuchó y luego dijo: "Es sólo que yo tenía que estar aquí en la mañana
de todos modos, para esa reunión en el nuevo comunicado de prensa. De todos modos, ¿le dieron el correo electrónico
sobre el acuerdo de Thompson? Que necesitamos para cumplir con Jim lunes por la mañana por lo que
No pierda esta. Y todavía estoy almorzando con que el martes, ¿verdad? "
Escuchó un poco más y dijo adiós y colgó.
Que cogió por sorpresa a Leroy, había pensado que conseguiría el teléfono por lo que la señora
podría decirle que todo estaba bien. Se preguntó si tal vez debería llamar a su
una y otra pregunta, pero lo pensó mejor. Él ya le había molestado una vez en el
medio de la noche, si llama por segunda vez, tal vez ella podría molestarse y
presentar una queja ante su jefe. "¿Por qué hacer olas?" -pensó-.
Está bien si le muestro a mi amigo el resto de la línea de producción? Stilton preguntó Leroy
¿Quieres venir a lo largo de, mantener un ojo sobre nosotros?
"Vamos, Leroy dijo." Mira a tu alrededor. Pero no se olvide de su tiempo insignia próximo. Y dejar que
Seguridad saber si usted necesita para estar en el piso de la planta después de horas - que es la regla ".
Voy a recordar que, Leroy ", dijo Stilton. Y se fueron.
Apenas diez minutos habían pasado antes de que el teléfono sonó en la Oficina de Seguridad.
La señora Underwood estaba en la línea. "¿Quién era ese tipo?" ella quería saber. Ella
dijo que seguía tratando de hacer preguntas, pero él siguió hablando de tener
almuerzo con ella y ella no sabe quién demonios es.
Los chicos de seguridad llamado el vestíbulo y el guardia en la puerta del estacionamiento.
Ambos informaron a los dos jóvenes habían salido unos minutos antes.
Contar la historia más tarde, Leroy siempre terminaba diciendo: "Dios, qué jefe masticar
me a un lado y por el otro. Tengo la suerte de que todavía tengo un trabajo. "
Historia de Joe Harper
Sólo para ver lo que podía salirse con la suya, de diecisiete años de edad, Joe Harper había sido
colarse en los edificios de más de un año, a veces durante el día,

a veces por la noche. El hijo de un músico y una camarera, tanto de trabajo
el turno de noche, Joe tenía mucho tiempo por sí mismo. Su historia de ese mismo incidente
arroja luz instructivo sobre cómo ocurrió todo.
Tengo un amigo que Kenny piensa que quiere ser piloto de helicóptero. -Le preguntó
me, podría meterlo en la fábrica Skywatcher para ver la línea de producción donde
que hacen los helicópteros. Él sabe lo que tengo en otros lugares antes. Se trata de un
adrenalina para ver si usted puede caer en lugares que no debes ser.
Pero no basta con entrar a una fábrica o edificio de oficinas. Tengo que pensar en ello,
hacer un montón de planificación, y hacer un reconocimiento pleno en el objetivo. Compruebe la
empresa página web los nombres y títulos, estructura de reporte, y el teléfono
números. Leer recortes de prensa y artículos de revistas. La investigación meticulosa es mi
propia marca de precaución, así que podía hablar con nadie que me retó, con lo
conocimiento tanto como cualquier otro empleado.
¿Por dónde empezar? Primero busqué en Internet para ver si la empresa había
oficinas, y vio a la sede central estaba en Phoenix. Perfecta. Me llamó y
pidió Marketing, cada empresa tiene un departamento de marketing. Una señora
contestó, y me dijo que yo estaba con gráficos lápiz azul y queríamos ver si nos
podía interés en el uso de nuestros servicios y que iba a hablar. Dijo que
sería Tom Stilton. Le pedí su número de teléfono y me dijo que no se dio
que la información, sino que me podía pasar por. La llamada sonó en el correo de voz,
y su mensaje dijo: "Este es Tom Stilton en gráficos, extensión 3147, por favor
dejar un mensaje "Por supuesto -. no dar a conocer las extensiones, sino que deja este tipo de su
a la derecha en su buzón de voz. Para que se enfríe. Ahora tenía un nombre y extensión.
Otra llamada, de nuevo a la misma oficina. "Hola, yo estaba buscando Tom Stilton. Es
no in me gustaría preguntarle a su jefe una pregunta rápida. "El jefe estaba fuera, también, pero
por el
vez que se terminó, me sabía el nombre del jefe. Y ella se había ido muy bien su extensión
número de su buzón de voz, también.
Probablemente podría llevarnos más allá de la guardia del vestíbulo, sin sudar, pero he conducido
por ese
planta y pensé me acordé de un cerco alrededor de la playa de estacionamiento. Una valla de un
medio
guardia que se comprueba cuando se trate de conducir pulgadas y por la noche, podría ser
anotando los números de licencia, también, así que tendría que comprar una placa de edad en
una pulga
del mercado.
Pero primero tendría que obtener el número de teléfono en la caseta de seguridad. Esperé un
poco por lo que si
Tengo el mismo operador, cuando marqué de nuevo, ella no reconoce mi voz.
Después de un rato me llamó y me dijo, "Tenemos una denuncia de que el teléfono en la
cordillera
Camino guardia choza ha informado de problemas intermitentes - se siguen teniendo
problemas? "Ella dijo que no lo sabía, pero me conecte.
El hombre respondió: "Ridge Road puerta, se trata de Ryan". Le dije: "Hola, Ryan, este es Ben.
Se está teniendo problemas con sus teléfonos no? "Él es sólo un título de baja remuneración
guardia, pero supongo que había algún tipo de formación debido a que de inmediato dijo: "Ben,
que -
¿Cuál es tu apellido? "Seguí derecho como si yo ni siquiera había oído.
"Alguien reportó un problema antes."
Yo podía oír lo sostenía el teléfono y gritando: "Hey, Bruce, Roger,
hubo un problema con este teléfono. El vino de nuevo y dijo: "No, no
los problemas que conocemos. "
"¿Cuántas líneas de teléfono tienes ahí?"
Se había olvidado de mi nombre. "Dos", dijo. "¿Cuál eres tú ahora?"
"3140".

Gotcha! "Y los dos están trabajando bien?"
"Parece".
Bueno, le dije. Escucha, Tom, si usted tiene algún problema de teléfono, sólo tiene que llamarnos en
Telecom cualquier momento. Estamos aquí para ayudar. "
Mi amigo y yo decidimos visitar la planta de la noche siguiente. Esa tarde
Llamé a la caseta de guardia, utilizando el nombre del tipo de marketing. Le dije: "Hola, esto es Tom Stilton en gráficos. Estamos en un plazo de accidente y tengo un par de chicos conducir al pueblo a ayudar. Probablemente no va a estar aquí hasta la una o las dos de la por la mañana. ¿Seguirá en la entonces? "
Estaba feliz de decir que no, que se bajó a la medianoche.
Le dije: "Bueno, acaba de salir de una nota para el tipo de al lado, ¿de acuerdo? Cuando dos hombres aparecen
y dicen que han venido a ver a Tom Stilton, sólo la onda em 'en el - está bien "
Sí, dijo, que estaba bien. Él anotó mi nombre, departamento, y la extensión
número y dijo que él se ocuparía de ello.
Nos condujo hasta la puerta poco después de las dos, me dio el nombre de Tom Stilton, y un sueño
guardia acaba de señalar a la puerta por la que debe ir y por dónde puedo estacionar debe.
Cuando entramos en el edificio, había otro puesto de guardia en el vestíbulo,
con el libro de costumbre después de horas ins de inicio de sesión. Yo le dije al guardia que había un informe que
necesarios para estar listos en la mañana, y este amigo mío quería ver el
de la planta. "Está loco por helicópteros", dijo que "piensa que quiere aprender a piloto una. "Me pidió mi tarjeta de identificación. Metí la mano en un bolsillo, y luego dio unas palmaditas en la vuelta y
me dijo que debía haber dejado en el coche, voy a ir a por él. Me dijo: "Tomará unos diez minutos."
Él dijo: No te preocupes, está bien, sólo tiene que registrarse in "
Caminando por la línea de producción - lo que es un gas. Hasta ese tronco de un Leroy
nos detuvo.
En la oficina de seguridad, me imaginé a alguien que no pertenecía realmente se vería
nerviosa y asustada. Cuando las cosas se ponen tensos, acabo de empezar a sonar como que estoy muy
al vapor. Como si yo fuera realmente quien decía ser y que es molesto que no creen
mí.
Cuando empezaron a hablar de tal vez debería llamar a la señora que dijo que era mi
jefe y fue a buscar su número de teléfono desde el ordenador, me quedé allí
pensando: "Un buen tiempo para hacer sólo un descanso para él." Pero había que en aparcamientos
puerta - incluso si salimos del edificio, que cerraba la puerta y nunca habíamos
hacer que fuera.
Cuando Leroy llamó a la señora que era el jefe de Stilton y luego me dio el teléfono,
la mujer comenzó a gritarme "¿Quién es, quién es usted!" y yo seguí
hablando como si estuviéramos teniendo una conversación agradable, y luego colgó.
¿Cuánto tiempo se tarda en encontrar a alguien que le puede dar una empresa de telefonía
número en el medio de la noche? Me imaginé que tenía menos de quince minutos para
salir de allí antes de que la señora estaba sonando la oficina de seguridad y poner un error
en sus oídos.
Salimos de allí tan rápido como pudimos, sin mirar como si estuviéramos en un apuro.
Claro que se alegró de que el hombre en la puerta sólo nos saludó con la mano a través de.
Con el análisis de la
Vale la pena señalar que en el incidente real esta historia se basa en, a los intrusos
en realidad eran adolescentes. La intrusión fue una broma, sólo para ver si podían obtener
con la suya. Pero si era tan fácil para un par de adolescentes, que habría sido aún

más fácil para los ladrones de adultos, espías industriales, o de los terroristas.
¿Cómo tres agentes de seguridad con experiencia permite un par de intrusos que se encuentra a sólo
de distancia? Y no sólo a cualquier intruso, pero un par de jóvenes para que cualquier persona razonable
debería haber sido muy sospechoso?
Leroy fue debidamente sospechoso, en un primer momento. Él estaba en lo correcto al tomar a la Oficina de Seguridad, y en el interrogatorio el hombre que se hacía llamar Tom y Stilton verificar los nombres y números de teléfono que él dio. Estaba en lo correcto en hacer la llamada al supervisor.
Pero al final fue trasladado por vía aérea del joven de la confianza y la indignación. No era el comportamiento que cabe esperar de un ladrón o intruso - sólo un empleado real habría actuado de esa manera .., o al menos eso se supone. Leroy debe han sido entrenados para contar con la sólida identificación, no la percepción.
¿Por qué no se lo más sospechoso cuando el joven colgó el teléfono sin devolverlo para Leroy podía oír la confirmación directamente de Judy Underwood y recibir la garantía de que el chico tenía una razón de ser en el planta tan tarde en la noche?
Leroy fue recogida por una estratagema tan audaz que debería haber sido obvio. Pero considerar el momento en que desde su perspectiva: un graduado de secundaria, preocupado por su trabajo, sin saber si él podría tener problemas para molestar a una empresa director por segunda vez en el medio de la noche. Si usted hubiera estado en su zapatos, ¿le han hecho la llamada de seguimiento?
Pero, por supuesto, una segunda llamada no fue la única acción posible. ¿Qué otra cosa el guardia de seguridad podría haber hecho?
Incluso antes de realizar la llamada telefónica, él podría haber pedido tanto de la pareja para mostrar
algún tipo de identificación con foto, sino que se dirigió a la planta, por lo que al menos uno de ellos deben tener una licencia de conducir. El hecho de que había dado origen falso nombres habría sido obvio (un profesional que ha venido
equipado con identificación falsa, pero estos jóvenes no habían tomado esa precaución). En cualquier
caso, Leroy debería haber examinado las credenciales de identificación y por escrito por la información. Si ambos insistieron en que no tenía identificación, se debe luego tener que caminar o el coche para recuperar la tarjeta de identificación que la empresa "Tom
Stilton "afirmó que había dejado allí.
Mitnick MENSAJE
Los manipuladores suelen tener personalidades muy atractivo. Por lo general son rápido en sus pies y articular bien. Los ingenieros sociales son también expertos en distraer los procesos de la gente pensaba de modo que cooperen. Pensar que cualquier una persona en particular no es vulnerable a esta manipulación es subestimar la habilidad y el instinto asesino del ingeniero social.
Un ingeniero de bien social, por otro lado, nunca subestima a su adversario.
Después de la llamada telefónica, una de las personas de seguridad debería haberse quedado con la
par hasta que salieron del edificio. Y luego se dirigió a su coche y por escrito por el número de la matrícula. Si hubiera sido lo suficientemente atento, se habría señaló que la placa (la que el atacante había comprado en un mercado de pulgas) se no tener una etiqueta de registro válido - y que debería haber sido motivo suficiente para detener a la pareja para una mayor investigación.
Basurero de buceo
Basurero de buceo es un término que describe pateando la basura de un objetivo en búsqueda de información valiosa. La cantidad de información que usted puede aprender acerca de un

objetivo es asombrosa.
La mayoría de las personas no dan mucha importancia a lo que están descartando en casa: teléfono
facturas, estados de tarjetas de crédito, botellas de prescripción médica, estados de cuenta bancarios, relacionadas con el trabajo
materiales, y mucho más.
En el trabajo, los empleados deben ser conscientes de que las personas se ven en la basura para obtener información que pueda beneficiar.
Durante mis años de escuela secundaria, solía ir a cavar a través de la basura detrás de la locales edificios teléfono de la empresa - a menudo solo, pero de vez en cuando con los amigos que
comparten un interés en aprender más sobre la compañía telefónica. Una vez que
se convirtió en un basurero buzo con experiencia, usted aprenderá algunos trucos, como por ejemplo cómo hacer
esfuerzos especiales para evitar las bolsas de los baños, y la necesidad de utilizar
guantes.
Basurero de buceo no es agradable, pero el resultado fue extraordinario - interna
directorios de empresas telefónicas, manuales de informática, listas de empleados, descartado impresiones que muestra cómo el equipo del programa de conmutación, y más - todo lo que hay para
la toma.
Me horario de visitas para las noches, cuando los nuevos manuales estaban siendo emitidas, debido a que el
los contenedores de basura que tiene un montón de viejos, sin pensar tirado. Y
Yo iría a otros ratos libres, así, en busca de los memos, cartas, informes, etc
sucesivamente, que podrían ofrecer algunas joyas de información interesante.
Al llegar me iba a encontrar algunas cajas de cartón, sacarlos y ponerlos de lado. Si
alguien me desafió, que pasó de vez en cuando, yo diría que fue un amigo
moviendo y yo estaba buscando las cajas para ayudar a empacar. El guardia no
cuenta todos los documentos que había puesto en los cuadros para llevar a casa. En algunos casos, había
me dicen que se pierden, por lo que acababa de mudarse a otra compañía de teléfono de la oficina central.
LINGO
CONTENEDOR DE CONDUCCIÓN Al pasar por la basura de una empresa (a menudo en un contenedor exterior y vulnerables) para encontrar la información que se descarta cualquier
tiene un valor, o una herramienta para utilizar en un ataque de ingeniería social, tales como la interna
números de teléfono o títulos
No sé lo que es hoy en día, pero en aquel entonces era fácil de decir que las bolsas
puede contener algo de interés. La basura y la basura del piso cafetería
estaban sueltas en las bolsas grandes, mientras que las papeleras de oficina fueron alineados con blanco bolsas de basura desechable, que el equipo de limpieza que salir uno por uno
y envuelve una eliminatoria.
Una vez, mientras buscaba con unos amigos, nos encontramos con unas hojas de
trozos de papel con la mano. Y no sólo roto: alguien se había tomado la molestia de
extracción de las hojas en trozos pequeños, todos convenientemente expulsado en una sola fivegallon
saco de basura. Nos llevó la bolsa a un local de tienda de donas, objeto de dumping las piezas sobre
una mesa, y se empezaron a reunir uno por uno.
Estábamos todos los hacedores de rompecabezas, por lo que ofreció el reto estimulante de un gigante
rompecabezas. . . pero resultó tener más de un premio infantil. Cuando haya terminado,
que había reconstruido el nombre de cuenta y toda la lista de contraseñas de uno de los

los sistemas críticos de la empresa informática.
Fueron nuestros basurero de buceo explota la pena el riesgo y el esfuerzo? Que se apuesta se. Incluso más de lo que imagina, porque el riesgo es cero. Era cierto, entonces y aún hoy cierto: mientras no estás invadiendo, estudiando a través de alguien la basura de otra es de 100 por ciento legal.
Por supuesto, phreakers y hackers no son los únicos con la cabeza en botes de basura. Los departamentos de policía en todo el país a través de la pata de la basura con regularidad, y un desfile de personas de capos de la mafia de estafadores menores han sido condenados basado en parte en las pruebas obtenidas a partir de la basura. Las agencias de inteligencia, incluido el nuestro, han recurrido a este método desde hace años.
Puede ser una táctica demasiado bajo para James Bond - los amantes del cine hubiese preferido verlo outfoxing el villano y ropa de cama de una belleza que de pie a su las rodillas en la basura. La vida real, los espías son menos aprensivos cuando algo de valor puede ser en bolsas entre las cáscaras de plátano y café, periódicos y listas de la compra. Especialmente si la recopilación de información no los pone en peligro manera.
Dinero por basura
Corporaciones en el juego contenedor de buceo, también. Los periódicos tuvieron un día de campo en Junio de 2000, informa que Oracle Corporation (cuyo CEO, Larry Ellison, es Probablemente enemigos más directos de la nación de Microsoft) había contratado a un investigador empresa que había sido atrapado con las manos en la masa. Parece que el Los investigadores querían basura de un equipo de presión compatibles con Microsoft, ACT, pero que no querían arriesgarse a ser capturados. Según informes de prensa, el firma de investigación enviado en una mujer que ofreció los trabajadores de limpieza de $ 60 a dejarla han la basura ACT. Que la rechazó. Ella fue a la siguiente noche, aumentando el oferta de $ 500 para la limpieza y $ 200 para el supervisor.
Los trabajadores de limpieza la rechazó y luego se volvió a su in Líder en línea McCullah periodista Declan, tomando una hoja de la literatura, titulado su historia Wired News sobre el episodio, "Era de Oracle que espiaba a la EM". Tiempo revista, clavando Ellison de Oracle, titulado su artículo simplemente "Peeping Larry".
Con el análisis de la
Con base en mi propia experiencia y la experiencia de Oracle, puede que se pregunte por qué alguien se tomaría la molestia de tomar el riesgo de robo de la basura de alguien.
La respuesta, creo, es que el riesgo es nulo y los beneficios pueden ser sustanciales.
Bueno, tal vez tratando de sobornar a los trabajadores de limpieza aumenta la probabilidad de consecuencias, pero para cualquiera que esté dispuesto a ser un poco sucio, los sobornos no son necesarios.
Para un ingeniero social, basurero de buceo tiene sus beneficios. Se puede obtener suficiente información para orientar su asalto contra la empresa objetivo, incluyendo notas, agendas de reuniones, cartas y similares, que revelan los nombres de los departamentos, los títulos, teléfono números, y las asignaciones del proyecto. La basura puede generar organización de la compañía gráficos, información sobre la estructura corporativa, los horarios de viaje, y así sucesivamente. Todos los detalles puede parecer trivial para los iniciados, sin embargo, puede ser de gran valor información a un atacante.
Mark Joseph Edwards, en su libro Seguridad en Internet con Windows NT, las conversaciones sobre "informes de todo descartado debido a errores tipográficos, las contraseñas escritas en pedazos de papel, "Mientras no estabas 'mensajes con números de teléfono, carpetas completas de archivos con los documentos todavía en ellos, disquetes y cintas que no fueron borrados o destruidos-

, Todo lo cual podría ayudar a un intruso-ser ".
El escritor pasa a preguntar, "¿Y quiénes son esas personas en su equipo de limpieza? Usted ha decidido que el personal de limpieza no se [les permitirá] entrar en el equipo habitación, pero no se olvide de las latas de la basura común. Si las agencias federales consideren necesario para
hacer verificaciones de antecedentes de las personas que tienen acceso a los botes de basura y trituradoras, probablemente debería también ".
Mitnick MENSAJE
La basura puede ser el tesoro de tu enemigo. No toman en cuenta más a
los materiales que desechamos en nuestra vida personal, ¿por qué creemos que la gente tener una actitud diferente en el lugar de trabajo? Todo se reduce a la educación de la trabajadores sobre el peligro (gente sin escrúpulos excavar en busca de valiosos información) y la vulnerabilidad (la información no está picado o
correctamente borrado).
EL JEFE humillado
Nadie pensó nada al respecto cuando Harlan Fortis llegaron a trabajar el lunes mañana como de costumbre en el Departamento de Carreteras del Condado, y dijo que salió de su casa en
a toda prisa y olvidado de su tarjeta de identificación. El guardia de seguridad había visto venir en Harlan
y salir todos los días laborables durante los dos años que había estado trabajando allí. Ella le hizo firmar para una credencial de empleado temporal, se lo dio a él, y él continuó a su manera.
No fue sino hasta dos días después de que todo el infierno se empezó a romper suelto. La historia se difundió a través de todo el departamento como la pólvora. La mitad de las personas que
oído decir que no podía ser cierto. Del resto, nadie parecía saber si reír a carcajadas o sentir lástima por la pobre alma.
Después de todo, George Adamson fue una persona amable y compasivo, la mejor cabeza del departamento al que jamás había tenido. Él no se merece tener esto le suceda a él. Suponiendo que la historia era verdad, por supuesto.
El problema empezó cuando George llamado Harlan en su oficina un viernes tarde y le dijo, tan suavemente como pudo, que vienen Lunes Harlan sería la presentación de informes a un nuevo trabajo. Con el Departamento de Sanidad. A Harlan, esto no era como estar despedido. Era peor: era humillante. Él no iba a tener acostado.
Esa misma noche se sentó en el porche a ver el con rumbo a casa tráfico. Por fin vio el muchacho de barrio llamado David que todo el mundo
llamado "La Guerra Juegos de Niños" que pasaban por su ciclomotor en el camino a casa desde lo alto
la escuela. David se detuvo, le dio un rocío Code Red Montaña que había comprado especialmente para el propósito, y le ofreció un trato: el reproductor de vídeo más reciente del juego
y seis partidos a cambio de alguna ayuda de la computadora y la promesa de mantener su la boca cerrada.
Después de Harlan explica el proyecto - sin dar ninguna de las comprometer específicos - David estuvo de acuerdo. Él describió lo que él quería hacer Harlan. Él fue a comprar un módem, ir a la oficina, encontrar computadora de alguien que no era un repuesto teléfono cerca del gato, y conectar el módem. Deje el módem en la
mesa en la que nadie es probable que se vea. Luego vino la parte más arriesgada. Harlan tuvo que sentarse en la computadora, instalar un paquete de software de acceso remoto, y obtener
funcionando. En cualquier momento el hombre que trabajaba en la oficina puede ser que aparezca, o
alguien podría pasar y verlo en la oficina de otra persona. Estaba tan tenso que apenas podía leer las instrucciones que el niño había escrito para él.

Pero lo logramos, y salió del edificio sin ser notado.
Colocar la bomba
David se detuvo después de cenar esa noche. Los dos se sentaron a Harlan
equipo y dentro de unos minutos el muchacho se había marcado en el módem,
tenido acceso, y llegó a máquina George Adamson. No es muy difícil, ya que
George nunca tuvo tiempo para cosas como cambiar de precaución
contraseñas, y siempre estaba haciendo esta persona o que para descargar un archivo o correo electrónico
para él. Con el tiempo, todos en la oficina conocía su contraseña. Un poco de caza
subió el archivo llamado BudgetSlides2002.ppt, que el niño descargado
en el equipo de Harlan. Harlan dijo entonces a los niños para ir a casa, y vienen
en un par de horas.
Cuando David regresó, Harlan le pidió que vuelva a conectarse a la carretera
Sistema de departamento de informática y poner el mismo archivo de vuelta a donde había
encontró, sobrescribir la versión anterior. Harlan David mostró el video
jugador del juego, y prometió que si las cosas iban bien, había que tener al día siguiente.
Sorprendente George
Usted no pensaría que algo que suena tan aburrido como audiencias sobre el presupuesto
sería de mucho interés para nadie, pero la cámara de reunión del Condado
Consejo estaba lleno, lleno de periodistas, representantes de especial interés
grupos, los miembros del público, e incluso dos equipos de noticias de televisión.
George siempre sentí que estaba en juego para él en estas sesiones. El Condado
Consejo ha procedido a la billetera, y menos que George podría poner en un convincente
presentación, el presupuesto de carreteras se redujo. Entonces todo el mundo
empezar a quejarse de los baches y las luces de tráfico atascado y peligroso
las intersecciones, y culpando a él, y la vida sería miserable capaz de todo
próximos años. Pero cuando se introdujo por la noche, se levantó con la sensación de
confianza. Había trabajado seis semanas en esta presentación de PowerPoint y el
visuales, que había probado en su esposa, a su pueblo el personal superior, y algunos
amigos respetados. Todos coincidieron en que era su mejor carta de presentación siempre.
Las tres primeras imágenes de PowerPoint jugó bien. Para variar, cada Consejo
miembro estaba prestando atención. Estaba haciendo sus puntos de manera efectiva.
Y luego todos a la vez todo empezó a ir mal. La cuarta imagen se
supone que es una foto de la puesta de sol de la extensión de la nueva carretera abierta
el año pasado. En cambio, era algo más, algo muy embarazoso. A
fotografía de una revista como Penthouse o Hustler. Podía oír el
audiencia jadeo como se apresuró a apretar el botón en su ordenador portátil para pasar a la siguiente
imagen.
Esto fue peor. No es una cosa se deja a la imaginación.
Todavía estaba tratando de hacer clic en la imagen a otra cuando alguien en la audiencia
sacó el cable de alimentación al proyector mientras que el presidente golpeó fuertemente con
el mazo y gritó por encima del ruido que se levantó la sesión.
Con el análisis de la
Usando los conocimientos de un hacker adolescente, un empleado descontento logró acceder a la
equipo de la cabeza de su departamento, descarga una importante PowerPoint
presentación, y sustituir algunas de las diapositivas con algunas imágenes de causar grave
vergüenza. Luego puso la presentación de nuevo en el ordenador del hombre.
Con el módem conectado a un enchufe y se conecta a una de las oficinas
computadoras, el joven hacker fue capaz de marcar desde el exterior. El chico se había puesto
el software de acceso remoto con antelación para que, una vez conectado a la
equipo, tendría pleno acceso a todos los archivos almacenados en el sistema.
Puesto que la computadora estaba conectada a la red de la organización y que ya
sabía el nombre de usuario y contraseña jefe, fácilmente podría acceder a la del jefe
archivos.

Incluyendo el tiempo de escaneado de imágenes en la revista, todo el esfuerzo había tomado sólo unas pocas horas. Los daños causados a la reputación de un buen hombre estaba más allá de
imaginar.
Mitnick MENSAJE
La gran mayoría de los empleados que son transferidos, despedidos o puestos en libertad en un reducción de personal no son un problema. Sin embargo, sólo se tiene que hacer una empresa se dan cuenta demasiado tarde las medidas que podrían haber tomado para evitar el desastre. La experiencia y las estadísticas han demostrado claramente que la mayor amenaza para la la empresa es de adentro. Es la información privilegiada que tienen un conocimiento íntimo de donde la valiosa información que reside, y donde golpear a la empresa a causa
el mayor daño.
EL BUSCADOR DE PROMOCIÓN
A última hora de la mañana de un día de otoño agradable, Peter Milton entré en el vestíbulo de las oficinas regionales de Denver Auto Parts Honorable, una parte nacional
mayorista para el mercado del automóvil. Esperó en la recepción, mientras que
la joven firma de un visitante, dio indicaciones para llegar a la persona que llama, y se ocupó con el hombre de UPS, todos más o menos al mismo tiempo.
"Entonces, ¿cómo aprender a hacer muchas cosas a la vez?" Pete dijo que cuando ella tenía tiempo para ayudarlo. Ella sonrió, obviamente complacido se había dado cuenta. Fue a partir de Marketing en la oficina de Dallas, le dijo, y dijo que Mike Talbott de
Las ventas de Atlanta campo iba a ser su reunión. "Tenemos un cliente que visita
juntos esta tarde ", explicó. Voy a esperar aquí en el vestíbulo."
"Marketing". Ella dijo que la palabra casi con nostalgia, y Pete le sonreía, a la espera escuchar lo que se avecinaba. "Si yo pudiera ir a la universidad, que es lo que yo tome", dijo. "Me encantaría trabajar en Marketing."
Él sonrió de nuevo. "Kaila," dijo, leyendo su nombre de la señal en el mostrador,
"Tenemos una señora en la oficina de Dallas que era una secretaria. Ella se mudó a sí misma a de marketing. Eso fue hace tres años, y ahora es un asistente
gerente de marketing, lo que hace el doble de lo que era. "
Kaila mirada soñadora. Él continuó, "¿Se puede utilizar una computadora?" "Claro", que
, dijo.
"¿Cómo quieres que me ponga su nombre en el de trabajo de una secretaria en la comercialización.
Sonrió. "Para que incluso me iría a vivir a Dallas".
"Vas a amar a Dallas", dijo. "No puedo prometer un abrir de inmediato,
pero voy a ver lo que puedo hacer. "
Ella pensó que este buen hombre en el traje y corbata y con el bien recortada,
pelo bien peinado puede hacer una gran diferencia en su vida laboral.
Pete se sentó frente al vestíbulo, abrió su laptop, y comenzó a recibir algo de trabajo hacer. Después de diez o quince minutos, dio un paso atrás hacia el mostrador. "Escucha", que dijo, "parece que Mike debe haber sido retenido. ¿Hay una sala de conferencias donde puede sentarse y revisar mi correo electrónico mientras estoy esperando? "
Kaila llamar al hombre que coordinó la programación de la sala de conferencias y arreglos para que Pete utilizar uno que no estaba reservado. Siguiendo un modelo recogido de las empresas de Silicon Valley (Apple fue probablemente el primero en hacerlo) algunos de los las salas de conferencias fueron nombrados después de personajes de dibujos animados, otros después de restaurante
las cadenas o las estrellas de cine o héroes del cómic. Le dijeron que se busque la Minnie Mouse habitación. Ella le hizo firmar en el, y le dio instrucciones para encontrar Minnie Ratón.
Él encuentra la sala, se instaló en, y se conecta a su computadora portátil al puerto Ethernet.
¿Usted consigue el cuadro todavía?
Derecho - que el intruso se había conectado a la red detrás del firewall corporativo.
Historia de Anthony

Creo que se puede llamar a Anthony Lake, un hombre de negocios perezoso. O tal vez "dobladas" se
más cerca.
En lugar de trabajar para otras personas, había decidido que quería ir a trabajar para
sí mismo, que quería abrir una tienda, donde podía estar en un lugar todos los días y no
tiene que correr por todo el campo. Sólo quería tener un negocio que se
podría ser lo más seguro posible que pudiera hacer dinero en.
¿Qué tipo de tienda? Que no tardó mucho en descubrir. Él sabía acerca de la reparación
coches, así que una tienda de auto partes.
Y ¿cómo construir en una garantía de éxito? La respuesta le llegó en un
flash: convencer a las partes de autopartes mayorista Auto Honorable le venden todos los
mercancías que necesitaba a su costo.
Por supuesto que no lo haría de buena gana. Pero Anthony supo Con la gente,
su amigo Mickey sabía de intrusión en los ordenadores de otras personas, y
Juntos elaboraron un plan inteligente.
Aquel día de otoño que de manera convincente se hizo pasar por un empleado llamado Pedro
Milton, y que había estafado a su manera dentro de la Honorable Auto Parts y oficinas
ya había conectado su ordenador portátil a su red. Hasta ahora, todo bien, pero que se
sólo el primer paso. Lo que él todavía tenía que hacer no sería fácil, sobre todo porque
Anthony se había fijado un límite de tiempo de quince minutos - por más tiempo y pensó que
que el riesgo de ser descubierto sería demasiado alto.
Mitnick MENSAJE
Capacitar a su gente a no juzgar un libro por su cubierta exclusivamente - sólo porque alguien
está bien vestido y bien peinado no debe ser más creíble.
En una llamada telefónica a principios de pretextos como una persona de apoyo de su equipo
proveedor, que se había puesto un acto de canto y baile. "Su empresa ha comprado un
de dos años de apoyar el plan y le estamos poniendo en la base de datos para que podamos
saber
cuando un programa de software que está utilizando ha salido con un parche o una nueva
una versión actualizada. Así que tengo que tener que decirme lo que las aplicaciones que está
utilizando. "
La respuesta le dio una lista de programas, y un amigo contador identificado el
una llamada MAS 90, el objetivo - el programa que se mantendrían en sus lista de
los vendedores y las condiciones de descuento y el pago de cada uno.
Con ese conocimiento clave, junto utilizó un programa de software para identifiy, "todos los
trabajando las máquinas de la red, y no tardó mucho en encontrar la correcta
servidor utilizado por el departamento de Contabilidad. Desde el arsenal de herramientas de
hackers en
su ordenador portátil, se puso en marcha un programa y lo utilizó para identificar a todos los
autorizados
los usuarios en el servidor de destino. Con otro, que corrió una lista de uso común
contraseñas, tales como "blanco" y "password" en sí mismo. "Password" trabajado. No
hay sorpresa. La gente acaba de perder toda la creatividad a la hora de elegir
contraseñas.
Sólo seis minutos de partido, y el juego fue más de la mitad. Fue pulg
Otros tres minutos con mucha atención agregar su nueva compañía, dirección, teléfono
número y nombre de contacto a la lista de clientes. Y después de la entrada crucial,
el que marca la diferencia, la entrada que decía que todos los elementos iban a ser
vendió a él en un 1 por ciento sobre el costo de piezas Honorable Auto '.
En poco menos de diez minutos, se llevó a cabo. Se detuvo el tiempo suficiente para decir Kaila
gracias, fue a través de la comprobación de su correo electrónico. Y que había llegado a Mike
Talbot,
cambio de planes, que estaba en el camino a una reunión en la oficina de un cliente. Y
No se olvide de recomendarla para que el trabajo en la comercialización, ya sea.
Con el análisis de la

El intruso que se hacía llamar Peter Milton utilizó dos subversión psicológica
técnicas - una planificada, la otra improvisada en el fragor del momento.
Se vestía como un trabajador de la gestión de ganar buen dinero. Traje y corbata, cabello
cuidado estilo - Estos parecen pequeños detalles, pero dejar una buena impresión. Yo
descubierto por mí mismo, sin darse cuenta. En un corto tiempo como programador en GTE
California - una compañía telefónica importante ya no existe - he descubierto que
si me vino en un día sin una tarjeta de identificación, bien vestido pero informal - por ejemplo,
camisa deportiva,
chinos, y los cargadores de muelle - I'd ser detenido e interrogado. ¿Dónde está su tarjeta de
identificación, que se
usted, ¿dónde trabajas? Otro día me llegan, aún sin una tarjeta de identificación, pero en un
traje y corbata, con aire corporativo. Que haría uso de una variante de la antigua
cuestas técnica, que se mezclan con una multitud de personas que caminan en un
edificio o una entrada segura. Me pegan a algunas personas que se acercaron a
la entrada principal, y caminar en la charla con la gente como si fuera uno de ellos. Yo
pasó por delante, e incluso si los guardias me di cuenta de tarjeta de identificación-menos, no se
me molesta porque me parecía que la gestión y yo estaba con personas que se
llevan placas.
De esta experiencia, me di cuenta de cuán predecible el comportamiento de la seguridad
guardias es. Al igual que el resto de nosotros, que estaban haciendo juicios basados en las
apariencias-
-Una grave vulnerabilidad que los ingenieros sociales aprenden a aprovechar.
El atacante arma psicológica segundo entró en juego cuando se dio cuenta de la
esfuerzo inusual que la recepcionista estaba haciendo. Manejo de varias cosas a la vez,
ella no enojarán, pero logró que todos se sientan que había toda su atención.
Lo tomó como la marca de alguien interesado en salir adelante, para demostrar
ella misma. Y luego, cuando él demandó a trabajar en el departamento de Marketing,
miró para ver su reacción, en busca de pistas para indicar si fue el establecimiento de un
relación con ella. Que era. Para el atacante, esto sumado a alguien que pudiera
manipular a través de una promesa de tratar de ayudarla a entrar en un mejor trabajo. (Por
Por supuesto, si ella había dicho que quería entrar en el departamento de Contabilidad, que
tendría que afirmó que había contactos para conseguir un puesto de trabajo que, en su lugar.)
Los intrusos también son aficionados de un arma psicológica utilizados en esta historia:
construcción de confianza con un ataque en dos etapas. Se utilizó por primera vez que la
conversación locuaz sobre
el trabajo en la comercialización, y también se utiliza "el nombre-que cae" - con el nombre del
otro empleado - una persona real, dicho sea de paso, al igual que el nombre que se utiliza
era el nombre de un empleado real.
Él pudo haber seguido hasta la primera conversación de inmediato a una solicitud de
entrar en una sala de conferencias. Pero en lugar de eso se sentó por un momento y fingió
trabajo, supuestamente esperando a su socio, otra manera de disipar cualquier posible
sospechas, ya que un intruso no colgar alrededor. No colgar alrededor de
mucho tiempo, aunque, los ingenieros sociales saben que no deben permanecer en el lugar de la
el crimen más tiempo del necesario.
Mitnick MENSAJE
Lo que permite a un extraño en un área donde se puede conectar un ordenador portátil en la
empresa
la red aumenta el riesgo de un incidente de seguridad. Es perfectamente razonable que una
los empleados, especialmente uno de fuera de la oficina, a desear para comprobar su correo
electrónico de un
sala de conferencias, pero menos que el visitante se establece como un empleado de confianza o
la
red está segmentada para evitar conexiones no autorizadas, esta puede ser la débil
enlace que permite a los archivos de la empresa se vea comprometida.
Sólo para que conste: Por las leyes en los libros en el momento de escribir esto, Anthony

no había cometido un delito cuando entró en el vestíbulo. Que no había cometido un crimen cuando él utilizó el nombre de un empleado real. Que no había cometido un crimen cuando hablaba de su camino en la sala de conferencias. Que no había cometido un crimen cuando se conecta a la red de la empresa y el objetivo buscado
equipo.
No hasta que realmente se rompió en el sistema informático hizo que violan la ley.
Recorriendo la lista de KEVIN
Hace muchos años cuando yo estaba trabajando en una empresa pequeña, empecé a darme cuenta de que
cada vez que entré en la oficina que compartía con el equipo otros tres
las personas que componían el departamento de TI, a este tipo en particular (Joe, voy a llamarlo aquí) rápidamente cambiar la pantalla de su ordenador a una ventana diferente. Yo inmediatamente lo reconoció como sospechoso. Cuando ocurrió dos veces más la
Ese mismo día, yo estaba seguro de que algo estaba pasando que me debe conocer. ¿Qué fue este hombre hasta que él no quería que yo viera?
Equipo de Joe actuó como un terminal para acceder a las minicomputadoras de la compañía, por lo que
instalado un programa de monitoreo en el sombrero minicomputadora VAX me permitió espiar en lo que estaba haciendo. El programa actuó como si una cámara de televisión estaba mirando por encima de su
hombro, y me mostró exactamente lo que estaba viendo en su computadora.
Mi escritorio estaba al lado de Joe, me volví a mi monitor lo mejor que pude a la parte máscara de su punto de vista, pero podía haber mirado más de un momento a otro y me di cuenta estaba espiando a él. No es un problema, estaba demasiado embelesado en lo que se haciendo notar.
Lo que vi me hizo caer la mandíbula. Yo observaba, fascinado, como el hijo de puta llamado mis datos de la nómina. Él estaba buscando a mi salario! Yo sólo había estado allí unos pocos meses en el momento y supuse Joe no podía soportar la idea de que podía
han estado haciendo más de lo que era.
Unos minutos más tarde vi que estaba descargando las herramientas utilizadas por hackers menos
hackers experimentados que no saben lo suficiente acerca de la programación para elaborar el herramientas por sí mismos. Así que Joe no tenía ni idea, y no tenía idea de que uno de American hackers más experimentados estaba sentado junto a él. Me pareció muy divertida.
Él ya tenía la información sobre mi sueldo, así que ya era demasiado tarde para detenerlo.
Además, cualquier empleado con acceso a computadoras del IRS o de la Seguridad Social
La administración puede buscar su salario para arriba. Estoy seguro que no quería que mi mano por la punta
haciéndole saber que había encontrado lo que estaba haciendo. Mi principal objetivo en el momento de
mantener un perfil bajo, y un ingeniero de bien social no hace publicidad de su habilidades y conocimientos. Uno siempre quiere que la gente te subestime, no ver que como una amenaza.
Así que lo dejé pasar, y se echó a reír a mí mismo que Joe pensaba que conocía algunos secretos sobre
yo, cuando era al revés: tenía la ventaja de saber lo que
había estado haciendo.
Con el tiempo descubrí que mis tres compañeros de trabajo en el grupo de TI divertido mismos buscando el salario neto de esta o aquella linda secretaria o (para
la chica en el grupo) de aspecto pulcro hombre que habían visto. Y todos eran averiguar el sueldo y las primas de nadie en la empresa tenían curiosidad alrededor, incluyendo la alta gerencia.
Con el análisis de la
Esta historia ilustra un problema interesante. Los archivos de nómina son accesibles para las personas que tenían la responsabilidad de mantener la computadora de la compañía

sistemas. Por lo tanto, todo se reduce a una cuestión personal: decidir a quién se puede confiar. En algunos casos, el personal que le resulte irresistible para husmear. Y tienen la capacidad para hacerlo porque no tienen los privilegios que les permite evitar el acceso controles en los archivos.

Uno de salvaguardia sería para auditar cualquier acceso a los archivos especialmente sensibles, tales como la nómina. Por supuesto, cualquier persona que tenga los privilegios necesarios puede desactivar auditoría o posiblemente eliminar cualquier entrada que apunte de nuevo a ellos, pero cada paso adicional requiere más esfuerzo para ocultar por parte de un empleado sin escrúpulos.

PREVENCIÓN DE LA CON

De patear a través de su basura para engañar a un guardia de seguridad o recepcionista, social ingenieros físicamente pueden invadir su espacio corporativo. Sin embargo, se le alegra escuchar que existen medidas preventivas que puede tomar.

Después del horario de protección

Todos los empleados que llegan a trabajar sin su tarjeta de identificación deberán ser obligados a parada en el mostrador del vestíbulo o en la oficina de seguridad para obtener una tarjeta de identificación temporal para el día.

El incidente en la primera historia de este capítulo podría haber llegado a un muy diferente conclusión, si los guardias de seguridad la empresa había tenido un conjunto específico de medidas para seguir cuando se enfrentan a cualquier persona sin la credencial de empleado requerido.

Para las empresas o áreas de una empresa donde la seguridad no es un alto nivel preocupación, tal vez no sea importante insistir en que cada persona tiene una tarjeta de identificación visible en todo momento. Pero en las empresas de las áreas sensibles, esto debería ser un estándar requisito, cumplir estrictamente. Los empleados deben ser capacitados y motivados para personas desafío que no muestran una insignia, y los empleados de alto nivel debe se les enseña a aceptar estos desafíos sin causar vergüenza a la persona que se lo impide.

Política de la empresa debe informar a los empleados de las sanciones para aquellos que forma sistemática no se llevan sus insignias, las sanciones pueden incluir el envío de la empleado en casa para el día sin goce de sueldo, o una anotación en su expediente personal. Algunos empresas en marcha una serie de sanciones cada vez más estrictas que pueden incluyen la presentación de informes el problema al gerente de la persona, entonces la emisión de una formal advertencia.

Además, cuando se dispone de información sensible a la protección, la empresa debe establecer procedimientos para las personas que necesitan autorización para visitar durante no comerciales horas. Una solución: requerir que se tomen medidas a través de las empresas de seguridad o algún otro grupo designado. Este grupo habitualmente se verifique la la identidad de cualquier empleado de llamar para concertar una hora fuera de la visita de una llamada al supervisor de la persona o algún otro método razonablemente seguro.

El tratamiento de la basura con respecto

La historia basurero de buceo excavado en el mal uso potencial de la basura corporativa.

Las ocho llaves de la sabiduría con respecto a la basura:

Clasificar toda la información sensible en función del grado de sensibilidad.

Establecer en toda la empresa los procedimientos para desechar la información sensible.

Insisten en que toda la información sensible que descartar primero ser triturados, y proporcionar de una manera segura para deshacerse de la información importante sobre trozos de papel también pequeño para la trituración. Trituradoras no debe ser el tipo de presupuesto de gama baja, que a su vez

de tiras de papel que un atacante determinado, dada la suficiente paciencia, puede volver a montar. En su lugar, tienen que ser del tipo llamado cross-trituradoras de papel, o los que hacer que la producción de celulosa en inútil.

Proporciona una forma de inutilización o borrado por completo los medios informáticos - disquetes, discos Zip, CD y DVD usado para almacenar archivos, cintas removibles, viejos discos duros y otros medios de comunicación computadora - antes de que se descartan. Recordar que la eliminación de archivos en realidad no eliminarlos, sino que todavía se puede recuperar - como Ejecutivos de Enron y otros muchos han aprendido a su pesar. Simplemente dejar caer los medios informáticos en la basura es una invitación a su contenedor ambiente local buceador. (Véase el capítulo 16 de directrices específicas sobre la eliminación de los medios y dispositivos.)

Mantener un adecuado nivel de control sobre la selección de las personas en su los equipos de limpieza, con antecedentes en su caso.

Recuerde a los empleados periódicamente para reflexionar sobre la naturaleza de los materiales que se tirar a la basura.

Bloqueo de contenedores de basura.

Use recipientes separados de eliminación de materiales de riesgo, y el contrato para que el materiales dispuestos por una empresa en régimen de servidumbre que se especializa en este trabajo.

Di adiós a los empleados

El punto se ha hecho anteriormente en estas páginas acerca de la necesidad de una férrea procedimientos cuando un empleado que se marcha ha tenido acceso a información sensible, contraseñas, números de acceso, etc. Los procedimientos de seguridad deben proporcionan una forma de no perder de vista que tiene autorización para varios sistemas. Es posible que ser duro para mantener un ingeniero social determinada que se deslice más allá de su seguridad barreras, pero no hacen que sea fácil para un ex-empleado.

Otro paso por alto fácilmente: Cuando un empleado que estaba autorizado a recuperar las cintas de respaldo de las hojas de almacenamiento, con una política escrita debe llamar a la empresa de almacenamiento para ser notificado inmediatamente para eliminar su nombre de su lista de autorizaciones.

Capítulo 16 de este libro proporciona. Información detallada sobre este tema vital, pero será útil para enumerar aquí algunas de las disposiciones clave de seguridad que deben estar en lugar, como se destaca en esta historia:

Una lista completa y exhaustiva de los pasos a seguir después de la salida de un empleado, con disposiciones especiales para los trabajadores que tenían acceso a datos sensibles.

Una política de terminar el acceso del empleado equipo de forma inmediata - preferiblemente antes de que la persona siquiera ha salido del edificio.

Un procedimiento de recuperación de la insignia de identificación de la persona, así como las llaves o electrónicos dispositivos de acceso.

Disposiciones que exigen que los guardias de seguridad para ver una identificación con foto antes de admitir cualquier empleado que no tiene pase su seguridad, y para comprobar el nombre con una lista para verificar que la persona sigue siendo empleado de la organización.

Algunos pasos más se parece excesivo o demasiado caros para algunas empresas, pero son apropiados para los demás. Entre estas medidas de seguridad más estrictos son los siguientes:

Tarjetas de identificación electrónica en combinación con los escáneres en las entradas, cada empleado

golpes a su tarjeta de identificación a través del escáner de una instantánea electrónica determinación de que la persona sigue siendo un empleado actual y con derecho a entrar en el edificio. (Nótese, sin embargo, que los guardias de seguridad que se deben estar capacitados para estar en la
alerta a cuestas - una persona no autorizada por el deslizamiento en la estela de un empleado legítimo.)
El requisito de que todos los empleados en el mismo grupo de trabajo como la persona que se va (Especialmente si la persona es ser despedido) cambiar sus contraseñas. (¿Esto se parece extrema? Muchos años después de poco tiempo que llevo trabajando en el teléfono general, que se enteró de que el Pacific Bell personal de seguridad, cuando se enteraron Teléfono General me había contratado ", rodó por el suelo de la risa." Pero a General Telephone
de crédito cuando se dieron cuenta que tenían una reputación de hacker trabajando para ellos después de que
establecidas fuera de mí, entonces requiere que las contraseñas se cambió para todos en la empresa!)
Usted no quiere que sus instalaciones para sentirse como las cárceles, pero al mismo tiempo que necesita para
defenderse contra el hombre que fue despedido ayer, pero hoy está de vuelta la intención de hacer
daños.
No se olvide Cualquiera
Las políticas de seguridad tienden a pasar por alto el trabajo de nivel de entrada, la gente le gusta recepcionistas que no manejan información confidencial de la empresa. Hemos visto
en otros lugares que las recepcionistas son un blanco muy útil para los atacantes, y la historia de la
robo en la empresa de piezas de automóviles es otro ejemplo: una persona amable,
vestido como un profesional, que dice ser empleado de una empresa de otro
institución no puede ser lo que parece. Recepcionistas tienen que estar bien entrenado sobre cortésmente pidiendo identificación de la compañía en su caso, y las necesidades de formación que se
no sólo por la recepcionista principal, pero también para todo aquel que se sienta en el alivio de la recepción durante las pausas para el almuerzo o un café.
Para los visitantes de fuera de la empresa, la política debe exigir que una identificación con foto se muestra y registra la información. No es difícil obtener documentos de identidad falsos, pero por lo menos
exigentes ID hace pre-texto de un grado más difícil para el atacante-ser.
En algunas empresas, tiene sentido de seguir una política que exige que los visitantes se escoltado desde el vestíbulo y de reunión en reunión. Los procedimientos deben requerir
que la escolta de dejar en claro al entregar al visitante a su primera cita que
esta persona ha entrado en el edificio como un empleado o no empleado. ¿Por qué es
esto es importante? Porque, como hemos visto en anteriores
historias, un atacante a menudo se hace pasar en un pretexto para la primera persona encontrado, y que otra persona a otra. Es demasiado fácil para un atacante para mostrar
En el vestíbulo, convencer a la recepcionista que tiene una cita con, por ejemplo, un ingeniero .., y luego ser escoltado a la oficina del ingeniero en la que dice ser un representante de de una empresa que quiere vender algún producto a la empresa .., y luego, después de
la reunión con el ingeniero, que tiene acceso libre para vagar por el edificio.
Antes de admitir a un empleado fuera de las instalaciones de los locales, los procedimientos adecuados que
seguir para verificar que la persona es realmente un empleado, recepcionistas y
los guardias deben ser conscientes de los métodos utilizados por los atacantes para pretexto de la identidad de un
empleado con el fin de tener acceso a los edificios de la empresa.
¿Qué hay de la protección contra el atacante que tima a su manera dentro del edificio
y se las arregla para conectar su computadora portátil en un puerto de red detrás del firewall

corporativo?
Dada la tecnología actual, esto es un desafío: salas de conferencias, salas de formación, y áreas similares, no deben salir de los puertos de la red no segura, pero debe proteger con cortafuegos o routers. Sin embargo, una mejor protección que provienen de la utilización de un método seguro para autenticar a los usuarios que se conectan a la red.
Secure IT!
Una palabra al sabio: En su propia empresa, todos los trabajadores de TI probablemente sabe o puede encontrar en los momentos cuánto ganan, cuánto tarda el CEO
casa, y que está utilizando el avión de la empresa para ir de vacaciones a esquiar.
Es posible, incluso en algunas empresas de TI la gente o la gente de contabilidad para aumento de sus salarios, los pagos a un proveedor de falso, eliminar negativos
Calificaciones de los registros de recursos humanos, y así sucesivamente. A veces es sólo el temor de quedar atrapados
que los mantiene honestos .., y un día a lo largo viene alguien cuya codicia
o deshonestidad natal lo hace (o ella) ignorar el riesgo y tomar todo lo que
cree que puede salirse con la suya.
Hay soluciones, por supuesto. Archivos confidenciales se pueden proteger mediante la instalación de
acceso a los debidos controles para que sólo personas autorizadas pueden abrir. Algunos los sistemas operativos tienen controles de auditoría que puede ser configurado para mantener un registro de
ciertos eventos, como cada persona que intenta acceder a un archivo protegido, independientemente de si el intento tiene éxito.
Si su empresa ha entendido este problema y ha puesto en marcha un acceso adecuado controles y auditorías que protege los archivos confidenciales - usted está tomando medidas de gran alcance en el
la dirección correcta.

Capítulo 11
La combinación de la tecnología y la ingeniería social

Una vida de ingeniero social por su capacidad para manipular a la gente a hacer cosas que ayudarle a lograr su objetivo, pero a menudo el éxito también requiere un alto grado de conocimientos y habilidades con los sistemas informáticos y los sistemas de telefonía.
Esta es una muestra típica de las estafas de ingeniería social, donde la tecnología juega un papel importante.
HACKING TRAS LAS REJAS
¿Cuáles son algunas de las instalaciones más seguras que se pueda imaginar, protegidos contra robo, si? física, telecomunicaciones, electrónica o en la naturaleza Fuerte
Knox? Seguro. La Casa Blanca? Por supuesto. NORAD, el aire de América del Norte
Instalación de defensa enterrado bajo una montaña? Por supuesto que sí.
¿Qué hay de las prisiones federales y centros de detención? Se debe ser tan segura como en cualquier lugar del país, ¿verdad? La gente rara vez escapan, y cuando lo hacen, normalmente son atrapados en el corto plazo. Se podría pensar que una institución federal invulnerable a los ataques de ingeniería social. Pero sería un error - no hay
no hay tal cosa como la seguridad a toda prueba, en cualquier lugar.
Hace unos años, un par de timadores (estafadores profesionales) se encontró con un problema. Lo
Resultó que había levantado un gran paquete de dinero en efectivo de un juez local. La pareja se había
tenido problemas con la ley y fuera a través de los años, pero esta vez los federales
Las autoridades se interesaron. Que atrapó a uno de los timadores, Charles Gondorff, y le arrojó en un centro penitenciario cerca de San Diego. El magistrado federal
ordenó que lo detuvieron como riesgo de fuga y un peligro para la comunidad.
Su amigo Johnny Hooker sabía que Charlie iba a necesitar un abogado defensor.

Pero ¿dónde estaba el dinero va a venir? la mayoría de los tramposos, el dinero había siempre ha ido por la buena ropa, cámara de lujo y las damas tan rápido como entró Johnny larely tenía lo suficiente para vivir.
El dinero para un buen abogado tendría que venir la ejecución de otra estafa.
Johnny no estaba en condiciones de hacer esto en este mismo. Charlie Gondorff siempre había sido
el cerebro detrás de sus contras. Pero Johnny no se atrevió a visitar el centro de detención para Charlie pregunta qué hacer, no cuando los federales sabían que había dos hombres involucrados en la estafa y estaban tan ansiosos de poner sus manos sobre la otra. Especialmente ya que la familia sólo se puede visitar. lo que significaba que tendría que mostrar una identificación falsa
y pretende ser un miembro de la familia. Tratar de usar identificaciones falsas en una prisión federal no
suena como una idea inteligente.
No, tendría que ponerse en contacto con Gondorff alguna otra manera.
No sería fácil. Ningún preso en todas las instalaciones federales, estatales o locales, se permite que
recibir llamadas telefónicas. Un letrero colocado por cada teléfono interno en un federal centro de detención, dice algo así como: "Este aviso es para informar al usuario que todos los las conversaciones de este teléfono están sujetos a control. y el uso de la
teléfono constituye el consentimiento a la supervisión. Hacer que los funcionarios del gobierno escuchar sus llamadas telefónicas, mientras que la comisión
un delito tiene una forma de extender el financiamiento federal los planes de vacaciones.
Johnny sabía, sin embargo, que ciertas llamadas telefónicas no fueron controlados: las llamadas entre el recluso y su abogado, protegido por la Constitución como clientattorney comunicaciones, por ejemplo. De hecho, las instalaciones donde Gondorff
se encontraba detenido había teléfonos conectados directamente a la Administración Pública Federal
Oficina del Defensor. Tome uno de esos teléfonos, y una conexión directa
está hecho para el teléfono correspondiente en la Denominación de Origen. La compañía telefónica llama
este servicio de Conexión Directa. Las autoridades desprevenidas asumir el servicio es seguro e invulnerable a las manipulaciones, porque saliente
llamadas sólo pueden ir a la Denominación de Origen, y las llamadas entrantes están bloqueadas. Incluso si alguien
eran de alguna manera capaz de averiguar el número de teléfono, los teléfonos están programados
en el interruptor de la compañía telefónica como negar terminar, que es un torpe
plazo la compañía telefónica para el servicio en las llamadas entrantes no están permitidos.
Ya que cualquier estafador medianamente decente está bien versado en el arte del engaño, Johnny
imaginé que tenía que haber una solución a este problema. Desde el interior, Gondorff ya había intentado recoger uno de los teléfonos DOP y diciendo: "Este es Tom, en la compañía de teléfonos centro de reparación.
LINGO
DIRECTO teléfono, conecte plazo para la empresa una línea telefónica que va directamente a un número específico al recogerlo
NEGAR terminar una compañía telefónica opción de servicio donde el cambio de equipo se encuentra que las llamadas entrantes no se pueden recibir a un número de teléfono
Estamos corriendo una prueba en esta línea y necesito que intente marcar nueve, y luego CEROACERO ".
Los nueve que han tenido acceso a una línea exterior, el cero-cero, entonces se han llegado a un operador de larga distancia. No funcionó la persona que contesta la teléfono en la denominación de origen fue de la cadera ya que ese truco.
Johnny estaba teniendo más éxito. Él rápidamente se enteró de que había diez

unidades de vivienda en el centro de detención, cada uno con una línea telefónica directa para conectar
la Oficina del Defensor Público. Johnny encontró con algunos obstáculos, sino como una ingeniero social, fue capaz de pensar en su camino alrededor de estos obstáculos molestos bloques. ¿Qué unidad se Gondorff en? ¿Cuál fue el número de teléfono a la
conexión directa de servicios en esa unidad de vivienda? ¿Y cómo en un principio conseguir una mensaje a Gondorff sin que sea interceptada por funcionarios de la prisión?
Lo que parece ser lo imposible para gente común, como la obtención de los secretos números de teléfono situado en las instituciones federales, es muy a menudo no es más que una cuantas llamadas telefónicas de distancia de un estafador. Después de un par de lanzar-y-vuelta noches
un plan de intercambio de ideas, Johnny se despertó una mormng con todo el asunto presentado en su mente, en cinco pasos.
En primer lugar, que iba a encontrar los números de teléfono de las diez de conexión directa a los teléfonos
la Denominación de Origen.
Tendría que los diez cambiado de modo que los teléfonos que permiten las llamadas entrantes.
Había que encontrar vivienda Gondorff estaba en marcha.
Luego se descubriría que el número de teléfono fue a esa unidad.
Por último, había arreglos con Gondorff cuando se espera su llamado, sin la
Gobierno sospechar algo.
Pieza de un pastel ", pensó.
Llamar a Ma Bell ...
Johnny empezó llamando a la compañía de teléfonos de oficinas de negocios, con el pretexto de siendo de la Administración de Servicios Generales, el responsable de agenc
compra de bienes y servicios para el gobierno federal.
Dijo que estaba trabajando en una orden de adquisición de servicios adicionales y necesarios para conocer la información de facturación para los servicios de conexión directa en la actualidad
en uso, incluyendo los números de teléfono de trabajo y el costo mensual en el San Diego el centro de detención. La señora estaba feliz de ayudar.
Sólo para asegurarse, trató de marcar en una de esas líneas y fue contestado por el grabación audichron típica: "Esta línea ha sido desconectada o ya no está en
servicio ", que él sabía que no significaba nada de clase, pero en lugar de decir que la línea fue programado para bloquear las llamadas entrantes, así como él esperaba.
Sabía, por su amplio conocimiento de las operaciones de la compañía telefónica y los procedimientos que había que llegar a un departamento llamado el reciente cambio Centro de Autorización de la memoria o RCMAC (yo siempre pregunto quién
hace estos nombres!). Empezó llamando a la compañía de teléfonos de negocios Oficina, dijo que estaba en reparación y es necesario saber el número de la RCMAC que se encargó del área de servicio para el código de área y el prefijo que dio, que fue servido de la misma oficina central para todas las líneas telefónicas para la detención centro. Fue una solicitud de rutina, tal como se contempla para los técnicos en el campo en necesidad de algún tipo de asistencia, y el secretario no dudó en darle la
número.
Llamó a RCMAC, dio un nombre falso y otra vez dijo que estaba en reparación
Él tenía la señora que contestó acceder a uno de los números de teléfono que había estafado fuera de la oficina de negocios un par de llamadas antes, cuando ella tenía arriba, Johnny
preguntó: "¿Es el número establecido para negar la terminación?
"Sí", dijo.
"Bueno, eso explica por qué el cliente no es capaz de recibir llamadas!" Johnny dijo.
"Oye, ¿me haces un favor. Tengo que cambiar el código de la clase o la línea
eliminar la función de negar terminar, ¿de acuerdo? "Hubo una pausa mientras comprobaba otro sistema informático para verificar que una orden de servicio se había colocado a

autorizar el cambio. Ella dijo: "Ese número se supone que es restringido por
llamadas salientes. No hay orden de servicio para un cambio. "
"Cierto, es un error. Se suponía que el proceso para ayer, pero la
representante de cuenta que se encarga de regular este cliente fue a su casa enfermo y se olvidó de tener
otra persona se encargue de la orden de ella. Así que ahora, por supuesto, el cliente es de hasta en los brazos de él. "
Después de una pausa momentánea mientras que la mujer reflexionó sobre esta solicitud, que se fuera de lo común y en contra de los procedimientos de operación estándar, dijo, "Está bien". Podía oír su escritura, entrando en el cambio. Y unos segundos más tarde, fue
hacer.
El hielo se había roto, una especie de complicidad establecida entre ellos. Lectura
la actitud de la mujer y la voluntad de ayudar, Johnny no duda en ir a por ello
todos. Él dijo, "¿Tiene usted unos minutos más para que me ayude?"
"Sí," respondió ella. "¿Qué necesita?"
"Tengo una varias líneas de otros que pertenecen a un mismo cliente, y todos tienen la
mismo problema. Voy a leer los números, por lo que puede asegurarse de que no están establecidos
para negar a terminar - está bien ", dijo ella que estaba bien.
Unos minutos más tarde, las diez líneas telefónicas habían sido "arreglado" para aceptar de entrada
llamadas.
Encontrar Gondorff
A continuación, averiguar lo que la unidad de vivienda Gondorff estaba en marcha. Esta es la información que el
personas que dirigen los centros de detención y prisiones definitivamente no quieren a los forasteros
saben. Una vez más, Johnny tuvo que confiar en sus habilidades de ingeniería social.
Él hizo una llamada a una prisión federal en otra ciudad - que él llamó Miami,
pero cualquiera hubiera funcionado - y afirmó que estaba llamando desde la detención
centro de Nueva York. Pidió hablar con alguien que trabajó con la Oficina de
Sentry ordenador, el sistema informático que contiene información sobre todos los
preso detenido en una Oficina de Prisiones instalación en cualquier lugar del país.
Cuando esa persona se puso al teléfono, Johnny se puso el acento de Brooklyn. "Hola"
dijo. "Se trata de Thomas en la Nueva York FDC. Nuestra conexión con Sentry mantiene
bajando, se puede encontrar la ubicación de un prisionero de mí, creo que este preso
puede ser en su institución, "y le dio el nombre de Gondorff y su registro
número.
"No, él no está aquí", dijo el hombre después de un par de momentos. "Está en el
centro correccional de San Diego. "
Johnny fingió estar sorprendido. "San Diego! Se suponía que debía ser transferido
a Miami el puente aéreo de la Mariscal, la semana pasada! Estamos hablando del mismo tipo - Fecha de nacimiento lo que el tipo es? "
03/12/60 ", dice el hombre de su pantalla.
"Sí, es la misma persona. ¿Qué unidad de vivienda que está en?"
"Él es el Diez del Norte", dijo el hombre - alegremente responder a la pregunta
a pesar de que no hay ninguna razón concebible por qué un empleado de la prisión en
Nueva York tendría que saber esto.
Johnny ya se había convertido en los teléfonos para llamadas entrantes, y sabía que
unidad de vivienda Gondorff estaba en marcha. A continuación, determinar qué número de teléfono conectado a
Diez unidades del Norte.
Esto fue un poco difícil. Johnny llamó a uno de los números. Sabía que el
timbre del teléfono se apaga, y nadie sabría que estaba sonando. Por lo que
sentado leyendo Europa Fodor} guía de viajes a Gran ciudades. mientras escucha la

un zumbido constante en el altavoz, hasta que finalmente alguien recogió. El preso en el otro extremo, por supuesto, estar tratando de llegar a su abogado de oficio. Johnny fue preparado con la respuesta esperada. "Defensoría del Pueblo", que anunció.

Cuando el hombre le preguntó a su abogado, Johnny dijo: "Voy a ver si está disponible, lo que unidad de vivienda está llamando? "Él anotó por la respuesta del hombre, hace clic en en espera, volvió después de medio minuto y le dijo: "Está en la corte, usted tendrá que llame más tarde ", y colgó.

Había pasado la mayor parte de la mañana, pero podría haber sido peor, su cuarto intento que resultó ser de diez Norte. Así que Johnny ya sabía el número de teléfono en el teléfono DOP en la unidad de vivienda de Gondorff.

Sincronizar sus relojes

Ahora para conseguir un mensaje a través de Gondorff en cuando para recoger la línea telefónica que conecta a los presos directamente a la Oficina del Defensor Público.] "Era más fácil su de lo que parece.

Johnny llamó al centro de detención con su oficial de sonido de voz, identificada a sí mismo como un empleado, y pidió ser trasladado a diez del Norte. La llamada fue puesto a través. Cuando el funcionario de prisiones se recogió, Johnny estafado lo mediante el uso de la abreviatura de información privilegiada para la recepción y descarga, la unidad que

procesos internos nuevos, y salen los que: "Este es Tyson en I + D", que , dijo. "Tengo que hablar con Gondorff preso. Tenemos alguna propiedad de sus tenemos para enviar y necesitamos una dirección donde quiere que lo envió. ¿Podría usted lo llama a la teléfono para mí? "

Johnny podía oír la guardia gritando a través del cuarto día. Después de un impaciente varios minutos, una voz familiar se puso al aparato.

Johnny le dijo: "No digas nada hasta que me explique de qué se trata." Explicó con el pretexto de que Johnny podría sonar como si estuviera discutiendo en su propiedad se entregará. Johnny dijo entonces: "Si se puede llegar a la Defensoría del Pueblo teléfono en una de esta tarde, no responden. Si no puede, entonces decir una vez que se puede estar ahí ". Gondorff no respondió. Johnny continuó:" Bien. Estar allí en un en punto. Te llamo luego. Levante el teléfono.

Si empieza a sonar a la Oficina de Defensores Públicos, flash del conmutador cada gancho veinte segundos. Sigue intentándolo hasta que me oye en el otro extremo. "

A la una, Gondorff cogió el teléfono, y Johnny estaba allí esperando para él. Tenían un hablador, conversación agradable, sin prisas, dando lugar a una serie de llamadas similar al plan de la estafa que conseguir el dinero para pagar Gondorff legal de honorarios - todo libre de la vigilancia gubernamental.

Con el análisis de la

Este episodio ofrece un excelente ejemplo de cómo un ingeniero social puede hacer que el aparentemente imposible pasar por estafar a varias personas, cada uno haciendo algo que, por sí mismo, parece intrascendente. En realidad, cada acción proporciona una pequeña pieza del rompecabezas hasta que la estafa es completa.

El empleado de la compañía telefónica primero pensó que estaba dando información a alguien de la oficina del gobierno federal de Contabilidad General.

El empleado de la compañía telefónica próxima sabía que no iba a cambiar la clase del servicio telefónico sin una orden de servicio, sino que ayudó a que el hombre amable de todos modos. Esto hizo posible realizar llamadas a través de las diez de la opinión pública defensor de las líneas telefónicas en el centro de detención.

Para el hombre en el centro de detención en Miami, la petición para ayudar a alguien en otra instalación federal con un problema parecía perfectamente razonable.

Y a pesar de que no parecía ninguna razón por la que se quiere conocer la vivienda, ¿por qué no responder a la pregunta?

Y el guardia de Diez Norte que creía que la llamada era realmente desde dentro la misma instalación, llamando en comisión de servicio? Fue una muy razonable

solicitud, por lo que llamó la Gondorff preso al teléfono. No es gran cosa.
Una serie de historias bien planificado que se acercaba a completar la picadura.
LA DESCARGA SPEEDY
Diez años después de haber terminado la escuela de leyes, Ned Racine vio a sus compañeros de clase
que viven en casas bonitas con césped delante, que pertenecen a clubes de campo, jugar al golf una o dos veces por semana, mientras él estaba todavía tratando penique-ante los casos para el tipo de
gente que nunca había suficiente dinero para pagar su factura. Los celos pueden ser un desagradable
compañero. Finalmente, un día, Ned había tenido suficiente.
El cliente una buena que había tenido era una firma de contabilidad pequeña pero muy exitosa que se especializa en fusiones y adquisiciones. Que no habían usado Ned por mucho tiempo, sólo tiempo suficiente para darse cuenta de que estaban involucrados en negocios que, una vez que lleguen a la
periódicos, podría afectar el precio de las acciones de uno o dos que cotizan en bolsa
las empresas. Ante Penny, tablón de anuncios de las existencias, pero de alguna manera que era aún
mejor - un pequeño salto en los precios podría representar una ganancia en un gran porcentaje inversión. Si pudiera aprovechar sus archivos y averiguar lo que estaban
trabajando en ...
Él sabía que un hombre que conocía a un hombre que era sabio no sobre las cosas exactamente en el
la corriente principal. El hombre escuchó el plan, fue despedido y acordó ayudar. Para una menor costo de lo que suele cobrar, frente a un porcentaje del mercado de valores de Ned
la muerte, el hombre dio instrucciones Ned sobre qué hacer. También le dio una mano pequeño dispositivo a utilizar, algo nuevo en el mercado.
Por unos días en una fila Ned vigilaban el estacionamiento de la pequeña empresa
parque en el que la empresa tuvo su contabilidad sin pretensiones, como escaparate de las oficinas.
La mayoría de la gente que queda entre las 5:30 y las 6. A las 7, el lote estaba vacío. El equipo de limpieza
se presentaron alrededor de las 7:30. Perfecta.
La noche siguiente, en unos pocos minutos antes de las 8 en punto, Ned aparcado al otro lado de la calle
desde el estacionamiento. Tal como esperaba, la suerte estaba vacía excepto por el camión de la compañía de servicios de limpieza. Ned puso la oreja a la puerta y escuchó el vacío
más limpia en funcionamiento. Llamó a la puerta muy fuerte, y se quedó esperando en
su traje y corbata, la celebración de su gastada cartera. No hubo respuesta, pero él estaba enfermo.
Llamó a la puerta de nuevo. Un hombre del equipo de limpieza finalmente apareció. "Hola," Ned gritó a través de la puerta de cristal, mostrando la tarjeta de visita de uno de los socios
que él había tomado un tiempo anterior. "Cerré mis llaves de mi coche y necesito
para llegar a mi escritorio. "
El hombre abrió la puerta, la cerró de nuevo detrás de Ned, y luego bajó por la
corredor de encender las luces para Ned podía ver a dónde iba. ¿Y por qué no - se estaba siendo amable con una de las personas que ayudaron a poner comida en su mesa. O así lo
había muchas razones para pensar.
Mitnick MENSAJE
Espías industriales e intrusos informáticos a veces hacer una entrada física en
la empresa objetivo. En lugar de usar una palanca para entrar, el ingeniero social utiliza el arte del engaño para influir en la persona del otro lado de la puerta
abiertas para él.
Ned se sentó en la computadora de uno de los socios, y lo encendió. A pesar de que

fue la puesta en marcha, se instaló el pequeño dispositivo que le habían dado en el puerto USB de la computadora, un aparato lo suficientemente pequeño para llevar en un llavero, y sin embargo capaz de mantener
más de 120 megabytes de datos. Que conectado a la red con el nombre de usuario y la contraseña de la secretaria de la pareja, que fueron escritas por conveniente en un post-it pegado a la pantalla. En menos de cinco minutos, Ned descargar todas las hojas de cálculo y archivos de documentos almacenados en la estación de trabajo y
del directorio de la red de la pareja y se dirigía a su casa.

DINERO FACIL

Cuando tuve mi primer contacto con las computadoras en la escuela secundaria, había que conectarse a través de
un módem a una central minicomputadora DEC PDP 11 en el centro de Los Angeles que todas las escuelas secundarias en Los Ángeles compartida. El sistema operativo en ese equipo
fue llamado RSTS / E, y fue el sistema operativo que aprendió a trabajar con ellos.

En ese momento, en 1981, diciembre patrocinó una conferencia anual para usuarios de su producto,
y un año leí que la conferencia iba a realizarse en Los Ángeles una popular la revista para los usuarios de este sistema operativo llevado a un anuncio sobre un nuevo la seguridad del producto, LOCK-11. El producto se está promoviendo con un anuncio inteligente campaña que dice algo como, "son las 3:30,. M. y Johnny en la calle
Encontré su número telefónico, 555-0336, en su intento 336a. Está dentro y estás fuera. Obtener bloqueo-11. "El producto, el anuncio sugerido, fue prueba de hackers. Y fue va a ser expuesto en la conferencia.

Yo estaba ansioso por ver el producto por mí mismo. Un compañero de la escuela secundaria y un amigo, Vinny,
mi compañero de hacking desde hace varios años que más tarde se convirtió en un informante federal
en mi contra, compartía mi interés en el nuevo producto de diciembre, y me animó a ir a la conferencia con él.

Dinero en efectivo en la línea

Llegamos a encontrar un zumbido grande ya van alrededor de la multitud en la feria sobre el lock-11. Parecía que los desarrolladores se apostando dinero en efectivo en la línea en un
Apuesto a que nadie podía entrar en su producto. Sonaba como un desafío que podía no resistir.

Nos dirigimos directamente a que el bloqueo-11 cabina y lo encontró tripulada por tres hombres que fueron los desarrolladores del producto, que los reconoció y reconoce que
me - incluso en la adolescencia, ya tenía una reputación como un hacker y phreaker, porque de una gran historia Los Angeles Times, se había quedado en mi primer contacto de menores con la
autoridades. El artículo informaba de que había hablado a mi manera en un teléfono del Pacífico edificio en el medio de la noche y salió con manuales de informática, derecho
bajo las narices de la guardia de seguridad. (Al parecer, el Times quería correr un historia sensacionalista y que servían a sus propósitos de publicar mi nombre, porque yo era todavía menor de edad, el artículo violado la costumbre, si no la ley de retenciones los nombres de los menores acusados de mala conducta.)

Cuando Vinny y yo fuimos para arriba, ir creado un cierto interés en ambos lados. No se el interés de su parte porque me reconoció como el hacker que había leído
acerca y que eran un poco sorprendido de verme. Se creó un interés de nuestro lado porque cada uno de los tres desarrolladores estaba de pie allí con un billete de $ 100 se pegue de su tarjeta de identificación de la feria. El dinero del premio para alguien que podía derrotar a sus
sistema sería el conjunto $ 300 - que suena como un montón de dinero a un par de

adolescentes. Casi no podía esperar para empezar.
BLOQUEO-11 fue diseñado en un principio básico que se basó en dos niveles de
la seguridad. Un usuario tenía que tener un ID y una contraseña válidos, como es habitual, sino que además
ID y la contraseña que sólo funciona cuando entró en los terminales autorizados,
un enfoque llamado terminal basado en la seguridad. Para derrotar el sistema, un hacker
necesidad no sólo de tener conocimiento de un ID de usuario y contraseña, sino que también
tiene que introducir la información de la terminal correcta. El método fue así
establecidos, y los inventores de BLOQUEO-11 fueron convencidos de que mantendrá el mal
chicos a cabo. Decidimos que íbamos a darles una lección, y ganar tres
cientos de dólares para arrancar.
Un hombre que sabía que era considerado un RSTS / E gurú ya nos había golpeado a la
cabina. Años antes había sido uno de los chicos que había desafiado a mí para romper
en el equipo de desarrollo interno de diciembre, después de que sus asociados habían
me dio vuelta pulg Desde esos días se había convertido en un programador respetado. Nosotros
se enteró de que había tratado de derrotar a los BLOQUEO-11 programa de seguridad no mucho
antes de llegar, pero no había podido. El incidente había dado a los desarrolladores
una mayor confianza de que su producto realmente seguro.
LINGO
TERMINAL DE SEGURIDAD BASADA Seguridad basada en parte en la identificación
de la terminal de computadora empleada en particular, este método de seguridad se
especialmente popular entre los mainframes de IBM.
El concurso fue todo un reto sencillo: entrar, usted gana el dinero. A
truco de la publicidad .. bueno, a menos que alguien fue capaz de avergonzar y tomar la
dinero. Ellos estaban tan seguros de su producto que se alcanza ni siquiera audaz
para tener una impresión publicado en el stand de dar los números de cuenta y
contraseñas correspondientes a algunas cuentas en el sistema. Y no sólo regular
las cuentas de usuario, pero todas las cuentas privilegiadas.
Que en realidad era menos audaz de lo que parece: En este tipo de set-up, lo sabía, cada
terminal está conectado a un puerto en la computadora en sí misma. No era un genio para
averiguar que habían establecido las cinco terminales en la sala de conferencias para un visitante
pueden conectarse de forma única como un usuario sin privilegios - es decir, inicios de sesión
sólo fueron posibles a
cuentas sin privilegios de administrador del sistema. Parecía como si sólo hubiera
dos vías: o bien pasar por alto el software de seguridad completo - exactamente lo que el
BLOQUEO-11 fue diseñado para prevenir, o de alguna forma todo el software de una manera
que los desarrolladores no se había imaginado.
Aceptar el reto
Vinny y yo se alejó y habló sobre el desafío, y se me ocurrió una
plan. Estamos recorriendo el lugar inocentemente, manteniendo un ojo en el stand de una
distancia. A la hora del almuerzo, cuando la multitud adelgazado, los tres desarrolladores se
ventaja de la ruptura y se quitó juntos para conseguir algo de comer, dejando
detrás de una mujer que podría haber sido la esposa o la novia de uno de ellos. Nosotros
paseó de nuevo una y me distrae de la mujer, hablando de su en torno a esta y
que, "¿Cuánto tiempo ha estado en la compañía?" ¿Qué otros productos se
Su empresa tiene en el mercado? "y así sucesivamente.
Mientras tanto, Vinny, de su línea de visión, había ido a trabajar, haciendo uso de una habilidad
él y yo habíamos desarrollado. Además de la fascinación de la intrusión en los ordenadores,
y mi propio interés en la magia, que habían estado intrigados por aprender a
abrir cerraduras. Como un chico joven, que había rastreado los estantes de un metro
librería en el Valle de San Fernando que tuvieron un volumen de cerraduras picking, consiguiendo
de las esposas, la creación de identidades falsas - de todo tipo de cosas que un niño no se
se supone que conoce.
Vinny, como yo, había practicado la cerradura-cosecha hasta que estaban bastante bien con
cualquier

ejecución de la fábrica de hardware de la tienda de bloqueo. Había habido un tiempo en que de una patada
participación de las cerraduras de las bromas, como si alguien que estaba manchado con dos cerraduras de
mayor protección, recogiendo las cerraduras, y los puso el anillo de nuevo en los lugares opuestos,
que desconciertan y frustran al propietario cuando trató de abrir cada uno con la tecla equivocada.
En la sala de exposiciones, que continuó manteniendo la joven distraído mientras Vinny, en cuclillas en la parte posterior de la cabina para que no pudiera beseen, recogió el bloqueo el gabinete que albergaba su minicomputadora PDP-11 y las terminaciones de cable.
Para llamar a la caja estaba cerrada casi una broma. Fue asegurado con lo que los cerrajeros se refieren a un bloqueo de la oblea, notablemente fácil de aprender, incluso para los muy torpes, amateur
lock-recolectores como nosotros.
Se llevó a Vinny todos alrededor de un minuto para abrir la cerradura. En el interior del gabinete se encontró
justo lo que habíamos anticipado: la banda de los puertos para conectar los terminales de usuario, y
un puerto para lo que se llama la terminal de consola. Este fue el utilizado por el terminal equipo operador o administrador del sistema para controlar todos los ordenadores. Vinny conectado el cable que va desde el puerto de la consola en uno de los terminales de la mostrar suelo.
Eso significaba que este terminal fue un reconocido ahora como un terminal de consola. Me senté abajo en la máquina y recabled iniciado sesión con una contraseña los desarrolladores tenían tan audaz siempre. Porque el bloqueo de software-11 ahora se identifica que
Se conecta desde un terminal autorizado, que me concedió el acceso, y se me conectado con privilegios de administrador del sistema. Yo parcheado el sistema operativo cambiando de tal manera que desde cualquiera de los terminales en el suelo, yo sería capaz de iniciar la sesión como usuario con privilegios.
Una vez que el parche se ha instalado en secreto, Vinny regresó al trabajo de desconectar el terminal del cable que conectar de vuelta en donde había estado originalmente. Luego tomó el bloqueo una vez más, esta vez para sujetar la puerta del armario cerrado.
Hice un listado de directorio para averiguar qué archivos estaban en el equipo, en busca de el programa de la cerradura-11 y los archivos asociados y tropezó con algo que encontré impactante: un directorio que no debería haber estado en esta máquina. Los desarrolladores había sido tan confiado, tan seguro de su software era invencible, que
no se había molestado en quitar el código fuente de sus nuevos productos. Pasando a la adyacentes en papel terminal, empecé a imprimir porciones del código fuente
en las hojas de papel continuo de la computadora de rayas verdes utilizadas en los días.
Vinny sólo había apenas terminado de recoger el candado cerrado y se reunió conmigo cuando los chicos de volver de almorzar. Me encontraron sentado en la computadora golpes
las teclas mientras la impresora sigue rotación de distancia. "What'cha haciendo, Kevin?" preguntó uno de ellos.
"Oh, sólo imprimir su código fuente," le dije. Se suponía que yo estaba bromeando, de Por supuesto. Hasta que miró a la impresora y vio que realmente u, como los celos guardado código fuente de su producto.
Ellos no creían que era posible que yo era iniciar la sesión como un usuario privilegiado.
"Escriba un Control-T", ordenó uno de los desarrolladores. Yo lo hice. La pantalla que apareció en la pantalla confirma mi afirmación. El chico se golpeó la frente, como Vinny dijo: "Trescientos dólares, por favor."
Mitnick MENSAJE
He aquí otro ejemplo de gente inteligente subestimar al enemigo. ¿Qué tal
que - usted está tan seguro acerca de las garantías de seguridad de su empresa que le

apuesta de $ 300 contra un atacante en romper? A veces el camino en torno a un dispositivo de seguridad tecnológica no es el esperado.
Que pagó. Vinny y yo caminamos por la pista de feria para el resto de la día con los billetes de cien dólares clavados en insignias de nuestra conferencia. Todo el mundo que vieron los billetes sabía lo que representaban.
Por supuesto, Vinny y yo no había derrotado a su software, y si el equipo de desarrollo había pensado en establecer mejores reglas para el concurso, o que habían utilizado un cierre muy seguro, o había visto a su equipo con más cuidado, no habría sufrido el humillación de ese día - la humillación a manos de un par de adolescentes.
Más tarde me enteré de que el equipo de desarrollo tuvo que pasar por el banco para obtener dinero en efectivo: los billetes de cien dólares representa el gasto todo el dinero que habían traído con ellos.

El diccionario como una herramienta de ataque

Cuando alguien obtiene la contraseña, que es capaz de invadir el sistema. En la mayoría de circunstancias, usted ni siquiera sabe que algo malo ha sucedido.
Un joven atacante Voy a llamar a Ivan Peters tenía una meta de recuperar el código fuente de un juego electrónico de nuevo. No tenía problemas para entrar en zona amplia de la empresa red, ya que un amigo hacker de su se había comprometido ya una de las compañía de los servidores Web. Después de encontrar una vulnerabilidad sin parchear en la Web software de servidor, su amigo había casi caído de su silla cuando se dio cuenta el sistema se había establecido como una serie de base dual, lo que significaba que había una entrada punto en la red interna. .
Pero una vez que Ivan estaba conectado, entonces frente a un desafío que fue como estar dentro de el Louvre y la esperanza de encontrar a la Mona Lisa. Sin un plan de piso, se puede vagar durante semanas. La empresa fue global, con cientos de oficinas y miles de servidores de un ordenador, y no precisamente proporcionar un índice de el desarrollo de sistemas o de los servicios de un guía para dirigirlo a la derecha.
En lugar de utilizar un enfoque técnico para averiguar qué servidor que tenía que objetivo, Ivan utiliza un enfoque de ingeniería social. Puso sobre la base de las llamadas telefónicas métodos similares a los descritos en este libro. En primer lugar, llama soporte técnico, que decía ser empleado de una empresa que tiene una interfaz problema en un producto que su grupo estaba diseñando. y le pidió el número de teléfono de el líder del proyecto para el equipo de desarrollo de juegos.
Entonces llamó el nombre que le habían dado, haciéndose pasar por un chico de TI. "Más tarde esta noche ", dijo," estamos cambiando a un router y la necesidad de asegurarse de que la gente en su equipo no pierda la conectividad con el servidor. Así que tenemos que saber qué servidores que utiliza su equipo. "La red se está actualizando todo el tiempo. Y dando el nombre del servidor no estaría de más nada de todos modos, ahora que?
Desde que fue protegido por contraseña, al igual que el nombre no podía ayudar a nadie forzar la entrada Así que el tipo le dio el atacante el nombre del servidor. Ni siquiera se molestó en llamar al hombre de vuelta para verificar su historia, o escribir su nombre y número de teléfono. Él acaba de dar el nombre de los servidores, y ATM5 ATM6.

El ataque de contraseña

En este punto, Iván cambió a un enfoque técnico para obtener la autenticación de la información. El primer paso con la mayoría de los ataques técnica sobre los sistemas que proporcionan capacidad de acceso remoto es la identificación de una cuenta con una contraseña débil, que proporciona un punto de entrada inicial en el sistema.

Cuando un atacante trata de usar herramientas de hacking para identificar de forma remota contraseñas, el esfuerzo puede requerir que se mantenga conectado a la compañía la red durante horas a la vez. Es evidente que lo hace bajo su propio riesgo: cuanto más tiempo se queda conectados, mayor es el riesgo de detección y atrapado.

Como paso preliminar, Ivan haría una enumeración, que revela detalles sobre un sistema de destino. Una vez más el Internet convenientemente ofrece software para el objetivo (en http://ntsleuth.0catch.com, el personaje antes de "coger" es un cero).

Ivan encontrado varias herramientas de hacking a disposición del público en la Web que automatizado el proceso de enumeración, evitando la necesidad de hacerlo a mano, que tendría más largo y por lo tanto corren un mayor riesgo. Saber que la organización en su mayoría desplegados Servidores basados en Windows, que se descargó una copia de NBTEnum, un NetBIOS (básica de entrada / salida) enumeración de servicios públicos. Entró en el IP (protocolo de Internet) dirección del servidor ATM5, y comenzó a correr el programa. La enumeración herramienta es capaz de identificar varias cuentas que existían en el servidor.

LINGO

ENUMERACIÓN Un proceso que pone de manifiesto el servicio habilitado en el objetivo sistema, la plataforma de sistema operativo, y una lista de nombres de cuentas de los usuarios que tienen acceso al sistema.

Una vez que las cuentas existentes han sido identificados, la herramienta misma enumeración había la capacidad de lanzar un ataque de diccionario contra el sistema informático. Un diccionario ataque es algo que muchas personas la seguridad informática y los intrusos íntimamente familiarizados, pero que la mayoría de otros probablemente se sorprendería al aprender es posible. Este tipo de ataque está dirigido a descubrir la contraseña de cada usuario en el sistema mediante el uso de palabras de uso común.

Todos somos perezosos en algunas cosas, pero nunca deja de sorprenderme que cuando la gente elige sus contraseñas, su creatividad y la imaginación parecen desaparecer. La mayoría de nosotros queremos una contraseña que nos da protección, sino que está en el mismo tiempo fácil de recordar, lo que normalmente significa algo estrechamente relacionado para nosotros. Nuestras iniciales, nombre, apodo, nombre del cónyuge, canción favorita, películas, o cerveza, por ejemplo. El nombre de la calle en que vivimos o la ciudad en que vivimos, el tipo de coche que conducimos, el pueblo frente a la playa que nos gusta alojarse en Hawai, o esa corriente favorito con la mejor pesca de la trucha en todo. Reconocer el patrón aquí? En su mayoría son nombres propios, nombres de lugares, o las palabras del diccionario. A ataque de diccionario funciona a través de palabras comunes a un ritmo muy rápido, tratando cada uno como una contraseña en una o más cuentas de usuario.

Ivan corría el ataque de diccionario en tres fases. Para los primeros, se utiliza una lista simple de unas 800 de las contraseñas más comunes, la lista incluye el trabajo en secreto, y contraseña. También el programa de permutaciones las palabras del diccionario para tratar de cada palabra con un dígito anexos, o de agregar el número del mes en curso. La programa intentó cada intento en contra de todas las cuentas de usuario que se había identificados. No hubo suerte.

Para el siguiente intento, Iván fue el motor de búsqueda de Google y escribir ", listas de palabras diccionarios ", y miles de sitios encontrados con listas de palabras y de amplia diccionarios de lenguas extranjeras Inglés y varios. Descargó toda una Inglés diccionario electrónico. A continuación mejorada descargando una serie de listas de palabras que se encontró con Google. Iván eligió el sitio en www.outpost9.com/files/WordLists.html.

Este sitio le permitió descargar (todo esto de forma gratuita) una selección de archivos incluyendo apellidos, Namek, los nombres y las palabras del Congreso, actor los nombres y las palabras y los nombres de la Biblia.
Otro de los muchos sitios que ofrecen listas de palabras en realidad es siempre a través de Oxford
Universidad, en ftp://ftp.ox.ac.uk/pub/wordlists.
Otros sitios ofrecen listas con los nombres de personajes de dibujos animados, las palabras utilizadas en
Shakespeare, en la Odisea, de Tolkien, y la serie de Star Trek, así como en la ciencia y la religión, y así sucesivamente. (Uno en-línea de la compañía vende una lista que contiene
4.400.000 palabras y nombres por sólo $ 20.) El programa de ataque se puede configurar para poner a prueba
los anagramas de las palabras del diccionario, y - otro método favorito que muchos usuarios de computadoras que incrementa su seguridad.
Más rápido de lo que piensa
Una vez que Iván había decidido que lista de palabras de uso, y comenzó el ataque, el software corrió en piloto automático. Él fue capaz de volver su atención a otras cosas. Y aquí está la parte increíble: Se podría pensar que este tipo de ataque que permitiría al hacker tomar un Rip van Winkle de repetición y el software todavía se han hecho pocos progresos cuando se despertó. De hecho, dependiendo de la plataforma de ser atacado, la seguridad configuración del sistema y conectividad de red, cada palabra en un Inglés diccionario puede, increíblemente, se intentará en menos de treinta minutos!
Aunque este ataque se estaba ejecutando, Iván comenzó a otro equipo con una similar ataque en el otro servidor utilizado por el grupo de desarrollo, ATM6. Veinte minutos más tarde, el software de ataque se había hecho lo que los usuarios más confiados como para
creo que es imposible: se había roto una contraseña, que revela que uno de los usuarios tenían elegido la contraseña de "Frodo", uno de los Hobbits en el libro El Señor de los Anillos.
Con esta contraseña en la mano, Iván fue capaz de conectar con el servidor utilizando ATM6 de cuenta del usuario.
Hubo buenas noticias y malas noticias para nuestro atacante. La buena noticia es que el cuenta de que había roto los privilegios de administrador, lo que sería esencial para la el siguiente paso. La mala noticia es que el código fuente para el juego no estaba en ninguna parte
que se encuentran. Debe ser, después de todo, en la otra máquina, el ATM5, que Ya sabía que era resistente a un ataque de diccionario. Pero Iván no estaba dando justo sin embargo, todavía tenía algunos trucos más para probar.
En algunos sistemas Windows y UNIX, los hashes de la contraseña (cifrada contraseñas) están a disposición de cualquiera que tenga acceso a la computadora son almacenada en. El razonamiento es que las contraseñas encriptadas no se puede romper y por lo tanto no necesitan ser protegidos. La teoría está equivocada. Uso de otra herramienta llamado pwdump3, también está disponible en Internet, que fue capaz de extraer la hashes de las contraseñas de la máquina ATM6 y descargarlos.
Un archivo típico de los hashes de contraseñas se parece a esto:
administrador:
500:95 E4321A38AD8D6AB75EOC8D76954A50: 2E48927AO
BO4F3BFB341E26F6D6E9A97:::
akasper:
1110:5 A8D7E9E3C3954F642C5C736306CBFEF: 393CE7F90A8357
F157873D72D0490821:::
digger: 1111:5 D15COD58DD216C525AD3B83FA6627C7:
17AD564144308B4 2B8403DOIAE256558:::
ellgan:

1112:2017 D4A5D8D1383EFF17365FAFIFFE89: O7AEC950C22CBB9
C2C734EB89320DB13:::
tabeck: 1115:9 F5890B3FECCAB7EAAD3B435B51404EE:
1FO115A72844721 2FCO5EID2D820B35B:::
vkantar:
1116:81 A6A5DO35596E7DAAD3B435B51404EE: B933D36DD12258
946FCC7BD153F1CD6E:::
vwallwick: 1119: 25904EC665BA30F4449AF42E1054F192: 15B2B7953FB6
32907455D2706A432469:::
mmcdonald: 1121: A4AEDO98D29A3217AAD3B435B51404EE:
E40670F936B7 9C2ED522F5ECA9398A27:::
kworkman: 1141: C5C598AF45768635AAD3B435B51404EE:
DEC8E827A1212 73EFO84CDBF5FD1925C:::
Con los hashes ahora descargado a su computadora, Ivan utilizar otra herramienta que realizó un sabor diferente de ataque de contraseña conocida como la fuerza bruta. este tipo de ataque intenta todas las combinaciones de caracteres alfanuméricos y especiales más símbolos.
Con los hashes ahora descargado a su computadora, Ivan utilizar otra herramienta que realizó un sabor diferente de ataque de contraseña conocida como la fuerza bruta. Este tipo de ataque intenta todas las combinaciones de caracteres alfanuméricos y especiales más símbolos.
Ivan utiliza una herramienta de software llamada L0phtcrack3 (pronunciado loft crack, disponible en www.atstake.com, otra fuente de algunas herramientas de recuperación de contraseña de excelente
es www.elcomsoft.com). Los administradores de sistemas utilizar L0pht-crack3 de auditoría débil contraseñas, los atacantes lo utilizan para romper las contraseñas. La función de la fuerza bruta en LC3
trata de las contraseñas con las combinaciones de letras, números y símbolos más incluyendo !@#$%^&. Se trata de manera sistemática todas las combinaciones posibles de la mayoría de
personajes. (Nótese, sin embargo, que si los caracteres no imprimibles se utilizan, LC3 se incapaz de descubrir la contraseña)
El programa cuenta con una velocidad casi increíble, que puede alcanzar hasta un máximo de 2,8 millones de intentos de un segundo en una máquina con un procesador de 1 GHz. Incluso con esta
velocidad, y si el administrador del sistema ha configurado el operativo de Windows sistema correctamente (deshabilitar el uso de hashes LANMAN), rompiendo una contraseña todavía puede tomar una cantidad excesiva de tiempo.
LINGO
Un ataque de fuerza bruta Nuestra estrategia de detección de contraseñas que trata por todos los posible combinación de caracteres alfanuméricos y símbolos especiales.
Por esta razón, el atacante a menudo descarga el hash y ejecuta el ataque a su
o en otra máquina, en lugar de permanecer en la línea en la red de la empresa objetivo y correr el riesgo de detección.
Para Iván, la espera no fue tanto tiempo. Varias horas después, el programa presentado él con las contraseñas para cada uno de los miembros del equipo de desarrollo. Sin embargo, estos
fueron las contraseñas de los usuarios del equipo ATM6, y él ya sabía que el código fuente del juego que estaba buscando no era en este servidor.
¿Y ahora qué? Todavía no había sido capaz de obtener una contraseña de una cuenta en el ATM5 máquina. Usando su mentalidad hacker, la comprensión de los hábitos de seguridad pobres
de los usuarios típicos, pensó uno de los miembros del equipo podría haber elegido el mismo contraseña para ambas máquinas.
De hecho, eso es exactamente lo que encontró. Uno de los miembros del equipo estaba usando

el
contraseña "graneros" de ambos ATM5 y ATM6.
La puerta se había abierto de par en par para Iván que buscar alrededor hasta que encontró el los programas que estaba buscando. Una vez que se encuentra el árbol de código fuente y alegremente
descargado, dio un paso más típica de las galletas del sistema: Cambió
la contraseña de una cuenta inactiva que tenía derechos de administrador, en caso de que quiso obtener una versión actualizada del software en algún momento en el futuro.
Con el análisis de la
En este ataque que se pedía a las vulnerabilidades técnicas y de las personas basada en el atacante comenzó con una llamada telefónica de pretexto para obtener la ubicación y nombres de host
de los servidores de desarrollo que contenía la información confidencial.
A continuación, utiliza una utilidad de software para identificar la cuenta de usuario válido para todos los nombres
que tenía una cuenta en el servidor de desarrollo. A continuación dirigió sucesivos de dos ataques de contraseña, incluyendo un ataque de diccionario, que busca comúnmente utilizar contraseñas probando todas las palabras en un diccionario de Inglés, a veces aumentado por varias listas de palabras que contiene los nombres, lugares y objetos de especial de interés.
Debido a que ambas herramientas de hacking comerciales y de dominio público, se puede obtener
cualquier persona para cualquier propósito que tienen en mente, es más importante que que estar vigilantes en la protección de sistemas de la empresa informática y la red infraestructura.
La magnitud de esta amenaza no puede ser sobrestimada. De acuerdo a la computadora
La revista World, un análisis en Nueva York, Oppenheimer Funds llevó a una descubrimiento sorprendente. El vicepresidente de la compañía de seguridad de la red y Desastres
Recuperación corrió un ataque de contraseña en contra de los empleados de su empresa utilizando una de
los paquetes de software estándar. La revista informó que en tres minutos
se las arregló para romper las contraseñas de los 800 empleados.
Mitnick MENSAJE
En la terminología del juego Monopoly, si se utiliza una palabra del diccionario para su contraseña - Ir directamente a la cárcel. No pase Vaya, no cobrar $ 200. Usted tiene que enseñar a sus empleados cómo elegir contraseñas que realmente proteger sus activos.
PREVENCIÓN DE LA CON
Ataques de ingeniería social puede ser aún más destructivas cuando el atacante
añade un elemento de la tecnología. La prevención de este tipo de ataque normalmente implica la adopción de medidas tanto a nivel humano y técnico.
Decir que no
En la primera historia de este capítulo, la compañía telefónica secretario RCMAC no debe han eliminado las negar suprimir la calidad de las diez líneas de teléfono cuando no hay servicio Para existido autorizar el cambio. No es suficiente para que los empleados conocen la políticas y procedimientos de seguridad, los empleados deben entender la importancia de estas políticas están a la empresa en la prevención de daños.
Las políticas de seguridad deben desalentar desviación del procedimiento a través de un sistema de
recompensas y consecuencias. Naturalmente, las políticas deben ser realistas, no se pide a empleados para llevar a cabo medidas tan agobiante que es probable que sea ignorada.
Además, un programa de concienciación sobre la seguridad tiene que convencer a los empleados que, si bien es
importantes para completar las asignaciones de trabajo de manera oportuna, teniendo un acceso directo que

elude los procedimientos adecuados de seguridad puede ser perjudicial para la compañía y co-los trabajadores.
La misma precaución que deben estar presentes cuando el suministro de información a un extraño en
el teléfono. No importa qué tan convincente que la persona se presenta,
independientemente de su condición de la persona o la antigüedad en la empresa, sin ningún
Se deberá proporcionar información que no sea designado como disponible al público hasta el
la identidad de la persona que llama se ha verificado positivamente. Si esta política había sido estrictamente
observa, el esquema de ingeniería social en esta historia que han fracasado y
Gondorff detenido federal nunca habría sido capaz de planificar un susto nuevo
su amigo Johnny.
Este punto es tan importante que lo reitero en este libro: Verificar,
comprobar, verificar. Cualquier solicitud que no hizo en persona nunca debe ser aceptado sin verificar la identidad del solicitante - período.
Limpieza
Para cualquier empresa que no tiene guardias de seguridad durante todo el día, el esquema
en el que un atacante obtiene acceso a una oficina después de horas presenta un desafío.
La gente de limpieza normalmente se trata con el respeto a nadie, que parece ser con
la empresa y parece legítima. Después de todo, se trata de alguien que pudiera obtener
en problemas o ser despedido. Por esa razón, los equipos de limpieza, ya sea interna o
contratado con una agencia externa, debe estar capacitado en materia de seguridad física.
Trabajo de limpieza no es exactamente requieren una formación universitaria, o incluso la posibilidad de
hablan Inglés, y el entrenamiento habitual, en su caso, implica la no-las cuestiones de seguridad relacionadas con
tales como qué tipo de productos de limpieza a utilizar para las diferentes tareas. En general, estos
la gente no recibe una instrucción como: "Si alguien te pide que les permiten después de
horas, usted necesita ver a su tarjeta de identificación de la empresa, y luego llamar a la limpieza
oficina de la empresa, explicar la situación y esperar la autorización. "
Una organización necesita para planificar una situación como la que en este capítulo antes de que
pasa y la gente del tren en consecuencia. En mi experiencia personal, he encontrado
que la mayoría, si no todas, las empresas del sector privado son muy laxas en esta área de física
la seguridad. Usted puede tratar de abordar el problema desde el otro extremo, poniendo el
carga para los propios empleados de su empresa. Una empresa sin las 24 horas de guardia
servicio debe informar a sus empleados que para llegar después de las horas, van a llevar a sus
propias llaves o tarjetas electrónicas de acceso, y nunca se deben poner a la gente de limpieza en
la posición de decidir quién está bien admitirlo. Entonces decirle a la empresa de limpieza
que su pueblo siempre debe estar capacitado que nadie para ser admitido en su
locales por ellos en cualquier momento. Esta es una regla simple: No abra la puerta para
nadie. En su caso, esto podría ser puesta por escrito como condición del contrato
con la empresa de limpieza.
Además, los equipos de limpieza deben ser capacitados en técnicas de cuestas
(Personas no autorizadas a raíz de una persona autorizada en una entrada segura).
También deben ser entrenados para no permitir que otra persona les siguen en la
edificio sólo porque la persona que parece que podría ser un empleado.
Seguimiento de vez en cuando - por ejemplo, tres o cuatro veces al año - por la organización de un
la penetración de prueba o evaluación de la vulnerabilidad. Pídale a alguien que aparecen en la puerta
cuando el equipo de limpieza está en el trabajo y tratar de hablar a su manera en el edificio.
En lugar de utilizar sus propios empleados, puede contratar a una empresa especializada en este tipo de pruebas de penetración.
Pass It On: Proteja sus contraseñas

Cada vez más, las organizaciones son cada vez más atentos a la aplicación de
las políticas de seguridad a través de medios técnicos - por ejemplo, la configuración de la operación
sistema para hacer cumplir las políticas de contraseñas y limitar el número de acceso no válido los intentos que se pueden hacer antes de bloquear la cuenta. De hecho, Microsoft Plataformas Windows negocios en general tienen esta característica construido adentro Sin embargo,
el reconocimiento de la facilidad con clientes insatisfechos son las características que requieren extra
esfuerzo, los productos se entregan normalmente con funciones de seguridad desactivadas. Es realmente hora de que los fabricantes de software deje de entregar productos con características de seguridad desactivado por defecto, cuando debería ser al revés. (I Sospecho que va a resolver esto pronto.)
Por supuesto, la política de seguridad de la empresa debe exigir a los administradores de sistemas
hacer cumplir las políticas de seguridad a través de medios técnicos siempre que sea posible, con el objetivo
de no depender de los seres humanos falibles más de lo necesario. Es una obviedad que cuando se limita el número de los sucesivos intentos de acceso no válido a un particular cuenta, por ejemplo, que hacen que la vida de un atacante mucho más difícil.
Cada organización se enfrenta a ese difícil equilibrio entre la seguridad y la fuerte productividad de los empleados, lo que lleva a algunos empleados a ignorar las políticas de seguridad,
no aceptar lo esencial que estas medidas de seguridad son para proteger la integridad del información confidencial de la empresa.
Si las políticas de la empresa deja algunas cuestiones sin abordar, los empleados pueden utilizar el
camino de menor resistencia y que cualquier acción que sea más conveniente y lo hace su trabajo más fácil. Algunos empleados pueden resistirse al cambio y abiertamente caso omiso de una buena
hábitos de seguridad. Es posible que haya encontrado como un empleado, que sigue reglas impuestas por contraseña y duración de la complejidad, pero luego escribe los contraseña en un post-it y desafiante que se pega a su monitor.
Una parte vital de la protección de su organización es el uso de difíciles de descubrir contraseñas, en combinación con la configuración de seguridad fuerte en su tecnología.
Para una discusión detallada de las políticas de contraseña recomendadas, consulte el Capítulo 16.

Capítulo 12

Los ataques contra el empleado de nivel de entrada

Como muchas de las historias aquí demuestran, el ingeniero social calificado a menudo el blanco bajo nivel de personal en la jerarquía de la organización. Puede ser fácil de
manipular estas personas para que revelen información aparentemente inocua que la atacante utiliza para avanzar un paso más hacia la obtención de la compañía más sensible de la información.
Un atacante objetivos de nivel de entrada empleados, ya que suelen ser conscientes de el valor de la información específica de la empresa o de los posibles resultados de ciertas las acciones. Además, tienden a ser fácilmente influenciable por algunos de los más comunes métodos de ingeniería social - la persona que llama que llama a la autoridad, una persona que parece agradable y simpático, una persona que parece conocer a la gente en el empresa que se conocen a la víctima, una solicitud para que el atacante se afirma urgente, o la inferencia de que la víctima obtener alguna clase de favor o reconocimiento.
Aquí están algunos ejemplos del ataque a los empleados de nivel inferior en la acción.

LA GUARDIA DE SEGURIDAD ÚTIL

Los estafadores esperan encontrar a una persona que es codiciosa, porque son los más probabilidades de caer en una estafa. Los ingenieros sociales, al orientar a alguien como un miembro de un equipo de saneamiento o de un guardia de seguridad, la esperanza de encontrar a alguien que está
bondadoso, amable y de confianza de los demás. Ellos son los más propensos a ser dispuestos a ayudar. Eso es lo que el atacante tenía en mente en la siguiente historia.
Ver Elliot
Fecha / hora: 3:26 de la mañana del martes por la mañana en febrero de 1998.
Ubicación: Marchand Microsystems instalación, Nashua, Nueva Hampshire
Elliot Staley sabía que no iba a dejar su puesto cuando él no estaba en su programado rondas. Pero fue el medio de la noche, por el amor de Dios, y él no había visto a una sola persona desde que llegó en el servicio. Y era casi la hora de hacer sus rondas de todos modos. El pobre hombre en el teléfono sonaba como si realmente necesitaba ayuda. Y que hace que una persona se siente bien cuando puede hacer un poco de bien para
alguien.
La historia de Bill
Bill Goodrock tenía un objetivo simple, que él se había aferrado a, sin modificaciones, ya que la edad
doce: a retirarse a la edad de veinticuatro años, no tener que tocar ni un centavo de su fondo fiduciario.
Para mostrar a su padre, el todopoderoso y el banquero no perdona, que podría ser un éxito por su cuenta.
Sólo dos años y es ahora perfectamente claro que no va a hacer su fortuna en los próximos veinticuatro meses por ser un brillante hombre de negocios y no lo hará por ser un inversionista fuerte. En una ocasión pregunté a robar bancos con un arma, pero eso es sólo la materia de la ficción - el riesgo-beneficio
trade-off es muy malo. En su lugar, soñando con hacer un Rifkin - robar un banco por vía electrónica. El proyecto de ley fue la última vez en Europa con la familia, él abrió un banco cuenta en Mónaco, con 100 francos. Todavía tiene sólo 100 francos en el mismo, pero tiene un plan que podría ayudarle a alcanzar los siete dígitos en un apuro. Tal vez hasta ocho si es suerte.
Novia de Bill Anne-Marie trabajó en M & A para un gran banco de Boston. Un día a la espera en sus oficinas hasta que salió de una reunión a finales, cedió a curiosidad y conectado a su ordenador portátil a un puerto Ethernet en la sala de conferencias que
estaba usando. Sí - estaba en su red interna, conectados en el interior del banco de la red .., detrás del firewall corporativo. Que le dio una idea.
Se combinaron su talento con un compañero que conocí a una mujer joven llamada Julia, una brillante informática Ph.D. candidato a hacer una pasantía en Marchand
Microsystems. Julia parecía una gran fuente de información privilegiada esencial.
Ellos le dijeron que estaban escribiendo un guión para una película y ella cree que en realidad ellos. Ella pensó que era divertido hacer una historia con ellos y darles todas las detalles acerca de cómo en realidad se podría llevar de la travesura que había descrito. Ella que la idea era brillante, en realidad, y se mantiene molestando acerca de darle un crédito en pantalla, también.
Se le advirtió acerca de la frecuencia ideas guión a robar y le hizo jurar ella nunca se lo diría a nadie.
Adecuadamente entrenado por Julia, Bill hizo la parte de riesgo a sí mismo y nunca dudó podría traer apagado.
Me llamó por la tarde y logró averiguar que el supervisor nocturno de la las fuerzas de seguridad fue un hombre llamado Isaías Adams. A las 9:30 de la noche llamé a la la construcción y hablé con el guardia de seguridad en el escritorio del vestíbulo. Mi historia era sobre la base de la urgencia y me hice sonar un poco de pánico. "Tengo coche problemas y no puedo llegar a las instalaciones ", dije." No tengo esta emergencia y que

realmente
Necesitamos su ayuda. Traté de llamar al supervisor de guardia, Isaías, pero no está en casa. ¿Puedes hacerme este favor sola vez, yo realmente lo aprecian? "
Las habitaciones en este gran facilidad fueron cada uno marcado con un código electrónico dejar así que le di
él por correo-parada de la sala de ordenadores y le preguntó si sabía dónde estaba.
Él dijo que sí, y de acuerdo en ir allí para mí. Él dijo que le llevaría unos cuantos
minutos para llegar a la habitación, y yo le dije que lo llamaría en el laboratorio, con la excusa que yo estaba usando la línea telefónica disponible sólo para mí, y yo lo usaba para llamar al la red para tratar de solucionar el problema.
Él ya estaba allí, esperando el momento en que llamó, y le dije dónde
encontrar la consola me interesaba, en busca de uno con una pancarta de papel
"Elmer" - el host que Julia había dicho fue utilizado para construir las versiones de lanzamiento de la
sistema operativo que la empresa comercializa. Cuando él dijo que lo había encontrado, estaba segura de que Julia había sido una buena información nos alimenta y mi corazón
dio un vuelco. Yo le había presione la tecla Enter un par de veces, y lo dijo
imprimió un signo de libra. Que me dijo que el equipo fue registrado como usuario root, el super-usuario cuenta con todos los privilegios del sistema. Él era una mecanógrafa buscar-y-Peck y
tiene todo a sudar cuando traté de hablar a través de entrar en mi siguiente orden,
que era más que un poco de trampa:
"arreglo: x: 0:0 ::/:/ bin / sh 'echo>> / etc / passwd
Finalmente, lo hizo bien, y nos ha proporcionado ahora una cuenta con una solución nombre. Y entonces yo le escriba
"arreglo:: 10300:0:0 'echo 55 / etc / shadow
Esto estableció la contraseña cifrada, que va entre los dos puntos dobles.
Poner nada entre los dos puntos significa la cuenta que tiene un nulo
contraseña. Por lo que sólo estos dos comandos fue todo lo que añadir la solución cuenta al archivo de contraseñas con una contraseña nula. Lo mejor de todo, la cuenta tendría el mismos privilegios que un super-usuario.
Lo siguiente que él había no era para introducir un comando recursivo de directorios que imprime una larga lista de nombres de archivo. Luego tuve que darle de comer el papel hacia adelante, arráncalo
fuera, y llevarlo con él a su escritorio guardia porque "puede ser necesario que usted lea me algo de él más adelante. "
La belleza de esto fue que él no tenía idea que había creado una nueva cuenta. Y yo
le imprime el listado del directorio de nombres de archivos, ya que necesitaba para asegurarse de que
los comandos que escribe antes que salir de la sala de ordenadores con él. Que
forma en que el administrador del sistema o el operador no se mancha todo lo que el próximo por la mañana que les alerta se había producido una violación de la seguridad.
Yo estaba ahora con una cuenta, una contraseña y los privilegios. Un poco antes de
Marqué en la medianoche y seguido las instrucciones de Julia había escrito cuidadosamente hasta
"Por el guión." En un abrir y cerrar tuve acceso a uno de los sistemas de desarrollo
que contenía la copia maestra del código fuente de la nueva versión de la
compañía de software del sistema operativo.
He subido un parche que Julia había escrito, que dijo que modificó una rutina en un
de las bibliotecas del sistema operativo. Que el parche, en efecto, crear un agente encubierto puerta trasera que permite el acceso remoto al sistema con una contraseña secreta.
NOTA
El tipo de backdoor utiliza aquí no cambia el inicio de sesión del sistema operativo
programa en sí, sino una función específica contenida en la biblioteca dinámica
utilizado por el programa login se sustituye para crear el punto de entrada secreto. En el típico

los ataques, los intrusos informáticos suele reemplazar o parchear el programa de inicio de sesión en sí, sino
administradores fuerte sistema puede detectar el cambio mediante la comparación con la versión enviado a los medios de comunicación, como el CD, o por métodos de distribución.
Con mucho cuidado de seguir las instrucciones que ella había escrito para mí, la primera instalación
el parche, tomar las medidas necesarias que elimina la cuenta de arreglar y limpiar todos los de auditoría
los registros para que no hubiera ni rastro de mis actividades, efectivamente borrar mis huellas.
Pronto, la compañía comenzará a distribuir la actualización del sistema operativo nuevo
sus clientes: instituciones financieras de todo el mundo. Y todos los que copian
enviado incluiría la puerta de atrás yo había colocado en la distribución de maestros
antes de que fuera enviado, que me permite acceder a cualquier sistema informático de todos los bancos
y Casa de Bolsa que instaló la actualización.
LINGO
PARCHE Tradicionalmente, un pedazo de código que, cuando se coloca en un archivo ejecutable programa, corrige un problema.
Por supuesto, yo no estaba en casa gratis - aún habría que hacer. Aún tendría
para acceder a la red interna de cada institución financiera que quería
"La visita". Entonces tendría que averiguar cuál de sus ordenadores fue usado para el dinero transferencias, e instalar el software de vigilancia para conocer los detalles de sus operaciones
y exactamente como la transferencia de fondos.
Todo lo que podía hacer a larga distancia. Desde un ordenador ubicado en cualquier lugar. Por ejemplo,
con vistas a una playa de arena. Tahití, allá voy.
Llamé a la parte de atrás de guardia, le dio las gracias por su ayuda, y le dijo que podía seguir adelante
y lanzar la impresión.
Con el análisis de la
El guardia de seguridad había instrucciones sobre sus funciones, pero wellthought incluso a fondo,
instrucciones de que no puede prever todas las situaciones posibles. Nadie le había dicho
lo el daño que puede hacerse escribiendo unas pocas teclas en un ordenador para una persona que él creía que era un empleado de la compañía.
Con la colaboración de la guardia, que era relativamente fácil para acceder a una
críticos del sistema que almacena el patrón de distribución, a pesar de que era
detrás de la puerta cerrada de un laboratorio seguro. El guardia, por supuesto, tenía las llaves de todas las puertas con llave.
Incluso un empleado básicamente honesto (o, en este caso, el estudiante de doctorado y interno de la empresa, Julia) pueden ser sobornados o engañados para que revelen
información de vital importancia para un ataque de ingeniería social, tales como dónde
el equipo de destino y se encuentra - la clave para el éxito de este ataque ---
cuando se va a construir la nueva versión del software para su distribución.
Eso es importante, ya que un cambio de este tipo realizado demasiado pronto tiene una mayor probabilidad
de ser detectado o se anula si el sistema operativo se reconstruye a partir de una limpieza fuente.
¿Entendió el detalle de tener la guardia tener la impresión de nuevo al pasillo
escritorio y luego lo destruye? Este fue un paso importante. Cuando el equipo
los operadores llegaron a trabajar al siguiente día laboral, el atacante no quería que se encuentran
esta evidencia condenatoria en el terminal en papel, o el aviso a la basura. Dando
el guardia de una excusa plausible para tomar la impresión con él evita ese riesgo.
Mitnick MENSAJE

Cuando el intruso equipo no puede tener acceso físico a un sistema informático o red de sí mismo, va a tratar de manipular a otra persona que lo haga por él. En los casos en que el acceso físico es necesario para el plan, con la víctima como un proxy es incluso mejor que hacerlo por sí mismo, porque el atacante asume un riesgo mucho menor de detección y captura.

EL PARCHE DE EMERGENCIA

Se podría pensar que un tipo de soporte técnico que comprende los peligros de dar el acceso a la red informática a un extraño. Pero cuando el extranjero es una inteligente ingeniero social haciéndose pasar por un proveedor de software útil, los resultados pueden no ser lo que usted espera.

Un llamado útiles

La persona que llama quería saber quién está a cargo de los ordenadores no? y el operador de telefonía le pone en contacto con el chico de soporte técnico, Pablo Ahearn.

La persona que llamó se identificó como "Edward, con SeerWare, el proveedor de bases de datos.

Al parecer, un grupo de nuestros clientes no recibieron el correo electrónico de nuestro emergencia
actualización, por lo que estamos llamando a algunos para un control de calidad de verificación para ver si había
un problema al instalar el parche. ¿Ha instalado la actualización todavía? "

Pablo dijo que él estaba bastante seguro de que no había visto nada parecido.

Edward dijo, "Bueno, podría causar la pérdida intermitente de datos catastrófica, por lo que recomendamos que se ha instalado tan pronto como sea posible. "Sí, eso era algo que sin duda quería hacer, dijo Paul. "Está bien", respondió la llamada. "Podemos enviar que una cinta o CD con el parche, y yo quiero decirles, que es muy importante - dos empresas ya han perdido varios días de datos. Por lo que no deberían hacer esto instalado tan pronto como llegue, antes de que suceda a su empresa. "

"¿No puedo descargar desde su sitio Web?" Pablo quería saber.

"Debe estar disponible pronto -. El equipo técnico ha estado poniendo todas estas incendios Si desea, podemos tener nuestro centro de soporte al cliente lo instale por usted, de forma remota. Tenemos la posibilidad de acceso telefónico o usar Telnet para conectarse al sistema, si usted puede apoyar a
que. "

"No permitimos que Telnet, especialmente de la Internet - no es seguro", dijo Paul respondió. "Si usted puede utilizar SSH, que iba a estar bien", dijo, nombrando a un producto que ofrece transferencias seguras de archivos.

"Sí. Tenemos SSH. ¿Cuál es la dirección IP?"

Pablo le dio la dirección IP, y cuando Andrés le preguntó, "y qué nombre de usuario y contraseña se pueden utilizar ", Pablo le dio a ellos, también.

Con el análisis de la

Por supuesto que la llamada telefónica en realidad podría haber salido de la base de datos fabricante. Pero entonces la historia no pertenece a este libro.

El ingeniero social en este caso influyó la víctima, creando una sensación de miedo que los datos críticos se pueden perder, y ofreció una solución inmediata que resuelva el problema.

Además, cuando un ingeniero de los objetivos sociales a alguien que conoce el valor de la información que necesita para llegar a argumentos muy convincentes y persuasivos para dar acceso remoto. A veces se tiene que agregar el elemento de urgencia así lo la víctima está distraída por la necesidad de acometer, y que cumple antes de que él ha tenido un oportunidad de dar mucha importancia a la solicitud.

LA CHICA NUEVA

¿Qué tipo de información en los archivos de su empresa puede utilizar un atacante quiere ganar el acceso a la? A veces puede ser algo que no creo que sea necesario para proteger en absoluto.

Llame a Sara

"Recursos Humanos, se trata de Sarah".
"Hola, Sarah. Se trata de George, en el garaje. Usted sabe la tarjeta de acceso
que se utiliza para entrar en el garaje y ascensores? Bueno, hemos tenido un problema y
tenemos que volver a programar las tarjetas para todas las nuevas contrataciones de los últimos
quince días. "
"Por lo que necesita su nombre?"
"Y sus números de teléfono."
"Puedo ver la lista de nuevas contrataciones y devolver la llamada. ¿Cuál es tu número de
teléfono?"
"Estoy a 73... Eh, estoy pasando. Descanso, ¿qué tal si te llamo de vuelta en un halfhour?"
"Oh. Está bien."
Cuando me llamó, me dijo:
"Oh, sí. Bueno, hay sólo dos. Myrtle Anna, en Finanzas, es una secretaria. Y
que nuevo vicepresidente, el Sr. Underwood ".
"Y los números de teléfono?"
"En este acuerdo, el Sr. Underwood es 6973. Myrtle Anna es 2127."
"Oye, has sido de gran ayuda." Gracias ".
Llame a Anna
"Finanzas, Anna habla."
"Me alegro de haber encontrado a alguien trabajando hasta tarde. Oye, este es Ron Vittaro, estoy
editor de la división de negocios. No creo que nos han presentado. Bienvenida
a la empresa. "
"Oh, gracias."
"Anna, estoy en Los Angeles y tengo una crisis. Tengo que tomar unos diez minutos
de su tiempo. "
"Por supuesto. ¿Qué se necesita?"
"Sube a mi oficina. ¿Sabes dónde está mi oficina?
"No."
"Está bien, es la oficina de la esquina en el décimo quinto piso de la habitación 1502. Te llamo no
en pocos minutos. Al llegar a la oficina, usted tendrá que pulsar el delantero
botón en el teléfono para que mi llamada no se va directamente a mi correo de voz. "
"Bueno, estoy en mi camino."
Diez minutos más tarde estaba en su oficina, había cancelado su desvío de llamadas y se
espera cuando el teléfono sonó. Le dije que se sentara frente al ordenador y lanzar
Internet Explorer. Cuando se estaba ejecutando él le dijo que escribir en una dirección:
www.geocities.com / ron-INSEN / manuscript.doc.exe.
Un cuadro de diálogo apareció y le dijo que haga clic en Abrir. El equipo parecía
empezar a descargar el manuscrito, y después la pantalla quedó en blanco. Cuando
informó de que algo parecía estar mal, contestó: "Oh, no. No de nuevo. He
estado teniendo un problema con la descarga de ese sitio Web de vez en cuando, pero me
pensé que era fijo. Bueno, está bien, no te preocupes, voy a conseguir el archivo de otra manera
en el futuro. "
Entonces él le pidió que reinicie su computadora para poder estar seguro de que sería puesta en
marcha
correctamente después de que el problema que ella acababa de tener. Él le habló a través de los
pasos para
necesidad de reiniciar.
Cuando el equipo estaba funcionando correctamente de nuevo, le dio las gracias calurosamente y
lo colgó
, y Anna volvió al departamento de finanzas para terminar el trabajo que había sido
trabajando.
Historia de Kurt Dillon
Millard-Fenton Editores se mostró entusiasmado con el nuevo autor que se acaba de
a punto de registrarse, el ejecutivo retirado de una empresa Fortune 500 que tenía una
fascinante historia que contar. Alguien había conducido el hombre a un gerente de negocios para

manejo de sus negociaciones. El gerente de negocios no quieren admitir que sabía zip
sobre los contratos de edición, por lo que contrató a un viejo amigo que le ayudara a averiguar lo que
lo que necesitaba saber. El viejo amigo, por desgracia, no fue una muy buena elección.
Kurt Dillon utiliza lo que podríamos llamar métodos inusuales en su investigación, los métodos de no del todo éticos.
Kurt se inscribió en un sitio gratuito en Geocities, en el nombre de Ron Vittaro, y
cargar un programa de spyware en el nuevo sitio. Le cambió el nombre de la
programa para manuscript.doc.exe, por lo que el nombre parece ser una palabra
documento y no levantar sospechas. De hecho, este trabajo aún mejor que Kurt había
anticipado, porque el verdadero Vittaro nunca había cambiado la configuración por defecto en su
El sistema operativo Windows llamada "Ocultar las extensiones de archivo para tipos de archivo conocidos".
Debido a que la creación del archivo se muestra en realidad con el nombre
Manuscrito.
Entonces había una señora secretaria amigo que llame a la Vittaro. Después de entrenar Dillon,
ella dijo: "Yo soy la asistente ejecutiva de Pablo Spadone, presidente de Ultimate
Librerías, en Toronto. Sr. Vittaro conocí a mi jefe en una feria del libro hace un tiempo, y
le pidió que le llame para discutir un proyecto que podríamos hacer juntos. Sr. Spadone es el
el camino mucho, así que él dijo que yo debía saber que el señor Vittaro será en la oficina. "
En el momento en que los dos habían terminado de comparar los horarios, el amigo de la señora había
suficiente información para proporcionar al atacante con una lista de fechas en las que el Sr. Vittaro
estaría en la oficina. Lo cual significaba que él también sabía cuando Vittaro estaría fuera de
la oficina. No había requerido conversación extra tanto para descubrir que es Vittaro
Secretario se aprovechan de su ausencia para entrar en un poco de esquí. Para una
corto espacio de tiempo, tanto estaría fuera de la oficina. Perfecta.
LINGO
Software espía especializado que se utiliza para controlar secretamente una computadora objetivos
las actividades. Una forma utilizada para rastrear los sitios visitados por los compradores de Internet, para que en línea
anuncios pueden ser adaptados a sus hábitos de navegación. La otra forma es
análoga a una intervención telefónica, con la excepción de que el dispositivo de destino es una computadora. El software
captura de las actividades del usuario, incluyendo contraseñas y pulsaciones de teclas,
correo electrónico, conversaciones de chat, mensajería instantánea, todos los sitios web visitados, y
imágenes de la pantalla.
LINGO
Instalación silenciosa Un método de instalación de una aplicación de software sin la
usuario de la computadora o el operador consciente de que tal acción se lleva a cabo.
El primer día que se supone que se ha ido él hizo una llamada urgente pretexto sólo para
asegurarse de que, y me dijeron que una recepcionista que "el señor Vittaro no está en la oficina y
tampoco lo es su secretaria. Ninguno de ellos se espera en cualquier momento, hoy o mañana
o al día siguiente. "
Su primer intento de estafar a un empleado de menor a tomar parte en su esquema se
éxito, y ella no parecía abrir y cerrar de ojos después de haber escuchado a ayudarle por
la descarga de un "manuscrito", que en realidad era un popular y comercialmente
programa de spyware disponible, que el atacante había modificado para una instalación silenciosa.
Usando este método, la instalación no sea detectado por ningún antivirus
software. Por alguna extraña razón, los fabricantes de antivirus no de mercado
productos que detecta spyware disponible en el mercado.

Inmediatamente después de la joven se había cargado el software en la Vittaro
equipo, Kurt volvió a subir al sitio de Geocities y se sustituye el archivo doc.exe
con un libro manuscrito que encontró en Internet. Sólo en caso de que alguien tropezó con
el engaño y regresó al lugar para investigar lo que había ocurrido, todo lo que habían
encontramos sería una inocua, amateur, sin publicable manuscrito del libro.
Una vez que el programa se ha instalado y reiniciado el ordenador, se fijó para
inmediatamente se activan. Ron Vittaro volvería a la ciudad en pocos días,
empezar a trabajar, y el spyware se iniciaría el reenvío de todas las pulsaciones de teclado
en su ordenador, incluyendo todos los correos salientes y capturas de pantalla que muestra lo que
se muestra en su pantalla en ese momento. Todo sería enviado a intervalos regulares
intervalos de un proveedor de servicios de correo electrónico gratuito en Ucrania.
A los pocos días después del regreso de Vittaro, Kurt estaba arando a través de los archivos de registro
acumulando en su buzón de Ucrania y en poco tiempo se había situado confidencial
correos electrónicos que indican hasta qué punto Millard-Fenton publicación estaba dispuesto a ir en
hacer un trato con el autor. Armado con ese conocimiento, fue fácil para el
autor del agente para negociar los términos mucho mejor de lo que se ofrece, sin
corriendo el riesgo de perder la oferta total. Que, por supuesto, significó una mayor
comisión para el agente.
Con el análisis de la
En este ardid, el atacante hizo su éxito sea más probable eligiendo a un nuevo empleado
para actuar como su apoderado, contando con su ser más dispuestos a cooperar y ser una
jugador de equipo, y ser menos propensos a tener conocimiento de la empresa, su gente,
y buenas prácticas de seguridad que podría frustrar el intento.
Debido a que Kurt estaba pretextos como vicepresidente en su conversación con Anna, una
secretario de Finanzas, sabía que sería muy poco probable que ella se pregunta
su autoridad. Por el contrario, ella debería recibir a la idea de que ayudar a un vicepresidente
podría ganar su favor.
Y el proceso entró a través de Anna que tuvo el efecto de la instalación
el spyware parece inocua en su cara. Anna no tenía idea de que su apariencia
acciones inocentes había un atacante a obtener información valiosa que podría ser
contra los intereses de la empresa.
¿Y por qué optar por reenviar el mensaje del vicepresidente a una cuenta de correo electrónico
en Ucrania? Por varias razones, un destino lejano hace el seguimiento o de tomar
acción contra un atacante mucho menos probable. Este tipo de delitos en general
considerada de baja prioridad en países como este, donde la policía tiende a mantener la
opinión de que la comisión de un delito a través de Internet no es un delito digno de mención.
Para
esa razón, el uso de gotas de correo electrónico en los países en que es poco probable que
coopere con
Aplicación de la ley EE.UU. es una estrategia atractiva.
PREVENCIÓN DE LA CON
Un ingeniero social siempre ha de preferir a la meta de un empleado que es poco probable que
reconocer que hay algo sospechoso en sus peticiones. Hace su trabajo
no sólo más fácil, pero también menos arriesgado - como las historias de este capítulo muestran.
Mitnick MENSAJE
Pedirle a un compañero de trabajo o subordinados a hacer un favor es una práctica común. Social
Los ingenieros saben cómo explotar el deseo natural de la gente para ayudar y ser un equipo
jugador. Un atacante aprovecha esta característica humana para engañar a incautos positivo
empleados en la realización de acciones que le avanzar hacia su objetivo. Es
importante entender este concepto tan simple que será más probable que
reconocer cuando otra persona está tratando de manipular.
Engañando a los incautos
He señalado anteriormente la necesidad de capacitar a los empleados a fondo suficiente como

para que se
nunca se dejan convencer de llevar a cabo las instrucciones de un
extraño. Todos los empleados también deben comprender el peligro de llevar a cabo un
solicitud de iniciar cualquier acción en el equipo de otra persona. Política de la empresa debe
prohibir esto, excepto cuando sea específicamente autorizado por un administrador. Admisible
situaciones incluyen:
Cuando la solicitud sea hecha por una persona bien conocida por usted, con la solicitud formulada
ya sea cara a cara o por teléfono al reconocer el inconfundible
voz de la persona que llama.
Cuando positivamente verificar la identidad del solicitante a través de aprobados
procedimientos.
Cuando la acción sea autorizado por un supervisor u otra persona con autoridad que se
personalmente familiarizado con el solicitante.
Los empleados deben ser entrenados para no asistir a las personas que no conocen
personalmente, aunque
si la persona que realiza la solicitud pretende ser un ejecutivo. Una vez que las políticas de
seguridad
en materia de verificación se han puesto en marcha, la gerencia debe apoyar
empleados en la adhesión a estas políticas, aún cuando esto significa que un empleado
desafía a un miembro del personal ejecutivo que está pidiendo que el empleado
eludir una política de seguridad.
Cada empresa también debe tener políticas y procedimientos que los empleados de guía
responder a las solicitudes para tomar cualquier acción con las computadoras o relacionados con
la informática
equipo. En la historia de la editorial, el ingeniero social
dirigido a un nuevo empleado que no habían recibido formación sobre seguridad de la información
políticas y procedimientos. Para evitar este tipo de ataque, todos los actuales y nuevos
los empleados deben ser informados de seguir una regla simple: No utilice ningún sistema
informático
para realizar una acción solicitada por un extraño. Período.
Recuerde que cualquier empleado que tiene acceso físico o electrónico a un
ordenador o un elemento de Equipo relacionado con la es vulnerable a ser
manipulados para tomar alguna acción maliciosa por parte de un atacante.
Empleados, y en especial el personal de TI, tienen que entender que lo que permite una
afuera para ganar acceso a sus redes informáticas es como darle a su banco
número de cuenta a un número de tarjeta de telemarketer o dar su teléfono llamando al
un extraño en la cárcel. Los empleados deben darle mucha atención a si la realización
una solicitud puede llevar a la revelación de información sensible o comprometer la
del sistema informático de la empresa.
La gente de TI también deben estar en guardia contra llamadores desconocidos se hacen pasar
por vendedores.
En general, una empresa debería considerar la posibilidad de determinadas personas designadas
como
contactos para cada proveedor de tecnología, con una política en el lugar que los demás
empleados
no responderá a las solicitudes de proveedor para obtener información acerca de los cambios o
para cualquier
teléfono o equipo de cómputo. De esta manera, las personas designadas se
familiarizado con el personal vendedor que llama o visita, y es menos probable que se
engañados por un impostor. Si un vendedor de llamadas incluso cuando la empresa no tiene
un contrato de soporte, que también debe levantar sospechas.
Todos en la organización tiene que estar al tanto de seguridad de la información
amenazas y vulnerabilidades. Tenga en cuenta que los guardias de seguridad y como la
necesidad de dar
no sólo de capacitación en seguridad, pero la formación en seguridad de la información, también.

Porque
guardias de seguridad con frecuencia tienen acceso físico a toda la instalación, deben ser capaz de reconocer los tipos de ataques de ingeniería social que puede ser usada contra ellos.

Cuidado con Spyware

Programas espía comerciales que una vez fue utilizado principalmente por los padres para controlar su lo
los niños estaban haciendo en la Internet, y por los empleadores, supuestamente para determinar que los empleados estaban perdiendo el tiempo navegando por la Internet. Un uso más graves fue detectar posibles robos de los activos de información o espionaje industrial.

Los desarrolladores comercializar sus spyware, ofreciendo como una herramienta para proteger a los niños,
cuando en realidad su verdadero mercado es la gente que desea espiar a alguien. Hoy en día, la venta de software espía está impulsado en gran medida por el deseo de la gente para saber si su
cónyuge o pareja es infiel.

Poco antes de empezar a escribir la historia de spyware en este libro, la persona que recibe el correo para mí (porque no se me permite el uso de Internet) que se encuentran un spam mensaje de correo electrónico publicitario a un grupo de productos de software espía. Uno de los artículos que se ofrecen
fue descrita así:

FAVORITO! Debe tener:

Este poderoso programa de vigilancia y espionaje secreto captura todas las pulsaciones de teclas y
la hora y el título de todas las ventanas activas en un archivo de texto, mientras se ejecuta oculto en el
de fondo. Los registros pueden ser cifrados y enviados automáticamente a un correo electrónico especificada
dirección, o acaba de grabar en el disco duro. El acceso al programa es la contraseña protegidos y que se pueden ocultar las teclas CTRL + ALT + SUPR menú.

Utilizarla para supervisar URLs, sesiones de chat, correos electrónicos y muchas otras cosas (incluso
contraseñas).

Instalar sin necesidad de la detección en cualquier PC y correo electrónico a ti mismo los registros!

Brecha de antivirus?

El software antivirus no detecta spyware comercial, con lo que el tratamiento de la software malicioso que no, aunque la intención es la de espiar a otras personas. Por lo que el equivalente informático de las escuchas telefónicas pasa desapercibido, creando el riesgo de que cada uno de
nos podría estar bajo la vigilancia ilegal en cualquier momento. Por supuesto, el antivirus fabricantes de software pueden argumentar que el spyware puede ser utilizado para legitimar fines, y por lo tanto no debe ser entendido como malicioso. Pero los desarrolladores de ciertas herramientas, una vez utilizada por la comunidad de hackers, que ahora se están libremente
distribuida o vendida comercialmente como relacionados con la seguridad del software, sin embargo, se trata como
código malicioso. Hay un doble rasero, y yo me quedo preguntándome por qué.

Otro artículo que se ofrece en el mismo correo electrónico se comprometió a realizar capturas de pantalla de la
la computadora del usuario, así como tener una cámara de video mirando sobre su hombro. Algunos
de estos productos de software ni siquiera se requiere el acceso físico a la víctima equipo. Sólo tiene que instalar y configurar la aplicación de forma remota, y tiene una escuchas telefónicas ordenador al instante! El FBI debe amar a la tecnología.

Con spyware tan fácilmente disponibles, la empresa necesita para establecer dos niveles de protección. Usted debe instalar software de detección de spyware, como SpyCop (Disponible en www.spycop.com) en todas las estaciones de trabajo, y usted quiere que que los empleados de iniciar exploraciones periódicas. Además, se debe capacitar a los empleados
contra el peligro de ser engañado para que descargue un programa o abrir un adjunto de correo electrónico que pueden instalar software malicioso.
Además de prevenir el spyware se instalen mientras que un empleado es lejos de su escritorio para tomar un café, un almuerzo o una reunión, una política de ordena que todos los empleados de bloqueo de sus sistemas informáticos con una contraseña de protector de pantalla o
método similar sustancialmente mitigar el riesgo de una persona no autorizada poder acceder al ordenador de un trabajador. Nadie caiga en la persona de cubículo u oficina, se podrá acceder a ninguna de sus archivos, leer su correo electrónico, o instalación de spyware u otro software malicioso. Los recursos necesarios para que la contraseña del protector de pantalla son nulas, y el beneficio de la protección de los empleados estaciones de trabajo es considerable. El análisis de costo-beneficio de esta circunstancia ser una obviedad.

Capítulo 13

Contras inteligente

Ahora usted ha descubierto que cuando un extraño llama a una solicitud de sensibilidad información o algo que pudiera ser de valor para un atacante, la persona
que recibe la llamada deben estar capacitados para obtener el número de teléfono del llamante, y devolver la llamada
para verificar que la persona es realmente quien dice ser - un empleado de la empresa, o un empleado de un socio de negocios, o un representante de soporte técnico de un de sus proveedores, por ejemplo.
Incluso cuando una empresa tiene un procedimiento establecido que los empleados siguen cuidadosamente para verificar que llaman, los atacantes sofisticados todavía son capaces de utilizar un
serie de trucos para engañar a sus víctimas haciéndoles creer que son lo que dicen a ser. Incluso los empleados conscientes de la seguridad pueden ser engañados por métodos tales como la
siguientes.

El Caller ID ENGAÑOSA

Cualquiera que haya recibido una llamada en un teléfono celular se ha observado la función conocido como identificador de llamadas - que muestran familiar que muestra el número de teléfono de la
persona que llama. En un entorno de negocios, ofrece la ventaja de permitir a un trabajador a decir en
de un vistazo si la llamada entrante es de un compañero de trabajo o desde el exterior de la empresa.
Hace muchos años, algunos phreakers teléfono ambiciosos se presentaron a la maravillas del identificador de llamadas antes de que la compañía telefónica siquiera se le permitió ofrecer el
servicio al público. Que lo pasamos muy bien volviendo loco a la gente respondiendo a las teléfono y saludar a la persona que llama por su nombre antes de decir una palabra.
Justo cuando se pensaba que era seguro, la práctica de la verificación de la identidad por medio de confiar
lo que se ve - lo que aparece en la pantalla del identificador de llamadas - es exactamente lo que el atacante
se puede contar con.

Llame al teléfono de Linda

Día / Hora: Martes, 23 de julio, 15:12

Su lugar. "Las oficinas del Departamento de Finanzas, Starbeat Aviación

Linda Hill teléfono sonó justo cuando estaba en el medio de escribir una nota a su
jefe. Miró a su identificador de llamadas, que mostró que la llamada era de la
oficina corporativa en Nueva York, sino de alguien que se llama Víctor Martín - no es una
nombre, reconoció.
Pensó en dejar que el rollo de llamada a través de mensajes de voz para no romper el
el flujo de pensamiento en la nota. Pero la curiosidad pudo más que ella. Cogió
el teléfono y la persona que llama se presentó y dijo que era de relaciones públicas, y
trabajando en un poco de material para el CEO. "Él está en su camino a Boston para reuniones
con algunos de nuestros banqueros. Que necesita los datos financieros de primera línea para el
actual
trimestre ", dijo." Y una cosa más. Él también necesita las proyecciones financieras de
el proyecto Apache ", agregó Víctor, con el nombre código para un producto que era
ser uno de los grandes lanzamientos de la compañía en la primavera.
Ella le pidió su dirección de correo electrónico, pero dijo que estaba teniendo un problema en la
recepción
correo electrónico que el soporte técnico está trabajando en, por lo que podía por fax en su lugar?
Dijo que
estaría bien, y él le dio la extensión telefónica interna de su máquina de fax.
Ella envió el fax a los pocos minutos.
Pero Víctor no trabajó para el departamento de relaciones públicas. De hecho, ni siquiera el
trabajo de
de la empresa.
La historia de Jack
Jack Dawkins había comenzado su carrera profesional a temprana edad como un carterista
trabajo juegos en el Yankee Stadium, en las plataformas del metro lleno de gente, y entre
la multitud durante la noche de los turistas en Times Square. Él demostró ser tan ágil y astuto
que podía tener un reloj de muñeca de un hombre sin que él supiera. Pero en su
torpe adolescencia se había criado torpe y sido atrapados. En la Sala de Menores,
Jack se enteró de un nuevo oficio con un riesgo mucho menor de conseguir atrapó.
Su actual llamados por él para obtener sus ganancias trimestrales de la empresa y la pérdida de
declaración y la información de flujos de efectivo, antes de que los datos se han presentado ante
la Securities
and Exchange Commission (SEC) y hecho público. Su cliente era un dentista que
no quiso explicar por qué quería la información. Para Jack cuidado del hombre
era ridículo. Lo había visto antes - el tipo probablemente tenía un problema con el juego,
o bien una novia cara que su esposa no se había enterado todavía. O tal vez
acababa de alardear de su esposa sobre lo inteligente que era en el mercado de valores;
Ahora que había perdido un montón y quería hacer una gran inversión en una cosa segura por
saber de qué manera el precio de la acciones de la compañía que iba a ir cuando
anunció sus resultados trimestrales.
La gente se sorprende al descubrir lo poco tiempo que tarda un reflexivo social
ingeniero para encontrar una manera de manejar una situación que nunca ha enfrentado antes.
Por
Jack el tiempo de llegar a casa de su reunión con el dentista, él ya se había formado
un plan. Su amigo Charles Bates trabajó para una compañía, Panda Importación, que
tenía su propia central telefónica o PBX.
En términos familiares para los conocedores de los sistemas de teléfono, la central se
conectado a un servicio de telefonía digital conocido como T1, configurado como principal
Tasa de interfaz ISDN (Integrated Services Digital Network) o RDSI PRI. Lo que esto
quería decir es que cada vez que se colocó un anuncio de Panda, la configuración y otra llamada
procesamiento de la información salió en un canal de datos para los que la compañía telefónica
interruptor, la información que se incluye el número que llama, que (a menos que
) bloqueado se entrega con el dispositivo identificador de llamadas en el extremo receptor.
Amigo de Jack sabía cómo programar el interruptor para que la persona que recibe la llamada
se vería en su identificador de llamadas, no el número de teléfono real en la oficina de Panda,

pero
cualquiera que sea el número de teléfono que había programado en el interruptor. Este truco funciona
porque las compañías telefónicas locales no se molestan en validar el número de llamadas recibido del cliente en contra de los números de teléfono real del cliente es
pagando.
Todos los Jack Dawkins necesitaba era el acceso a cualquier servicio telefónico tales. Felizmente su
amigo y alguna vez compañero de crimen, Charles Bates, siempre se alegraba de prestar un ayudando a mano por un precio nominal. En esta ocasión, Jack y Charles temporalmente cambiar reprogramado teléfono de la compañía para que las llamadas de un particular línea de teléfono ubicado en las instalaciones de Panda se parodia Victor Martin número de teléfono interno, lo que hace la llamada parece que puede venir desde dentro Starbeat Aviación.
La idea de que su identificador de llamadas se puede hacer para mostrar cualquier número que usted desea es tan poco
sabe que es rara vez se cuestiona. En este caso, Linda estaba feliz de fax de la información solicitada para el hombre que pensó que era de relaciones públicas.
Cuando Jack colgó, Charles reprogramado cambiar su compañía de teléfono, restaurar el número de teléfono a la configuración original.
Con el análisis de la
Algunas empresas no quieren que los clientes o proveedores para conocer el teléfono número de sus empleados. Por ejemplo, Ford puede decidir que las llamadas de sus Centro de atención al cliente debe mostrar el número 800 para el Centro y el nombre de una como "el apoyo de Ford," en lugar del número de teléfono de marcación directa real de cada soporte
representante de realizar una llamada. Microsoft puede dar a sus empleados la opción de decirle a la gente su número de teléfono, en vez de tener a todos los que llaman ser capaz de echar un vistazo a su identificador de llamadas y conocer su extensión. De esta manera el
empresa es capaz de mantener la confidencialidad de los números internos.
Pero esta misma capacidad de reprogramación ofrece una táctica útil para la bromista, proyecto de colector, telemarketer, y, por supuesto, el ingeniero social.
VARIACIÓN: EL PRESIDENTE DE LOS ESTADOS UNIDOS ES
LLAMADA
Como co-presentador de un programa de radio en Los Angeles llamado "lado oscuro de Internet" en la
Radio FKI Talk, que trabajó bajo la dirección de programa de la estación. David, uno de los personas más comprometidas y trabajadoras que he conocido, es muy difícil llegar a por teléfono porque está muy ocupado. Él es uno de esas personas que no responde a una llame a menos que vea el identificador de llamadas que se trata de alguien que tiene que hablar.
Cuando yo le había teléfono, porque tengo el bloqueo de llamadas en mi teléfono celular, no podía
saber quién estaba llamando y no contestar la llamada. Que se diera la vuelta a la voz mail, y se hizo muy frustrante para mí.
He hablado sobre qué hacer acerca de esto con un amigo de mucho tiempo, que es el co-fundador
de una empresa de bienes raíces que ofrece espacio de oficina para empresas de alta tecnología. Juntos
se nos ocurrió un plan. Tenía acceso a Meridian teléfono de su compañía interruptor, lo que le da la posibilidad de programar el número de quien llama, como se describe en la historia anterior. Cada vez que necesitaba para llegar a la directora del programa
y no podía obtener a través de una llamada, le pido a mi amigo para programar cualquier número de

mi elección a aparecer en el identificador de llamadas. A veces me lo han hacer la llamada parece como si viniera de la asistente de la oficina de David, o, a veces de la holding que posee la estación.
Pero mi favorito era la programación de la llamada a aparecer desde casa de David número de teléfono, que siempre recogido. H1 conceder su crédito al hombre, sin embargo. Él siempre tenía un buen sentido del humor acerca de que cuando cogía el teléfono y descubrir que le había engañado una vez más. La mejor partwas que luego quedaría en el línea de tiempo suficiente para averiguar lo que quería y resolver lo que la edición fue.
Cuando me demostró este pequeño truco en el show de Art Bell, que falsa de identidad del llamante
para mostrar el nombre y el número de la sede de Los Ángeles del FBI. Arte se sorprendió bastante de todo el asunto y advirtió a mí para hacer algo ilegal. Pero yo le señaló que es perfectamente legal, siempre y cuando sea no un intento de cometer un fraude. Después de que el programa que he recibido varios cientos de
mensajes de correo electrónico que me pide que explique cómo lo había hecho. Ahora ya lo sabes.
Esta es la herramienta perfecta para aumentar la credibilidad de la ingeniería social. Si, por ejemplo,
durante el periodo de investigación del ciclo de ingeniería social de ataque, se descubrió que el destino tenía identificador de llamadas, el atacante podría suplantar su número propio ser de una empresa de confianza o empleados. Un cobrador puede hacer su llamadas parecen provenir de su lugar de trabajo.
Sin embargo, detenerse y pensar en las consecuencias. Un intruso informático puede llamar al casa que dice ser del departamento de TI de su empresa. La persona en el línea con urgencia las necesidades de su contraseña para poder restaurar los archivos desde una caída del servidor. O el
identificador de llamadas muestra el nombre y número de su banco o casa de corretaje de valores,
la niña bonita que suena sólo tiene que verificar sus números de cuenta y su nombre de soltera de su madre. Por si fuera poco, también tiene que verificar su tarjeta de ATM PIN debido a algún problema del sistema. Un mercado de valores de la caldera, sala de operaciones puede
hacer sus llamadas parecen provenir de Merrill Lynch o Citibank. A alguien para que robar su identidad podría llamar, al parecer, de Visa, y convencerlos de que le digas su número de tarjeta Visa. Un hombre con un rencor podían llamar y dicen ser de la IRS o el FBI.
Si usted tiene acceso a un sistema telefónico conectado a un PRI, además de un poco de conocimientos de programación que es probable que pueda adquirir en el sistema de proveedor Sitio web, puede utilizar esta táctica para jugar trucos con tus amigos. Saber cualquier persona con aspiraciones políticas exageradas? Usted puede programar el envío número como 202 456-1414, y su identificador de llamadas muestra el nombre de "BLANCO CASA ".
Va a pensar que está recibiendo una llamada del presidente!
La moraleja de la historia es simple: identificador de llamadas no se puede confiar, excepto cuando se
utiliza para identificar las llamadas internas. Tanto en el trabajo y en casa, todo el mundo necesita darse cuenta del truco identificador de llamadas y reconocer que el nombre o número de teléfono se muestra en una pantalla de identificador de llamadas no siempre se puede confiar para la verificación de la identidad.
Mitnick MENSAJE
La próxima vez que usted recibe una llamada y muestra su identificador de llamadas es de su querido y viejo
madre, nunca se sabe - que podría ser de un poco de dulce ingeniero social de edad.
EL EMPLEADO INVISIBLE

Shirley Cutlass ha encontrado una nueva y emocionante manera de hacer dinero rápido. No más largas horas en la mina de sal. Ella se ha unido a los cientos de otra estafa
artistas que participan en el crimen de la década. Ella es un ladrón de identidad.
Hoy se ha puesto sus ojos en conseguir información confidencial de la
cliente departamento de servicio de una compañía de tarjetas de crédito. Después de hacer el tipo normal
de las tareas, que ella llama la empresa objetivo y le dice a la telefonista
que las respuestas que le gustaría estar conectado con el Departamento de Telecomunicaciones.
Llegar a Telecom, pide al administrador de correo de voz.
Utilizando la información obtenida de su investigación, explica que su nombre es
Norma Todd de la oficina de Cleveland. El uso de un ardid que debe ahora ser
familiar, ella dice que va a viajar a la sede corporativa de una semana,
y ella necesita un buzón de voz que por lo que no tendrá que hacer de larga distancia
llamadas para revisar sus mensajes de correo de voz. No hay necesidad de un teléfono físico
sentido, dice, sólo un buzón de voz. Él dice que va a cuidar de él, que llamaremos
la espalda cuando está creado para darle la información que necesita.
En una voz seductora, que dice: "Yo estoy en camino a una reunión, ¿te puedo llamar
en una hora.
Cuando ella vuelve a llamar, él dice que es todo listo, y le da la información - su
número de extensión y una contraseña temporal. Él le pregunta si sabe cómo
cambiar la contraseña del correo de voz, y ella le deja que hable a través de los pasos,
a pesar de que los conoce por lo menos tan bien como él.
"Y, por cierto," ella pregunta, "desde mi hotel, ¿qué número debo llamar para comprobar mi mensajes? "Él le da el número.
Shirley en los teléfonos, se cambia la contraseña, y los registros de su saludo saliente.
Shirley ataques
Hasta ahora todo ha sido una fácil configuración. Ella está ahora listo para utilizar el arte del engaño.
Ella llama al departamento de servicio al cliente de la empresa. "Estoy con las colecciones,
en la oficina de Cleveland ", dice ella, y luego se lanza a una variación en el bynow
excusa familiar. "Mi equipo está siendo fijado por el apoyo técnico y yo
Necesitamos su ayuda para buscar a esta información. "Y se va a proporcionar el
nombre y fecha de nacimiento de la persona cuya identidad se tiene la intención de robar.
Entonces
que enumera la información que quiere: el apellido de soltera de direcciones, la madre, número de tarjeta,
límite de crédito, crédito disponible y el historial de pagos. "Llámame a este número",
, dice ella, dando el número de extensión interno que el administrador de correo de voz
preparado para ella. "Y si no estoy disponible, deje la información en mi voz
mail ".
Ella se mantiene ocupado con las diligencias para el resto de la mañana, y luego revisa su
correo de voz de la tarde. Todo está ahí, todo lo que ella pidió. Antes de colgar
arriba, Shirley borra el mensaje de salida, sino que sería imprudente dejar una grabación
de su voz detrás.
Y el robo de identidad, el delito de más rápido crecimiento en Estados Unidos, el "en" El crimen de la
nuevo siglo, está a punto de tener otra víctima. Shirley utiliza la tarjeta de crédito y
información de identidad que acaba de obtener, y empieza a correr hasta los cargos en el
víctima de la tarjeta.
Con el análisis de la
En este ardid, el atacante engañó administrador de la empresa de correo de voz en
creyendo que era un empleado, por lo que iba a crear una voz temporal
buzón de correo. Si se molestó en comprobar en todo, se habría dado cuenta de que el nombre y la
número de teléfono que ella dio a juego con el listados en el empleado de la empresa

base de datos.
El resto fue simplemente una cuestión de dar una excusa razonable acerca de un equipo problema, solicitando la información deseada, y solicitando que la respuesta sea a la izquierda en el correo de voz. ¿Y por qué un empleado se muestran reacios a compartir información con un compañero de trabajo? Dado que el número de teléfono que Shirley estaba previsto claramente una extensión interna, no había ninguna razón para sospechar.

Mitnick MENSAJE

Trate de llamar a su buzón de voz propia de vez en cuando, si oye un mensaje de salida que no es tuyo, es posible que acabamos de encontrar a su ingeniero social en primer lugar.

EL SECRETARIO ÚTIL

Cracker Robert Jorday había sido regularmente irrumpir en la red informática de obras de una compañía global, Rodolfo Shipping, Inc. La compañía finalmente reconocido que alguien se la piratería en su servidor de terminales, una, que a través de ese servidor el usuario puede conectarse a cualquier sistema informático en la empresa. Para salvaguardar la red corporativa, la empresa decide, para solicitar una contraseña de acceso telefónico en cada Terminal Server.

Robert llamó al Centro de Operaciones de la Red haciéndose pasar por un abogado de la Departamento Jurídico y dijo que estaba teniendo problemas para conectarse a la red. La administrador de la red llegó a explicar que había habido algunos recientes cuestiones de seguridad, por lo que todos los usuarios de acceso telefónico se necesitan para obtener el mes contraseña de su jefe. Robert se preguntó qué método se utiliza para comunicar la contraseña de cada mes a los gerentes y cómo podía obtenerla.

La respuesta, resultó ser que la contraseña para el próximo mes se envió un memo a través de la oficina, por correo a cada gerente de la empresa.

Que hizo las cosas fáciles. Robert ha hecho un poco de investigación, llamó a la compañía poco después de el primer día del mes, y llegó a la secretaria de un gerente que le dio nombre como Janet. Él dijo, "Janet, hola. Este es Randy Goldstein en Investigación y Desarrollo. Sé que probablemente tiene la nota con la contraseña de este mes para sesión en el servidor Terminal Server desde fuera de la empresa, pero no puedo encontrarlo en cualquier lugar. ¿Recibió la nota de esto, al mes? "

Sí, me dijo, ella lo entendía.

Él le preguntó si iba a enviar por fax a él, y ella estuvo de acuerdo. Él le dio el fax número de la recepcionista del vestíbulo en un edificio diferente en el campus de la compañía, donde ya había hecho los arreglos para los faxes que se celebrará por él, y se a continuación, organizar para el fax contraseña que se transmitirá. Esta vez, sin embargo, Robert utilizar otro método de reenvío de faxes. Dio al recepcionista un número de fax que fue a un servicio de fax en línea. Cuando este servicio recibe un fax, el sistema automatizado que envía a la dirección de correo electrónico del suscriptor.

La nueva contraseña llegó a la caída de correo electrónico muertos que Robert establecido en un país libre servicio de correo electrónico en China. Estaba seguro de que si el fax se ha trazado nunca, la investigador sería tirar de los pelos tratando de obtener la cooperación de China funcionarios, que, sabía, era más que un poco reacios a ser de ayuda en materia de de esta manera. Lo mejor de todo, nunca había tenido que presentarse físicamente en el lugar del fax de la máquina.

Mitnick MENSAJE

El ingeniero social especializada es muy inteligente a influir en otras personas para hacer favores para él. Recepción de un fax y enviarlo a otro lugar aparece tan inofensivo que es muy fácil convencer a una recepcionista o alguien más está de acuerdo para hacerlo. Cuando alguien pide un favor, relacionados con la información, si no lo conocen o no puede verificar su identidad, sólo decir que no.

Tribunal de Tránsito
Probablemente todos los que se ha dado un exceso de velocidad ha soñado
de alguna manera de derrotarlo. No por ir a la escuela de tráfico, o simplemente pagar el
multa, o correr el riesgo de tratar de convencer al juez sobre algún tecnicismo
como cuánto tiempo ha pasado desde que el indicador de velocidad de coches o la policía era la pistola de radar
marcada. No, la más dulce de escenario sería vencer a los billetes de engañar a los
del sistema.
Con el
Aunque yo no recomendaría probar este método de golpear a una multa de tráfico (como
dice el refrán, no intente esto en casa) sin embargo, este es un buen ejemplo de cómo el arte
de engaño puede ser usado para ayudar al ingeniero social.
Vamos a llamar a este tráfico violater Pablo Durea.
Primeros pasos
"Policía de Los Ángeles, la División Hollenbeck".
"Hola, me gustaría hablar con el control de una citación judicial."
"Soy el empleado de una citación judicial."
"Está bien. Esto es abogado John Leland, de Meecham, Meecham y Talbott. Necesito
para citar a un funcionario en un caso. "
"Bueno, qué oficial?"
"¿Tienes Oficial de Kendall en su división?"
"¿Cuál es su número de serie?"
"21349".
"Sí. ¿Cuándo se le necesita?"
"En algún momento del próximo mes, pero tengo que citar a otros testigos en el
caso y luego decirle a la corte qué días va a trabajar para nosotros. ¿Hay alguna próximos días
meses Oficial de Kendall no estará disponible? "
"Vamos a ver ... Tiene días de vacaciones el día 20 al 23, y lo ha hecho
días de entrenamiento los días 8 y 16. "
"Gracias. Eso es todo lo que necesito ahora mismo. Me volveré a llamar cuando la fecha de corte se establece."
Corte Municipal, Contador secretario
Pablo: ". Me gustaría programar una cita en la corte en esta multa de tráfico"
Secretario: ".. Bueno te puedo dar el día 26 del mes que viene"
"Bueno, me gustaría hacer una lectura de cargos."
"¿Quieres una comparecencia en una multa de tráfico?"
"Sí".
"Está bien. Podemos establecer la comparecencia de mañana en la mañana o la tarde. ¿Qué
quieres? "
"Tarde".
"Acusación es mañana a las 1:30 PM en la Sala Seis". "Gracias. Estaré
allí. "
Corte Municipal, Sala Seis
Fecha: Jueves, 13:45
Secretario: "El señor Durea, por favor acercarse al estrado."
Juez: "El señor Durea, ¿entiende los derechos que se han explicado
esta tarde? "
Pablo: ". Sí, su señoría"
Juez: "¿Quieres tener la oportunidad de asistir a la escuela de tráfico de su caso?
serán despedidos después de la finalización con éxito de un curso de ocho horas. He
verificar su registro y que están actualmente elegibles. "
Pablo:.. "No, su señoría pido respetuosamente que el caso fuera a juicio Uno
cosa más, su honor, voy a viajar fuera del país, pero estoy disponible en
el 8 o 9. ¿Sería posible establecer mi caso a juicio en cualquiera de los
días? Me voy en un viaje de negocios para el futuro de Europa, y que yo vuelva en cuatro

semanas. "
Juez: ". Muy bien juicio está programado para el 08 de junio, 8:30 AM, Sala Cuatro".
Pablo: "Gracias, su señoría".
Corte Municipal, Sala Cuatro
Pablo llegó a la corte a principios de la octava. Cuando el juez llegó, el recepcionista le dio una lista de los casos en los que los agentes no habían aparecido. El juez llamó al los acusados, incluyendo a Pablo, y les dijo que sus casos fueron desestimados.
Con el análisis de la
Cuando un funcionario escribe un billete, lo firma con su nombre y su número de placa (O lo que sea su número de personal que se llama en su agencia). Encontrar su estación es un pedazo de la torta. Una llamada a la asistencia de directorio con el nombre de la aplicación de la ley
la agencia se muestra en la cita (la patrulla de caminos, sheriff del condado, o lo que sea) es lo suficiente como para poner un pie en la puerta. Una vez que la agencia está en contacto, pueden referirse al
llamadas al número de teléfono correcto para el empleado al servicio de la citación área geográfica donde se realizó la parada de tráfico.
Los oficiales de policía son citados para comparecencias ante los tribunales con regularidad; viene con el territorio. Cuando un fiscal de distrito o un abogado de la defensa necesita una oficial para testificar, si sabe cómo funciona el sistema, primero se asegura de el oficial estará disponible. Eso es fácil de hacer, sólo se necesita una llamada a la citación empleado de esa agencia.
Por lo general, en esas conversaciones, el abogado le pregunta si el oficial en cuestión se disponible en tal y tal fecha. Para este truco, Pablo necesitaba un poco de tacto, se había para ofrecer una razón plausible de por qué el empleado debería decirle lo que el oficial de fechas no estaría disponible.
La primera vez que fui a la sede del tribunal, por qué Pablo no simplemente decirle a la actuario del tribunal lo que la fecha que quería? Fácil - por lo que entiendo, el tráfico de la cancha empleados en la mayoría de lugares no permiten que los miembros del público para seleccionar las fechas de corte. Si un
fecha en que el secretario sugiere que no funciona para la persona, que va a ofrecer una alternativa o
dos, pero eso es en lo que se dobla. Por otra parte, cualquiera que esté dispuesto a tomar el tiempo adicional de la muestra para la lectura de cargos es probable que tenga mejor suerte.
Pablo sabía que él tenía derecho a pedir una comparecencia. Y sabía que los jueces son menudo están dispuestos a adaptarse a una solicitud de una fecha específica. Con mucho cuidado pedido
fechas que coincidían con los días de entrenamiento del oficial, a sabiendas de que en su estado, capacitación de funcionarios tiene prioridad sobre una aparición en la corte de tráfico.
Mitnick MENSAJE
La mente humana es una creación maravillosa. Es interesante observar cómo imaginativa la gente puede estar en el desarrollo de formas engañosas para conseguir lo que quieren o para salir de la
una situación difícil. Usted tiene que utilizar la misma creatividad e imaginación para salvaguardar la información y sistemas informáticos en los sectores público y privado. Por lo tanto, gente, la hora de diseñar las políticas de su empresa de seguridad - ser creativo y pensar fuera del área.
Y en el corte de tráfico, cuando el funcionario no se presenta - caso sea desestimado. No las multas. No hay escuela de tráfico. No hay puntos. Y lo mejor de todo, no hay registro de una infracción de tránsito!
Mi conjetura es que algunos funcionarios policiales, funcionarios judiciales, fiscales de distrito y el como va a leer esta historia y mueven la cabeza, porque saben que este
truco funciona. Sin embargo, meneando la cabeza es todo lo que voy a hacer. Nada va a cambiar. Me

estar dispuestos a apostar por ello. Como el personaje de Cosmo dice en la película Sneakers 1992,
"Se trata de los unos y ceros" - lo que significa que al final, todo se
abajo a la información.
Mientras las fuerzas del orden están dispuestos a dar información sobre un
horario oficial para cualquiera que se hace virtualmente, la posibilidad de salir de tráfico
entradas siempre van a existir. ¿Tiene diferencias similares en su empresa o
procedimientos de la organización de que un ingeniero social inteligente puede aprovechar para
obtener la información que preferiría no tener?
LA VENGANZA DE SAMANTHA
Samantha Gregson estaba enojado.
Había trabajado duro para su título universitario en negocios, y apilados un montón de
préstamos a los estudiantes a hacerlo. Siempre había sido inculcado a ella que un título
universitario
Fue así como se tiene una carrera en lugar de un trabajo, como usted ganó mucho dinero. Y
luego se graduó y no podía encontrar un trabajo digno en cualquier lugar.
Lo contenta que había sido conseguir que la oferta de fabricación Lambeck. Claro, es
Fue humillante para aceptar un puesto de secretaria, pero el señor dijo que tenía la forma
Cartright
ansiosos que estaban a su haber, y de tomar el trabajo de secretaría que la puso en el
lugar cuando la próxima administración no la posición de abierto.
Dos meses más tarde se enteró de que uno de los jefes de producto junior Cartright fue
dejando. Apenas pudo dormir esa noche, imaginándose en el quinto piso, en
una oficina con una puerta, asistiendo a las reuniones y la toma de decisiones.
A la mañana siguiente ella fue lo primero a ver al señor Cartright. Dijo que se sentía
tenía que aprender más sobre la industria antes de que ella estaba lista para un profesional
posición. Y entonces se fue y contrató a un aficionado de fuera de la empresa
que sabía menos sobre la industria que ella.
Se trataba entonces que comenzó a caer en ella: La compañía tenía un montón de
las mujeres, pero casi todos los secretarios. No se les iba a dar una
administración de trabajos. Nunca.
Recuperación de la inversión
Le llevó casi una semana para saber cómo iba a pagar.
Aproximadamente un mes antes, un chico de una revista de negocios de la industria ha tratado de
un golpe en
ella cuando entró en el lanzamiento de nuevos productos. Unas semanas más tarde la llamó
en el trabajo y dijo que si ella le enviaremos información sobre el avance
Cobra 273 productos, que enviaría sus flores, y si era realmente caliente que la información
que utilizó en la revista, que sería un viaje especial desde Chicago sólo para tomar su
salir a cenar.
Ella había estado en la oficina de jóvenes Johannson señor es un día poco después de que,
cuando
conectado a la red corporativa. Sin pensarlo, había visto los dedos
(Hombro surf, esto a veces se llama). Había entrado en "marty63" como su
contraseña.
Su plan estaba empezando a unirse. Había una nota que recordaba
escribir, no mucho después de que llegó a la empresa. Ella encontró una copia en los archivos y
escribió una nueva versión, con un lenguaje de la original. Su versión de lectura:
A: C. Pelton, departamento de TI.
DE: L. Cartright, Desarrollo
Martin Johansson va a trabajar con un equipo de proyectos especiales en mi departamento.
Por la presente le autoriza a tener acceso a los servidores utilizados por la ingeniería
grupo. Perfil de seguridad de Johansson se va a actualizar de concederle la misma
los derechos de acceso, como desarrollador de productos.
Louis Cartright

LINGO
HOMBRO DE SURF El acto de ver a un tipo de persona en su equipo
teclado para detectar y robar sus contraseñas o información de otros usuarios.
Cuando la mayoría de todo el mundo se había ido a almorzar, se cortó la firma del Sr. Cartright es de
la nota original, se pega en su nueva versión, y embadurnado Wite-fuera por
los bordes. Ella hizo una copia de los resultados, y luego hizo una copia de la copia. Usted
Apenas podía ver los bordes alrededor de la firma. Ella envió el fax de la
máquina ", cerca de la oficina del Sr. Cartright es.
Tres días más tarde, ella se quedó después de hora y esperó hasta que dejó a todos. Caminó
en la oficina de Johannson, y trató de acceder a la red con su nombre de usuario y
la contraseña, marry63. Funcionó.
En cuestión de minutos había localizado los archivos de especificación de producto para el Cobra 273, y
descargar en un disco Zip.
El disco estaba a salvo en su bolso mientras caminaba en el frío durante la noche a la brisa
el estacionamiento. Sería en su camino hacia el reportero de la noche.
Con el análisis de la
Un empleado descontento, una búsqueda a través de los archivos, una rápida cortar-pegar-y-Wite
A cabo la operación, una copia poco creativo, y un fax. Y, voila - tiene acceso a
comercialización confidencial y especificaciones del producto.
Y unos días más tarde, un periodista de la revista de comercio tiene una gran primicia con las especificaciones
y los planes de comercialización de un producto nuevo que estará en las manos de la revista
suscriptores en todo el mes de la industria antes de la liberación del producto.
Empresas de la competencia tendrá inicio la cabeza de varios meses en el desarrollo de
productos equivalentes y tener sus campañas publicitarias listo para socavar la Cobra
273.
Naturalmente, la revista nunca dicen de dónde sacaron la bola.
PREVENCIÓN DE LA CON
Cuando se le preguntó por la información valiosa y sensible, o críticos que podrían ser de
beneficio de un competidor o cualquier otra persona, los empleados deben ser conscientes de que el uso de llamadas
ID como una forma de verificar la identidad de un usuario externo no es aceptable.
Algunos otros medios de verificación debe ser utilizado, como la comprobación con la
supervisor de la persona que la solicitud era apropiada y que el usuario ha
autorización para recibir la información.
El proceso de verificación requiere un acto de equilibrio que cada empresa debe definir
por sí mismo: seguridad frente a la productividad. ¿Qué prioridad se va a asignar a
la aplicación de las medidas de seguridad? ¿Los empleados son resistentes a la seguridad de los siguientes
procedimientos, e incluso evitar el fin de completar su trabajo
responsabilidades? ¿Los empleados entienden por qué la seguridad es importante para la
empresa y de ellos mismos? Estas preguntas deben ser respondidas para desarrollar un
la política de seguridad basada en la cultura corporativa y las necesidades del negocio.
La mayoría de la gente, inevitablemente, ver cualquier cosa que interfiera con conseguir su trabajo hecho
como una molestia, y puede eludir las medidas de seguridad que parece ser un
pérdida de tiempo. Motivar a los empleados para hacer la parte de seguridad de su vida cotidiana
responsabilidades a través de la educación y el conocimiento es la clave.
A pesar de servicio de Caller ID no deben usarse nunca como un medio de autenticación para
llamadas de voz desde fuera de la empresa, otro método llamado número automático
identificación (ANI) puede. Este servicio se ofrece cuando una empresa se adhiere a
teléfono huir de servicios donde la empresa paga por las llamadas entrantes y es confiable
para su identificación. A diferencia de identificador de llamadas, el interruptor de la compañía

telefónica no utiliza
cualquier información que se envía de un cliente al proporcionar el número que llama.
El número transmitida por ANI es el número de facturación asignado a la convocatoria
partido.
Tenga en cuenta que muchos fabricantes modernos han añadido una característica de
identificador de llamadas en su
productos, la protección de la red corporativa, permitiendo el acceso remoto sólo llamadas
de una lista ofpreauthorized números de teléfono. Módems de identificación de llamadas son un
medios aceptables de autenticación en un entorno de baja seguridad, pero, al igual que
estar claro, ID de llamadas spoofing es una técnica relativamente fácil para el ordenador
intrusos, por lo que no debe ser invocado para probar la identidad de la persona que llama o
ubicación en un entorno de alta seguridad.
Para abordar el caso de robo de identidad, como en la historia de un engaño
administrador para crear un buzón de voz en el sistema telefónico corporativo, lo convierten en un
política de que todos los servicios de teléfono, todos los buzones de voz, y todas las entradas a la
empresa
directorio, tanto en forma impresa y en línea, debe ser solicitada por escrito, en un formulario
previsto a tal efecto. El gerente del empleado debe firmar la solicitud, y
el administrador de correo de voz debe verificar la firma.
Política de seguridad corporativa deben exigir que las cuentas de equipo nuevo o aumenta
los derechos de acceso sólo se concederá después de la verificación positiva de la persona que
la solicitud, tales como una devolución de llamada con el gerente o administrador del sistema, o
de su o
la persona designada, en el número de teléfono que aparece en la impresión o de la empresa on-
line
directorio. Si la empresa utiliza el correo electrónico seguro, donde los empleados pueden firmar
digitalmente
mensajes, este método de verificación alternativas también pueden ser aceptables.
Recuerde que todos los empleados, independientemente de si tiene acceso a la empresa
sistemas informáticos, puede ser engañado por un ingeniero social. Todo el mundo debe ser
incluidos en la formación de la conciencia de seguridad. Auxiliares administrativos, recepcionistas,
los operadores de telefonía, y los guardias de seguridad debe estar familiarizado con los tipos de
ataque de ingeniería social más probabilidades de ser dirigidos en su contra para que se
estar mejor preparados para defenderse de esos ataques.
Capítulo 14
Espionaje industrial
La amenaza de ataques contra el gobierno de la información, las empresas y
los sistemas universitarios está bien establecida. Casi todos los días, los medios de comunicación
informa de una nueva
virus informáticos, ataques de denegación de servicio, o el robo de información de tarjetas de
crédito
un comercio electrónico del sitio Web.
Leemos acerca de los casos de espionaje industrial, como Borland acusando a Symantec
del robo de secretos comerciales, Cadence Design Systems presentar una demanda de carga del
robo
del código fuente de un competidor. Muchas personas de negocios leer estas historias y
creo que nunca podría ocurrir en su empresa.
Lo que está ocurriendo todos los días.
VARIACIÓN EN UN SISTEMA DE
El ardid se describe en la siguiente historia ha sido probablemente arrancó muchas veces,
a pesar de que suena como algo sacado de una película de Hollywood como El
Información privilegiada, o desde las páginas de una novela de John Grisham.
Clase de Acción
Imagine que una masiva demanda colectiva se está librando en contra de una de las principales
compañía farmacéutica, Pharmomedic. La demanda alega que conocía a uno de

sus medicamentos muy popular tenía un efecto secundario devastador, pero que no sería evidente hasta que el paciente había estado tomando la medicación durante años. La demanda alega que
que había resultado de una serie de estudios de investigación que reveló el peligro, pero suprimió la evidencia y nunca se lo entregó a la FDA según sea necesario.
William ("Billy") Chaney, el abogado del caso en la cabecera de la Nueva
Firma de Nueva York la ley que presentó la demanda colectiva, tiene testimonios de dos Médicos Pharmomedic apoyar la reclamación. Pero ambos están jubilados, ni tiene documentos o archivos, y tampoco sería un testimonio fuerte, convincente.
Billy sabe que está en un terreno inestable. A menos que se puede obtener una copia de uno de esos
informes, o alguna nota interna o la comunicación entre los ejecutivos de la compañía, su caso, todo se vendrá abajo.
Por lo que contrata a una empresa que ha utilizado antes: Andreeson e Hijos, los investigadores privados.
Billy no sabe cómo Pete y su gente las cosas que hacen, y no
quiero saber. Todo lo que sabe es que Pete es un Andreeson buen investigador.
Para Andreeson, una misión de este tipo es lo que él llama un trabajo bolsa de color negro. La primera
la regla es que nunca las firmas de abogados y empresas que lo contratan aprender cómo él consigue su
información de manera que siempre lo han hecho una negación completa, plausible. Si alguien va a tener los pies metido en agua hirviendo, va a ser Pete, y para
lo que se acumula en las tasas en los puestos de trabajo grande, él calcula que vale la pena el riesgo. Además, se
obtiene satisfacción personal, de burlar a la gente inteligente.
Si los documentos que Chaney quiere que encuentre realmente existían y no han sido destruidos, van a estar en algún lugar en los archivos de Pharmomedic. Sin embargo, encontrar en
los archivos masivo de una gran empresa sería una tarea enorme. Por otro lado,
Supongo que han convertido las copias a su bufete de abogados, Jenkins y Petry? Si el abogados de la defensa sabía que existían esos documentos y no darles la vuelta como parte del proceso de descubrimiento, a continuación, han violado el canon de la profesión legal de la ética, y ha violado la ley, también. En el libro de Pete, que hace que cualquier ataque justo juego.
Ataque de Pete
Pete consigue un par de su pueblo comenzó en la investigación y en cuestión de días que él sabe lo que la empresa Jenkins y Petty utiliza para almacenar sus copias de seguridad fuera del sitio. Y sabe que la empresa de almacenamiento mantiene una lista de los nombres de las personas a quienes los
bufete de abogados ha autorizado a recoger las cintas de almacenamiento. También sabe que cada uno de
estas personas tiene su contraseña propia. Pete envía a dos de su pueblo en un trabajo bolsa de color negro.
Los hombres frente a la cerradura con una pistola de ganzúa ordenada en la Web en www.southord.com. En pocos minutos se deslizan en las oficinas de la
la empresa de almacenamiento de alrededor de 3 am una noche y el arranque de un PC. Ellos sonríen cuando ven
el logotipo de Windows 98, ya que significa que será un pedazo de pastel. Windows 98 no requiere ningún tipo de autenticación. Después de buscar algo exagerado, que localizar a un Microsoft base de datos con los nombres de las personas autorizadas por cada uno de los
los clientes de almacenamiento compañía para recoger las cintas. Que añadir un nombre falso a la
autorización de la lista de Jenkins y Petry, el mismo nombre que un conductor en un falso de licencia de uno de los hombres ya ha obtenido. ¿Podrían haber entrado en el

área de almacenamiento cerrada y trató de localizar a las cintas de su cliente quería? Seguro - pero
entonces todos los clientes de la compañía, incluyendo la firma de abogados, que sin duda han sido notificado de la violación. Y los atacantes se han perdido una ventaja:
Profesionales de siempre como para dejar una abertura para el acceso futuro, en caso de necesidad
surgir.
Después de una práctica habitual de los espías industriales para mantener algo en la espalda bolsillo para su uso futuro, por si acaso, también hizo una copia del archivo que contiene la autorización de la lista en un disquete. Ninguno de ellos tenía ni idea de cómo podría siempre ser útil, pero es sólo una de esas "Estamos aquí, sólo puede ser que también" cosas que de vez en cuando resulta ser valiosa.
Al día siguiente, uno de los mismos hombres llamó a la compañía de almacenamiento, utiliza el nombre
se había añadido a la lista de autorizaciones, y le dio la contraseña correspondiente. Él pidió las cintas Jenkins y Petry fecha en el último mes, y dijo que
un servicio de mensajería vendría a recoger el paquete. A media tarde,
Andreeson tenía las cintas. Su pueblo restaurado todos los datos a su propio ordenador sistema, listo para buscar en el ocio. Andreeson estaba muy contento de que la firma de abogados,
como la mayoría de otras empresas, no se molestó en cifrar sus datos de copia de seguridad. Las cintas fueron entregadas a la empresa de almacenamiento al día siguiente y uno no fue el más sabio.
Mitnick MENSAJE
Valiosa información debe ser protegida sin importar la forma que adopte o donde
se encuentra. Lista de una organización cliente tiene el mismo valor, ya sea en impresa forma o un archivo electrónico en su oficina o en una caja. Social
ingenieros prefieren siempre el más fácil de eludir, al menos, defendió el punto de ataque.
Una empresa de instalaciones fuera del sitio de almacenamiento de copia de seguridad es visto como un menor riesgo de
detección o quedar atrapados. Toda organización que almacena todos los valiosos y sensibles, o los datos críticos con terceros debe cifrar sus datos para proteger su confidencialidad.
Con el análisis de la
Debido a la seguridad física relajada, los malos eran fácilmente capaces de forzar la cerradura de la compañía de almacenamiento, el acceso a la computadora, y modificar el
base de datos que contiene la lista de personas autorizadas a tener acceso al almacenamiento la unidad. Agregar un nombre a la lista de permitidos los impostores para obtener el equipo las cintas de respaldo que buscaban, sin tener que entrar en la unidad de almacenamiento de la empresa.
Porque la mayoría de las empresas no cifrar los datos de copia de seguridad, la información era de ellos
para tomar.
Este incidente es un ejemplo más de cómo una empresa de proveedores que no precauciones de seguridad razonables de ejercicio puede hacer que sea fácil para un atacante comprometer los activos de sus clientes información.
El nuevo socio de negocios
Los ingenieros sociales tienen una gran ventaja sobre los estafadores y timadores, y el ventaja es la distancia. Un estafador sólo se puede engañar al estar en su presencia,
lo que le permite dar una buena descripción de él más tarde o incluso llamar a la policía si se captura en el engaño a tiempo.
Ingenieros sociales que normalmente evitar ese riesgo, como la peste. A veces, sin embargo, el riesgo es necesario y justificado por la recompensa potencial.
Historia de Jessica
Jessica Andover sentía muy bien sobre conseguir un trabajo con un pez gordo robótica

de la empresa. Claro, era sólo una puesta en marcha y que no podían pagar mucho, pero fue pequeños, la gente era amable, y allí estaba la emoción de conocer a su
opciones sobre acciones podría llegar a hacer su rica. Bueno, tal vez un millonario
como los fundadores de la empresa sería, pero lo suficientemente rico.
¿Qué fue lo que sucedió que Rick Daggot tiene una sonrisa radiante, cuando
entré en el vestíbulo de la mañana del martes en agosto. En su cara al futuro
traje (Armani) y su gran reloj de pulsera de oro (un Rolex Presidente), con su
corte de pelo impecable, tenía el mismo varonil, seguro de sí mismo aire que se había llevado a todos los
las chicas locas cuando Jessica estaba en la secundaria.
"Hola", dijo. "Estoy Daggot Rick y yo estoy aquí por mi encuentro con Larry."
Jessica sonrisa se desvaneció. "Larry?" dijo. "Larry está de vacaciones durante toda la semana." "He
una cita con él en uno. Sólo voló desde Louisville para cumplir
con él ", dijo Rick, ya que sacó su Palm, lo encendió, y le mostró.
Ella lo miró y le dio una pequeña sacudida de la cabeza. "El 20", dijo. "Eso es
la próxima semana. "Tomó el bolsillo de vuelta y lo miró." Oh, no! "se quejó." I
No puedo creer lo que es un error estúpido que cometí. "
"¿Puedo reservar un vuelo a cambio de que, al menos?" -preguntó, sintiendo lástima por él.
Mientras que ella hizo la llamada telefónica, Rick le confió que él y Larry había acordado
establecer una alianza estratégica de comercialización. Compañía de Rick fue la producción de productos para
la línea de fabricación y montaje, elementos que perfectamente se complementan
su nuevo producto, el C2Alpha. Productos de Rick y el conjunto se C2Alpha
hacer una solución fuerte que sería importante abrir los mercados industriales, tanto para las empresas.
Cuando Jessica se había terminado de hacer su reserva en un vuelo de la tarde, Rick
dijo: "Bueno, al menos podía hablar con Steve si está disponible." Pero Steve, el
VP compañía y cofundador, también estaba fuera de la oficina.
Rick, que es muy amigo de Jessica y coqueteando un poco, y luego sugirió que, como
siempre y cuando él estaba allí y su vuelo de regreso no fue sino hasta la tarde, que le gustaría
tomar algunas de las personas clave para el almuerzo. Y añadió: "Incluso tú, por supuesto - es
hay alguien que puede llenar para que la hora del almuerzo.
Vacían en la idea de ser incluidos, Jessica preguntó: "¿Quién quiere
? venir "Él tocó su bolsillo una y otra llamada a algunas personas - dos ingenieros
de I + D, las nuevas ventas y el hombre de marketing, las finanzas y el tipo asignado a la
del proyecto. Rick le sugirió que hablara de su relación con la sociedad,
y que le gustaría presentarse ante ellos. Él nombró el mejor restaurante de la
la zona, un lugar donde Jessica siempre había querido ir, y dijo que el libro
mesa de sí mismo, para las 12:30, y que volvería a llamar más tarde en la mañana para asegurarse de que
, todo estaba arreglado.
Cuando se reunieron en el restaurante - el cuatro de ellas además de Jessica a su mesa
no estaba lista todavía, así que se establecieron en el bar, y Rick dejó en claro que las bebidas y el almuerzo se encontraban en él. Rick era un hombre con estilo y clase, la clase de persona que te hace sentir cómodo desde el primer momento, de la misma manera que se siente con
alguien que has conocido durante años. Siempre parecía saber exactamente lo correcto
decir, había una frase alegre o algo divertido cada vez que la conversación
rezagado, y te hizo sentir bien sólo estar cerca de él.
Compartió sólo suficientes detalles acerca de los productos de su propia compañía de que podrían
prever la solución de marketing conjunto que parecía tan animada sobre. Nombró
varias compañías Fortune 500 que su empresa ya estaba vendiendo a, hasta que todo el mundo
en la mesa comenzaron a imagen de sus productos convirtiéndose en un éxito desde el día de la

Las primeras unidades salieron de la fábrica.
Luego Rick se acercó a Brian, uno de los ingenieros. Mientras que los otros charlaban entre ellos, Rick compartió algunas ideas en privado con Brian, y lo llevó a cabo sobre las características únicas de la C2Alpha y lo que lo diferencia de cualquier cosa la competencia había. Se enteró de un par de características de la empresa fue restando importancia a que Brian estaba orgulloso de pensamiento y realidad "limpio".
Rick abrió camino a lo largo de la línea, charlando tranquilamente con cada uno. La comercialización
hombre estaba feliz por la oportunidad de hablar acerca de la fecha puesta en marcha y los planes de marketing.
Y el contador de frijol sacó un sobre de su bolsillo y escribió los detalles de los materiales y los costes de fabricación, de precio y el margen de espera, y qué tipo de acuerdo que estaba tratando de trabajar con cada uno de los vendedores, que mencionadas por su nombre.
En el momento en su mesa estaba lista, Rick había intercambiado ideas con todo el mundo y había ganado admiradores en toda la línea. Al final de la comida, cada uno de ellos sacudió la mano de Rick a su vez y le dio las gracias. Rick intercambiar tarjetas de visita con cada uno y menciona de pasada a Brian, el ingeniero, que quería tener un ya la discusión tan pronto como Larry regresó.
Al día siguiente, Brian cogió su teléfono para descubrir que la llamada era de Rick, quien dijo que acababa de hablar con Larry. Voy a volver en el
De lunes a trabajar en algunos de los detalles con él ", dijo Rick," y quiere que me para estar al tanto de su producto. Él dijo que usted debe de correo electrónico los últimos diseños
y las especificaciones para él. Él va a elegir las piezas que él quiere que yo tenga y las remitirá a mí. "
El ingeniero dijo que iba a estar bien. Bueno, Rick respondió. Continuó, "Larry
quería que supieras que él está teniendo un problema al recuperar su correo electrónico. En lugar de
enviar el material a su cuenta regular, se las arregló con el negocio del hotel centro para establecer una cuenta de correo Yahoo para él. Él dice que usted debe enviar los archivos
a larryrobotics@yahoo.com ".
La mañana del lunes siguiente, cuando Larry entró en la oficina en busca bronceada y relajada, Jessica estaba preparada y con ganas de brotar más de Rick. "¡Qué gran tipo. Tomó un montón de nosotros a comer, incluso para mí. "Larry parecía confundido. "Rick? ¿Quién diablos es Rick?"
"¿De qué estás hablando - su socio de negocios nuevos." "Lo que !!!???"
"Y todo el mundo estaba tan impresionado con lo que las buenas preguntas-le preguntó." "Yo no conozco a ningún Rick ... "
"¿Qué le pasa a usted ¿Es una broma, Larry - Tú estás engañando sólo conmigo, ¿no? "
"Obtener el equipo ejecutivo en la sala de conferencias. Como ahora. No importa lo que que están haciendo. Y todo el mundo que estaba en ese almuerzo. Incluyéndote a ti. "
Se sentaron alrededor de la mesa de un humor sombrío, casi sin hablar. Larry entró, se sentó y dijo: "Yo no conozco a nadie llamado Rick. Yo no tengo un nuevo socio de negocios que he estado guardando el secreto de todos ustedes. Que habría pensaba que era obvio. Si hay un bromista, en medio de nosotros, quiero que hable hasta ahora. "
No es un sonido. La habitación parecía estar cada vez más oscuro a cada momento.
Finalmente Brian habló. "¿Por qué no dijiste nada cuando le envié que el correo electrónico con las especificaciones del producto y el código fuente? "
"Lo de correo electrónico?"
Brian se puso rígido. "Oh ... mierda!"

Cliff, el otro ingeniero, intervino in "Él nos dio todas las tarjetas de visita. Sólo necesitamos para llamarlo y ver lo que la campana que está pasando. "
Brian sacó su ordenador de mano, llamó a una entrada, y deslizó que el dispositivo encima de la mesa de Larry. Aún con la esperanza contra toda esperanza, que todos los miraba como si en trance, mientras que Larry marcado. Después de un momento, apuñaló el altavoz botón y todo el mundo escuchó la señal de ocupado. Después de intentar varias veces el número durante un período de veinte minutos, un frustrado Larry marcó el operador para pedir una interrupción de emergencia.
Unos momentos más tarde, el operador de regreso en la línea. Ella dijo en una tono desafiante: "Señor, ¿dónde conseguiste este número?" Larry le dijo que estaba en la tarjeta de visita de un hombre que tenía que ponerse en contacto urgentemente. El operador, dijo: "Yo soy lo siento. Eso es una empresa de telefonía número de prueba. Que siempre suena ocupado. "
Larry comenzó a hacer una lista de lo que la información había sido compartida con Rick. La imagen no era bastante.
Dos detectives de la policía vino y se llevó un informe. Después de escuchar la historia, señaló que ningún crimen se había cometido estatal, no había nada que pudieran hacer. Se aconseja ponerse en contacto con Larry el FBI debido a que tienen jurisdicción sobre los delitos relacionados con el comercio interestatal. Cuando Rick Daggot preguntó el ingeniero que transmita los resultados de la prueba al tergiversar sí mismo, puede haber cometido un delito federal, pero Rick tendría que hablar con el FBI para descubrir.
Tres meses después, Larry se encontraba en su cocina, leyendo el periódico más desayuno, y casi derrama su café. Lo que había estado temiendo desde que había oído por primera vez acerca de Rick se había hecho realidad, su peor pesadilla. Allí estaba en blanco y negro, en la primera página de la sección de negocios: una empresa que nunca había fue oído hablar de anunciar el lanzamiento de un nuevo producto que sonaba exactamente como la C2Alpha su compañía había estado desarrollando durante los últimos dos años.
A través del engaño, estas personas lo habían golpeado al mercado. Su sueño fue destruido. Los millones de dólares invertidos en investigación y desarrollo en vano. Y probablemente no podría ser una sola cosa en contra de ellos.
Historia de Sammy Sanford
Suficientemente inteligente como para estar ganando un gran salario en un trabajo legítimo, pero lo suficientemente torcida que prefieren ganarse la vida como un estafador, Sammy Sanford había ido muy bien para sí mismo. Con el tiempo llegó a la atención de un espía que se había visto obligada a principios de jubilación a causa de un problema con la bebida, amargo y vengativo, el hombre había encontró la manera de vender los talentos que el gobierno había hecho de él un experto in Siempre a la búsqueda de las personas que podrían utilizar, que había visto la primera Sammy Cuando se conocieron. Sammy había sido fácil, y muy rentable, a cambio de su enfoque de levantar dinero de la gente a levantar secretos de la compañía.
La mayoría de la gente no tiene las agallas para hacer lo que hago. Tratar de engañar a la gente sobre el teléfono o por Internet y nadie llega a ver. Sin embargo, cualquier Con buena el hombre, la antigua usanza, cara a cara de bueno (y hay muchos de ellos todavía alrededor, más de lo que piensan) puede mirar a los ojos, le dice una mentira, y conseguir que lo creas. He conocido a un fiscal o dos que creo que es criminal. Creo que es un talento.
Pero no se puede ir caminando a ciegas, hay que cosas de tamaño en primer lugar. Con A la calle, usted puede tomar la temperatura de un hombre con un poco de conversación amistosa y un par de cuidadosamente redactado sugerencias. Obtener las respuestas correctas y Bingo - que haya

bolsas
una paloma.
Un trabajo de la empresa es más parecido a lo que llamamos una estafa grande. Tienes que hacer la configuración. Encontrar
cuáles son sus botones son, saber lo que quieren. Lo que necesitan. Plan de una
ataque. Sea paciente, hacer su tarea. Averiguar el papel que va a jugar
y aprender sus líneas. Y no entrar por la puerta hasta que esté listo.
Pasé más de tres semanas de ponerse al día para éste. El cliente dio
me una sesión de dos días en lo que debería decir "mi" empresa hizo y cómo
describir por qué iba a ser una buena alianza de comercialización conjunta.
Luego tuve suerte. Llamé a la compañía y me dijo que era de una sociedad de capital riesgo
y estamos interesados en la creación de una reunión y yo estaba haciendo malabares con los horarios
encontrar un momento en que todos nuestros socios estarán disponibles en los próximos
par de meses, y hubo algún espacio de tiempo que deben evitar, en qué época
Larry no iba a estar en la ciudad? Y ella dijo: Sí, él no había tenido tiempo libre
en los dos años transcurridos desde que comenzó la compañía, pero su esposa lo estaba arrastrando
de distancia en unas vacaciones de golf de la primera semana de agosto.
Eso fue sólo dos semanas. Yo podía esperar.
Mientras tanto, una revista de la industria me dio el nombre de la empresa de la firma de relaciones públicas. Yo
dije que me gustaba la cantidad de espacio que estaban recibiendo por su empresa de robótica
cliente y que quería hablar con quien estaba manejando la cuenta sobre el manejo de
mi empresa. Que resultó ser una mujer enérgica joven que le gustaba la idea de que
podría ser capaz de traer una nueva cuenta. Durante un almuerzo caro con una copa más
de lo que realmente quería, ella hizo todo lo posible para convencerme de que eran oh, tan bueno en
comprensión de los problemas de un cliente y encontrar la correcta solución de relaciones públicas. Jugué
difícil de convencer. Necesitaba un poco de detalles. Con un poco de insistencia, por el momento en que el
placas se estaban quedando sin ella me había dicho más sobre el nuevo producto y la
problemas de la empresa de lo que podía haber esperado.
La cosa fue como un reloj. La historia trata de ser tan avergonzado de que el
reunión la próxima semana, pero que también podría reunirse con el equipo mientras yo estoy aquí, el
recepcionista tragarse enteras. Incluso sentí lástima por mí en el negocio. La
almuerzo me retrasó todos los de $ 150. Con la punta. Y yo tenía lo que necesitaba. Teléfono
números, títulos de trabajo, y un tipo muy clave que cree que fui yo quien me dijo que yo era.
Brian me había engañado, lo admito. Parecía el tipo de persona que acababa de correo electrónico
me lo he pedido. Pero su voz sonaba como si estuviera frenando un poco cuando me
trajo a colación el tema. Vale la pena esperar lo inesperado. Que en la cuenta de correo electrónico
El nombre de Larry, que lo tenía en mi bolsillo trasero por si acaso. La gente de seguridad Yahoo
Probablemente todavía sentado allí esperando a que alguien utilice la cuenta de nuevo para
pueden encontrarlo. Van a tener que esperar mucho tiempo. La mujer gorda ha cantado. Me voy a otro proyecto.
Con el análisis de la
Cualquier persona que trabaja una estafa cara a cara tiene a sí mismo manto de un aspecto que hacerlo aceptable a la marca. Él se puso juntos una manera de aparecer en
la pista de carreras, otro para aparecer en un pozo de agua local, otro para un
bar de lujo en un hotel de lujo.
Es de la misma manera con el espionaje industrial. Un ataque puede requerir un traje y corbata

y un maletín caro si el espionaje se hace pasar por un ejecutivo de una establecida empresa, consultor, o un representante de ventas. En otro trabajo, tratando de hacerse pasar por un software de
ingeniero, un técnico, o alguien de la sala de correo, la ropa, el
uniforme - la mirada del conjunto sería diferente.
Para infiltrarse en la empresa, el hombre que se llama Rick Daggot sabía que
tenía que proyectar una imagen de confianza y competencia, respaldada por un fondo
conocimiento de los productos de la empresa y la industria.
No mucha dificultad poniendo las manos sobre la información que necesitaba antes.
Él ideó una artimaña fácil de encontrar cuando el presidente iba a estar. Un pequeño
reto, pero todavía no es muy difícil, fue encontrar los detalles suficientes acerca de la
proyecto que podría sonar "en el interior" acerca de lo que estaban haciendo. A menudo
esta información se conoce a los proveedores de la empresa diferentes, así como los inversores,
los capitalistas de riesgo que han abordado sobre la recaudación de dinero, su banquero, y
su bufete de abogados. El atacante tiene que tener cuidado, sin embargo: Encontrar a alguien que
parte con conocimiento de información privilegiada puede ser difícil, pero tratar de dos o tres
fuentes a su vez
alguien que se puede extraer de la información corre el riesgo de que la gente
captura en el juego. De esta forma reside el peligro. El Daggots Rick del mundo necesitan
para recoger con cuidado y la banda de rodamiento de cada ruta de información una sola vez.
La comida era otra proposición pegajosa. Primero fue el problema de la
arreglar las cosas por lo que tendría unos minutos a solas con cada persona, de
alcance del oído de los demás. Él le dijo a Jessica 12:30 pero reservado la mesa para la 1 pm, en un
de lujo, los gastos por cuenta del tipo de restaurante. Se espera que significaría que habían
tiene que tomar una copa en el bar, que es exactamente lo que pasó. Un perfecto
oportunidad de moverse y hablar con cada persona.
Sin embargo, hay muchas maneras de que un paso en falso - una respuesta incorrecta o negligente un
observación podría revelar Rick ser un impostor. Sólo una muy confiado y astuto
espionaje industrial se atrevería a correr el riesgo de exponerse de esa manera. Pero años
de trabajar en las calles como un hombre de confianza había construido habilidades Rick y le ha dado
él la confianza de que, aunque tuvo un desliz, él sería capaz de cubrir bien
suficiente para calmar las sospechas. Este fue el más difícil, más peligrosa
tiempo de toda la operación, y el júbilo que sentía al traer de una picadura de este
le hizo darse cuenta por qué no tiene que conducir coches rápidos o saltar en paracaídas o engañar a su
mujer - que tiene un montón de emoción sólo hace su trabajo. ¿Cuántas personas, que
se preguntaba, podía decir lo mismo?
Mitnick MENSAJE
Aunque la mayoría de los ataques de ingeniería social se producen a través del teléfono o correo electrónico, no
suponer que un atacante atrevido nunca van a aparecer en persona en su negocio. En la mayoría de
de los casos, el impostor utiliza alguna forma de ingeniería social para obtener acceso a una
edificio después de la falsificación de una tarjeta de empleado con una frecuencia disponible
programa de software como Photoshop.
¿Qué pasa con las tarjetas de visita con la línea telefónica pruebas de la compañía? La televisión
show The Rockford Files, que era una serie sobre un detective privado,
ilustra una técnica ingeniosa y divertida un poco. Rockford (interpretado por el actor
James Garner) tenía un portátil con tarjeta de negocio de máquinas de impresión en su coche, que
utiliza para imprimir una tarjeta adecuada a lo que la ocasión lo requería. Estos
día, un ingeniero social puede obtener tarjetas de presentación impresas en una hora, en

cualquier copia
guardar o imprimir en una impresora láser.
NOTA
John Le Carré, autor de El espía que surgió del frío, Un espía perfecto,
y muchos otros libros notables, y creció como el hijo de un pulido, con la participación
toda la vida puede el hombre. Le Carré se pareció a un joven a descubrir que, con éxito
como su padre era engañar a otros, él era también ingenuo, una víctima más de una vez
a otro estafador o una mujer. Que sólo sirve para demostrar que todo el mundo está en riesgo de
de ser acogido por un ingeniero social, incluso otro ingeniero social.
¿Qué lleva a un grupo de hombres inteligentes y las mujeres a aceptar un impostor? Nos tamaño de un
situación tanto por el instinto y la inteligencia. Si la historia se suma - que es el intelecto
parte - y un estafador logra proyectar una imagen creíble, por lo general estamos dispuestos
a bajar la guardia. Es la imagen creíble que separa una estafa éxito
hombre o de un ingeniero social que rápidamente tierras tras las rejas.
Pregúntese: ¿Qué tan seguro estoy de que nunca se enamoraría de una historia como la de Rick? Si
estás seguro de que no, pregúntese si alguien ha puesto nada
más en ti. Si la respuesta a esta segunda pregunta es sí, es probablemente la correcta
respuesta a la primera pregunta, también.
LEAPFROG
Un reto: La siguiente historia no involucra el espionaje industrial. A medida que
leerlo, a ver si puedo entender por qué me decidí a poner en este capítulo!
Tarde Harry estaba de vuelta viviendo en casa, y estaba amargado. La Infantería de Marina había
Parecía un gran escape, hasta que lavado de campo de entrenamiento. Ahora que había
regresó a la ciudad que odiaba, estaba tomando cursos de informática a nivel local
la comunidad universitaria ", y buscando una manera de atacar a todo el mundo.
Finalmente se le ocurrió un plan. Unas cervezas con un chico en una de sus clases, que había sido
quejándose de su instructor, un sarcástico sabe-lo-todo, y juntos
cocinado un esquema perverso de quemar al hombre: Se agarraba el código fuente de un
popular asistente digital personal (PDA) y enviarlo a la del instructor
equipo, y asegúrese de dejar un rastro de lo que la empresa podría pensar que el
instructor era el malo.
El nuevo amigo, Karl Alexander, dijo que "sabía un par de trucos" y dicen que
Harry cómo llevar esto adelante. Áridas salirse con la suya.
Hacer su tarea
Una investigación inicial mostró poco a Harry que el producto había sido diseñado en el
Centro de Desarrollo ubicado en la sede del fabricante de PDA en el extranjero.
Pero había también un centro de I + D en los Estados Unidos. Eso era bueno, Karl
señaló, ya que por el intento de trabajar que tenía que haber un poco de compañía
instalaciones en los Estados Unidos, que también es necesario el acceso al código fuente.
En ese momento, Harry estaba listo para llamar al Centro de Desarrollo de Ultramar. Aquí está
en una declaración de simpatía vino, el "Oh, querido, estoy en problemas, necesito ayuda,
por favor, por favor, ayúdame. "Naturalmente, el motivo fue un poco más sutil que eso. Karl
escribió un guión, pero Harry parecía completamente falsa tratando de leer. En el
final, se practica con Karl para que pudiera decir lo que necesitaba en una conversación
tono.
Lo que Harry finalmente dijo, con Karl sentado a su lado, fue algo como esto:
"Voy a llamar a la I + D Minneapolis. Nuestro servidor tenía un gusano que infectó a los
departamento. Tuvimos que instalar el sistema operativo de nuevo y luego, cuando
fuimos a restaurar la copia de seguridad, ninguna de las copias de seguridad era bueno. Adivina quién
Se supone que el control de la integridad de las copias de seguridad? Atentamente. Así que estoy
conseguir gritado por mi jefe, y la gestión se levanta en armas que hemos perdido la

de datos. Mira, tengo que tener la última versión del árbol de código fuente tan rápido como que pueda. Necesito que gzip el código fuente y enviar a mí. "
En este punto, Karl le escribió una nota, y Harry le dijo al hombre en el otro extremo del teléfono que él sólo quería que transferir el archivo interno, a Minneapolis I + D. Esto fue muy importante: Cuando el hombre en el otro extremo del teléfono Estaba claro que era sólo les pide que enviar el archivo a otra parte de la empresa, su mente estaba en paz - lo que podría ser malo en eso?
LINGO
GZIP para comprimir archivos en un solo archivo comprimido con una utilidad de Linux GNU.
Estuvo de acuerdo en gzip y enviarlo. Paso a paso, con Karl a su lado, Harry habló el hombre que a través de empezar en el procedimiento para la compresión de los grandes código fuente en un archivo único y compacto. También le dio un nombre de archivo para su uso en
el archivo comprimido ", newdata", explicando que este nombre podría evitar confusión con los archivos viejos, dañados.
Karl tuvo que explicar el próximo paso dos veces antes de que Harry lo consiguió, pero fue fundamental para
el pequeño juego de salto Karl había soñado. Harry fue a llamar a la I + D Minneapolis y contarle a alguien ahí "Quiero enviar un archivo a usted, y luego quiero que lo envíe a otro lugar para mí ", por supuesto, todos vestidos con razones que hacen que todo suenan plausibles. Lo que confunde Harry era el siguiente: El Se suponía que decir "yo voy a enviar un archivo," cuando no iba a ser Harry enviar el archivo en absoluto. Tuvo que hacer el hombre que estaba hablando con el R & D Center que el archivo fue viniendo de él, cuando lo que el Centro se realmente va a recibir es el archivo de código fuente propietario de Europa. "¿Por qué le diría a él que viene de mí cuando en realidad viene del extranjero? "
Harry quería saber.
"El hombre en el Centro de I + D es la pieza clave", explicó Karl. "Él tiene que pensar que sólo está haciendo un favor a un compañero de trabajo aquí en los EE.UU., consiguiendo un archivo de
usted y luego solo envío para usted. "
Harry finalmente entendí. Llamó al Centro de I + D, donde pidió a los recepcionista que lo conectan con el Centro de Cómputo, donde pidió hablar con un de operador de computadoras. Un hombre se puso al aparato que sonaba tan jóvenes como Harry
sí mismo. Harry le saludó, explicó que llamaba desde Chicago fabricación de la división de la empresa y que había este archivo que había estado tratando de enviar a uno de sus socios trabajando en un proyecto con ellos, pero, dijo, "Hemos tiene este problema del router y no puede alcanzar la red. Me gustaría transferir el archivo a usted, y después de recibirlo, ¿Llamaremos por teléfono para que yo pueda caminar a través de transferir a la computadora de la pareja.
Hasta ahora, todo bien. Harry le preguntó al joven si su centro de cómputo tenía una cuenta FTP anónimo, una configuración que permite a cualquier persona para transferir archivos en
y de un directorio en el que no se requiere contraseña. Sí, un FTP anónimo estaba disponible, y dio a Harry el protocolo interno de Internet (IP) para llegar a ella.
LINGO
FTP anónimo Un programa que proporciona acceso a una computadora a distancia, incluso aunque usted no tiene una cuenta utilizando el protocolo de transferencia de archivos (FTP).
A pesar de FTP anónimo se puede acceder sin una contraseña, por lo general useraccess los derechos a determinadas carpetas se encuentran restringidas.
Con esa información en mano, Harry volvió a llamar al Centro de Desarrollo en el extranjero. Por ahora el archivo comprimido estaba listo, y Harry le dio las instrucciones para transferir el archivo al sitio FTP anónimo. En menos de cinco minutos, el

comprimido archivo de código fuente fue enviado a la niña en el Centro de I + D.
Configuración de la Víctima
A mitad de camino a la meta. Ahora Harry y Karl tuvo que esperar para asegurarse de que el expediente había
llegó antes de proceder. Durante la espera, que cruzó la habitación a la
escritorio del instructor y se hizo cargo de dos pasos necesarios. En primer lugar establecer un servidor FTP anónimo en su máquina, que servirá como destino de
el archivo en la última etapa de su programa.
El segundo paso proporcionado una solución para un problema de otra manera difícil. Está claro que
No podría decir a su hombre en el Centro de I + D para enviar el archivo a una dirección como, por ejemplo, warren@rms.ca.edu. La ". Edu" de dominio sería un claro indicativo, ya que cualquier tipo de la computadora medio despierto lo reconocería como la dirección de una escuela,
inmediatamente soplando toda la operación. Para evitar esto, entraron en Windows
en el ordenador del profesor y miró la dirección IP de la máquina, que
daría como dirección para el envío del archivo.
Para entonces, ya era hora de devolver la llamada al operador de la computadora en el Centro de I + D. Harry
tiene él por teléfono y le dijo: "Me acaba de transferir el archivo que te hablé
acerca. ¿Se puede comprobar que lo ha recibido "
Sí, había llegado. Harry le preguntó a tratar de enviarlo, y le dio el
Dirección IP. Se quedó en el teléfono, mientras que el joven hizo la conexión
y comenzó a transmitir el archivo, y que miraba con grandes sonrisas de todo el ambiente como la luz en el disco duro del ordenador del profesor parpadeó y
parpadeó - ocupada recibiendo la descarga.
Harry intercambiaron un par de comentarios con el hombre acerca de cómo tal vez un día ordenadores y periféricos sería más fiable, se lo agradeció y le dijo
adiós.
Los dos copiado el archivo de la máquina del profesor en un par de discos Zip, un
para cada uno de ellos, sólo para que pudieran verlo más tarde, como el robo de una pintura de una
museo que se puede disfrutar, pero no se atreven a mostrar a tus amigos. Excepto,
en este caso, era más como si hubieran tomado un duplicado original de la pintura,
y el museo todavía tenía su propio y original.
Karl luego habló Harry a través de los pasos de quitar el servidor FTP de la
máquina del instructor, y borrar la pista de auditoría para que no hubiera ninguna evidencia de lo que habían hecho - sólo el archivo de robo, a la izquierda, donde podría ser ubicado fácilmente.
Como paso final, se publicó una sección del código fuente en Usenet directamente de
el instructor de la computadora. Sólo una sección, por lo que no haría ningún gran daño
a la empresa, pero dejando huellas claras directamente al instructor. Él
tienen algunas dificultades para explicar que hacer.
Con el análisis de la
A pesar de que tomaron la combinación de una serie de elementos para hacer esta escapada trabajo, no habría tenido éxito sin una comedia de habilidad útil de un recurso de apelación
de simpatía y ayuda: me estoy gritaba por mi jefe, y la gestión es en
los brazos, y así sucesivamente. Eso, combinado con una explicación de cómo señaló el hombre en
el otro extremo del teléfono podría ayudar a resolver el problema, resultó ser un poderosamente convincente en contra. Que trabajaron aquí, y ha trabajado en muchas otras ocasiones.
El segundo elemento crucial: el hombre que entiende el valor del archivo se
pidió que se lo envíe a una dirección dentro de la empresa.
Y la tercera pieza del rompecabezas: El operador de la computadora podía ver que el archivo habían sido transferidos a él desde dentro de la empresa. Eso sólo podía significar - o

por lo que parece - que el hombre que lo envió a él pudo haber enviado a la
destino final, si sólo su conexión de red externa había estado trabajando. ¿Qué
podría estar mal con él para ayudar a cabo mediante el envío de él?
Pero ¿qué pasa con el archivo comprimido le asigna un nombre diferente? Aparentemente
un objeto pequeño, pero importante. El atacante no puede permitirse correr el riesgo
del archivo de llegar con un nombre que lo identifica como el código fuente, o un nombre
relacionado con
el producto. Una solicitud para enviar un archivo con un nombre como que fuera de la empresa
podría haber hecho sonar la alarma. Tener el archivo de re-etiquetado con un nombre inocuo
fue crucial. Como elaborados por los atacantes, el segundo joven no tenía
reparos en enviar el archivo fuera de la empresa, un archivo con un nombre como nuevo
datos, sin dar pista sobre la verdadera naturaleza de la información, no haría
lo sospechoso.
Mitnick MESSGAE
La regla de fondo que cada empleado debe tener bien plantados en su
cerebro: Excepto con la aprobación de la gestión, no la transferencia de archivos a personas no
conozco personalmente, incluso si el destino parece estar dentro de su empresa
red interna.
Por último, te diste cuenta de lo que esta historia está haciendo en un capítulo sobre la industria
espionaje? Si no, aquí está la respuesta: Lo que estos dos estudiantes hicieron como maliciosos
broma podría fácilmente haber sido hecho por un espía industrial, profesional,
tal vez en el pago de un competidor, o quizás en el pago de un gobierno extranjero.
De cualquier manera, el daño podría haber sido devastador para la empresa, severamente
erosionando las ventas de su nuevo producto una vez que el producto de la competencia llegó a
la
del mercado.
¿Cómo podría el mismo tipo de ataque se llevó a cabo en contra de su empresa?
PREVENCIÓN DE LA CON
Espionaje industrial, que ha sido durante mucho tiempo un desafío para las empresas, ha
convertido en el pan y la mantequilla de espías tradicionales que han centrado sus esfuerzos en
obtener secretos de la compañía por un precio, ahora que la Guerra Fría ha terminado. Extranjero
gobiernos y las empresas están utilizando freelance espías industriales para robar
de la información. Las empresas nacionales también contratan a agentes de información que
cruzan la
línea en sus esfuerzos por obtener información de inteligencia competitiva. En muchos casos se
trata
ex espías militares convertidos en agentes de la industria de la información que tiene la
Conocimientos y experiencia para explotar fácilmente las organizaciones, especialmente
aquellos que no han logrado implementar salvaguardias para proteger su información y
educar a su gente.
Seguridad fuera del sitio
Lo que podría haber ayudado a la compañía que iba a tener problemas con su ex situ
instalación de almacenamiento? El peligro podría haberse evitado si la empresa había
ha cifrado sus datos. Sí, el cifrado requiere más tiempo y dinero, pero
vale la pena el esfuerzo. Los archivos cifrados deben ser terreno controlada regularmente para
Asegúrese de que el cifrado / descifrado está funcionando adecuadamente.
Siempre existe el peligro de que las claves de cifrado se pierde o que la única
persona que conoce las claves será atropellado por un autobús. Sin embargo, el nivel de molestia
se puede
reducirse al mínimo, y cualquiera que almacena la información fuera del sitio con un
empresa comercial y no utiliza cifrado, perdón por ser contundente, una
idiota. Es como caminar por la calle en un barrio peligroso, con veinte dólares
facturas que salen de los bolsillos, pregunta, en esencia al ser robado.
Dejando a los medios de comunicación copia de seguridad en la que alguien podría marcharse
con él es un defecto común

en materia de seguridad. Hace varios años, yo trabajaba en una empresa que podría haber hecho mejores esfuerzos para proteger la información del cliente. El personal de la operación que queda de la empresa
las cintas de respaldo fuera de la puerta de la sala de cómputos bloqueado por un mensajero para recoger
todos los días. Cualquiera pudo haber se fue con las cintas de respaldo, que contenía
todos los documentos procesados palabra-de la empresa sin codificar texto. Si los datos de copia de seguridad
encriptada, la pérdida del material es una molestia, si no está encriptada - así, se puede
prever el impacto sobre su empresa mejor que yo.
La necesidad de las empresas más grandes para el almacenamiento fuera del sitio confiable es casi un hecho.
Sin embargo, todos los procedimientos de seguridad deben incluir una investigación de su empresa de almacenamiento de conciencia para ver cómo son por su propia seguridad
políticas y prácticas. Si no son tan dedicados como su propia empresa, todos sus
los esfuerzos de seguridad podría verse afectada.
Las empresas más pequeñas tienen una buena opción alternativa para copia de seguridad: Enviar el nuevo y
cambios en los archivos cada noche a una de las empresas que ofrecen almacenamiento en línea. Nuevo,
es esencial que los datos sean encriptados. De lo contrario, la información está disponible
no sólo a un empleado se inclinó en la empresa de almacenamiento, sino a todos los intrusos informáticos
que puede romper el almacenamiento en línea los sistemas de computación o red de Companys.
Y, por supuesto, al configurar un sistema de encriptación para proteger la seguridad de
los archivos de copia de seguridad, también debe establecer un procedimiento de alta seguridad para el almacenamiento de la
claves de cifrado o las frases de paso que desbloquearlos. Claves secretas utilizadas para cifrar datos deben ser almacenados en una caja fuerte o bóveda. La práctica estándar de la compañía necesita
prever la posibilidad de que el empleado de manejo de estos datos de forma repentina puede salir, morir, o tener otro trabajo. Siempre debe haber al menos dos personas que
conocer el lugar de almacenamiento y los procedimientos de cifrado / descifrado, así como la políticas sobre cómo y cuándo las claves se deben cambiar. Las políticas también deben exigir que las claves de encriptación se cambió inmediatamente después de la salida de cualquier
los empleados que tenían acceso a ellos.
¿Quién es?
El ejemplo de este capítulo de un estafador que utiliza la mancha de encanto para que los empleados
para compartir la información refuerza la importancia de la verificación de la identidad. La solicitar que el código fuente de enviar a un sitio FTP también apunta a la
importancia de conocer su solicitante.
En el capítulo 16 se encuentran las políticas específicas para la verificación de la identidad de cualquier
extraño que se formule una solicitud de información o la solicitud de que algún tipo de acción se tomadas. Hemos hablado de la necesidad de verificación en todo el libro, en
Capítulo 16 que obtendrá detalles de cómo debe hacerse.
Parte 4
Elevar el nivel de
Capítulo 15
Information Awareness de Seguridad y Formación
Un ingeniero social se le ha dado la tarea de obtención de los planes para su
nuevo producto caliente que se estrenará en dos meses.
¿Qué va a detenerlo?
El servidor de seguridad? No.

Dispositivos de autenticación fuerte? No. Los sistemas de detección de intrusos? No. cifrado? No.
Acceso limitado a los números de teléfono de dial-up módems? No.
Nombres en clave para los servidores que hacen que sea difícil para un extraño para determinar qué
servidor podrían contener los planes de producto? No.
La verdad es que no hay tecnología en el mundo que puede impedir que un social ataque de ingeniería.
Seguridad a través de tecnología, capacitación, y
PROCEDIMIENTOS
Empresas que realizan pruebas de seguridad de penetración informe que sus intentos de entrar en un sistema informático de la empresa cliente por métodos de ingeniería social son casi el 100 por ciento de éxito. Las tecnologías de seguridad puede hacer que estos tipos de los ataques más difíciles de sacar a la gente en el proceso de toma de decisiones.
Sin embargo, la única manera realmente eficaz para mitigar la amenaza de la ingeniería social es a través del uso de tecnologías de seguridad combinado con políticas de seguridad que establecer las reglas básicas de comportamiento de los empleados, y la educación y formación adecuadas
para los empleados.
Sólo hay una manera de mantener sus planes de producto seguro y que es por tener un formación, conocimiento, y una fuerza de trabajo de conciencia. Esto implica la formación en el políticas y procedimientos, sino también - y probablemente aún más importante - un curso programa de sensibilización. Algunos expertos recomiendan que el 40 por ciento de una empresa presupuesto general de la seguridad estar dirigida a la concienciación.
El primer paso es hacer que todos en la empresa consciente de que sin escrúpulos existen personas que se utilice el engaño para manipular psicológicamente.
Los empleados deben ser educados acerca de qué información debe ser protegida, y cómo protegerlo. Una vez que la gente tiene una mejor comprensión de cómo se pueden manipulado, se encuentran en una posición mucho mejor para reconocer que un ataque es en marcha.
Concienciación sobre la seguridad también significa educar a todos en la empresa en el compañía de las políticas y procedimientos de seguridad. Como se discutió en el capítulo 17, las políticas
son las reglas necesarias para guiar la conducta de los empleados a proteger la información corporativa
sistemas y la información confidencial.
En este capítulo y el siguiente ofrecen un plan de seguridad que le puede ahorrar de costosos ataques. Si usted no tiene personal capacitado y alerta tras wellthought-procedimientos, no es una cuestión de si, pero cuando se pierde valiosa información a un ingeniero social. No espere a que un ataque a pasar antes de institución de estas políticas: podría ser devastador para su negocio y su el bienestar de los empleados.
ENTENDER cómo los atacantes APROVECHE
LA NATURALEZA HUMANA
Para desarrollar un programa de formación con éxito, usted tiene que entender por qué la gente se
vulnerables a los ataques en el primer lugar. Al identificar estas tendencias en su formación - por ejemplo, al llamar la atención en las discusiones de rol - puede ayudar a sus empleados a entender por qué todos podemos ser manipulados por ingenieros sociales.
La manipulación ha sido estudiado por los científicos sociales, por lo menos cincuenta años. Robert
B. Cialdini, escribiendo en la revista Scientific American (Febrero 2001), resumió este la investigación, la presentación de seis "tendencias básicas de la naturaleza humana" que están involucrados en

un intento de obtener el cumplimiento de una solicitud.
Estas seis tendencias son las que los ingenieros sociales se basan en (consciente o más, a menudo, inconscientemente) en sus intentos de manipular.
Autoridad
La gente tiene una tendencia a respetar en la solicitud se realice por una persona en autoridad. Como se señala en estas páginas, una persona puede estar convencida de que cumplir con una solicitud si él o ella cree que el solicitante es una persona con autoridad o una persona que está autorizado para hacer tal solicitud.
En su libro Influencia, el Dr. Cialdini escribe acerca de un estudio a los tres del medio oeste hospitales en los que las estaciones de enfermeras veintidós por separado "fueron contactados por una persona que llama
que decía ser un médico del hospital, y las instrucciones dadas por la administración de una de medicamentos con receta a un paciente en la sala. Las enfermeras que recibieron estos instrucciones de no conocer la persona que llama. Ni siquiera sabía si estaba realmente un médico (que no lo era). Ellos recibieron las instrucciones para la prescripción por teléfono, que era una violación de la política del hospital. La droga se les dijo que administración no estaba autorizado para su uso en las salas, y la dosis que se les dijo para administrar el doble de la dosis máxima diaria, y por lo tanto podría haber puesto en peligro la vida del paciente. Sin embargo, en el 95 por ciento de los casos, Cialdini informó que "la enfermera procedió a obtener la dosis necesaria de la sala de botiquín y se dirigía a administrar al paciente "antes de ser interceptados por un observador y habló de la experiencia.
Ejemplos de ataques: Un ingeniero social intentos por envuelves en el manto de la autoridad al afirmar que él está con el departamento de TI, o que es un ejecutivo o trabaja para un ejecutivo de la empresa.
Gusto
La gente tiene la tendencia a respetar en la persona que hace la solicitud ha sido capaz de establecerse como agradable, o que tienen intereses similares, creencias y actitudes como la víctima.
Ejemplos de ataques: A través de la conversación, el atacante se las arregla para aprender afición o interés de la víctima, y reivindica un interés y entusiasmo por la misma afición o interés. O se puede pretender ser del mismo estado o en la escuela, o que tienen objetivos similares. La ingeniería social también se tratará de imitar el los comportamientos de su objetivo de crear la apariencia de la semejanza.
Reciprocidad
De manera automática, puede cumplir con una solicitud cuando se nos ha dado o prometió algo de valor. El regalo puede ser un elemento material, o un consejo o ayuda. Cuando alguien ha hecho algo para usted, se siente una inclinación a corresponder. Esta fuerte tendencia a la reciprocidad que existe incluso en situaciones en la persona que recibe el regalo no lo ha pedido. Una de las maneras más eficaces de influir en las personas que nos hacen un "favor" (cumplir con una solicitud) es dar un regalo r la ayuda que se forma la obligación subyacente.
Miembros de la secta religiosa Hare Krishna son muy eficaces para influir la gente a donar a su causa, en primer lugar les da un libro o una flor como regalo. Si el receptor trató de devolver el regalo, el dador se negarían señalando que "es nuestra regalo para ti. "Este principio de reciprocidad de conducta fue utilizada por los Krishnas aumentar sustancialmente las donaciones.
Ejemplos de ataques: Un empleado recibe una llamada de una persona que se identifica sí mismo como del departamento de TI. La persona que llama, explica que algunas empresas los ordenadores han sido infectados con un virus nuevo no reconocidos por el antivirus software que puede destruir todos los archivos en un ordenador, y ofrece a hablar a la persona a través de algunas medidas para evitar problemas. Después de esto, la persona que llama le pide al
persona para probar una utilidad de software que ha sido recientemente actualizado para permitir que

a los usuarios cambiar las contraseñas. El empleado se niega a rechazar, porque la persona que llama
acaba de ayudar, siempre que, supuestamente, proteger al usuario de un virus. Él
retribuye al cumplir con la petición de la persona que llama.

Consistencia

La gente tiene la tendencia a cumplir después de haber hecho un compromiso público o
apoyo para una causa. Una vez que hemos prometido que vamos a hacer algo, no
desea que aparezca poco fiables o no deseables y tienden a seguir a través de
Para ser coherentes con nuestra declaración o promesa.

Ejemplo de ataque: El atacante en contacto con un empleado relativamente nuevo y asesora
la del acuerdo para cumplir con las políticas de seguridad y ciertos procedimientos como
condición de ser permitido el uso de sistemas de información de la empresa. Después de discutir
una serie de prácticas de seguridad unos pocos, la persona que llama le pide al usuario su
contraseña "para verificar
cumplimiento "de la política en la elección de una difícil de adivinar. Una vez que el usuario
revela su contraseña, la persona que llama hace una recomendación a la construcción del futuro
contraseñas de tal manera que el atacante será capaz de adivinar. La víctima
cumple debido a su acuerdo previo para cumplir con políticas de la empresa y su
supuesto de que la persona que llama no es más que la verificación de su cumplimiento.

La validación social

La gente tiene la tendencia a cumplir antes de hacerlo parece estar en línea con
lo que están haciendo. La acción de los demás es aceptada como la validación de que el
comportamiento en cuestión es la acción correcta y apropiada.

Ejemplos de ataques: La persona que llama dice que está realizando una encuesta y otros
nombres
personas en el departamento de quien dice que ya colaboró con él. La
víctima, creyendo que la cooperación de otros valida la autenticidad de la
solicitud, se compromete a participar. La persona que llama se hace una serie de preguntas, entre
que son cuestiones que atraen a la víctima para que revele su nombre de usuario informático
y una contraseña.

Escasez

La gente tiene la tendencia a cumplir cuando se cree que el objeto buscado es
escasos y otros están compitiendo por él, o que sólo está disponible para un
corto período de tiempo.

Ejemplo de ataque: El atacante envía mensajes de correo electrónico afirmando que las primeras
500 personas
para registrarse en el sitio web de la empresa nueva va a ganar entradas gratis para un nuevo
caliente
película. Cuando un empleado desprevenido se registra en el sitio, se le pide que
proporcionar su dirección de correo de la empresa y elegir una contraseña. Muchas personas,
motivado por la conveniencia, tienen la tendencia a utilizar la misma o similar
contraseña en cada sistema informático que utilizan. Aprovechando esto, el
Seguidamente, los intentos de comprometer el trabajo del objetivo y del ordenador personal
sistemas con el nombre de usuario y contraseña que se han introducido en la Web
Sitio proceso de registro.

CREACIÓN DE PROGRAMAS DE FORMACIÓN Y SENSIBILIZACIÓN

Emisión de un folleto de la política de seguridad de la información o dirigir a los empleados a un
intranet página que las políticas de los detalles de seguridad no lo hará, por sí mismo, mitigar el
riesgo.

Todos los negocios no sólo debe definir las normas con las normas escritas, sino que debe
hacer un esfuerzo extra para dirigir todos los que trabajan con información de la empresa o
los sistemas de computadora para aprender y seguir las reglas. Además, debe asegurarse de
que todo el mundo entiende la razón detrás de cada política para que la gente no
eludir la regla como una cuestión de conveniencia. De lo contrario, la ignorancia siempre
se excusa de los trabajadores, y la vulnerabilidad preciso que los ingenieros sociales

explotar.
El objetivo central de cualquier programa de concienciación sobre la seguridad es influir en la gente
cambiar su comportamiento y actitudes de motivar a todos los empleados a querer
chip y que haga su parte para proteger los activos de la organización de la información. Un gran
motivación en este caso es el de explicar cómo su participación no sólo beneficie a
la empresa, pero los empleados individuales. Desde que la compañía mantiene
cierta información privada acerca de todos los trabajadores, cuando los empleados hacen su parte para
proteger la información o los sistemas de información, en realidad son la protección de sus propios
información, también.
Un programa de entrenamiento de seguridad requiere un apoyo sustancial. El esfuerzo de las necesidades de capacitación
para llegar a cada persona que tenga acceso a información sensible o corporativos
sistemas informáticos, debe ser continua, y deben ser revisados continuamente para actualizar
personal sobre las nuevas amenazas y vulnerabilidades. Los empleados deben ver que los altos
gestión está plenamente comprometida con el programa. Ese compromiso debe ser real,
no sólo un sello de goma "Le damos nuestras bendiciones" memo. Y el programa debe
ser respaldado con recursos suficientes para desarrollar, comunicar, prueba de ello, y para
medir el éxito.
Objetivos
La directriz básica que debe tenerse en cuenta durante el desarrollo de un
formación en seguridad y programa de concienciación es que el programa necesita
centrarse en la creación de todos los empleados una conciencia de que su empresa podría estar
bajo ataque en cualquier momento. Tienen que aprender que cada empleado desempeña un papel en
la defensa contra cualquier intento de entrar en los sistemas informáticos o robar a
los datos sensibles.
Debido a que muchos aspectos de la seguridad de la información implica la tecnología, es muy fácil
que los empleados piensen que el problema está siendo manejado por los firewalls y otros
tecnologías de seguridad. Un objetivo primordial de la capacitación debe ser la creación de conciencia en
cada empleado que son la primera línea para proteger la seguridad general de
de la organización.
Capacitación de seguridad debe tener un objetivo mucho mayor que simplemente impartir
reglas. El diseñador del programa de capacitación debe reconocer la fuerte tentación de la
parte de los empleados, bajo la presión de conseguir realizar su trabajo, a pasar por alto o ignorar
las responsabilidades de seguridad. El conocimiento sobre las tácticas de ingeniería social
y la forma de defenderse de los ataques es importante, pero sólo será de valor si
La capacitación está diseñada para enfocarse fuertemente en la motivación de los empleados a usar el
del conocimiento.
La empresa puede contar con el programa en su reunión de abajo a la línea de meta si todo el mundo
completar la formación está totalmente convencido y motivado por una base
idea: que la seguridad de la información es parte de su trabajo.
Los empleados deben llegar a apreciar y aceptar que la amenaza de la social
los ataques de ingeniería es real, y que una importante pérdida de sensibilidad corporativa
información podría poner en peligro la empresa, así como su personal
información y el empleo. En cierto sentido, ser muy cuidadosos acerca de seguridad de la información en
de trabajo es equivalente a no tener cuidado con un PIN del cajero automático o tarjeta de crédito.
Esto puede ser una analogía de peso para la construcción de entusiasmo por las prácticas de

seguridad.
El establecimiento del Programa de Formación y Sensibilización
La persona responsable de diseñar el programa de seguridad de la información tiene que
Reconocemos que esto no es una talla única para todos los proyectos. Por el contrario, las necesidades de formación para
ser desarrollado para satisfacer las necesidades específicas de diferentes grupos dentro de
de la empresa. Aunque muchas de las políticas de seguridad descritas en el capítulo 16 se aplican
a todos los empleados en general, muchos otros son únicos. Como mínimo, la mayoría de los
las empresas necesitan programas de formación adaptados a estos grupos distintos:
administradores; el personal de TI, los usuarios de computadoras, el personal no técnico, administrativo
asistentes, recepcionistas y guardias de seguridad. (Vea el detalle de por
asignación de trabajo en el capítulo 16.)
Ya que el personal de la fuerza de una empresa de seguridad industrial no son habitualmente
espera que sea equipo competente, y, salvo quizás en una forma muy limitada, lo
no entrar en contacto con computadoras de la compañía, que generalmente no se consideran
la hora de diseñar este tipo de formación. Sin embargo, los ingenieros sociales pueden engañar
guardias de seguridad u otros en lo que les permite en un edificio u oficina, o en
realizar una acción que resulta en una intrusión informática. Mientras que los miembros de la
guardia de la fuerza desde luego no tienes la formación completa del personal que maneja o usa
computadoras, sin embargo, no debe pasarse por alto en la conciencia de seguridad
del programa.
En el mundo empresarial hay temas sobre los que probablemente pocos los
los empleados necesitan ser educados que son a la vez tan importante y tan
intrínsecamente aburrida como la seguridad. La mejor información diseñada capacitación en seguridad
los programas deben también informar y captar la atención y el entusiasmo de los
los alumnos.
El objetivo debe ser hacer que la conciencia de seguridad de la información y la formación de un
experiencia divertida e interactiva. Técnicas podrían incluir demostrando
métodos de ingeniería social a través de juegos de rol, la revisión de informes de los medios de
los recientes ataques a otros negocios menos afortunados y discutir las formas de la
las empresas podrían haber evitado la pérdida, o mostrar un video de seguridad que se
entretenido y educativo al mismo tiempo. Hay varios de seguridad
conciencia de que las empresas del mercado de vídeos y otros materiales relacionados.
NOTA
Para las empresas que no tienen los recursos para desarrollar un programa de las instalaciones,
hay varias empresas de formación que ofrecen formación de sensibilización
los servicios. Ferias como Secure Expo Mundial (www.secureworldexpo.com)
son lugares de reunión para estas empresas
Las historias de este libro ofrecen un montón de material para explicar los métodos y
tácticas de ingeniería social, para crear conciencia de la amenaza, y demostrar a los
las vulnerabilidades en el comportamiento humano. Considere el uso de los escenarios de base
para las actividades de juegos de rol. Las historias también ofrecen oportunidades de colores vivos para
discusión sobre cómo las víctimas pudieron haber respondido de manera diferente para evitar la
los ataques de tener éxito.
Un desarrollador de curso de experto y hábil entrenadores encontrarán una gran variedad de desafíos, pero
también un montón de oportunidades, para mantener el tiempo de clase animada, y, en el
proceso, motivar a la gente a formar parte de la solución.
Estructura de la Formación
Un conocimiento básico de seguridad de la formación debe ser desarrollado que todos los
los empleados están obligados a asistir. Los nuevos empleados deben ser obligados a asistir a

la formación como parte de su adoctrinamiento inicial. Recomiendo que ningún empleado se proporcionará acceso a la computadora hasta que haya asistido a una toma de conciencia de seguridad básicas sesión.

Para esta toma de conciencia y la formación inicial, sugiero una sesión se centró lo suficiente como para mantener atención, y lo suficientemente corto que los mensajes importantes que serán recordados. Aunque la cantidad de materia que hay que sin duda justifica ya la formación, el importancia de proporcionar a la sensibilización y motivación, junto con una razonable número de mensajes esenciales en mi opinión es mayor que cualquier noción de medio día o todo el día las sesiones que dejar a la gente adormecida con demasiada información.

El énfasis de estas sesiones debe ser el transporte de una apreciación de la daño que se puede hacer a la empresa y los empleados individualmente, a menos que todos los empleados siguen buenos hábitos de trabajo de seguridad. Más importante que aprender acerca de prácticas específicas de seguridad es la motivación que lleva a los empleados a aceptar la responsabilidad personal de seguridad.

En situaciones en que algunos empleados no fácilmente puede asistir a las sesiones en el aula, el empresa debe considerar el desarrollo de formación sobre sensibilización con otras formas de instrucción, tales como videos, capacitación por computadora, cursos en línea, o por escrito los materiales.

Después de la breve sesión de formación inicial, sesiones más largas deben ser diseñados para educar a los empleados acerca de las vulnerabilidades específicas y técnicas de ataque con respecto a su posición en la empresa. Cursos de actualización se debe exigir al menos una vez un año. La naturaleza de la amenaza y los métodos utilizados para explotar a la gente son siempre cambiantes, por lo que el contenido del programa debe mantenerse al día. Por otra parte, conciencia de la gente y el estado de alerta disminuye con el tiempo, lo que la capacitación se debe repetir a intervalos razonables para reforzar los principios de seguridad. Una vez más el énfasis tiene que ser tanto de mantener a los empleados convencidos de la importancia de políticas de seguridad y motivación para adherirse a ellos, como en la exposición de las amenazas específicas y métodos de ingeniería social.

Los gerentes deben establecer un plazo razonable para sus subordinados para familiarizarse con las políticas y procedimientos de seguridad, y para participar en la toma de conciencia de seguridad del programa. Los empleados no se debe esperar para estudiar las políticas de seguridad o asistir a clases de seguridad en su propio tiempo. Los nuevos empleados deben contar con tiempo suficiente para revisar las políticas de seguridad y publicó las prácticas de seguridad antes de iniciar sus responsabilidades de trabajo.

Los empleados que cambiar de posición dentro de la organización de un trabajo que implica el acceso a la información o los sistemas informáticos que, por supuesto, necesario para completar un programa de entrenamiento de seguridad adaptados a sus nuevas responsabilidades. Por ejemplo, cuando un operador de la computadora se convierte en un sistema administrador, o una recepcionista se convierte en un auxiliar administrativo de formación, las nuevas es necesario.

Contenido del Curso de Capacitación

Cuando se reduce a sus fundamentos, todos los ataques de ingeniería social tienen la misma elemento común: el engaño. La víctima es llevado a creer que el atacante es un

compañero de trabajo o alguna otra persona que está autorizado a acceder sensibles información, o está autorizado para dar las instrucciones de la víctima que implican tomar acciones con un ordenador o equipo de informática. Casi todos estos ataques podrían ser frustrado si el empleado blanco se limita a seguir dos pasos:

Verificar la identidad de la persona que realiza la solicitud: Es la persona que hace la solicitud realmente quien dice ser?

Verificar si la persona está autorizada: ¿La persona tiene la necesidad de conocer, o se le haya autorizado para hacer esta petición?

NOTA

Porque la conciencia de seguridad y formación nunca son perfectos, el uso de seguridad tecnologías siempre que sea posible para crear un sistema de defensa en profundidad. Este significa que la medida de seguridad es proporcionado por la tecnología en lugar de los empleados, por ejemplo, cuando el sistema operativo está configurado para evitar que los empleados de la descarga de software de Internet, o la elección de un corto, fácil de adivinar la contraseña.

Si sesiones de sensibilización formación podría cambiar el comportamiento para que cada empleado siempre sería coherente sobre las pruebas de cualquier solicitud en contra de estos criterios, la riesgos asociados con los ataques de ingeniería social se reduce drásticamente.

Una práctica de seguridad de información de sensibilización y formación del programa que se ocupa de el comportamiento humano y los aspectos de ingeniería social debe incluir lo siguiente:

Una descripción de cómo los atacantes utilizan técnicas de ingeniería social para engañar a la gente.

Los métodos utilizados por los ingenieros sociales para lograr sus objetivos.

¿Cómo reconocer a un posible ataque de ingeniería social.

El procedimiento para la tramitación de una solicitud sospechosa.

Dónde reportar los intentos de ingeniería social o de ataques con éxito.

La importancia de cualquier reto que se presente una solicitud sospechosa, independientemente de la posición de la persona reclamada o importancia.

El hecho de que no implícitamente debe confiar en los demás sin una verificación, a pesar de que su impulso es dar a los demás el beneficio de la duda.

La importancia de verificar la identidad y la autoridad de cualquier persona que haga una solicitud de información o acción. (Consulte la sección "Verificación y Autorización Procedimientos ", Capítulo 16, la manera de verificar la identidad.)

Procedimientos para proteger la información sensible, incluyendo familiaridad con los datos del sistema de clasificación.

La ubicación de las políticas de seguridad de la empresa y los procedimientos, y sus importancia a la protección de la información y sistemas de información corporativos.

Un resumen de las políticas clave de seguridad y una explicación de su significado. Para ejemplo, cada empleado debe recibir instrucciones sobre cómo diseñar una difícil toguess contraseña.

La obligación de todo trabajador a cumplir con las políticas y la consecuencias en caso de incumplimiento.

La ingeniería social, por definición, implica algún tipo de interacción humana. Un atacante con mucha frecuencia utilizan una variedad de métodos de comunicación y tecnologías para tratar de alcanzar su meta. Por esta razón, una wellrounded programa de sensibilización debe tratar de cubrir algunos o todos de los siguientes:

Relacionados con la seguridad en el ordenador y las contraseñas del correo de voz política.

El procedimiento para la divulgación de información sensible o material.

Política de uso de correo electrónico, incluyendo las garantías para evitar los ataques de códigos maliciosos incluyendo virus, gusanos y caballos de Troya.

Los requisitos físicos de seguridad, tales como el uso de una tarjeta de identificación.

La responsabilidad de desafiar a la gente en el local que no está usando un

tarjeta de identificación.
Las mejores prácticas de seguridad de uso de correo de voz.
¿Cómo determinar la clasificación de la información y las salvaguardas apropiadas para proteger la información sensible.
Eliminación adecuada de los documentos confidenciales y los medios informáticos que tienen, o han
en cualquier momento en los últimos contenidos, materiales confidenciales.
Además, si la empresa tiene previsto utilizar las pruebas de penetración para determinar la eficacia de las defensas contra los ataques de ingeniería social, se deberá advertir
da poner a los empleados de la notificación de esta práctica. Que los empleados saben que en un tiempo que puede recibir una llamada de teléfono u otra comunicación con un atacante técnicas como parte de una prueba. Utilizar los resultados de las pruebas no castigar, fresa para definir la necesidad de formación adicional en algunas áreas.
Los detalles relativos a todos los elementos anteriores se encuentran en el Capítulo 16.
PRUEBAS
Su empresa puede querer poner a prueba los empleados en su dominio de la información presentados en las sesiones de concienciación de seguridad, antes de permitir el sistema informático
acceso. Si las pruebas de diseño que ha de darse en la línea, la evaluación de muchos programas de diseño
programas le permiten analizar fácilmente los resultados de prueba para determinar las áreas de la
formación que necesitan ser fortalecidas.
Su empresa también podría considerar la posibilidad de un certificado acreditativo de la finalización de la formación en seguridad como una recompensa y motivación de los empleados.
Como una parte rutinaria de completar el programa, se recomienda que cada empleado deberá firmar un acuerdo para cumplir con las políticas de seguridad y principios que se enseñan en el programa. La investigación sugiere que una persona que hace el el compromiso de la firma de un acuerdo es más probable que hacer un esfuerzo para cumplir con los procedimientos.
CONCIENCIA EN CURSO
La mayoría de las personas son conscientes de que aprender, incluso acerca de cuestiones importantes, tiende a desaparecer
a menos que se refuerce periódicamente. Debido a la importancia de los empleados de mantenimiento
al día sobre el tema de la defensa contra los ataques de ingeniería social, una programa permanente de concienciación es vital.
Un método para mantener la seguridad en la vanguardia del pensamiento es hacer que los empleados
seguridad de la información la responsabilidad de trabajo específico para cada persona en el de la empresa. Esto anima a los empleados a reconocer su papel crucial en la general de seguridad de la empresa. De lo contrario existe una fuerte tendencia a sentir que de seguridad "no es mi trabajo."
Aunque la responsabilidad general de un programa de seguridad de la información es normalmente
asignado a una persona en el departamento de seguridad o la tecnología de la información departamento, el desarrollo de un programa de información acerca de la seguridad es probablemente el mejor estructurado como un proyecto conjunto con el departamento de formación.
El programa permanente de concienciación tiene que ser creativos y utilizar todos los disponibles canal para transmitir mensajes de seguridad de manera que son memorables por lo que los empleados se les recuerda constantemente sobre los hábitos de una buena seguridad. Los métodos deben
utilizar todos los canales tradicionales, además de que muchos no tradicionales como la gente asignado para desarrollar e implementar el programa se pueda imaginar. Como con las

tradicionales
la publicidad, el humor y ayudar a la inteligencia. La variación de la redacción de mensajes mantiene
que se conviertan en tan familiares que se ignoran.
La lista de posibilidades para un programa permanente de concienciación pueden incluir:
Proporcionar copias de este libro a todos los empleados.
Incluidos los elementos de información en el boletín de la empresa: artículos, en caja recordatorios (preferiblemente corta, para llamar la atención los elementos), o dibujos animados, por ejemplo.
Publicar una foto de la Oficina de Seguridad del Mes.
Colgando carteles en las áreas de los empleados.
Publicar avisos en tablón de anuncios.
Proporcionar recintos impresa en sobres sueldo.
El envío de recordatorios por correo electrónico.
Utilización de la seguridad relacionados con los protectores de pantalla.
Difusión de anuncios de seguridad recordatorio a través del sistema de correo de voz.
Impresión de etiquetas de teléfono con mensajes como "¿Es la persona que llama, que dice que es?"!
La creación de mensajes de aviso a aparecer en el equipo al iniciar la sesión, tales como "Si va a enviar información confidencial en un correo electrónico, cifrar".
Incluyendo temas de seguridad como un elemento estándar en los informes de rendimiento de los empleados
y revisiones anuales.
Suministro de avisos de seguridad en la intranet de la conciencia, tal vez utilizando dibujos animados o
humor, o de alguna otra forma atractiva a los empleados a leerlos.
El uso de un tablero de mensajes pantalla electrónica en la cafetería, con una frecuencia cambio de recordatorio de la seguridad.
La distribución de volantes o folletos.
Y pensar trucos, tales como galletas de la fortuna gratis en la cafetería, cada uno que contiene un recordatorio de seguridad en lugar de una fortuna.
La amenaza es constante, los recordatorios debe ser constante también.
¿QUÉ HAY EN TI PARA MÍ? "
Además de los temas de seguridad y programas de capacitación, recomiendo una recompensa activa y bien conocidos del programa. Debes reconocer los empleados que se han detectado y evitado un intento de ataque de ingeniería social, o en alguna otra manera ha contribuido significativamente al éxito de la información programa de seguridad. La existencia del programa de recompensas deben darse a conocer a los empleados en todas las sesiones de concienciación sobre la seguridad, y violaciónes de seguridad debe ser
amplia difusión en toda la organización.
En el otro lado de la moneda, las personas deben ser conscientes de las consecuencias de la no cumplir con las políticas de seguridad de la información, ya sea por descuido o resistencia. A pesar de que todos cometemos errores, repitió violaciónes de seguridad los procedimientos no deben ser toleradas.
Capítulo 16
Recomienda políticas corporativas de seguridad de la información
Nueve de cada diez grandes corporaciones y agencias del gobierno han sido atacados por los intrusos informáticos, a juzgar por los resultados de una encuesta realizada por el FBI y reportó la Associated Press en abril de 2002. Curiosamente, el estudio encontró que sólo una empresa en tres o informa al público reconoció los ataques. Que la reticencia a revelar su victimización hace sentido. Para evitar la pérdida de confianza de los clientes y para prevenir nuevos ataques por intrusos que saber que una empresa puede ser vulnerable, la mayoría de las empresas no informar públicamente de los incidentes de seguridad informática.

Parece que no hay estadísticas sobre los ataques de ingeniería social, y si hay
fueron los números sería muy poco fiable, una empresa que nunca en la mayoría de los casos
sabe cuándo un ingeniero social ha "robado" la información, por lo que muchos ataques van
desapercibido y no declarada.
Contramedidas eficaces se pueden poner en su lugar contra la mayoría de los social
ingeniería de los ataques. Pero la realidad que vamos a enfrentar aquí - a menos que todos en la
empresa
entiende que la seguridad es importante y hace que su negocio para saber
y se adhieren a las políticas de seguridad de una empresa, ataques de ingeniería social se
siempre está presente un grave riesgo para la empresa.
De hecho, con estas mejoras si las armas tecnológicas contra la seguridad
infracciones, el enfoque de ingeniería social para con las personas para acceder a propiedad
información de la empresa o de penetrar en la red de la empresa es casi seguro que
ser significativamente más frecuentes y atractivas para los ladrones de información. Un
espionaje industrial, naturalmente, tratar de lograr su objetivo mediante la
método más fácil y la que implica el menor riesgo de detección. Como una cuestión de
De hecho, una empresa que ha protegido a sus sistemas informáticos y de red
desplegar el estado de las tecnologías más modernas de seguridad a partir de entonces pueden
correr un mayor riesgo
de los atacantes que utilizan estrategias de ingeniería social, los métodos y tácticas para
lograr sus objetivos.
Este capítulo presenta las políticas específicas destinadas a minimizar el riesgo de una empresa
con respecto a los ataques de ingeniería social. Los ataques de las políticas de dirección que se
no se basa estrictamente en la explotación de las vulnerabilidades técnicas. Que involucran el uso
de algunos
tipo de pretexto o artimaña para engañar a un empleado de confianza en el suministro de
información
o la realización de una acción que da acceso al agresor a empresas sensibles
información o en los sistemas informáticos y redes de empresas.
¿QUÉ ES UNA POLÍTICA DE SEGURIDAD?
Las políticas de seguridad son las instrucciones claras que regulen las directrices para los
empleados
comportamiento para salvaguardar la información, y son un elemento fundamental en
el desarrollo de controles eficaces para contrarrestar las amenazas potenciales de seguridad.
Estas políticas
son aún más importantes cuando se trata de prevenir y detectar social
ingeniería de los ataques.
Controles efectivos de seguridad se aplican en la capacitación de empleados con bien
documentado
políticas y procedimientos. Sin embargo, es importante señalar que
las políticas de seguridad, incluso si la religión seguida por todos los empleados, no son
garantizada de prevenir todos los ataques de ingeniería social. Por el contrario, el objetivo
razonable
siempre es para mitigar el riesgo a un nivel aceptable.
Las políticas que aquí se presenta incluye las medidas que, aunque no estrictamente centrado en
temas de ingeniería social, sin embargo, estar aquí porque tienen que ver con
técnicas comúnmente usadas en los ataques de ingeniería social. Por ejemplo, las políticas
sobre la apertura de archivos adjuntos de correo electrónico - que permitía instalar troyano
malicioso
software que permite al atacante tomar el control del ordenador de la víctima - frente a una
método utilizado frecuentemente por los intrusos informáticos.
Pasos para desarrollar un programa de
Un programa de seguridad de la información completa por lo general comienza con un riesgo
evaluación destinada a determinar:
Lo que los activos de información de la empresa necesita para estar protegido?

Lo que existen amenazas específicas contra estos activos?
¿Qué daño causaría a la empresa, si estas amenazas potenciales fueron
se materializan?
El objetivo principal de la evaluación de riesgos es dar prioridad a que los activos de información son
en la necesidad de salvaguardias inmediata, y si las garantías institución será rentable
basado en un análisis costo-beneficio. En pocas palabras, qué activos van a ser
protegidos en primer lugar, y cuánto dinero debe ser gastado para proteger estos activos?
Es esencial que la alta dirección en la compra y apoyar con fuerza la necesidad
de las políticas de seguridad y el desarrollo de un programa de seguridad de la información. Al igual que con cualquier
programa corporativo, si un programa de seguridad tenga éxito, la gerencia debe
hacer algo más que proporcionar un respaldo, debe demostrar un compromiso
con el ejemplo personal. Los empleados deben ser conscientes de que la gestión de fuerza
se suscribe a la creencia de que la seguridad de la información es vital para la empresa
operación, que la protección de información de la empresa de negocios es esencial para la
empresa a permanecer en el negocio, y que el trabajo de cada empleado puede depender de la
éxito del programa.
La persona asignada a proyectos de políticas de seguridad de información debe comprender
que las políticas deben estar escritos en un estilo libre de la jerga técnica y de fácil
entendido por el empleado no técnico. También es importante que el documento
dejar claro por qué es importante la política de cada uno, de lo contrario los empleados pueden hacer caso omiso
algunas políticas, como una pérdida de tiempo. El escritor política debe crear un documento que
presenta las políticas, y un documento separado de procedimientos, políticas, porque
probablemente va a cambiar mucho menos frecuencia que los procedimientos específicos utilizados para
ponerlas en práctica.
Además, el escritor políticas deben ser conscientes de las formas en que la seguridad
tecnologías pueden ser utilizadas para hacer cumplir las buenas prácticas de seguridad de la información. Para
ejemplo, la mayoría de los sistemas operativos permiten a requerir que las contraseñas de usuario
cumplir con ciertas especificaciones, como la longitud. En algunas empresas, una política
los usuarios de la prohibición de los programas de descarga puede ser controlada a través de locales o
configuración de políticas globales en el sistema operativo. Las políticas deben exigir
uso de la tecnología de seguridad cada vez que rentable para eliminar humanos basada en
la toma de decisiones.
Los empleados deben ser advertidos de las consecuencias por no cumplir con
políticas y procedimientos de seguridad. Un conjunto de consecuencias apropiadas por la violación de
las políticas deben ser desarrolladas y ampliamente publicitados. Además, un programa de recompensas
deberían ser creados para los empleados que demuestran las buenas prácticas de seguridad o que
reconocer y reportar un incidente de seguridad. Cuando un empleado es recompensado por
frustrar un fallo de seguridad, debe ser ampliamente difundido en toda la empresa,
por ejemplo, en un artículo en el boletín de la empresa.
Uno de los objetivos de un programa de concienciación sobre la seguridad es para comunicar la importancia de
políticas de seguridad y el daño que puede derivarse del incumplimiento de seguir estas normas.
Dada la naturaleza humana, los empleados, a veces, ignorar o eludir las políticas que
parece injustificada o demasiado tiempo. Se trata de una responsabilidad de la administración
asegurar que los empleados comprendan la importancia de las políticas y se
motivados para cumplir, en lugar de tratarlos como un obstáculo para ser burladas.

Es importante tener en cuenta que las políticas de seguridad de la información no puede ser escrito en piedra.
Como cambian las necesidades empresariales, como las nuevas tecnologías de seguridad llegan al mercado, y como
las vulnerabilidades de seguridad evolucionan, las políticas tienen que ser modificados o completados.
Un proceso de revisión y actualización periódicas se debe poner en su lugar. Hacer que el las políticas corporativas y procedimientos de seguridad disponibles en la intranet corporativa o mantener las políticas de este tipo en una carpeta a disposición del público. Esto aumenta la probabilidad
que tales políticas y procedimientos serán revisados con más frecuencia, y proporciona un método conveniente para que los empleados encontrar rápidamente la respuesta a cualquier seguridad de la información relacionada con la pregunta.
Finalmente, las pruebas de penetración periódicas y evaluaciones de la vulnerabilidad social con métodos de ingeniería y tácticas deben llevarse a cabo para exponer cualquier debilidad en la formación o la falta de adherencia a las políticas y procedimientos. Antes de utilizar cualquier engañosa pruebas de penetración, las tácticas, los empleados deben ser puestos sobre aviso de que
estas pruebas pueden ocurrir de vez en cuando.
Cómo utilizar estas políticas
Las medidas concretas presentadas en este capítulo representan sólo un subconjunto de la las políticas de seguridad de la información que creo que son necesarias para mitigar los riesgos de seguridad.
En consecuencia, las políticas incluidas aquí no debe ser considerado como un lista completa de las políticas de seguridad de la información. Por el contrario, son la base para la construcción de un amplio conjunto de políticas de seguridad adecuadas a la específica necesidades de su empresa.
Escritores de política para una organización tendrá que elegir las políticas que se apropiado basado en el entorno único de su empresa y sus objetivos de negocio.
Cada organización, teniendo distintos requisitos de seguridad sobre la base de negocio necesidades, requisitos legales, la cultura organizacional y los sistemas de información utilizados por la empresa, se llevará a lo que necesita de las políticas presentadas, y omitir el resto.
También hay decisiones que deben tomarse acerca de cómo las políticas estrictas estarán en cada
categoría. Una pequeña empresa ubicada en un centro único en el que la mayoría de los empleados
se conocen entre sí, no tiene que ser mucho más preocupado por llamar a un atacante en el (teléfono y haciéndose pasar por un empleado, aunque, por supuesto, un impostor puede hacerse pasar por un proveedor). Además, a pesar de los mayores riesgos, una empresa enmarcado en una cultura informal, relajado corporativa podría aprobar sólo una subconjunto limitado de las políticas recomendadas para cumplir con sus objetivos de seguridad.
DATOS DE CLASIFICACIÓN
Una política de clasificación de datos es fundamental para la protección de una organización de los activos de información, y establece categorías para que regulan la liberación de la sensibilidad de la información. Esta política proporciona un marco para proteger a las empresas información por lo que todos los empleados saben el nivel de sensibilidad de cada parte de la información.
Que operan sin una política de clasificación de datos - el status quo en casi todos los las empresas de hoy - deja a la mayoría de estas decisiones en manos de cada uno de los trabajadores. Naturalmente, las decisiones de los empleados se basan principalmente en factores subjetivos,
y no en la sensibilidad, la criticidad y el valor de la información. La información es también dio a conocer porque los empleados son ignorantes de la posibilidad de que en la respuesta

a una solicitud de la información, es posible que sea puesta en manos de un atacante.

La política de clasificación de datos establece las directrices para la clasificación de valor información en uno de varios niveles. Con cada elemento que se asigna una clasificación, los empleados pueden seguir una serie de procedimientos de manejo de datos que protegen a la empresa de una fuga accidental o negligente de la información sensible. Estos procedimientos mitigar la posibilidad de que los empleados serán engañados para que revelen sensibles información a personas no autorizadas.

Cada empleado debe estar capacitado en la política de clasificación de datos corporativos, incluyendo a aquellos que no suelen utilizar los ordenadores o las comunicaciones corporativas sistemas. Debido a que todos los miembros de la fuerza laboral corporativa - incluyendo el personal de limpieza, la construcción de los guardias y el personal de copy-habitación, así como consultores, contratistas, e incluso los internos - pueden tener acceso a información sensible, cualquier persona podría ser el blanco de un ataque.

La gerencia debe asignar un propietario a la información será responsable de cualquier información que está actualmente en uso en la empresa. Entre otras cosas, la Información del propietario es responsable de la protección de los activos de información. Normalmente, el propietario decide qué nivel de clasificación para asignar sobre la base de la necesidad de proteger la información, periódicamente vuelve a evaluar el nivel de clasificación asignado, y decide si es necesario algún cambio. El propietario La información puede también delegar la responsabilidad de la protección de los datos a un custodio o persona designada.

Categorías de clasificación. y definiciones

La información debe ser dividido en varios niveles de clasificación en función de su sensibilidad. Una vez que un sistema de clasificación particular se establece, es una cara y proceso que consume tiempo para reclasificar la información en nuevas categorías. En nuestro ejemplo, la política que elegí cuatro niveles de clasificación, lo cual es apropiado para la mayoría de medianas y grandes empresas. Dependiendo del número y tipo de sensibilidad información, las empresas pueden optar por añadir más categorías para un mayor control tipos específicos de información. En las empresas más pequeñas, una clasificación de tres niveles esquema puede ser suficiente. Recuerde - cuanto más compleja sea la clasificación esquema, el gasto más para la organización en la formación de los empleados y la aplicación del sistema.

Confidencial. Esta categoría de información es la más sensible. Confidencial información está destinada para uso exclusivo dentro de la organización. En la mayoría de los casos, sólo debe ser compartida con un número muy limitado de personas con una absoluta necesita saber. La naturaleza de la información confidencial es tal que cualquier la divulgación no autorizada podría afectar seriamente a la compañía, sus accionistas, sus socios comerciales, y / o sus clientes. Elementos de información confidencial generalmente se dividen en las siguientes categorías:

La información relativa a los secretos comerciales, el código fuente propietario, técnico o especificaciones funcionales, o la información del producto que podría ser una ventaja para una competidor.

Comercialización y la información financiera no está disponible al público.

Cualquier otra información que es vital para el funcionamiento de la empresa, tales como el futuro estrategias de negocio.

Privado. Esta categoría incluye información de carácter personal que se pretende para uso exclusivo dentro de la organización. La difusión no autorizada de la soldado información podría afectar seriamente los empleados, o la empresa si se obtienen por cualquier personas no autorizadas (especialmente ingenieros sociales). Elementos de información privada

se incluyen los antecedentes médicos de los empleados, beneficios para la salud, la cuenta bancaria
información, el salario de la historia, o cualquier otra información de identificación personal que se no de dominio público.
NOTA
La categoría de la información interna se denomina a menudo sensible por la seguridad de personal. Tengo que usar interna debido a que el término en sí mismo explica la intented audiencia. He utilizado el término sensible no como una clasificación de seguridad, sino como una método conveniente de referirse a la información confidencial, privada, e internos;
Dicho de otra manera, sensible se refiere a cualquier información de la compañía que no es específicamente como público.
Interno. Esta categoría de la información puedan prestarse libremente a cualquier persona empleados por la organización. Por lo general, la divulgación no autorizada de los internos información no se espera que cause un daño grave a la empresa, su accionistas, sus socios de negocio, sus clientes o sus empleados. Sin embargo, personas hábiles en técnicas de ingeniería social puede utilizar esta información para hacerse pasar como un empleado autorizado, contratista o proveedor para engañar a incautos personal que proporcione información más sensible que resulte en acceso no autorizado a sistemas informáticos corporativos.
Un acuerdo de confidencialidad debe ser firmado antes de la información interna puede ser revelada a terceros, como los empleados de las empresas de proveedores, mano de obra del contratista, empresas asociadas, y así sucesivamente. Internos de información general incluye todo lo utilizado en el curso de la actividad diaria que no debe ser liberado a los de afuera, como como las cartas de organización corporativa, la red de números de acceso telefónico, el sistema interno nombres, los procedimientos de acceso remoto, los códigos de centros de coste, y así sucesivamente.
Pública. Información que hayan sido expresamente designados para el lanzamiento al público. Este tipo de información puede ser distribuido libremente a cualquier persona, como comunicados de prensa, asistencia al cliente de la información de contacto, o folletos de productos. Tenga en cuenta que cualquier información que no esté designada como pública debe ser tratada como confidencial de la información.
Clasificados de datos terminológicos
Con base en su clasificación, los datos deben ser distribuidos a determinadas categorías de personas. Una serie de políticas en este capítulo se refieren a la información que ofrecen a una persona sin verificar. A los efectos de estas políticas, una persona sin verificar se alguien a quien el empleado no conoce personalmente a ser un empleado activo o b de un empleado con el rango adecuado para tener acceso a la información, o que no ha sido avalada por un tercero de confianza.
A los efectos de estas políticas, una persona de confianza es una persona que haya cumplido cara a cara que se conoce a usted como un empleado de la empresa, cliente o consultor de la empresa con el rango adecuado para tener acceso a la información. A Persona de confianza también podría ser un empleado de una empresa que carezcan de una relación con su empresa (por ejemplo, un cliente, proveedor o estratégica socio que ha firmado un acuerdo de confidencialidad).
En tercero dé fe, una persona de confianza proporciona la verificación de una persona empleo o estado, y la autoridad de la persona para solicitar información o una la acción. Tenga en cuenta que en algunos casos, estas políticas requieren que usted verifique que el

Persona de confianza sigue siendo empleado de la compañía antes de responder a una solicitud para obtener información o acción por alguien a quien han avalado.
Una cuenta privilegiada es un equipo o una cuenta de otro tipo que requieran permiso de acceso más allá de la cuenta de usuario básico, como una cuenta de administrador de sistemas.
Los empleados con unas cuentas privilegiadas, por lo general tienen la capacidad de modificar el usuario
privilegios o realizar funciones del sistema.
Un buzón departamental general es un buzón de voz respondió con un genérico
mensaje para el departamento. Como un buzón de correo se utiliza con el fin de proteger los nombres y
extensiones de teléfono de los empleados que trabajan en un departamento en particular.
VERIFICACIÓN y procedimientos de autorización
Los ladrones de información suelen utilizar tácticas engañosas para obtener el acceso o información confidencial de la empresa haciéndose pasar por empleados legítimos, contratistas, proveedores o socios comerciales. Para mantener la información efectiva
de seguridad, un empleado que recibe una solicitud para realizar una acción o proporcionar información confidencial de manera positiva debe identificar la persona que llama y verificar su autoridad
antes de conceder una solicitud.
Los procedimientos recomendados en este capítulo están diseñados para ayudar a un empleado que reciba una solicitud a través de cualquier medio de comunicación, tales como teléfono, correo electrónico o fax para determinar si la solicitud y la persona que lo
que son legítimos.
Las peticiones de una persona de confianza
Una solicitud de información o la acción de una persona de confianza puede requerir:
La verificación de que la compañía emplea activamente o tiene una relación con la
persona en una relación es una condición para el acceso a esta categoría de
de la información. Esto es para evitar que los empleados despedidos, vendedores, contratistas, y otros que ya no están asociados con la empresa de pasar por
personal activo.
Verificación de que la persona tiene una necesidad de saber, y está autorizado a tener acceso a la información o para solicitar la acción.
Las peticiones de una persona sin verificar
Cuando una petición es hecha por una persona sin verificar, una verificación razonable
proceso debe ser implementado para identificar positivamente a la persona que hace la solicitud como
autorizado para recibir la información solicitada, sobre todo cuando la solicitud de
ninguna manera implica computadoras o equipos relacionados con la informática. Este proceso es el
control fundamentales para prevenir con éxito los ataques de ingeniería social: si estos
los procedimientos de verificación se siguen, se reducirá drásticamente el éxito
ataques de ingeniería social.
Es importante que no haga el proceso tan engorroso que es costprohibitive,
o que los empleados lo ignoran.
Tal como se detalla a continuación, el proceso de verificación consiste en tres pasos:
Verificar que la persona es que él o ella dice ser.
Determinar que el solicitante es actualmente empleado o comparte una necesidad de saber relación con la sociedad.
Habiendo determinado que la persona está autorizada para recibir la información específica o llamado a la acción solicitada.
Un paso: Verificación de Identidad
Los pasos recomendados para la verificación se enumeran a continuación con el fin de eficacia - el más alto el número, más eficaz será el método. También
incluido con cada elemento es un statemen.t sobre la debilidad de ese particular
método y la forma en que un ingeniero social puede forzar o evadir la

método para engañar a un empleado.
1. Identificador de llamadas (suponiendo que esta característica se incluye en la compañía telefónica
del sistema). Desde la pantalla del identificador de llamadas, determinar si la llamada es desde el interior
o fuera de la empresa, y que el nombre o número de teléfono que aparece
coincide con la identidad proporcionada por la persona que llama.
Debilidad: La información externa identificador de llamadas puede ser falsificada por cualquier persona con acceso
a un conmutador PBX o teléfono conectado al servicio de telefonía digital.
2. De devolución de llamada. Busque el solicitante en el directorio de la compañía, y volver a llamar a la
extensión de la lista para verificar que therequester es un empleado.
Debilidad: Un atacante con suficientes conocimientos puede llamar el avance de una empresa extensión de modo que, cuando el empleado realiza la llamada de verificación a la lista número de teléfono, la llamada se transfiere al número de teléfono del atacante fuera.
3. Que dé fe. Una persona de confianza que da fe de la identidad del solicitante verifica el solicitante.
Debilidad: Los atacantes con un pretexto con frecuencia capaces de convencer a otra empleado de su identidad, y conseguir que los empleados para responder por ellos.
4. Secreto compartido. Use un secreto a toda la empresa compartida, como apassword o código de diario.
Debilidad. "Si muchas personas saben el secreto compartido, que puede ser fácil para un atacante
para aprender.
5. Empleado Supervisor / Manager. Teléfono del employee'simmediate supervisor y la solicitud de verificación.
Debilidad: Si el solicitante ha proporcionado el número de teléfono para alcanzar al su manager, la persona del empleado alcanza cuando se llama al número que no puede el gerente de reales, pero, de hecho, ser cómplice del atacante.
6. Correo electrónico seguro. Solicitud de un mensaje firmado digitalmente.
Debilidad: Si un atacante ha comprometido equipo de un empleado y instalado un capturador de teclado para obtener la frase del empleado pasar, puede enviar correo electrónico firmado digitalmente que parece estar de parte del empleado.
7. Reconocimiento de voz personal. La persona que recibe la solicitud se ha ocupado de el solicitante (preferiblemente cara a cara), sabe a ciencia cierta que la persona en realidad es una persona de confianza, y es lo suficientemente familiarizado con la persona a la reconocer su voz en el teléfono.
Debilidad: Este es un método bastante seguro, no fácil de eludir por un atacante, pero no sirve de nada si la persona que recibe la solicitud no se ha reunido o hablado con el solicitante.
8. Solución contraseña dinámica. El solicitante autentica a sí mismo mediante el uso de una solución de contraseña dinámicos como una identificación segura.
Debilidad: Para derrotar a este método, el atacante tendría que obtener una de las dispositivos dinámicos contraseña, así como el PIN de acompañamiento de los empleados a que el dispositivo le pertenece, o tendría que engañar a un empleado en lectura de la información en la pantalla del dispositivo y proporcionar el PIN.
9. En la persona con DI. El solicitante se presenta en persona andpresents un empleado tarjeta de identificación u otra identificación adecuada, preferiblemente una identificación con fotografía.
Debilidad: Los atacantes a menudo son capaces de robar una tarjeta de empleado, o crear una falsa
tarjeta de identificación que parece auténtico, sin embargo, los atacantes en general rechazan este enfoque
debido a que aparecen en persona pone al atacante en un riesgo significativo de ser

identificado y detenido.
Segundo paso: Verificación de la Situación Laboral
La amenaza más grande de información de seguridad no es de los profesionales sociales
ingeniero, ni de que el intruso informático especializado, sino de alguien mucho más cercano:
el empleado recién despedido en busca de venganza o con la esperanza de erigirse en los
negocios
utilizando la información robada de la empresa. (Tenga en cuenta que una versión de este
procedimiento
También se puede utilizar para verificar que alguien todavía disfruta de otro tipo de negocio
relación con su compañía, como un vendedor, consultor, o un contrato
de los trabajadores.)
Antes de proporcionar información confidencial a otra persona o aceptar
instrucciones para acciones de la computadora o equipo de informática,
verificar que el solicitante sigue siendo un empleado actual utilizando uno de estos métodos:
Directorio de empleados Check. Si la empresa mantiene un empleado en línea
directorio que refleje con precisión los empleados en activo, compruebe que el solicitante es
sigue apareciendo.
Solicitante de verificación de Manager. Llame al administrador de la solicitante, utilizando un
teléfono
número que aparece en el directorio de la empresa, no un número proporcionado por el
solicitante.
Solicitante o el Departamento de Verificación de grupo de trabajo. Llame a la del solicitante
departamento o grupo de trabajo y determinar a nadie en ese departamento o
grupo de trabajo que el solicitante sigue siendo empleado de la empresa.
Tercer paso: Verificación de la Necesidad de saber
Más allá de la verificación de que el solicitante es un empleado actual o tiene una relación
con su compañía, todavía queda la cuestión de si el solicitante es
autorizadas a tener acceso a la información que se solicita, ni está autorizado para
solicitud de que las acciones específicas que afectan a los ordenadores o equipos relacionados
con la informática
tomar.
Esta determinación se podrá hacer mediante el uso de uno de estos métodos:
Consulte puesto de trabajo / grupo de trabajo / listas de responsabilidades. Una empresa puede
proporcionar listas
el acceso a la información de autorización de publicación de listas de empleados que son
derecho a la información. Estas listas pueden ser organizadas en términos de empleados
título del trabajo, los departamentos de los empleados y grupos de trabajo, las responsabilidades
de los empleados, o por
alguna combinación de estos. Las listas de este tipo tendría que mantenerse en línea que se
mantener actualizada y proporcionar un acceso rápido a información de autorización. Por lo
general,
Propietarios sería responsable de supervisar la creación y
mantenimiento de las listas de acceso a la información bajo control del propietario.
NOTA
Es importante señalar que el mantenimiento de estas listas es una invitación a los interlocutores
sociales
ingeniero. Considere lo siguiente: Si un atacante se dirige a una empresa se da cuenta de que el
compañía mantiene esas listas, hay una fuerte motivación para obtener uno. Una vez en
mano, como una lista abre muchas puertas para el atacante y coloca a la empresa en
grave riesgo.
Obtener la autorización de un administrador. Un empleado contacta con su propio
gerente o el director de la solicitante, la autoridad para cumplir con los
solicitud.
Obtener autorización del propietario de Información o su designado. La información
El propietario es el último juez de si una persona en particular debe concederse

acceso. El proceso de control de acceso basado en computadora es para que el empleado
póngase en contacto con su superior inmediato para aprobar una solicitud de acceso a
información basada en los perfiles de los puestos existentes. Si un perfil no existe, es el
la responsabilidad del gerente en contacto con el titular de los datos relevantes para el permiso. Este
cadena de mando se deben seguir para que los dueños de la información no se
bombardeados con peticiones cuando hay una necesidad frecuente de saber.
Obtener autoridad por medio de un paquete de software de propiedad. Para una gran
empresa en una industria altamente competitiva, puede ser práctico para desarrollar un
paquete de software propietario que cubre las necesidades de saber autorización. Tal
base de datos almacena los nombres de los empleados y los privilegios de acceso a información clasificada.
Los usuarios no sería capaz de buscar los derechos de cada individuo el acceso, sino que
entraría en el nombre del solicitante, y el identificador asociado con la
información que se busca. Entonces, el programa ofrece una respuesta que indica
si el empleado está autorizado a acceder a dicha información. Este
alternativo evita el peligro de crear una lista del personal con acceso respectivos
los derechos a la información valiosa, crítica o sensible que podría ser robado.
POLÍTICAS DE GESTIÓN
Las siguientes políticas se refieren a los empleados de nivel gerencial. Estos son
dividido en las áreas de clasificación de datos, divulgación de información, Teléfono
Administración y Políticas Varios. Tenga en cuenta que cada categoría de las políticas de
utiliza una estructura de numeración única para facilitar la identificación de las pólizas individuales.
Políticas de clasificación de datos
Clasificación de datos se refiere a cómo su empresa califica la sensibilidad de
la información y quién debe tener acceso a esa información.
1.1 Asignación de clasificación de datos
Política: Toda la información valiosa del negocio, sensibles o críticos se debe asignar
a una categoría de clasificación por el propietario de Información designado o delegado.
Explicación / Notas: El propietario o un delegado designado asignará la correspondiente
los datos de clasificación de la información utilizan habitualmente para llevar a cabo negocios
metas. El propietario también controla quién puede acceder a dicha información y el uso de lo que
puede hacerse de él. El propietario de la información puede reasignar la clasificación
y podrá designar un período de tiempo para la desclasificación automática.
Cualquier elemento de otro modo no marcado deben ser clasificados como sensibles.
2.1 Publicar los procedimientos de manejo de clasificados
Política: La empresa debe establecer los procedimientos que rigen la liberación de
información en cada categoría.
Explicación / Notes. "Una vez que las clasificaciones se establecen los procedimientos para la liberación
de información a los empleados y para los forasteros deben establecer, como se detalla en el
Procedimientos de verificación y autorización descritos anteriormente en este capítulo.
Etiqueta todos los artículos 1.3
La política ". Detalle claramente los objetos tanto materiales impresos y de medios de almacenamiento que contiene
Información confidencial, privada o interna para mostrar los datos adecuados
clasificación.
Explicación / Notes. "Documentos en papel debe tener una hoja de cubierta, con una
clasificación de la etiqueta en lugar destacado, y una etiqueta de clasificación en cada
página que es visible cuando el documento está abierto.
Todos los archivos electrónicos que no pueden ser etiquetados con los datos adecuados
clasificaciones (base de datos o archivos de datos) deben ser protegidos a través de controles de acceso
para asegurar que dicha información no se divulguen indebidamente, y que no se puede

cambiado, destruidos o inaccesibles.
Todos los soportes informáticos, como disquetes, cintas y CD-ROM deben estar etiquetados con la clasificación más alta de toda la información contenida en él.
Divulgación de información
Divulgación de información implica la liberación de información a las distintas partes sobre la base de su identidad y su necesidad de saber.
2-1 Empleados procedimiento de verificación
Política: La empresa debe establecer procedimientos generales que se utilizados por los empleados para verificar la identidad, situación laboral, y autorización de una persona antes de soltar confidencial o sensible información o realizar cualquier tarea que implica el uso de cualquier hardware o software.
Explicación / Notas: Cuando esté justificado por el tamaño de la empresa y las necesidades de seguridad,
avanzadas tecnologías de seguridad se debe utilizar para autenticar la identidad. Lo mejor práctica de seguridad sería la de desplegar los tokens de autenticación en combinación con un secreto compartido para identificar positivamente a las personas que hacen peticiones. Si bien esta práctica
sustancialmente minimizar el riesgo, el costo puede ser prohibitivo para algunos las empresas. En estas circunstancias, la empresa debe utilizar una empresa en todo el secreto compartido, como una contraseña o el código de todos los días.
02.02 Entrega de información a terceros
Política: Un conjunto de procedimientos recomendados para la divulgación de información debe estar disponible y todos los empleados deben ser entrenados para seguir.
Explicación / Notas: Por lo general, los procedimientos de distribución deben ser establecidos para:
Información puesta a disposición dentro de la empresa.
Distribución de información a las personas y empleados de organizaciones que han una relación establecida con la empresa, tales como consultores, temporales los trabajadores, los internos, los empleados de las organizaciones que tienen una relación de proveedores o
acuerdo de asociación estratégica con la empresa, y así sucesivamente.
Información disponible fuera de la empresa.
Información en cada nivel de clasificación, cuando la información se entrega en persona, por teléfono, por correo electrónico, por fax, por correo de voz, por el servicio postal, por el servicio de firma de entrega, y por transferencia electrónica.
2.3 La distribución de información confidencial
Política: La información confidencial, que es información de la compañía que podrían hacer que daño sustancial si se obtiene por personas no autorizadas, pueden ser entregados sólo a un De confianza persona autorizada para recibirla.
Explicación / Notas: La información confidencial en una forma física (es decir, impresos copia o en un medio de almacenamiento extraíble) puede ser entregado:
En persona.
Por correo interno, cerrado y marcado con la clasificación de confidencial.
Fuera de la empresa por un servicio de entrega de reconocido prestigio (es decir, FedEx, UPS, etc
sobre) con la firma del destinatario es necesario, o por un servicio postal mediante un certificado o registrado clase de correo.
La información confidencial en forma electrónica (archivos de computadora, archivos de bases de datos, correo electrónico)
pueden ser entregados:
En el cuerpo del correo electrónico cifrado.
Por adjunto de correo electrónico, como un archivo encriptado.
Mediante transferencia electrónica a un servidor dentro de la red interna de la empresa.
Por un programa de fax desde un ordenador, a condición de que sólo el destinatario utiliza

la máquina de destino, o que el destinatario está esperando en el destino
máquina, mientras que el fax se ha enviado. Como alternativa, se pueden enviar faxes
sin la presencia del destinatario si envían a través de un enlace telefónico cifrado a un
protegido por contraseña del servidor de fax.
La información confidencial puede ser discutido en persona, por teléfono en el
empresa, por teléfono fuera de la compañía si están cifrados, encriptados por satélite
transmisión, mediante un enlace de videoconferencia codificados y encriptados por voz Más
Protocolo de Internet (VoIP).
Para la transmisión por fax, el método recomendado para las llamadas para el remitente
para transmitir una página de portada, y el receptor, al recibir la página, transmite una página en
respuesta, lo que demuestra que él / ella está en la máquina de fax. El remitente
transmite el fax.
Los siguientes medios de comunicación no son aceptables para la discusión o
distribución de información confidencial: sin encriptar mensajes de correo electrónico, correo de
voz,
correo ordinario, o cualquier otro método de comunicación inalámbrica (celulares mensaje, corto
Servicio, o inalámbrico).
2.4 La distribución de la información privada
Política: La información privada, que es la información personal de un empleado o
los empleados que, si se revela, se podría utilizar para dañar los empleados o la empresa,
pueden ser entregados sólo a una persona de confianza que está autorizado para recibirla.
Explicación / Notas: La información privada en una forma física (es decir, en papel o
datos en un medio de almacenamiento extraíble) puede ser entregado:
En persona
Por correo interno, cerrado y marcado con la clasificación privado
Por correo ordinario
Información privada en formato electrónico (archivos de computadora, archivos de bases de
datos, correo electrónico) puede
ser entregados:
Por correo electrónico interno.
Mediante transferencia electrónica a un servidor dentro de la red interna de la empresa.
Por fax, siempre que sólo el destinatario utiliza el destino
máquina, o que el destinatario está esperando en la máquina de destino, mientras que
el fax se ha enviado. Facsímiles también se pueden enviar a fax protegido por contraseña
servidores. Como alternativa, se pueden enviar faxes sin la presencia del destinatario si
enviados a través de un enlace telefónico cifrado a un servidor de fax protegido por contraseña.
Información privada puede ser discutido en persona, por teléfono, vía satélite
transmisión, mediante un enlace de videoconferencia, y por el ratón de cifrado
Los siguientes medios de comunicación no son aceptables para la discusión o
distribución de información privada: no cifrado de correo electrónico, mensaje de voz, regular
mail, y por cualquier método de comunicación inalámbrica (móvil, SMS, o inalámbrico).
2.5 La distribución de la información interna
Política: La información interna es la información sea compartida sólo dentro de la empresa
o con otras personas de confianza que han firmado un acuerdo de confidencialidad. Usted
debe establecer los lineamientos para la distribución de información interna.
Explicación / Notas: La información interna se puede distribuir de cualquier forma,
incluido el correo electrónico interno, pero no puede ser distribuida fuera de la empresa en el
correo electrónico
forma, a menos encriptada.
6.2 Discutir la información sensible a través del teléfono
Política: Antes de publicar cualquier información que no ha sido designada como pública por la
teléfono, la persona que la liberación de dicha información personal debe reconocer la
solicitante de voz a través del contacto de negocio antes, o el sistema de la compañía telefónica
debe identificar la llamada como de un número de teléfono interno que ha sido
asignado al solicitante.

Explicación / Notas: Si la voz de que el solicitante no se conoce, llame a la solicitante número de teléfono interno para verificar la voz solicitante a través de un correo de voz grabados mensaje, o el gerente de la solicitante de verificar la identidad del solicitante y la necesidad a saber.

2-7 Lobby o los procedimientos de personal de recepción

Política: El personal de recepción deberá obtener una identificación con foto antes de divulgar cualquier paquete a cualquier persona que no es conocido por ser un empleado activo. Un registro debe se mantendrá para el registro de nombre de la persona, el número de licencia de conducir, fecha de nacimiento, el elemento recogido, y la fecha y hora de recogida tal.

Explicación / Notas: Esta política se aplica también a la entrega de paquetes de salida a cualquier mensajero o servicio de mensajería como FedEx, UPS, o Airborne Express. Estas empresas emiten tarjetas de identificación que pueden ser utilizados para verificar los empleados identidad.

8.2 Transferencia de software a terceros

Política: Antes de la transferencia o divulgación de cualquier software, programa o equipo instrucciones, la identidad del solicitante debe ser verificada de manera positiva, y se debe establecer si dicha divulgación es coherente con la clasificación de datos asignado a dicha información. Por lo general, el software desarrollado in-house en el código fuente se considera de gran formato propietario, y clasificada como confidencial.

Explicación / Notas: Determinación de la autorización es por lo general en función de si el solicitante debe tener acceso al software a hacer su trabajo.

9.2 Ventas y marketing de calificación de los clientes lleva

Política: personal de ventas y marketing deben calificar lleva antes de la liberación números internos de devolución de llamada, planes de productos, contactos grupo de productos, o de otro tipo Información confidencial a cualquier cliente potencial.

Explicación / Notas: Se trata de una táctica común para los espías industriales en contacto con las ventas y representante de marketing y hacerle creer que una compra grande puede estar en el perspectiva. En un esfuerzo por aprovechar las oportunidades de ventas, ventas y marketing repeticiones a menudo compartir la información que puede ser usado por el atacante como una ficha de póquer de obtener acceso a información sensible.

10.2 Transferencia de archivos o datos

Política: Los archivos u otros datos electrónicos no deben ser transferidos a cualquier extraíble los medios de comunicación a menos que el solicitante es una persona de confianza, cuya identidad ha sido verificada y que tiene una necesidad de contar con tales datos en ese formato.

Explicación / Notas: Un ingeniero social puede engañar a un empleado, proporcionando una solicitud plausible por haber copiado información confidencial en una cinta, disco Zip, o otros medios extraíbles, y obrar en lugar en el vestíbulo para su recogida.

Administración Teléfono

Las políticas de Administración Teléfono asegurar que los empleados pueden verificar la identidad del llamante, y proteger su propia información de contacto de los que piden a la empresa.

Desvío de llamadas 3-1 en el dial-up o números de fax

Política: Los servicios Desvío de llamadas que permiten el reenvío de llamadas externas a números de teléfono no se puede colocar en cualquier módem o teléfono fax números dentro de la empresa.

Explicación / Notas: los atacantes sofisticados pueden tratar de engañar a teléfono personal de la empresa o los trabajadores internos de las telecomunicaciones en el reenvío de

números internos
a una línea telefónica externa bajo el control de un atacante. Este ataque permite a los intrusos para interceptar faxes, solicitar información confidencial a enviar por fax dentro de la empresa (personal de asumir que el fax de la organización deben ser seguros) o engañar a usuarios de acceso telefónico para que proporcionen sus contraseñas de cuenta mediante el envío de la
líneas dial-up a un equipo trampa que simula el proceso de inicio de sesión.
Dependiendo del servicio telefónico utilizado dentro de la empresa, el desvío de llamadas característica puede ser bajo el control del proveedor de comunicaciones, en lugar de la Departamento de Telecomunicaciones. En tales circunstancias, la solicitud se hará a el proveedor de comunicaciones para asegurar la función de desvío de llamadas no está presente en los números de teléfono asignados a dial-up y las líneas de fax.
2.3 Identificador de Llamadas
Política: El sistema telefónico corporativo deben aportar identificación de llamadas (Identificador de llamadas) en todos los teléfonos internos, y, si es posible, habilitar distintivo sonar para indicar cuando una llamada es desde fuera de la empresa.
Explicación / Notas: Si los empleados pueden verificar la identidad de las llamadas telefónicas de fuera de la empresa que les puede ayudar a prevenir un ataque, o identificar al atacante al personal de seguridad apropiados.
3.3 teléfonos de cortesía
Política: Para evitar que los visitantes pasar por trabajadores de la empresa, todos los teléfono de cortesía deberá indicar claramente la ubicación de la persona que llama (por ejemplo, "Lobby") en la identificación de llamada del destinatario.
Explicación / Notes. "Si el identificador de llamadas para las llamadas internas se muestra el número de extensión
sólo, la prestación que corresponda deberá hacerse para llamadas realizadas desde teléfonos de la compañía
en la zona de recepción y las áreas públicas. No debe ser posible para un atacante para realizar una llamada de uno de estos teléfonos y engañar a un empleado en la creencia de que la llamada ha sido colocado internamente de un teléfono de los empleados.
3-4 contraseñas por defecto del fabricante suministra con los sistemas de telefonía
Política: El administrador de correo de voz debe cambiar todas las contraseñas predeterminadas que
se suministra con el sistema de teléfono antes de su uso por personal de la empresa.
Explicación / Notas: Los ingenieros sociales pueden obtener listas de contraseñas por defecto de los fabricantes y los utilicen para acceder a las cuentas de administrador.
5.3 Departamento de buzones de voz
La política. "Configurar un buzón de voz genérica para todos los departamentos que normalmente tiene
contacto con el público.
Explicación / Notas: El primer paso de la ingeniería social consiste en la recolección información sobre la empresa objetivo y su personal. Al limitar el accesibilidad de los nombres y números de teléfono de los empleados, una empresa hace más difícil para la ingeniería social para identificar los objetivos de la empresa, o nombres de los empleados legítimos para su uso en engañar a otros miembros del personal.
3.6 Verificación de proveedor del sistema telefónico
Política: No los técnicos de soporte del proveedor se le permitirá acceder de forma remota el compañía del sistema de teléfono sin la identificación positiva de los proveedores y autorización para efectuar dicho trabajo.
Explicación / Notas: los intrusos informáticos que tener acceso a telefonía corporativa los sistemas de aumento de la capacidad de crear los buzones de voz, interceptar mensajes destinados
para otros usuarios, o hacer llamadas telefónicas gratis a costa de la corporación.
7.3 Configuración del sistema telefónico

La política. "El administrador de correo de voz cumplir los requisitos de seguridad
configurar los parámetros de seguridad adecuadas en el sistema telefónico.
Explicación / Notas: Sistemas de teléfono se puede configurar con mayor o menor grado de
de seguridad para mensajes de correo de voz. El administrador debe estar al tanto de la empresa
problemas de seguridad, y trabajar con el personal de seguridad para configurar el teléfono
sistema de protección de datos confidenciales.
8.3 Convocatoria característica de traza
Política: Dependiendo de las limitaciones del proveedor de comunicaciones, el seguimiento de
llamadas
característica se activará a nivel mundial para permitir a los empleados para activar la trampa y
rastreo
función cuando la persona que llama es sospechoso de ser un intruso.
Explicación / Notas: Los empleados deben ser entrenados en el uso de llamadas de seguimiento y
el
las circunstancias apropiadas, cuando debería ser utilizado. Un rastreo de llamadas se debe
iniciar
cuando la persona está claramente tratando de obtener acceso no autorizado a las empresas
sistemas informáticos o solicitando información confidencial. Siempre que un empleado
activa la función de rastreo de llamadas, notificación inmediata debe ser enviada a los incidentes
Informes del Grupo.
3.9 sistemas telefónicos automatizados
La política. "Si la empresa utiliza un sistema telefónico automatizado responder, el sistema
debe ser programado de tal manera que las extensiones de teléfono no se anuncian cuando
transferir una llamada a un empleado o departamento.
Explicación / Notas: Los atacantes pueden utilizar el sistema de una compañía telefónica
automatizada
para asignar nombres de los empleados de las extensiones telefónicas. Atacantes pueden utilizar
conocimiento de las extensiones para convencer a los destinatarios que se llame a los empleados
con derecho a la información privilegiada.
30-10 Buzones de voz para convertirse en discapacitados después de acceso no válido sucesivas
los intentos de
Política: El programa del sistema de telefonía corporativa para bloquear cualquier correo de voz
cuenta cada vez que un número determinado de sucesivos intentos de acceso no válidos
han hecho.
Explicación / Notes. "El administrador de telecomunicaciones deben bloquear un
buzón de voz después de cinco intentos consecutivos no válidos para entrar, el administrador
entonces debe restablecer los bloqueos de correo de voz de forma manual.
03/11 extensiones de teléfono restringido
La política. "Todas las extensiones telefónicas internas a los departamentos o grupos de trabajo
que
normalmente no recibe llamadas de personas externas (help desk, sala de informática,
apoyo de los empleados técnicos, etc) debe ser programado de tal manera que estos
teléfonos sólo se puede llegar desde las extensiones internas. Alternativamente, pueden ser
protegido por contraseña para que los empleados y otras personas autorizadas llama desde
el exterior debe introducir la contraseña correcta.
Explicación / Notas: Aunque el uso de esta política se bloqueará la mayoría de los intentos de los
aficionados
ingenieros sociales para alcanzar sus objetivos probable, cabe señalar que una determinada
atacante a veces se puede hablar de un empleado en llamar a la restringida
extensión y pidiendo a la persona que contesta el teléfono para llamar al atacante, o
simplemente conferencia en la extensión restringida. Durante el entrenamiento de seguridad, este
método de engañar a los empleados en ayudar a que el intruso debe ser discutido a
aumentar la concienciación de los empleados sobre estas tácticas.
Misceláneo
4-1 Empleados diseño de la insignia

Política: tarjetas de los empleados debe ser diseñado para incluir una foto de gran tamaño que pueden ser
reconocida desde la distancia.
Explicación / Notas: La fotografía en las tarjetas de identificación corporativa de diseño estándar, por razones de seguridad, sólo ligeramente mejor que nada. La distancia entre un
persona en el edificio y el protector o el recepcionista, que tiene la
la responsabilidad de verificar la identificación suele ser tan grande que la imagen es demasiado pequeña como para reconocer cuando la persona pasa por allí. Para que la foto sea de valor en
esta situación, un nuevo diseño de la insignia es necesario.
2.4 Los derechos de acceso revisión al cambiar de posición o de responsabilidades
Política: Siempre que un empleado de la compañía cambia de posición o se da un aumento o disminución de las responsabilidades del trabajo, el gerente del empleado se le notificará la cambio en las responsabilidades del empleado a fin de que el perfil de seguridad adecuado pueden ser asignados.
Explicación / Notas: Gestión de los derechos de acceso del personal es necesario
limitar la divulgación de información protegida. La regla de los privilegios mínimos se
aplicar: Los derechos de acceso asignados a los usuarios será el mínimo necesario para realizar sus trabajos. Cualquier petición de cambios que se traducen en derechos de acceso elevado
debe estar de acuerdo con una política de concesión de los derechos de acceso elevado. Director del trabajador o el departamento de recursos humanos tendrán la
responsabilidad de notificar al departamento de tecnología de la información adecuada para ajustar los derechos del titular de la cuenta de acceso, según sea necesario.
4.3 especial de identificación para los empleados que no
Política: Su empresa debe emitir una tarjeta de identificación especial para fotos empresa de confianza
gente de la entrega y no empleados que tienen una necesidad comercial para entrar en la empresa
locales sobre una base regular.
Explicación / Notas: los empleados que necesitan para no entrar en el edificio con regularidad (por ejemplo, para hacer las entregas de alimentos o bebidas en la cafetería, o reparación de fotocopiadoras o hacer instalaciones de teléfono) pueden representar una amenaza para su
de la empresa. Además de emitir la identificación de estos visitantes, asegúrese de que su empleados están capacitados para detectar un visitante sin una tarjeta de identificación y saber cómo actuar en
esa situación.
4.4 Desactivación de cuentas de equipo para contratistas
Política: Siempre que un contratista que se ha emitido una cuenta de equipo
ha completado su asignación, o cuando expire el contrato, el
gerente responsable notificará de inmediato a la tecnología de la información
departamento de deshabilitar su cuenta del contratista equipo, incluyendo las cuentas utilizados para el acceso de base de datos, dial-up o acceso a Internet desde lugares remotos.
Explicación / Notas: W-hen el empleo de un trabajador se termina, hay un
peligro de que él o ella va a utilizar el conocimiento de los sistemas de su empresa y procedimientos para acceder a los datos. Todas las cuentas de equipo utilizado por o se sabe que la
trabajador debe ser prontamente con discapacidad. Esto incluye las cuentas que proporcionan el acceso a
bases de datos de producción, marcación remota de cuentas, y todas las cuentas utilizadas para acceder a
dispositivos relacionados con la informática.
Incidente 4-5 la organización informante
Política: Una organización de notificación de incidentes deben ser establecidos o, en menor empresas, una notificación de incidentes persona y designado de respaldo, por

recepción y distribución de las descripciones relativas a los posibles incidentes de seguridad en progreso.
Explicación / Notas: Al centralizar la información sobre incidentes de seguridad sospechosos, un ataque que de otra manera han pasado desapercibidos puede ser detectado. En el caso de los ataques sistemáticos a través de la organización son detectados y notificados, la organización de notificación de incidentes pueden ser capaces de determinar lo que el atacante es
orientación para que los esfuerzos especiales se pueden hacer para proteger esos activos. Los empleados asignados a recibir reportes de incidentes deben familiarizarse con social métodos de ingeniería y tácticas, lo que les permite evaluar a los informes y reconocer cuando un ataque puede ser en curso.
6.4 Notificación de incidentes línea directa
Política: Una línea telefónica directa para la organización de notificación de incidentes o de la persona, lo que puede
consistirá en una fácil de recordar, extensión telefónica, debe ser establecido.
Explicación / Notas: Cuando los empleados sospechan que son el blanco de una social ataque de ingeniería, que debe ser capaz de notificar inmediatamente a la notificación de incidentes
la organización. Para que la notificación sea oportuna, toda la compañía telefónica operadores y recepcionistas deben tener el número publicado o inmediatamente disponibles para ellos.
Un sistema en toda la empresa de alerta temprana puede ayudar sustancialmente a la organización en
detectar y responder a un ataque en curso. Los empleados deben ser lo suficientemente bien capacitado que alguien que sospeche que ha sido objeto de un entorno social ataque de ingeniería de inmediato llame a la línea directa para reportar los incidentes. En acuerdo con los procedimientos publicados, el personal de la notificación de incidentes se notificar inmediatamente a los grupos de destinatarios que una intrusión pueden estar en curso para
personal estará en alerta. Para que la notificación sea oportuna, la información número de la línea debe estar ampliamente distribuida en toda la empresa.
4.7 Las zonas sensibles deben ser asegurados
Política: Un guardia de seguridad se proyectará el acceso a zonas sensibles o de seguro y debe requieren dos formas de autenticación.
Explicación / Notas: Una de las formas aceptables de autenticación utiliza una cámara digital cerradura electrónica que requiere que un empleado pase su credencial de empleado e introduzca un código de acceso. El mejor método para proteger áreas sensibles es el envío de una garantía guardia que observa una entrada de acceso controlado. En las organizaciones donde este se no rentables, dos formas de autenticación que se utilizará para validar su identidad. Según el riesgo y costo, una tarjeta de acceso biométrico-habilitado es recomendado.
8.4 Red y armarios de teléfono
Política: armarios, closets, habitaciones o que contiene el cableado de red, cableado telefónico, o puntos de acceso a la red debe estar asegurada en todo momento.
Explicación / Notas: Sólo el personal autorizado se permitirá
el acceso a cabinas telefónicas y de red, habitaciones o armarios. Todo exterior personal de mantenimiento o personal de proveedores deben ser identificados con el los procedimientos publicados por el departamento responsable de la seguridad de la información. Acceso a líneas telefónicas, concentradores de red, conmutadores, puentes, o relacionados con otros
equipo podría ser utilizado por un atacante comprometer la computadora y la red la seguridad.
4-9 cubos de correo electrónico dentro de una misma
Política: contenedores dentro de una misma electrónico no deben estar ubicados en áreas de acceso público.
Explicación / Notas: los espías industriales o intrusos informáticos que han

el acceso a los puntos de recogida dentro de la compañía de correo puede enviar fácilmente falsificados
cartas de autorización o de forma interna que autorizar al personal para liberar
La información confidencial o realizar. Una acción que ayuda a que el atacante.
Además, el atacante puede enviar por correo un disquete o en medios electrónicos con instrucciones para instalar una actualización de software, o abrir un archivo que se ha incorporado macro
comandos que sirven a los objetivos del intruso. Naturalmente, cualquier solicitud recibida por mail dentro de la compañía se supone que es auténtica por la persona que lo recibe.
10.04 El tablón de anuncios de la empresa
Política: Los tablones de anuncios en beneficio de los trabajadores de la empresa no debe ser publicado
en lugares donde el público tiene acceso.
Explicación / Notas: Muchas empresas tienen tablones de anuncios donde la empresa privada o la información personal se publica para que cualquiera pueda leer. Avisos empleador,
listas de empleados, memorandos internos, los empleados números de contacto que figuran en el hogar
anuncios, y otra información, con frecuencia similar en el tablón.
Los tablones de anuncios pueden estar ubicados cerca de comedores de la empresa, o en las proximidades de
fumar o áreas de descanso donde los visitantes tienen acceso gratuito. Este tipo de información no debe ponerse a disposición de los visitantes o del público.
11.4 Informática entrada del centro
Política: La sala de ordenadores o centro de datos debe ser cerrada en todo momento y personal deberá acreditar su identidad antes de entrar.
Explicación / Notas: seguridad de la empresa debería considerar la implementación de un sistema electrónico
tarjeta de identificación o lector de tarjetas de acceso para todas las entradas pueden ser por vía electrónica registrada y
auditados.
4-12 cuentas de clientes con los proveedores de servicios
Política: El personal de la empresa que hacen pedidos de servicios con proveedores que suministran
servicios críticos para la empresa debe establecer una contraseña de la cuenta para prevenir personas no autorizadas puedan realizar pedidos en nombre de la empresa.
Explicación / Notas: empresas de servicios públicos y muchos otros proveedores permiten a los clientes
establecer una contraseña de solicitud, la empresa debe establecer contraseñas con todas las proveedores que proporcionan servicios de misión crítica. Esta política es especialmente crítico para
telecomunicaciones y servicios de Internet. Cada vez que los servicios críticos pueden ser afectados, un secreto compartido es necesario verificar que la persona que llama está autorizada a poner
tales órdenes. Tenga en cuenta, también, de identificación como número de seguro social corporativa
número de identificación fiscal, nombre de soltera de la madre, o identificadores similares que no ser utilizado. Un ingeniero social puede, por ejemplo, llamar a la compañía telefónica
y dar órdenes para agregar características tales como transferencia de llamadas para marcar en las líneas de módem,
o hacer una solicitud al proveedor de servicios de Internet a cambio de traducción
información para proporcionar una dirección IP falsa cuando los usuarios realizan un nombre de host
de búsqueda.
13.4 persona de contacto del Departamento
Política: Su empresa puede establecer un programa bajo el cual cada departamento o

grupo de trabajo se asigna a un empleado la responsabilidad de actuar como un punto de contacto para
que todo el personal puede verificar la identidad de hombres desconocidos que
ser de ese departamento. Por ejemplo, la mesa de ayuda puede comunicarse con el
persona de contacto del departamento para verificar la identidad de un empleado que solicita apoyo.
Explicación / Notas: Este método de verificación de la identidad se reduce el grupo de
los empleados que están autorizados para dar fe de los empleados dentro de su departamento
cuando los empleados de dicha solicitud de apoyo, como la redefinición de contraseñas u otros
relacionada con su cuenta los problemas informáticos.
Ataques de ingeniería social tienen éxito en parte porque el apoyo técnico
personal está presionado por el tiempo y no verifica la identidad correcta de
los solicitantes. Normalmente el personal de apoyo, personalmente, no puede reconocer todos los autorizados
personal debido a la cantidad de empleados en grandes organizaciones. El pointperson
método de dar fe limita el número de empleados que el apoyo técnico
el personal debe estar familiarizado personalmente con fines de verificación.
14.04 contraseñas de los clientes
Política: Los representantes de servicio al cliente no tendrá la capacidad de recuperar
contraseñas de cuentas de los clientes.
Explicación / Notas: Los ingenieros sociales llaman con frecuencia los departamentos de servicio al cliente
y, bajo un pretexto, intentar obtener información de un cliente de autenticación,
como la contraseña o número de seguro social. Con esta información, el social
ingeniero puede llamar a otro representante de servicio, pretende ser el cliente,
y obtener información o realizar pedidos fraudulentos.
Para evitar que estos intentos de tener éxito, el software de servicio al cliente
debe estar diseñado para que los representantes sólo puede escribir en la autenticación
información proporcionada por la persona que llama, y recibir una respuesta del sistema
que indica si la contraseña es correcta o no.
4.15 Vulnerabilidad de pruebas
Política: La notificación de uso de la empresa de tácticas de ingeniería social para poner a prueba la seguridad
vulnerabilidades se requiere durante el entrenamiento de conciencia de seguridad y el empleado orientación.
Explicación / Notas: Sin notificación de la ingeniería social, pruebas de penetración,
personal de la empresa puede sufrir la vergüenza, la ira, o trauma emocional otras
a partir de la utilización de tácticas engañosas utilizadas en su contra por otros empleados o
los contratistas. Mediante la colocación de nuevas contrataciones en cuenta durante el proceso de orientación que
que pueden ser objeto de esta prueba, se evita que dicho conflicto.
04.16 Presentación de la información confidencial de la empresa
Política: Información de la empresa no designados para el lanzamiento público no se
aparece en todas las áreas de acceso público.
Explicación / Notas: Además de los productos de información confidencial o procedimiento,
información de contacto internos, tales como teléfono interno o listas de empleados, o
la construcción de listas que contienen una lista de personal de gestión para cada departamento
dentro de la empresa también debe mantenerse fuera de la vista.
17.4 Seguridad de formación sobre sensibilización
Política: Todas las personas empleadas por la empresa debe completar una seguridad
curso de formación de la conciencia durante la orientación de los empleados. Además, cada
los empleados deben tomar un curso de sensibilización sobre la seguridad de actualización a intervalos periódicos,
que no exceda de doce meses, como es requerido por el departamento asignado a
la seguridad de capacitación responsabilidad.

Explicación / Notas: Muchas organizaciones desprecio formación del usuario final la conciencia por completo. De acuerdo con la Encuesta Global 2001 de Seguridad de la Información, sólo el 30 por ciento de las organizaciones encuestadas gastar dinero en la concienciación de los su comunidad de usuarios. La sensibilización es un requisito esencial para mitigar infracciones de seguridad con éxito la utilización de técnicas de ingeniería social.

18.4 Seguridad curso de formación para acceso a la computadora

Política: El personal debe asistir y completar con éxito una seguridad de la información Por supuesto antes de dar acceso a todos los sistemas informáticos de las empresas.

Explicación / Notas: Los ingenieros sociales atacan con frecuencia a los nuevos empleados, a sabiendas de que como grupo por lo general son los menos propensos a ser conscientes de la empresa las políticas de seguridad y los procedimientos adecuados para determinar la clasificación y el manejo de información confidencial.

La capacitación debe incluir una oportunidad para que los empleados hagan preguntas sobre las políticas de seguridad. Después del entrenamiento, el titular de la cuenta deben ser obligados a firmar un documento de reconocimiento de su comprensión de las políticas de seguridad, y su acuerdo para cumplir con las políticas.

19.04 credencial de empleado debe ser un código de colores

Política: Tarjetas de identificación debe ser un código de colores para indicar si la tarjeta de identificación titular es un empleado, contratista, temporal, proveedor, consultor visitante, o interno.

Explicación / Notas: El color de la placa es una excelente manera de determinar el estado de una persona desde la distancia. Una alternativa sería el uso de grandes letras para indicar el estado del porta-tarjetas, pero utilizando un esquema de colores es inconfundible y fácil de ver.

Una táctica común de ingeniería social para obtener acceso a un edificio físico es vestirse como una persona de la entrega o el técnico de reparación. Una vez dentro de la instalación, el atacante hacerse pasar por otro empleado o mentir acerca de su estado para obtener la cooperación de los empleados incautos. El propósito de esta política es evitar que las personas entren en el edificio legítimamente y luego entrar en las zonas que no deberían tener acceso. Por ejemplo, una persona que entra en la instalación como técnico de reparación de teléfono no sería capaz de hacerse pasar por un empleado: El color de la insignia que lo delatan.

POLÍTICAS DE TECNOLOGÍA DE LA INFORMACIÓN

El departamento de tecnología de la información de cualquier empresa tiene una necesidad especial de políticas que ayuden a la protección de los activos de información de las organizaciones. Para reflejar la estructura típica de las operaciones de TI en una organización, que han dividido a la IT las políticas en general, Help Desk, Administración Informática, e Informática Las operaciones.

General

5.1 TI empleado del departamento de información de contacto

Política: Los números de teléfono y direcciones de correo electrónico de cada departamento de TI los empleados no debe ser revelada a cualquier persona sin necesidad de saber.

Explicación / Notas: El propósito de esta política es evitar que la información de contacto de ser abusados por los ingenieros sociales. Sólo por la divulgación de un contacto general número o dirección de correo electrónico de TI, los extranjeros serán bloqueados entren en contacto con TI departamento de personal directamente. La dirección de correo electrónico para el sitio de administración y

contactos técnicos sólo debe consistir en nombres genéricos tales como
admin@companyname.com; publicado los números de teléfono debe conectarse a una
buzón de voz departamentos, y no a los trabajadores.
Cuando la información de contacto directo está disponible, es fácil para un ordenador
intruso para llegar a los empleados de TI específicas y engañarlos para que proporcionen información
que pueden ser utilizados en un ataque, o para hacerse pasar por empleados mediante el uso de sus
nombres e información de contacto.
2.5 las solicitudes de soporte técnico
Política: Todas las solicitudes de asistencia técnica deben ser remitidos al grupo que se encarga de
tales solicitudes.
Explicación / Notas: Los ingenieros sociales pueden intentar objetivo personal que se
por lo general no manejar los problemas de soporte técnico, y que pueden no ser conscientes de la
procedimientos adecuados de seguridad cuando se manejan estas peticiones. En consecuencia, el personal de TI
deben estar capacitados para denegar estas solicitudes y se refieren a la persona que llama el grupo que ha
la responsabilidad de proporcionar apoyo.
Help Desk
1.6 los procedimientos de acceso remoto
Política: El personal del servicio de ayuda no debe divulgar los detalles o instrucciones relativas a
acceso remoto, incluyendo puntos de la red externa de acceso o números de acceso telefónico,
a menos que el solicitante ha sido:
Verificado lo autorizado para recibir información interna, y,
Verificado lo autorizado para conectarse a la red corporativa como un usuario externo.
Menos que se sepa sobre una base de persona a persona, el solicitante debe ser positiva
identificados de acuerdo con la verificación y Procedimientos de Autorización
se indica al comienzo de este capítulo.
Explicación / Notas: El servicio de asistencia corporativa a menudo es un objetivo principal para el
ingeniero social, tanto por la naturaleza de su trabajo es ayudar a los usuarios
relacionados con la informática los problemas, y porque por lo general tienen un sistema de elevación
privilegios. Todo el personal de mesa de ayuda deben estar capacitados para actuar como un servidor de seguridad humana
evitar la divulgación no autorizada de información que ayudará a cualquier uso no autorizado
personas tengan acceso a recursos de la empresa. Una regla sencilla es que nunca
conocer los procedimientos de acceso remoto a cualquier persona hasta que la verificación positiva de la identidad
se ha hecho.
6.2 Restablecimiento de contraseñas
Política: La contraseña de una cuenta de usuario solamente se puede restaurar, a petición de la titular de la cuenta.
Explicación / Notas: El truco más común utilizado por los ingenieros sociales es tener
otra persona restablecer contraseñas de cuentas o cambiado. El atacante se hace pasar por el
los empleados con el pretexto de que su contraseña se ha perdido u olvidado. En un esfuerzo por
para reducir el éxito de este tipo de ataque, un empleado de TI de recibir una solicitud
para restablecer la contraseña debe llamar al empleado volver antes de tomar cualquier acción, la
devolver la llamada no se debe hacer a un número de teléfono proporcionado por el solicitante, sino a una
número que se obtiene a partir de la guía telefónica de los empleados. Ver Verificación y
Procedimientos de Autorización para más información sobre este procedimiento.
6.3 Modificación de los privilegios de acceso

Política: Todas las peticiones para aumentar los privilegios de un usuario o de los derechos de acceso se debe
aprobado por escrito por el gerente de la titular de la cuenta. Cuando el cambio se realiza una confirmación debe ser enviada al administrador de solicitar a través de correo electrónico dentro de la compañía.
Además, estas solicitudes deben ser verificada como auténtica, de acuerdo con la Verificación y Procedimientos de Autorización.
Explicación / Notas: Una vez que un intruso informático ha puesto en peligro a un usuario estándar
cuenta, el siguiente paso es elevar sus privilegios a fin de que el atacante tiene un control completo sobre el sistema comprometido. Un atacante que tenga conocimiento del proceso de autorización puede falsificar una solicitud de autorización al correo electrónico, fax o
telefónicas son usadas para transmitir. Por ejemplo, el atacante podría técnico telefónico apoyo o la mesa de ayuda y tratar de convencer a un técnico para subvención adicional derechos de acceso a la cuenta comprometida.
6-4 autorización nueva cuenta
Política: A solicitud de crear una nueva cuenta para un empleado, contratista, u otra persona autorizada deberá presentarse por escrito y firmado por el jefe del empleado, o por correo electrónico firmado digitalmente. Estas solicitudes también debe ser verificada mediante el envío de una confirmación de la solicitud a través de mail dentro de la compañía.
Explicación / Notas: Dado que las contraseñas y otra información útil para romper en los sistemas informáticos son los objetivos de máxima prioridad de los ladrones de información para
acceso, se requieren medidas especiales. La intención de esta política es para evitar que intrusos informáticos de hacerse pasar por personal autorizado o forjar las solicitudes de nuevas cuentas. Por lo tanto, todas las solicitudes deben ser positivamente
verifica por medio de los procedimientos de verificación y autorización.
6.5 La entrega de las nuevas contraseñas
Política: Las nuevas contraseñas deben ser tratados como información confidencial de la empresa,
entregados por métodos seguros incluso en persona, por la entrega de firmas requeridas servicios como el correo certificado, o por UPS o FedEx. Ver las políticas relativas a distribución de información confidencial.
Explicación / Notas: correo electrónico dentro de una misma también se puede utilizar, pero se recomienda
que las contraseñas se envían en sobres de seguridad que oscurecen el contenido. A sugerido método consiste en establecer una persona de contacto de un ordenador en cada departamento que tiene la
responsabilidad de manejar la distribución de información de la cuenta nueva y dar fe de la identidad del personal que se pierde u olvida su contraseña. En estos circunstancias, el personal de apoyo siempre estará trabajando con un grupo más pequeño de los empleados que se reconoció personalmente.
6.6 Desactivación de una cuenta
Política: Antes de desactivar una cuenta de usuario debe requerir la verificación positiva que la solicitud fue hecha por personal autorizado.
Explicación / Notas: La intención de esta política es evitar que un atacante falsificación de una solicitud para desactivar una cuenta, y luego llamar para solucionar el la incapacidad del usuario para acceder al sistema informático. Cuando el ingeniero social requiere
haciéndose pasar por un técnico que ya tenían conocimiento de la incapacidad del usuario para iniciar sesión
en la víctima a menudo cumple con una solicitud para revelar su contraseña durante

el proceso de solución de problemas.
7.6 Desactivación de puertos de red o dispositivos
Política: Ningún empleado debe desactivar cualquier dispositivo de red o el puerto para cualquier verificadas personal de soporte técnico.
Explicación / Notas: La intención de esta política es evitar que un atacante falsificación de una solicitud para desactivar un puerto de red, y luego llamar al trabajador solucionar su incapacidad para acceder a la red.
Cuando el ingeniero social, haciéndose pasar por un técnico de ayuda, llama a pre-existentes conocimiento del problema en la red del usuario, la víctima a menudo cumple con una solicitud para revelar su contraseña durante el proceso de solución de problemas.
6.8 Divulgación de los procedimientos para el acceso inalámbrico
Política: Ningún miembro del personal debe revelar los procedimientos para acceder a los sistemas de la empresa
través de redes inalámbricas a terceros no autorizados a conectarse a la red inalámbrica de la red.
Explicación / Notas: siempre obtener una verificación previa de un solicitante como una persona autorizados a conectarse a la red corporativa como un usuario externo antes la divulgación de información de acceso inalámbrico. Ver la verificación y autorización Procedimientos.
6-9 entradas de usuario problemas
Política: Los nombres de los empleados que han reportado relacionados con la informática problemas no deben ser revelados fuera del departamento de tecnología de la información.
Explicación / Notas: En un ataque típico, un ingeniero social se llame a la mesa de ayuda y solicitar los nombres de todo el personal que han informado de los últimos problemas de la computadora. La persona que llama puede pretender ser un empleado, proveedor o un
empleado de la compañía telefónica. Una vez que obtiene los nombres de las personas informar problemas, el ingeniero social, haciéndose pasar por una mesa de ayuda o soporte técnico
persona, en contacto con el empleado y dice que él / ella está llamada a solucionar el problema. Durante la llamada, el atacante engaña a la víctima en el abastecimiento de la información deseada o en realizar una acción que facilita el intruso objetivo.
06.10 Inicio de los programas de ejecutar comandos o ejecutar
Política: El personal empleado en el departamento de TI que tienen cuentas con privilegios no debe ejecutar ningún comando o ejecutar cualquier programa de aplicación a petición de cualquier persona que no conoce personalmente a ellos.
Explicación / Notas: Un método común para los atacantes utilizar para instalar un caballo de Troya programa u otro software malicioso es cambiar el nombre de uno existente programa, y luego llamar a la mesa de ayuda quejándose de que un mensaje de error aparece cada vez que se intenta ejecutar el programa. El atacante
convence al técnico de servicio de asistencia para ejecutar el mismo programa. Cuando el técnico cumple, el software malicioso hereda los privilegios del usuario la ejecución del programa y realiza una tarea, que le da al atacante la misma privilegios de las computadoras como empleado del Help Desk. Esto puede permitir al atacante tomar el control del sistema de la compañía.
Esta política establece una medida para contrarrestar esta táctica, al exigir que el apoyo personal de verificar la situación laboral antes de ejecutar cualquier programa en la solicitud de la persona que llama.
Equipo de administración
1.7 Modificación de los derechos de acceso global
Política: Una solicitud de cambio de los derechos de acceso globales asociados con una red perfil de trabajo debe ser aprobado por el grupo asignado la responsabilidad de gestión de los derechos de acceso a la red corporativa.
Explicación / Notas: El personal autorizado a analizar cada solicitud de

determinar si el cambio podría suponer una amenaza para la seguridad de la información. Si es así,
el empleado responsable se ocupará de las cuestiones pertinentes con el solicitante y conjuntamente llegar a una decisión sobre los cambios a realizar.
7.2 peticiones de acceso remoto
Política: acceso remoto al ordenador sólo se proporcionará al personal que haya un demostrado la necesidad de acceder a los sistemas corporativos equipo de lugares fuera del sitio. La solicitud debe ser hecha por el gerente de un empleado y verificar como se describe en la verificación y la sección de Procedimientos de Autorización.
Explicación / Notas: Reconociendo la necesidad de acceso fuera de las instalaciones en la empresa
por personal autorizado de la red, lo que limita dicho acceso sólo a las personas con una necesidad
pueden reducir dramáticamente el riesgo y la gestión de usuarios de acceso remoto. La menor sea el número de personas con privilegios de acceso telefónico externo, menor será el conjunto de posibles objetivos para un atacante. No olvides nunca que el atacante también puede destino remoto a los usuarios con la intención de secuestrar su conexión a la empresa de la red, o haciéndose pasar por ellos durante una llamada de pretexto.
3.7 Restablecimiento de contraseñas privilegiadas cuenta
Política: Una petición para restablecer una contraseña de una cuenta con privilegios deben ser aprobados
por el gerente o administrador del sistema responsable del equipo en el que existe la cuenta. La nueva contraseña debe ser enviada por correo dentro de la compañía o entregadas en persona.
Explicación / Notes. "Cuentas privilegiadas tienen acceso a todos los recursos del sistema y los archivos almacenados en el sistema informático. Naturalmente, estas cuentas se merece el mayor protección posible.
7.4 Fuera de personal de apoyo de acceso remoto
Política: Ninguna persona de apoyo externo (por ejemplo, proveedor de software o hardware personal) se puede dar cualquier información de acceso remoto o se permitirá el acceso cualquier sistema informático de la empresa o dispositivos relacionados, sin la verificación positiva de
identidad y la autorización para realizar tales servicios. Si el proveedor requiere acceso privilegiado a proporcionar servicios de apoyo, la contraseña de la cuenta utilizada por el vendedor deberá ser cambiada inmediatamente después de que el proveedor de servicios han sido
completado.
Explicación / Notas: los atacantes ordenador puede pasar por los vendedores para acceder a informáticos de las empresas o las redes de telecomunicaciones. Por lo tanto, es esencial que la identidad del proveedor se verificará, además de su autorización para realizar cualquier trabajo en el sistema. Por otra parte, las puertas en el sistema debe ser portazo cierre una vez que su trabajo está hecho por cambiar la contraseña de la cuenta utilizada por el vendedor.
Ningún otro proveedor se debe permitir a recoger su contraseña para cualquier cuenta propia, ni siquiera temporalmente. Algunos vendedores han sido conocidos por usar la misma o similar contraseñas a través de los sistemas de varios clientes. Por ejemplo, una red de seguridad empresa creada cuentas privilegiadas en todos los sistemas de sus clientes con el mismo contraseña, y, para colmo de males, con el acceso de Telnet fuera habilitado.
5.7 La autenticación fuerte para el acceso remoto a los sistemas corporativos
Política: Todos los puntos de conexión a la red corporativa desde ubicaciones remotas deben ser protegidos a través del uso de dispositivos de autenticación fuerte, como contraseñas dinámicas o la biometría.
Explicación / Notas: Muchos negocios se basan en contraseñas estáticas como el único medio de autenticación para usuarios remotos. Esta práctica es peligrosa porque es
inseguro: los intrusos equipo de destino cualquier punto de acceso remoto que podría ser el

eslabón débil en la red de la víctima. Recuerde que nunca se sabe cuando
alguien más conoce su contraseña.
En consecuencia, todos los puntos de acceso remoto debe ser protegido con un fuerte
autenticación como los tokens basados en el tiempo, las tarjetas inteligentes o dispositivos
biométricos, por lo que
que las contraseñas interceptadas no tienen ningún valor para un atacante.
Cuando la autenticación basada en contraseñas dinámicas no es práctico, los usuarios de
computadoras
religiosos deben adherirse a la política para la elección difíciles de adivinar.
6.7 configuración del sistema operativo
Política: Los administradores de sistemas velarán por que, siempre que sea posible, de
funcionamiento
los sistemas están configurados para que sean compatibles con toda la seguridad pertinente
políticas y procedimientos.
Explicación / Notas: Redacción y distribución de las políticas de seguridad es un derecho
fundamental
paso hacia la reducción del riesgo, pero en la mayoría de los casos, el cumplimiento es
necesariamente deja a
cada empleado. Hay, sin embargo, cualquier número de relacionados con la informática
políticas que pueden ser obligatorios a través de la configuración del sistema operativo, como
la longitud requerida de contraseñas. Automatizar las políticas de seguridad según la
configuración
de los parámetros del sistema operativo de forma eficaz toma la decisión de los humanos
manos elemento, el aumento de la seguridad general de la organización.
7-7 de caducidad obligatorio
Política: Todas las cuentas de equipo debe estar a punto de expirar después de un año.
Explicación / Notas: La intención de esta política es eliminar la existencia de
cuentas de equipo que ya no se utiliza, ya que los intrusos informáticos
comúnmente objetivo de las cuentas inactivas. El proceso asegura que a cualquier equipo
cuentas que pertenecen a ex empleados o contratistas que hayan sido
sin querer dejar en su lugar se desactivan automáticamente.
A discreción de la administración, puede requerir que los empleados deben tener una seguridad
Curso de actualización en el momento de la formación, renovación o revisión de seguridad de la
información debe
políticas y firmar una declaración de su acuerdo a que se adhieran a ellos.
7-8 direcciones de correo electrónico genérico
Política: El departamento de tecnología de la información establecerá un correo electrónico
genérico
dirección de cada departamento dentro de la organización que normalmente se comunica
con la extensión. público.
Explicación / Notas: La dirección de correo electrónico genérica puede ser lanzado al público por
el
teléfono recepcionista o publicados en el sitio Web de la compañía. De lo contrario, cada
empleado sólo deberá revelar su dirección personal de correo electrónico a las personas que
tienen auténtica necesidad de saber.
Durante la primera fase de un ataque de ingeniería social, el atacante trata a menudo de
obtener números de teléfono, nombres y cargos de los empleados. En la mayoría de los casos,
esta
información está disponible públicamente en el sitio web de la empresa o simplemente para pedir.
La creación de buzones de voz genérica y / o direcciones de correo electrónico hace que sea
difícil
asociar los nombres de los empleados con determinados departamentos o funciones.
9.7 Información de contacto para las inscripciones de dominio
Política: Cuando se registra para la adquisición de espacio de direcciones de Internet o
los nombres de host, la información de contacto técnico y administrativo, u otros

El personal no debe identificar al personal por su nombre. En su lugar,
debe indicar una dirección de correo electrónico genérica y el número de teléfono principal de la empresa.
Explicación / Notas: El propósito de esta política es evitar que la información de contacto
de ser abusados por un intruso informático. Cuando los nombres y números de teléfono
de los individuos son siempre, un intruso puede utilizar esta información para comunicarse con el las personas y tratar de engañar al sistema de información reveladora, o
realizar un elemento de acción que facilite el objetivo de un atacante. O el social
ingeniero puede suplantar a una persona que figuran en un esfuerzo por engañar a otra compañía de personal.
En lugar de una dirección de correo electrónico a un empleado en particular, información de contacto
debe ser en forma de administrator@company.com. Telecomunicaciones
personal del departamento puede establecer un buzón de voz genérica de administración o contactos técnicos con el fin de limitar la divulgación de información que sería útil en un ataque de ingeniería social.
Instalación 7-10 de seguridad y actualizaciones del sistema operativo
Política: Todos los parches de seguridad para el sistema operativo y software de aplicación se ser instalado tan pronto como estén disponibles. Si esto entra en conflicto con la política el funcionamiento de aplicaciones críticas sistemas de producción, las actualizaciones deberían ser
realizarse tan pronto como sea posible.
Explicación / Notas: Una vez que la vulnerabilidad ha sido identificada, el software
fabricante debe ser contactado inmediatamente para determinar si un
parche o una solución temporal ha sido puesto a disposición cerca de la vulnerabilidad.
Un sistema informático sin parches representa uno de los mayores de seguridad
amenazas a la empresa. Cuando los administradores del sistema de procrastinar
aplicar las correcciones necesarias, la ventana de la exposición está abierta todo el fin de que cualquier atacante puede subir por.
Decenas de vulnerabilidades de seguridad se identifican y se publica semanalmente en el Internet. Hasta que el personal de tecnología de información están atentos en sus esfuerzos por aplicar
todos los parches de seguridad y correcciones lo antes posible, a pesar de estos sistemas se detrás del firewall de la compañía, la red de la empresa siempre estará en riesgo de
sufrir un incidente de seguridad. Es extremadamente importante mantenerse al tanto de publicó las vulnerabilidades de seguridad detectadas en el sistema operativo o cualquier programas de aplicación que se utiliza durante el curso de los negocios.
11.7 La información de contacto en los sitios Web
Política: El sitio web de la empresa externa no revelará ningún detalle de las empresas estructura o identificar los empleados por su nombre.
Explicación / Notas: La información Estructura de la empresa, tales como organigramas, gráficos de la jerarquía, listas de empleados o departamentos, la estructura de información, nombres,
posiciones, los números internos de contacto, número de empleados, o información similar que se utiliza para los procesos internos no deben ser puestos a disposición del público en sitios Web accesibles.
Intrusos informáticos suele obtener una información muy útil en el sitio Web de un objetivo.
El atacante utiliza esta información para que aparezca como un conocedor 206 empleados cuando se utiliza un pretexto o una trampa. La ingeniería social es más probable que establecer credibilidad por tener esta información en su disposición.
Por otra parte, el atacante puede analizar esta información para determinar los objetivos probables
que tienen acceso a información valiosa, sensible o crítica.
12.7 Creación de cuentas con privilegios
La política. "No cuenta con privilegios deben ser creadas o privilegios del sistema concedidos a

cualquier cuenta menos que sea autorizado por el administrador del sistema o administrador del sistema.
Explicación / Notes. "Intrusos PC con frecuencia se hacen pasar por hardware o software
los vendedores en un intento de engañar a personal de tecnología de información en la creación de
cuentas no autorizadas. La intención de esta política es bloquear estos ataques
establecer un mayor control sobre la creación de cuentas privilegiadas. El sistema
gerente o administrador del sistema informático debe aprobar cualquier solicitud de
crear una cuenta con privilegios elevados.
13.7 Las cuentas de invitado
Política: Las cuentas de invitado en el sistema informático o relacionado con los dispositivos de red
deberán ser desactivados o eliminados, a excepción de un FTP (File Transfer Protocol) del servidor
aprobadas por la administración con acceso anónimo habilitado.
Explicación / Notas: La intención de la cuenta de invitado es proporcionar temporal
acceso de las personas que no tienen que tener su propia cuenta. Funcionamiento de varios
sistemas se instalan por defecto con una cuenta de invitado habilitada. Las cuentas de invitado
siempre debe ser desactivado, porque su existencia viola el principio de usuario
la rendición de cuentas. TI debe ser capaz de cualquier actividad de auditoría relacionados con la informática y se relacionan
que a un usuario específico.
Los ingenieros sociales son fácilmente capaces de tomar ventaja de estas cuentas de invitados
obtener acceso no autorizado, ya sea directamente o por engañar a personal autorizado
a usar una cuenta de invitado.
7.14 El cifrado de datos de respaldo fuera del sitio
Política: Los datos de la empresa que se almacena fuera del sitio debe ser encriptada para evitar que
acceso no autorizado.
Explicación / Notas: El personal de operaciones debe asegurarse de que todos los datos son recuperables en el
caso de que cualquier información debe ser restaurado. Esto requiere la prueba regular
descifrado de un muestreo aleatorio de los archivos cifrados para asegurarse de que los datos pueden ser
recuperado. Además, las claves utilizadas para cifrar los datos se plica con una
gerente de confianza en el caso de las claves de cifrado son perdidas o no disponibles.
07.15 visitantes el acceso a conexiones de red
Política: Todos los puntos de acceso Ethernet de acceso público debe estar en una segmentación
la red para evitar el acceso no autorizado a la red interna.
Explicación / Notas: La intención de esta política es evitar que personas ajenas
conexión a la red interna cuando en las instalaciones de la empresa. Ethernet tomas
instalados en las salas de conferencias, la cafetería, centros de formación, u otras áreas
accesibles a los visitantes debe ser filtrado para evitar el acceso no autorizado por los visitantes
los sistemas informáticos corporativos.
El administrador de red o de seguridad puede optar por configurar una red
LAN en un interruptor, si está disponible, para controlar el acceso de estos lugares.
16.7 módems de acceso telefónico
Política: Los módems utilizados para la marcación de llamadas se debe configurar para responder, no antes
que el cuarto anillo.
Explicación / Notas: Como se muestra en la película Juegos de Guerra, los hackers utilizan un
técnica conocida como marcación de guerra para localizar las líneas telefónicas que tienen módems
conectados a ellos. El proceso comienza con el atacante identificar el teléfono
prefijos utilizados en la zona donde se encuentra la empresa objetivo. Una exploración

programa se utiliza para tratar todos los números de teléfono en los prefijos, para localizar aquellos que responden con un módem. Para acelerar el proceso, estos programas son configurado para esperar a que uno o dos anillos de una respuesta del módem antes de pasar a tratar el siguiente número. Cuando una empresa establece la respuesta automática en las líneas de módem en
por lo menos cuatro anillos, escanear los programas no reconocen la línea como un módem la línea.

7.17 El software antivirus

Política: Cada sistema informático tendrá versiones actuales de software antivirus instalado y activado.

Explicación / Notas: Para las empresas que no pasan automáticamente a empujar hacia abajo software antivirus y el patrón de archivos (programas que reconocen patrones comunes a software antivirus para reconocer los nuevos virus) para escritorios de los usuarios o estaciones de trabajo,
usuarios individuales deben asumir la responsabilidad de la instalación y el mantenimiento de la software en sus propios sistemas, incluidos los sistemas informáticos utilizados para la acceso a la red corporativa de forma remota.

Si es posible, este software se debe establecer para la actualización automática de virus y troyanos
firmas de todas las noches. Cuando las moscas patrón o la firma no se empuja hacia abajo para el usuario
computadoras de escritorio, los usuarios tendrán la responsabilidad de actualizar los archivos de patrones en
por lo menos una vez por semana.

Estas disposiciones se aplican a todas las máquinas de escritorio y portátiles utilizados para el acceso
sistemas de la compañía informática, y se aplican si el equipo es la empresa propiedad o propiedad personal.

18.07 adjuntos de correo electrónico entrante (requisitos de alta seguridad)

Política: En una organización con requerimientos de alta seguridad, el firewall de la empresa se puede configurar para filtrar todos los archivos adjuntos de correo electrónico.

Explicación / Notas: Esta política se aplica sólo a las empresas con alta seguridad requisitos, o para aquellos que no tienen nada que recibir archivos adjuntos a través de correo electrónico.

19.7 de autenticación de software

Política: Todo el software nuevo o correcciones o actualizaciones de software, ya sea física los medios de comunicación u obtenidos a través de Internet, debe ser verificada como auténtica antes de la
de la instalación. Esta política es especialmente relevante para la tecnología de la información departamento de la instalación de cualquier software que requiera privilegios de sistema.

Explicación / Notas: Los programas informáticos mencionados en esta política incluye componentes del sistema operativo, software de aplicaciones, revisiones, correcciones, o cualquier
actualizaciones de software. Muchos fabricantes de software han implementado métodos mediante el cual los clientes pueden comprobar la integridad de cualquier distribución, por lo general por un
la firma digital. En cualquier caso en que la integridad no puede ser verificada, el fabricante deben ser consultadas para verificar que el software es auténtico.

Los atacantes informáticos se han sabido para enviar el software a una víctima, empaquetado para
parece como si el fabricante del software había producido y enviado a la
de la empresa. Es esencial que verifique cualquier software que usted recibe como auténticas, sobre todo si no solicitados, antes de instalarlo en sistemas de la empresa.

Tenga en cuenta que un atacante sofisticado puede ser que descubra que su organización ha ordenó software de un fabricante. Con esa información en mano, el atacante

puede cancelar el pedido con el fabricante real, y para el software mismo.
El software se modifica para realizar alguna función maliciosa, y es enviado
o entregados a su empresa, en su embalaje original, con retractilado si
es necesario. Una vez que el producto está instalado, el atacante tiene el control.
07.20 contraseñas por defecto
Política: Todo el software del sistema operativo y los dispositivos de hardware que en un principio
tener una contraseña a un valor por defecto debe tener sus contraseñas restablecer en
acuerdo con la directiva de contraseñas de la empresa.
Explicación / Notas: Varios sistemas operativos y dispositivos relacionados con la informática son
entrega con contraseñas por defecto - es decir, con la misma contraseña habilitado en
cada unidad vendida. Si no cambia las contraseñas por defecto es un grave error que pone
la empresa en situación de riesgo.
Contraseñas por defecto son ampliamente conocidos y están disponibles en Internet Web
sitios. En un ataque, la primera contraseña que un intruso intenta es por defecto del fabricante s
contraseña.
7-21 intentos de acceso no válido de bloqueo (de menos a seguridad media)
Política: Sobre todo en una organización con bajos requisitos de seguridad media,
cada vez que un número determinado de intentos de acceso no válido sucesivas a un particular
cuenta se han realizado, la cuenta debe ser bloqueado por un período de tiempo.
Explicación / Notas: Todas las estaciones de trabajo y servidores de la empresa debe establecer
para limitar el número de los sucesivos intentos fallidos para iniciar sesión Esta política es
necesarias para evitar que adivinar la contraseña por ensayo y error, los ataques de diccionario, o
fuerza bruta intenta obtener acceso no autorizado.
El administrador del sistema debe configurar la configuración de seguridad para bloquear una
cuenta cada vez que el umbral deseado de los sucesivos intentos fallidos ha sido
alcanzado. Se recomienda que una cuenta sea bloqueada por al menos treinta
minutos después de siete intentos de conexión sucesivos.
7-22 intentos de acceso no válido cuenta deshabilitada (alta seguridad)
Política: En una organización con requerimientos de alta seguridad, cada vez que un determinado
número de los sucesivos intentos de acceso no válido a una cuenta particular, ha sido
hecho, la cuenta debe ser desactivado hasta que se restablece por el grupo responsable de la
la prestación de apoyo cuenta.
Explicación / Notas: Todas las estaciones de trabajo y servidores de la empresa debe estar en el
límite
número de sucesivos intentos fallidos para iniciar sesión Esta política es una condición necesaria
control para evitar que adivinar la contraseña por ensayo y error, los ataques de diccionario, o
fuerza bruta intenta obtener acceso no autorizado.
El administrador del sistema debe configurar la configuración de seguridad para desactivar el
cuenta después de cinco intentos de acceso no válido. A raíz de ese ataque, la cuenta
titular tendrá que llamar a soporte técnico o el grupo responsable de la cuenta
apoyo para activar la cuenta. Antes de restablecer la cuenta, el departamento
responsable debe identificar positivamente el titular de la cuenta, después de la
Verificación y Procedimientos de Autorización.
23.7 Cambio periódico de información privilegiada
Política: Todos los titulares de las cuentas privilegiadas tendrán la obligación de cambiar sus
contraseñas
por lo menos cada treinta días.
Explicación / Notas: Dependiendo de las limitaciones del sistema operativo, los sistemas de
administrador debe cumplir esta política por la configuración de los parámetros de seguridad en
sistema de software.
7.24 el cambio periódico de contraseñas de los usuarios
Política: Todos los titulares de las cuentas deben cambiar sus contraseñas al menos cada sesenta
días.
Explicación / Notas: Con los sistemas operativos que ofrecen esta característica, los sistemas de
administrador debe cumplir esta política por la configuración de los parámetros de seguridad en

el software.
25.7 contraseña de la cuenta de Nueva establecer
Política: Las nuevas cuentas de equipo se debe establecer una contraseña inicial que
es pre-vencido, lo que requiere el titular de la cuenta para seleccionar una nueva contraseña al inicial
uso.
Explicación / Notas: Este requisito garantiza que sólo el titular de la cuenta
tener conocimiento de su contraseña.
7.26 Boot-up contraseñas
Política: Todos los sistemas de equipo debe estar configurado para requerir una contraseña de arranque.
Explicación / Notas: Los ordenadores deben estar configurados de manera que cuando el equipo está
encendido, se requiere una contraseña antes de que el sistema operativo de arranque. Este evita que cualquier persona no autorizada de encendido y el uso de otra persona
equipo. Esta política se aplica a todos los equipos en las instalaciones de la empresa.
27.7 Requisitos de contraseña para cuentas privilegiadas
Política: M1 unas cuentas privilegiadas, debe tener una contraseña segura: la contraseña debe:
No ser una palabra en un diccionario en cualquier idioma
Se mezclan mayúsculas y minúsculas con al menos una letra, un símbolo, y un
numeral
Tener al menos 12 caracteres de longitud
No estar relacionado con la empresa o persona de ninguna manera.
Explicación / Notas: En la mayoría de los casos los intrusos informáticos se centrará en las cuentas específicas
que tienen los privilegios del sistema. En ocasiones, el atacante explotar otras vulnerabilidades para obtener control total sobre el sistema.
Las primeras contraseñas que un intruso se trate son las palabras simples, de uso común encontrar en un diccionario. La selección de contraseñas seguras mejora la seguridad de reducir la posibilidad de que un atacante se encuentra la contraseña por ensayo y error, ataque de diccionario o un ataque de fuerza bruta.
28.7 puntos de acceso inalámbrico
Política: Todos los usuarios que acceden a una red inalámbrica debe utilizar VPN (Virtual Private Red) para proteger la red corporativa.
Explicación / Notas: Las redes inalámbricas están siendo atacados por una nueva técnica llama conducir de la guerra. Esta técnica consiste simplemente en conducir o caminar alrededor de
con un ordenador portátil equipado con una tarjeta NIC 802.11b hasta que una red inalámbrica es detectado.
Muchas empresas han implementado redes inalámbricas sin habilitar WEP
(Inalámbrica equivalencia protocolo), que se utiliza para proteger la conexión inalámbrica a través del uso de la encriptación. Pero incluso cuando está activada, la versión actual del WEP (Mediados de 2002) no es efectivo: Se ha roto completamente abiertos, y varios sitios Web se dedican a proporcionar los medios para la localización de los sistemas abiertos inalámbricos y cracking WEP habilitado puntos de acceso inalámbricos.
Por consiguiente, es esencial para añadir una capa de protección alrededor de la 802.11B protocolo mediante el despliegue de la tecnología VPN.
29.7 Actualización de antivirus los archivos de patrones
Política: Cada sistema debe ser programado para que actualice automáticamente
antivirus / anti-troyano archivos de patrones.
Explicación / Notas: Como mínimo, estas actualizaciones se producen por lo menos una vez por semana. En
empresas donde los empleados dejan sus computadoras encendido, 302 es muy recomienda que los archivos de patrones se actualizará todas las noches.

El software antivirus es ineficaz si no se ha actualizado para detectar todas las nuevas formas de código malicioso. Dado que la amenaza de virus, gusanos, caballos de Troya y las infecciones se aumentar notablemente si los archivos de patrones no se actualizan, es esencial que antivirus o productos de código malicioso se mantendrá hasta la fecha.

Operaciones Informáticas

1.8 Introducción de programas o ejecutar comandos

Política:. Explotación del personal no debe introducir comandos o ejecutar programas, a petición de cualquier persona que no conocen. Si surge una situación Cuando una persona no verificadas parece haber razón para hacer tal solicitud, no debe ser cumplido sin obtener primero la aprobación del director.

Explicación / Notas:. Operaciones de ordenador empleados son blancos populares de social ingenieros, ya que sus posiciones por lo general requieren acceso a la cuenta privilegiada, y el atacante espera que sean menos experiencia y conocimientos menos de procedimientos de la compañía de otros trabajadores de TI. La intención de esta política consiste en añadir una verificación adecuada y el equilibrio para evitar que los ingenieros sociales de engañar las operaciones de personal de informática.

8.2 Los trabajadores con cuentas con privilegios

Política: Los empleados con unas cuentas privilegiadas, no debe proporcionar asistencia o información a cualquier persona sin verificar. En particular esto se refiere a no proporcionar ayuda de la computadora (como la formación en el uso de la aplicación), el acceso a cualquier empresa base de datos, descarga de software, y sin revelar los nombres del personal que capacidades de acceso remoto,

Explicación / Notas: Los ingenieros sociales a menudo los empleados con el objetivo privilegiado cuentas. La intención de esta política es orientar al personal de TI con unas cuentas privilegiadas para con éxito manejar las llamadas que pueda representar ataques de ingeniería social.

3.8 los sistemas de información interna

Política: personal de explotación no deben revelar ninguna información relacionada con sistemas de la empresa informática o dispositivos relacionados de manera positiva, sin la verificación de la identidad del solicitante.

Explicación / Notas: intrusos PC a menudo en contacto operaciones de la computadora empleados para obtener información valiosa, como los procedimientos de acceso al sistema, puntos externos para el acceso remoto y conexión telefónica en los números de teléfono que son de un valor sustancial para el atacante.

En las empresas que tienen personal de apoyo técnico o de un servicio de asistencia, peticiones al personal de operaciones de computadoras para obtener información sobre los sistemas informáticos o dispositivos relacionados debe considerarse inusual. Cualquier solicitud de información debe ser examinada en el marco de la política de clasificación de datos corporativa para determinar si el solicitante está autorizado a disponer de esta información. Cuando la clase de la información no puede ser determinado, la información debe ser considerada Interno.

En algunos casos, el soporte del proveedor técnica externa tendrá que comunicarse con personas que tienen acceso a los sistemas informáticos de la empresa. Los vendedores deben tener contactos específicos en el departamento de TI para que las personas pueden reconocer unos a otros con fines de verificación.

4.8 La divulgación de contraseñas

Política: personal de explotación no debe revelar su contraseña, o cualquier otra contraseña que se les confían, sin la aprobación previa de una información gerente de tecnología.

Explicación / Notas: En términos generales, sin revelar ninguna contraseña a otra es estrictamente
prohibido. Esta política reconoce que el personal de operaciones puede ser necesario revelar una contraseña a un tercero cuando las situaciones extremas, surgen. Esta excepción a la divulgación general de política que prohíbe cualquier contraseña requiere la aprobación específica de un gerente de tecnología de la información. Por precaución adicional, esta responsabilidad de divulgar la información de autenticación debe limitarse a un pequeño grupo de
individuos que han recibido entrenamiento especial en los procedimientos de verificación.
8.5 Los medios electrónicos
Política: Todos los medios de comunicación electrónica que contiene información no destinados a públicos
liberación se encerraron en una ubicación físicamente segura.
Explicación / Notas: La intención de esta política es para evitar el robo físico de
Información sensible almacenada en los medios electrónicos.
6.8 Copia de seguridad de los medios de comunicación
Política: El personal de operaciones debe guardar copia de seguridad de los medios de comunicación en un lugar seguro o la compañía
lugar seguro y otros.
Explicación / Notas: Copia de seguridad de los medios de comunicación es otro objetivo prioritario de los intrusos informáticos.
Un atacante no va a pasar el tiempo tratando de comprometer un ordenador
sistema o red cuando el eslabón más débil de la cadena podría estar físicamente
los medios de comunicación sin protección de copia de seguridad. Una vez que los medios de comunicación copia de seguridad es robado, el atacante puede
comprometer la confidencialidad de los datos almacenados en ella, a menos que los datos se cifrados. Por lo tanto, asegurar físicamente los medios de comunicación copia de seguridad es un proceso esencial para
proteger la confidencialidad de la información corporativa.
POLÍTICAS PARA TODOS LOS EMPLEADOS
Ya sea en informática o recursos humanos, el departamento de contabilidad, o la
personal de mantenimiento, hay ciertas políticas de seguridad que todos los empleados de su empresa debe saber. Estas políticas se dividen en las categorías de General, Informática
Uso, uso de correo electrónico, las políticas para teletrabajadores, uso del teléfono, uso de fax, correo de voz
Uso y contraseñas.
General
1.9 Informe llamadas sospechosas
Política: Los empleados que sospechen que pueden ser objeto de una fianza
violación, incluidas las solicitudes sospechosas de revelar información o llevar a cabo para los puntos de acción en un ordenador, debe informar inmediatamente el hecho a la compañía de notificación de incidentes grupo.
Explicación / Notas:. Cuando un ingeniero social no logra convencer a su objetivo de
cumplir con la demanda, el atacante siempre tratará de otra persona. Al informar sobre una sospechosas o evento, un empleado toma el primer paso para alertar a la compañía
que un ataque puede estar en camino. Por lo tanto, los empleados son la primera línea de defensa contra los ataques de ingeniería social.
9.2 Documentación de llamadas sospechosas
Política: En el caso de una llamada telefónica sospechosa que parece ser una social
ataque de ingeniería, el empleado deberá, en la medida de lo posible, sacar la persona que llama para conocer los detalles que puedan revelar lo que el atacante está tratando de lograr,
y tome nota de estos detalles para los informes.
Explicación / Notas: Cuando se informó al grupo de notificación de incidentes, tales detalles puede ayudarlos a identificar el objeto o el patrón de un ataque.
3.9 La divulgación de números de acceso telefónico
Política: personal de la empresa no deben revelar la compañía telefónica del módem

números, pero deben de conocer estas solicitudes al servicio de asistencia técnica o personal de apoyo.
Explicación / Notas: Acceso telefónico a los números de teléfono deben ser tratados como internos
información que debe facilitarse a los empleados que tienen necesidad de saber como información para llevar a cabo sus responsabilidades de trabajo.
Los ingenieros sociales rutinariamente objetivo empleados o departamentos que pueden ser menos de protección de la información solicitada. Por ejemplo, el atacante puede llamar al el departamento de cuentas por pagar haciéndose pasar por una compañía telefónica empleado que está tratando de resolver un problema de facturación. El atacante pide cualquier fax conocido o números de marcado para resolver el problema. El intruso a menudo se dirigen a un empleado que es poco probable que den cuenta del peligro de la liberación de tales
información, o que carece de formación con respecto a la política de la empresa y la divulgación procedimientos.
9-4 tarjetas de identificación corporativa
Política: Salvo cuando en su zona de trabajo inmediata, todo el personal de la empresa, incluyendo la gestión y el personal ejecutivo, deben llevar sus tarjetas de los empleados en todo el tiempo.
Explicación / Notas: Todos los trabajadores, incluidos los ejecutivos de las empresas, debe ser capacitado y motivado para comprender que el uso de una tarjeta de identificación es obligatoria por todas partes en las instalaciones de otra compañía que en las zonas públicas y la propia persona
oficina o área de grupo de trabajo.
9.5 Desafiando violaciónes ID insignia
Política: Todos los empleados de inmediato debe oponerse a cualquier persona desconocida que se
no usar una credencial de empleado o una insignia de visitante.
Explicación / Nota: Si bien ninguna empresa quiere crear una cultura en eagleeyed
los empleados buscan una manera de atrapar a los compañeros de trabajo para aventurarse en el pasillo sin sus tarjetas de identificación, sin embargo, las empresas afectadas con
la protección de sus necesidades de información para tomar en serio la amenaza de un ingeniero social
vagar sus instalaciones sin respuesta. Motivación para los empleados que demuestren diligentes en ayudar a hacer cumplir la política de insignias, siempre puede ser reconocido en formas familiares, como el reconocimiento en el periódico de la compañía o en el boletín juntas, unas horas libres con goce de sueldo, o una carta de recomendación de su personal registros.
09.06 a cuestas (que pasa a través de accesos seguros)
Política: Los empleados entrar a un edificio no debe permitir que nadie, personalmente, no sabe que detrás de ellos cuando se ha utilizado un medio seguro, como
como una llave de tarjeta, para poder entrar (a cuestas).
Explicación / Notes. "Los empleados deben entender que no es de mala educación requiere personas desconocidas se autentiquen antes de facilitar su integración en un centro
o acceder a un área segura.
Los ingenieros sociales utilizan con frecuencia una técnica conocida como cuestas, en la que que se encuentran a la espera de otra persona que está entrando en una instalación o zona sensible, y
luego entra con ellos. La mayoría de la gente se siente incómoda retar a otros, suponiendo que son probablemente los empleados legítimos. Otro a cuestas
técnica consiste en realizar varias cajas para que un trabajador desprevenido se abre o se mantiene
la puerta a la ayuda.
9.7 Destrucción documentos sensibles
Política: Los documentos sensibles que descartar debe ser cruzada rallado, los medios de

comunicación
incluidos los discos duros que he contenía información sensible o material
debe ser destruido de acuerdo con los procedimientos establecidos por el grupo
responsable de la seguridad de la información.
Explicación / Notas: trituradoras de papel estándar no adecuada destrucción de documentos;
cross-trituradoras de convertir documentos en pulpa. La mejor práctica de seguridad es
suponer que los principales competidores de la organización se rebuscar
materiales de desecho en busca de cualquier información que pueda ser beneficioso para ellos.
Espías industriales y equipo con regularidad los atacantes obtener información sensible
a partir de materiales arrojados a la basura. En algunos casos, las empresas competidoras se han
conocidos para intentar el soborno de los equipos de limpieza a entregar la basura de la empresa.
En una
ejemplo reciente, un empleado de Goldman Sachs, descubrió los elementos que se utilizaron
en un esquema de información privilegiada de la basura.
8.9 Identificadores personales
Política: Los identificadores personales tales como número de empleado, número de seguro
social,
licencia de conducir, fecha y lugar de nacimiento y nombre de soltera de la madre
nunca debe ser usado como un medio de verificación de la identidad. Estos identificadores no son
secreto y se puede obtener por numerosos medios.
Explicación / Notas: Un ingeniero social puede obtener personal de otras personas
identificadores de un precio. Y de hecho, contrariamente a la creencia popular, cualquier persona
con un crédito
tarjeta y el acceso a Internet pueden obtener estos documentos de identificación personal.
Sin embargo, a pesar del evidente peligro, bancos, empresas de servicios públicos, y la tarjeta de
crédito
las empresas suelen utilizar estos identificadores. Esta es una razón por la que el robo de
identidad
el crimen de más rápido crecimiento de la década.
09.09 Los organigramas
La política ". Datos que aparecen en el organigrama de la empresa no debe ser revelada
a nadie más que empleados de la compañía.
Explicación / Notas: La información incluye la estructura corporativa de los organigramas,
gráficos de la jerarquía, las listas de los departamentos de los empleados, la estructura de
informes, los empleados
nombres, cargos de los empleados, números de contacto interno, el número de empleados, o
información similar.
En la primera fase de un ataque de ingeniería social, el objetivo es reunir a
información sobre la estructura interna de la empresa. Esta información es luego
utiliza para crear una estrategia un plan de ataque. El atacante también puede analizar esta
información para
determinar qué empleados pueden tener acceso a los datos que busca.
Durante el ataque, la información hace que el atacante aparezca como un experto
empleado, por lo que es más probable que va a engañar a su víctima en el cumplimiento.
10.9 La información personal sobre los empleados
Política:. Cualquier solicitud de información de los empleados privados deben ser remitidos
a los recursos humanos.
Explicación / Notas: Una excepción a esta política puede ser el número de teléfono para
un empleado que tiene que ponerse en contacto con respecto a un problema relacionado con el
trabajo o que se
actuando en un rol de guardia. Sin embargo, siempre es preferible obtener el solicitante de
número de teléfono, y que el empleado le llaman o la espalda.
Uso de la computadora
1.10 Introducción de comandos en una computadora
Política: personal de la empresa no debe introducir comandos en una computadora o

Equipo relacionado con la petición de otra persona a menos que el solicitante
se ha comprobado que un empleado del departamento de tecnología de la información.
Explicación / Notas: Una táctica común de los ingenieros sociales es solicitar que un
empleado introducir un comando que realiza un cambio en la configuración del sistema,
permite al atacante acceder al ordenador de la víctima, sin proporcionar
autenticación, o le permite al atacante obtener información que puede ser usado para
facilitar un ataque técnico.
10.02 convenciones internas de nombres
Política: Los empleados no deben revelar los nombres internos de los sistemas informáticos o
bases de datos sin verificación previa de que el solicitante sea empleado por el
de la empresa.
Explicación / Notas: Los ingenieros sociales a veces intento de obtener los nombres de
de los sistemas informáticos de la compañía, una vez que los nombres son conocidos, el atacante
pone una
llamada a la empresa y se hace pasar por un empleado de legítima problemas
acceder o utilizar uno de los sistemas. Al conocer el nombre interno asignado a
el sistema particular, el ingeniero social gana en credibilidad.
10.3 Las solicitudes para ejecutar programas
Política: personal de la empresa nunca debe ejecutar cualquier aplicación informática o
programas, a petición de otra persona a menos que el solicitante ha comprobado
como un empleado del departamento de tecnología de la información.
Explicación / Notas: Las solicitudes para ejecutar programas, aplicaciones, o realizar cualquier
actividad en una computadora debe ser rechazada a menos que el solicitante es positiva
identificado como un empleado en el departamento de tecnología de la información. Si el
solicitud se refiere a revelar información confidencial de cualquier archivo o electrónico
mensaje, en respuesta a la solicitud debe estar de acuerdo con los procedimientos de
la divulgación de información confidencial. Consulte la política de divulgación de la información.
Los atacantes informáticos engañar a la gente en la ejecución de programas que permiten a los
intruso obtener el control del sistema. Cuando un usuario desprevenido se ejecuta un programa
de
plantado por un atacante, el resultado puede dar el acceso de intrusos a la víctima
sistema informático. Otros programas de registro de las actividades del usuario de la computadora
y
devolver esa información al atacante. Mientras que un ingeniero social puede engañar a una
persona
en la ejecución de instrucciones de computadora que puede hacer daño, de carácter técnico
ataque trucos del sistema operativo del equipo en la ejecución de equipo
instrucciones que puede causar el mismo tipo de daño.
10.4 de software para descargar o instalar
Política: El personal de la empresa no debe descargar ni instalar software en el
petición de otra persona, a menos que el solicitante ha comprobado que un empleado
con el departamento de tecnología de la información.
Explicación / Notas: Los empleados deben estar alerta para cualquier petición inusual que
implica ningún tipo de transacción con el Equipo relacionado.
Una táctica común utilizada por los ingenieros sociales es engañar a las víctimas inocentes en
descargar e instalar un programa que ayuda a que el atacante o lograr su
su objetivo de poner en peligro la seguridad de red o computadora. En algunos casos, la
programa de manera encubierta puede espiar a los usuarios o permitir al atacante tomar el control
de la
sistema informático a través del uso de una aplicación de control remoto encubierta.
05.10 contraseñas en texto plano y el correo electrónico
Política: Las contraseñas no se envían a través de correo electrónico a menos codificado.
Explicación / Notas: Si bien es desalentado, esta política puede ser renunciada
por sitios de comercio electrónico en ciertas circunstancias limitadas, tales como:
Enviar las contraseñas a los clientes que se han registrado en el sitio.

Enviar las contraseñas a los clientes que ha perdido u olvidado sus contraseñas.
6.10 relacionados con la seguridad del software
Política: personal de la empresa nunca se debe quitar o deshabilitar antivirus / troyano
Caballo, firewall, o software de otros relacionados con la seguridad sin la aprobación previa de la
Departamento de Informática.
Explicación / Notas: Los usuarios de computadoras a veces desactivar la seguridad relacionados con el software
sin provocación alguna, pensando que aumentarán la velocidad de su ordenador.
Un ingeniero social puede tratar de engañar a un empleado para deshabilitar o quitar
software que se necesita para proteger a la empresa contra las amenazas relacionadas con la seguridad.
10.7 La instalación de los modems
Política .. No módems se pueden conectar a cualquier ordenador hasta la aprobación previa ha
ha obtenido del departamento de TI.
Explicación / Notas:. Es importante reconocer que los módems en los escritorios o
estaciones de trabajo en el lugar de trabajo representa una amenaza de seguridad importante, especialmente si
conectado a la red corporativa. En consecuencia, esta política de control de módem
procedimientos de conexión.
Los hackers utilizan una técnica llamada guerra de marcación para identificar las líneas de módem activo
dentro de un rango de números de teléfono. La misma técnica puede utilizarse para localizar
números de teléfono conectado al módem dentro de la empresa. Un atacante puede
fácilmente comprometer la red corporativa si él o ella identifica a un ordenador
sistema conectado a un módem con software de acceso remoto vulnerables, que
está configurada con una contraseña fácil de adivinar o no una contraseña.
10.8 Módems y la configuración de respuesta automática
Política: M1 escritorios o estaciones de trabajo con la TI-módems aprobados tendrá
módem de respuesta automática característica desactivada para evitar que alguien en la marcación
sistema informático.
Explanation/Notes.- Siempre que sea posible, la información del departamento de tecnología
debe desplegar un conjunto de módems de marcación de salida para aquellos empleados que necesitan para llamar a
sistemas externos ordenador a través de módem.
10.9 herramientas Cracking
Política: Los empleados no descargar ni utilizar ninguna herramienta de software diseñada para derrotar a los mecanismos de protección de software.
Explicación / Notas: El Internet tiene docenas de sitios dedicados al software diseñado
para romper los productos de software shareware y comerciales. El uso de estas herramientas no sólo viola los derechos de autor dueño de un software, sino que también es extremadamente peligroso.
Dado que estos programas provienen de fuentes desconocidas, que pueden contener
código malicioso oculto que pueda causar daño a la computadora del usuario o de una planta
Caballo de Troya que le da el autor del programa de acceso a la computadora del usuario.
10.10 empresa Publicar información en línea
Política: Los empleados no deben divulgar ningún detalle sobre la empresa o de hardware
software en cualquier grupo de noticias público, foro o tablón de anuncios, y no revelará
póngase en contacto con otro tipo de información que, de acuerdo con la política.
Explicación / Notas: Cualquier mensaje enviado a la Usenet, foros en línea,
los tablones de anuncios o listas de correo pueden ser buscados a reunir información de inteligencia sobre un objetivo
empresa o un individuo objetivo. Durante la fase de investigación de la ingeniería social
ataque, el atacante puede buscar en Internet cualquier mensajes que contienen información útil
información sobre la empresa, sus productos o su gente.

Algunos mensajes contienen pedacitos de información muy útil que el atacante
puede utilizar para más de un ataque. Por ejemplo, un administrador de red puede enviar un
pregunta sobre la configuración de filtros de firewall en una determinada marca y modelo de
firewall. Un atacante que descubre este mensaje aprenderá una valiosa información
sobre el tipo y la configuración del firewall companys que le permite
sortear para poder acceder a la red de la empresa.
Este problema puede reducirse o evitarse mediante la aplicación de una política que
permite a los empleados después de que los grupos de noticias de las cuentas anónimas que no
identificar a la compañía de la que provienen. Naturalmente, la política debe
requieren que los empleados no incluir ninguna información de contacto que puede identificar al
de la empresa.
10.11 Los disquetes y otros medios electrónicos
Política: Si los medios de comunicación utilizan para almacenar información del equipo, tales
como disquetes
discos o CD-ROM se han quedado en un área de trabajo o en el escritorio de un empleado, y
que los medios de comunicación es de una fuente desconocida, no debe ser insertado en
cualquier computadora
del sistema.
Explicación / Nota: Un método utilizado por los atacantes para instalar código malicioso es
los programas de lugar en un disquete o CD-ROM y la etiqueta con algo muy
atractivo (por ejemplo, "Datos de nómina de personal - Confidencial"). A continuación, soltar
varios ejemplares en las zonas utilizadas por los empleados. Si un solo ejemplar, se inserta en un
ordenador y los archivos en que se abrió, el código malicioso del atacante se ejecuta.
Esto puede crear una puerta trasera, que se utiliza para comprometer el sistema, o puede
causar otros daños a la red.
10-12 descarte de medios extraíbles
Política: Antes de deshacerse de cualquier medio electrónico que contenía cada vez sensible
información de la compañía, incluso si esa información ha sido eliminada, el elemento se
fondo degaussed o dañados sin posibilidad de recuperación.
Explicación / Nota: Si bien la trituración documentos impresos es común en estos
días, trabajadores de la empresa puede pasar por alto la amenaza de desechar los medios
electrónicos
que contenía datos confidenciales de los ar escarcha. Los atacantes informáticos intento de
recuperar
los datos almacenados en medios electrónicos desechados. Los trabajadores puede suponer que
con sólo
eliminación de archivos, se aseguran de que esos archivos no se pueden recuperar. Esta
presunción
es absolutamente incorrecto y puede causar que la información confidencial de la empresa a caer
en
las manos equivocadas. En consecuencia, todos los medios electrónicos que contiene o
previamente
información contenida no designadas como públicas deben ser limpiados o destruidos
utilizando los procedimientos aprobados por el grupo responsable.
10-13 protegidos con contraseña los protectores de pantalla
Política: Todos los usuarios de computadoras deben establecer una contraseña de protector de
pantalla y la inactividad de la
límite de tiempo de bloquear el equipo después de un cierto período de inactividad.
Explicación / Notas: Todos los empleados son responsables de establecer un protector de
pantalla
contraseña, y establecer el tiempo de inactividad por no más de diez minutos. La
intención de esta política es evitar que cualquier persona no autorizada utilice otro
persona de la computadora. Además, esta política protege a los sistemas de empresa de
informática
de ser de fácil acceso para los extranjeros que han obtenido acceso al edificio.

10.14 La divulgación o el uso compartido de contraseñas declaración
Política: Antes de la creación de una nueva cuenta de equipo, el empleado o contratista deben firmar una declaración por escrito el reconocimiento de que él o ella entiende que las contraseñas nunca deben ser divulgada o compartida con nadie, y que él o ella se compromete a respetar esta política.
Explicación / Notas: El acuerdo también debe incluir un aviso de que la violación de tal acuerdo puede dar lugar a acciones disciplinarias hasta e incluyendo el despido.
El uso de correo electrónico
11.01 adjuntos de correo electrónico
Política: Los archivos adjuntos no se debe abrir el archivo adjunto a menos que se espera que en el curso de los negocios o fue enviado por una persona de confianza.
Explicación / Notas: Todos los adjuntos de correo electrónico deben ser analizados detenidamente. Es posible que
requiere que una notificación previa dada por una persona de confianza que un archivo adjunto de correo electrónico es
se envía antes de que el destinatario abre cualquier archivo adjunto. Esto reducirá el riesgo de atacantes que usan tácticas de ingeniería social para engañar a la gente en la apertura archivos adjuntos.
Un método para comprometer un sistema informático es engañar a un
empleado en ejecutar un programa malicioso que crea una vulnerabilidad, proporcionando el atacante con acceso al sistema. Al enviar un archivo adjunto de correo electrónico que ha código ejecutable o macros, el atacante puede ser capaz de ganar el control del usuario de equipo.
Un ingeniero social puede enviar un archivo adjunto de correo electrónico malicioso, a continuación, llamar y
tratar de convencer al destinatario a abrir el archivo adjunto.
02.11 automático de llamadas a direcciones externas
Política: envío automático de correo electrónico entrante a una dirección de correo electrónico externo
prohibido.
Explicación / Notas: La intención de esta política es evitar que una persona ajena a recepción de correo electrónico enviados a una dirección de correo electrónico interno.
Los empleados de vez en cuando configurar el reenvío de correo electrónico de su correspondencia de entrada a un
dirección de correo electrónico fuera de la empresa cuando se fuera de la oficina. O atacante puede engañar a un empleado en la creación de un correo electrónico interno dirección que reenvía a una dirección fuera de la empresa. El atacante puede
se presentan como una privilegiada por tener una legítima dirección de la empresa de correo electrónico interno y obtener
las personas a la información confidencial por correo electrónico a la dirección de correo electrónico interno.
3.11 Desvío de mensajes de correo electrónico
Política: Toda solicitud formulada por una persona no verificadas para transmitir un mensaje de correo electrónico
mensaje a otra persona sin verificar requiere la verificación de la del solicitante identidad.
11.4 Verificación de correo electrónico
Política: Un mensaje de correo electrónico que parece proceder de una persona de confianza que contiene
una solicitud de información no designada como pública, o para realizar una acción con cualquier equipo de informática, requiere una forma adicional de autenticación. Ver Verificación y Procedimientos de Autorización.
Explicación / Notas: Un atacante puede falsificar un mensaje de correo electrónico y su cabecera, haciendo que parezca como si el mensaje se originó en otra dirección de correo electrónico. Un atacante también puede enviar un mensaje de correo electrónico de un sistema informático

comprometido,
proporcionar autorización para divulgar información falsa o realizar una acción. Incluso examinando el encabezado de un mensaje de correo electrónico que usted no puede detectar mensajes de correo electrónico
enviados desde un sistema informático comprometido interna.
Uso del teléfono
1.12 Participar en las encuestas telefónicas
Política: Los empleados no pueden participar en encuestas por responder a las preguntas de cualquier organización externa o una persona. Dichas solicitudes se deben a que se refiere el departamento de relaciones públicas u otra persona designada.
Explicación / Notas: Un método utilizado por los ingenieros sociales para obtener valiosa información que pueda ser utilizado en contra de la empresa es llamar a un empleado y pretensión de estar haciendo una encuesta. Es sorprendente cómo muchas personas están felices de dar
información sobre la empresa y ellos mismos a los extranjeros cuando creen
que están tomando parte en una investigación legítima. Entre las preguntas inocuas, el persona que llama se inserta una serie de preguntas que el atacante quiere saber. Con el tiempo, dicha información puede ser utilizada para comprometer la red corporativa.
Divulgación 12.2 de números de teléfono interno
Política: Si una persona no verificadas pide a un empleado por su número de teléfono del empleado puede tomar una determinación razonable de si la divulgación es
necesarios para llevar a cabo negocios de la compañía.
Explicación / Notas: La intención de esta política consiste en exigir a los empleados para hacer una
decisión meditada sobre si la divulgación de su extensión telefónica es
es necesario. Cuando se trate de personas que no han demostrado una verdadera necesidad conocer la extensión, lo más seguro es que les obligan a llamar a los principales
número de la compañía de teléfono y transferir.
3.12 Las contraseñas en mensajes de correo de voz
Política:. Dejar mensajes que contienen información de la contraseña en la voz de nadie buzón de correo está prohibido.
Explicación / Notas: Un ingeniero social a menudo puede tener acceso a la cantidad de trabajo buzón de voz, porque es que no estén protegidos con un acceso fácil de adivinar
código. En un tipo de ataque, un intruso informático sofisticado es capaz de crear su propio buzón de voz falsa y persuadir a otro empleado para que deje un mensaje transmisión de información clave. Esta política de derrotas como un ardid.
Fax uso
13-1 faxes retransmisión
Política: No fax puede ser recibido y enviado a otra parte sin
verificación de la identidad del solicitante.
Explicación / Notas: La información se puede engañar a los ladrones de los empleados de confianza en el envío de faxes
información confidencial a una máquina de fax se encuentra en las instalaciones de la empresa. Anterior
al atacante dando el número de fax a la víctima, los teléfonos de un impostor
empleado insospechados, como una secretaria o asistente administrativa, y le pregunta si un documento puede ser enviado por fax a ellos para su posterior recogida. Posteriormente, después de la
empleado desprevenido recibe el fax, el atacante teléfono del empleado
y pide que se envíe el fax a otro lugar, tal vez diciendo que es
necesarios para una reunión urgente. Puesto que la persona le preguntó para transmitir el fax por lo general tiene
no comprensión del valor de la información, él o ella cumple con los
solicitud.
13-2 La verificación de las autorizaciones por fax

Política: Antes de llevar a cabo alguna instrucción recibida por fax, el remitente
debe verificar que un empleado o persona de confianza. Hacer una llamada telefónica
al remitente para verificar la solicitud es generalmente suficiente.
Explicación / Notas: Los empleados deben tener cuidado cuando las solicitudes son inusuales
enviado por fax, como por ejemplo una solicitud para introducir comandos en un equipo o mostrar
de la información. Los datos en el encabezado de un documento de fax pueden ser falsificados
por
cambiar la configuración de la máquina que envía el fax. Por lo tanto el encabezado de un fax
no debe ser aceptada como un medio para establecer la identidad o la autorización.
El envío de información sensible 13-3 por fax
Política: Antes de enviar información sensible por fax a una máquina que se encuentra
en un área accesible a los otros miembros del personal, el remitente deberá transmitir una
portada.
El receptor, al recibir la página, transmite una página en la respuesta, lo que demuestra
que él / ella está físicamente presente en la máquina de fax. El emisor transmite la
fax.
Explicación / Notas: Este proceso de negociación asegura que el remitente que el destinatario
está físicamente presente en el extremo receptor. Además, este proceso verifica que el
recibir el número de teléfono y fax no se ha remitido a otro lugar.
13-4 contraseñas fax prohibido
Política: Las contraseñas no deben ser enviados por fax, bajo ninguna circunstancia.
Explicación / Notas: El envío de la información de autenticación por fax no es seguro.
La mayoría de las máquinas de fax son accesibles a un número de empleados. Además,
dependen de la red telefónica pública conmutada, que puede ser manipulado por el llamado
enviar el número de teléfono del aparato de fax receptor para que el fax se
envíen al atacante a otro número.
El uso de correo de voz
14-1 contraseñas de correo de voz
Política: La voz de contraseñas de correo electrónico no debe ser revelada a nadie por ningún
motivo.
Además, las contraseñas de correo de voz debe ser cambiada cada noventa días o menos.
Explicación / Notas: La información confidencial de la empresa se puede dejar en el correo de voz
mensajes. Para proteger esta información, los empleados deben cambiar su correo de voz
contraseñas con frecuencia, y nunca divulgarlos. Además, los usuarios de correo de voz
No debe usar las contraseñas de voz igual o similar dentro de un correo electrónico de doce
meses
período.
14-2 contraseñas en varios sistemas
Política .. Los usuarios de correo de voz no debe utilizar la misma contraseña en cualquier otro
teléfono o
sistema informático, ya sea interno o externo a la empresa.
Explicación / Notes. "El uso de una contraseña similar o idéntico para varios dispositivos,
tales como correo de voz y la computadora, hace que sea más fácil para los ingenieros sociales
de adivinar todos los
las contraseñas de un usuario después de la identificación de uno solo.
14-3 Configuración de contraseñas de correo de voz
Política: Los usuarios de correo de voz y los administradores deben crear contraseñas de correo
de voz
que son difíciles de adivinar. Ellos no deben estar relacionados de alguna manera a la persona
su uso, o la empresa, y no debe contener un patrón predecible que es
probabilidades de ser adivinada.
Explicación / Notas: Las contraseñas no deben contener dígitos secuenciales o de repetición (es
decir,
1111, 1234, 1010), no debe ser el mismo o en base a la extensión telefónica
número, y no debe estar relacionado con la dirección, código postal, fecha de nacimiento,

matrícula,
número de teléfono, el peso, coeficiente intelectual, u otra información personal predecible.
14-4 Los mensajes de correo marcados como "viejo"
Política: Cuando los mensajes de voz inédita mail no están marcados como nuevos mensajes, el administrador de correo de voz debe ser notificado de una seguridad posible violación y la contraseña del correo de voz debe ser inmediatamente modificado.
Explicación / Notas: Los ingenieros sociales pueden tener acceso a un buzón de voz en un variedad de formas. Un empleado que tenga conocimiento de que los mensajes que no han escuchado, no se anuncian como nuevos mensajes debe asumir que otro
persona ha obtenido acceso no autorizado al buzón de voz y escuchar a la
mensaje en sí.
14-5 externo saludos de correo de voz
Política: La empresa los trabajadores deberán limitar su divulgación de información sobre sus saludo externo de salida en su buzón de voz. Por lo general la información relativa a un la rutina diaria del trabajador o itinerario de viaje no debe ser revelada.
Explicación / Notas: Un saludo externa (jugó para los solicitantes fuera) no debe incluir el apellido, la extensión o razón de la ausencia (por ejemplo, viajes, vacaciones horario o itinerario diario). Un atacante puede usar esta información para desarrollar un historia plausible en su intento de engañar a otros miembros del personal.
14-6 voz patrones de contraseña
Política: Los usuarios de correo de voz no deberá escoger una contraseña en una parte de la contraseña es fija, mientras que otra parte los cambios en un patrón predecible.
Explicación / Notas: Por ejemplo, no utilice una contraseña, como 743501, 743502, 743503, y así sucesivamente, en los dos últimos dígitos corresponden al mes en curso.
14-7 información confidencial o privada
Política: La información confidencial o privada no podrá ser divulgada en un correo de voz mensaje.
Explicación / Notas: El sistema telefónico corporativo suele ser más vulnerables
que los sistemas informáticos de las empresas. Las contraseñas suelen ser una cadena de dígitos,
que limita el número de posibilidades de que un atacante adivine.
Además, en algunas organizaciones, las contraseñas de correo de voz puede ser compartida con secretarios u otro personal administrativo que tienen la responsabilidad de tomar
mensajes para sus directivos. A la luz de lo anterior, no hay información sensible
nunca se debe dejar en el correo de voz de nadie.
Contraseñas
15-1 Teléfono de seguridad
Política: Las contraseñas no será revelada a través del teléfono en cualquier momento.
Explicación / Notas: Los atacantes pueden encontrar la manera de escuchar conversaciones telefónicas,
ya sea en persona oa través de un dispositivo tecnológico.
15-2 contraseñas de la computadora Revelando
Política: Bajo ninguna circunstancia, cualquier usuario de ordenador muestran su contraseña a nadie para ningún propósito sin el consentimiento previo por escrito de la responsable de la información gerente de tecnología.
Explicación / Notas: El objetivo de muchos ataques de ingeniería social consiste en engañar a personas inocentes para que revelen sus nombres de cuenta y
contraseñas. Esta política es un paso crucial en la reducción del riesgo de éxito social ingeniería de los ataques en contra de la empresa. En consecuencia, esta política tiene que ser seguido religiosamente toda la empresa.
15-3 contraseñas de Internet
Política: El personal que nunca se debe utilizar una contraseña que sea igual o similar a una que están utilizando en cualquier sistema corporativo en un sitio de Internet.
Explicación / Notas: operadores de sitios web maliciosos pueden crear un sitio que pretende para ofrecer algo de valor o la posibilidad de ganar un premio. Para registrarse, un

visitante de la página debe introducir una dirección de correo electrónico, nombre de usuario y contraseña. Desde
muchas personas utilizan el inicio de sesión igual o similar información en varias ocasiones, la operador de sitio Web malicioso intenta usar la contraseña elegida y
variaciones de la misma para atacar el sistema del objetivo de trabajo o computadora a su casa. La
equipo visitante el trabajo a veces puede ser identificado por la dirección de correo registrada durante el proceso de registro.

15-4 contraseñas en varios sistemas

Política: El personal de la empresa nunca se debe utilizar la misma contraseña o una similar en más de un sistema. Esta política se refiere a varios tipos de dispositivos (ordenador
o correo de voz); varios lugares de los dispositivos (casa o trabajo), y varios tipos de sistemas, dispositivos (router o firewall), o programas (base de datos o aplicación).

Explicación / Notas: Los atacantes se basan en la naturaleza humana de entrar en equipo sistemas y redes. Ellos saben que, para evitar la molestia de hacer el seguimiento de
varias contraseñas, muchas personas utilizan el mismo o una contraseña similar en todos los sistema tienen acceso. Como tal, el intruso tratará de aprender la contraseña de
un sistema en el que el objetivo tiene una cuenta. Una vez obtenida, es muy probable que esta contraseña o una variación del mismo permitirá el acceso a otros sistemas y dispositivos usado por el empleado.

La reutilización de las contraseñas 15-5

Política: No usuario de la computadora se utilice la misma contraseña o una similar en el mismo período de dieciocho meses.

Explicación / Nota: Si un atacante sea capaz de encontrar la contraseña de un usuario, con frecuencia
el cambio de la contraseña reduce al mínimo el daño que se puede hacer. Haciendo que el contraseña nueva y única de las contraseñas anteriores hace que sea más difícil para el atacante Supongo que.

15-6 patrones Contraseña

La política ". Los empleados no deben seleccionar una contraseña que una parte se mantiene fija, y
otro elemento de los cambios en un patrón predecible.

Explicación / Notas: Por ejemplo, no utilice una contraseña como Kevin01,
Kevin02, Kevin03, y así sucesivamente, en los dos últimos dígitos corresponden a la corriente mes.

Elegir contraseñas 15-7

Política: Los usuarios de computadoras deberían crear o elegir una contraseña que se adhiere a los siguientes requisitos. La contraseña debe:

Tener por lo menos ocho caracteres de longitud para las cuentas de usuario estándar y por lo menos doce
caracteres de longitud para las cuentas privilegiadas.

Contener al menos un número, por lo menos un símbolo (como $, -, I, y), por lo menos un letra en minúscula, y al menos una letra mayúscula (en la medida en que tales
variables son compatibles con el sistema operativo).

No ser cualquiera de los siguientes elementos: palabras en un diccionario en cualquier idioma, cualquier
palabra que está relacionada con la familia de un empleado, los pasatiempos, los vehículos, el trabajo, la matrícula,
número de seguro social, dirección, teléfono, nombre de su mascota, cumpleaños, o frases que contengan esas palabras.

No ser una variación de una contraseña previamente utilizados, con uno de los elementos restantes de la
mismo y otro de los elementos cambiantes, como kevin, kevin 1, kevin2, o kevinjan, kevinfeb.

Explicación / Notas: Los parámetros mencionados anteriormente se produce una contraseña que

sea
difícil para el ingeniero social de adivinar. Otra opción es la consonante-vocal
método, que ofrece una fácil de recordar y de pronunciar la contraseña. A
la construcción de este tipo de consonantes sustituto contraseña para cada letra C y las vocales de la letra V, con la máscara de la "CVCVCVCV". Ejemplos de ello serían
MIXOCASO; CUSOJENA.
15-8 contraseñas Escribir
Política: Los empleados deben escribir las contraseñas sólo cuando se los almacena en una seguro lugar lejos de la computadora u otro dispositivo de contraseña protegida.
Explicación / Notas: Los empleados no se animan a escribir alguna vez
contraseñas. Bajo ciertas condiciones, sin embargo, puede que sea necesario, para
ejemplo, para un empleado que tiene varias cuentas en el ordenador diferentes
sistemas. Las contraseñas escritas deben ser asegurados en un lugar seguro, lejos de
el ordenador. Bajo ninguna circunstancia puede ser una contraseña almacenada en el
teclado o el adjunto a la pantalla del ordenador.
15-9 contraseñas de texto sin formato en archivos de computadora
Política: contraseñas de texto no se pueden guardar en cualquier archivo de computadora o almacenadas en
texto llamado pulsando una tecla de función. Cuando sea necesario, las contraseñas se pueden guardar
utilizando una herramienta de cifrado aprobados por el departamento de TI para evitar cualquier divulgaciones no autorizadas.
Explicación / Notas: Las contraseñas pueden ser fácilmente recuperados por un atacante, si se almacena en
sin cifrar en los archivos de datos de computadora, archivos por lotes, las teclas de función de terminal, inicie sesión
archivos, macros o programas de secuencias de comandos, o cualquier archivo de datos que contienen las contraseñas
Los sitios FTP.
POLÍTICAS para teletrabajadores
Los teletrabajadores se encuentran fuera del firewall de la empresa, y por lo tanto más vulnerables
a los ataques. Estas políticas le ayudará a evitar que los ingenieros sociales el uso de la empleados teletrabajadores como puerta de entrada a sus datos.
16-1 Los clientes ligeros
Política: Todo el personal de la empresa que hayan sido autorizados a conectarse a través de control remoto
el acceso se utilice un cliente ligero para conectar a la red corporativa.
Explicación / Notas: Cuando un atacante analiza una estrategia de ataque, él o ella
tratar de identificar a los usuarios que acceden a la red corporativa desde ubicaciones externas. Como
teletrabajadores tales, son los principales objetivos. Sus equipos son menos propensos a tener estrictos controles de seguridad, y puede ser un punto débil que pueda comprometer la
red corporativa.
Cualquier ordenador que se conecta a una red de confianza puede ser una trampa explosiva con capturadores de teclado, o su conexión autenticada pueden ser secuestrados. Un cliente ligero estrategia se puede utilizar para evitar problemas. Un cliente ligero es similar a una estación sin estación de trabajo o un terminal tonto, el equipo remoto no tiene almacenamiento
capacidades, sino que el sistema operativo, programas de aplicación, y todos los datos
residen en la red corporativa. Acceso a la red a través de un cliente ligero
reduce sustancialmente el riesgo planteado por los sistemas sin parches, operativo obsoleto sistemas y códigos maliciosos. En consecuencia, la gestión de la seguridad de los teletrabajadores es eficaz y más fácil por la centralización de los controles de seguridad.
En lugar de confiar en el trabajador a distancia sin experiencia para gestionar adecuadamente cuestiones de seguridad, estas responsabilidades es mejor no con el sistema de formación,

de la red, o los administradores de seguridad.
16-2 de software de seguridad para los sistemas informáticos teletrabajador
Política: Cualquier sistema informático externo que se utiliza para conectarse a la empresa
la red debe tener un software antivirus, software anti-troyano y un personal
firewall (hardware o software). Archivos del antivirus y anti-troyanos patrón debe ser
actualizado por lo menos una vez por semana.
Explicación / Notas: Por lo general, los teletrabajadores no es experto en materia de seguridad relacionadas con el
temas, y se puede "o por negligencia dejan su sistema informático y la
red empresarial abierta al ataque. Teletrabajadores por lo tanto, plantean una grave
riesgos de seguridad si no están debidamente capacitados. Además de instalar un antivirus
anti-Trojan Caballo de software de protección contra código malicioso, un firewall es
necesarias para bloquear a cualquier usuario hostil de obtener acceso a cualquier servicio
habilitado en el sistema del teletrabajador es.
El riesgo de no implementar las tecnologías de seguridad mínimas para evitar maliciosos
código de propagación no puede ser subestimado, como un ataque a Microsoft
prueba. Un sistema informático de un teletrabajador Microsoft, utilizado para
conectarse a la red corporativa de Microsoft, se infectaron con un caballo de Troya
del programa. El intruso o intrusos fueron capaces de utilizar el teletrabajador es de confianza
conexión a la red de desarrollo de Microsoft para robar fuente de desarrollo
código.
POLÍTICAS DE RECURSOS HUMANOS
Los departamentos de recursos humanos tienen una carga especial para proteger a los empleados de
los que tratan de descubrir información personal a través de su lugar de trabajo. HR
profesionales también tienen la responsabilidad de proteger su empresa de las acciones
de ex empleados descontentos.
17-1 empleados que se van
Política: Siempre que una persona empleada por la empresa deja o es despedido,
Recursos Humanos inmediatamente debe hacer lo siguiente:
Quitar lista de la persona del empleado en línea / guía telefónica y
desactivar o reenviar sus mensajes de voz;
Notificar al personal en la construcción de las entradas o pasillos de la compañía, y
Añadir el nombre del empleado a la lista de salida de los empleados, que deberá ser enviado por correo electrónico
a todo el personal de no menos de una vez a la semana.
Explicación / Notas: Los empleados que están estacionados en entradas de edificios debe ser
notificado para evitar que un ex empleado de volver a entrar al local. Por otra parte,
notificar a otros miembros del personal pueden prevenir el ex-empleado de éxito
haciéndose pasar por un empleado activo y engañar al personal a tomar algunas
la acción perjudicial para la sociedad.
En algunas circunstancias, puede ser necesario exigir a todos los usuarios dentro de la
ex empleado del departamento de cambiar sus contraseñas. (Cuando yo era
terminado de GTE únicamente a causa de mi reputación como un hacker, de la empresa
exigió a todos los empleados de la empresa a cambiar su contraseña.)
17-2 departamento de TI de la notificación
Política: Siempre que una persona empleada por la empresa deja o es despedido,
Recursos Humanos debe notificar inmediatamente a la tecnología de la información
departamento para desactivar las cuentas del ex empleado de la computadora, incluyendo cualquier
cuentas utilizadas para el acceso a la base de datos, dial-up o acceso a Internet de forma remota
lugares.
Explicación / Notas: Es esencial para deshabilitar el acceso a cualquier trabajador a todos los ex-
sistemas informáticos, dispositivos de red, bases de datos, o cualquier otra relacionadas con la
informática

dispositivos inmediatamente después de la terminación. De lo contrario, la empresa podrá salir de la
puerta abierta para un empleado descontento para acceder a los sistemas de empresa de informática
y causar daños significativos.
17-3 La información confidencial utilizada en el proceso de contratación
Política: Los anuncios publicitarios y otras formas de solicitud pública de candidatos para cubrir ofertas de trabajo deberá, en la medida de lo posible, evitar la identificación de hardware de la computadora
y el software utilizado por la empresa.
Explicación / Notas: Los administradores y personal de recursos humanos sólo debe divulgar la información relacionada con la empresa de hardware y software que se razonablemente necesaria para obtener hojas de vida de los candidatos calificados.
Intrusos equipo lee los periódicos y comunicados de prensa de la compañía, y la visita
Los sitios de Internet, para encontrar ofertas de trabajo. A menudo, las compañías revelar demasiado
información sobre los tipos de hardware y software que se utiliza para atraer a posibles
los empleados. Una vez que el intruso tenga conocimiento de los sistemas de información del objetivo,
está armado para la siguiente fase de ataque. Por ejemplo, al saber que un
empresa en particular utiliza el sistema operativo VMS, el atacante puede colocar
pretexto de llamadas para determinar la versión de lanzamiento, y luego enviar una emergencia falsa
parche de seguridad se hacen aparecer como si proviniera de los desarrolladores de software. Una vez que el
parche está instalado, el atacante se in
17-4 información personal de los empleados
Política: El departamento de recursos humanos nunca deben dar información personal
acerca de cualquier empleado actual o anterior, contratista, consultor, trabajo temporal,
o interno, con excepción de previo y expreso consentimiento por escrito del empleado o humanos gerente de recursos.
Explicación / Notas: Head-hunters, los investigadores privados, y los ladrones de identidad
objetivo de información de los empleados privados, tales como el número de empleados, la seguridad social
números, fechas de nacimiento, historial de salarios, los datos financieros, incluyendo el depósito directo
información, y la salud relacionados con la información de beneficios. El ingeniero social puede obtener esta información con el fin de hacerse pasar por el individuo. Además,
revelar los nombres de los nuevos empleados puede ser muy valiosa a la información
los ladrones. Los nuevos contratados son propensos a cumplir con cualquier solicitud de las personas con
la antigüedad o en una posición de autoridad, o cualquier persona que dice ser de las empresas la seguridad.
17-5 verificación de antecedentes
Política: Una revisión de antecedentes se debería exigir a todos los nuevos empleados, contratistas,
consultores, trabajadores temporales o en prácticas antes de una oferta de empleo o
el establecimiento de una relación contractual.
Explicación / Notas: Debido a consideraciones de costo, el requisito de
verificación de antecedentes se puede limitar a las posiciones específicas de la confianza. Nótese, sin embargo,
que cualquier persona que tenga acceso físico a las oficinas de las empresas puede ser un amenaza potencial. Por ejemplo, los equipos de limpieza tienen acceso a las oficinas de personal, que les da acceso a ningún sistema informático se encuentra allí. Un atacante con
el acceso físico a un equipo se puede instalar un capturador de teclado de hardware en menos de

un minuto para capturar contraseñas.
Intrusos informáticos a veces hacer el esfuerzo de obtener un empleo como un medio de acceder a los sistemas informáticos de la compañía objetivo y de las redes. Un atacante puede obtener el nombre del contratista de limpieza de la compañía llamando al el empleado responsable de la empresa objetivo, que dice ser de una limpieza empresa en busca de su negocio, y luego obtener el nombre de la empresa que actualmente se prestan tales servicios.

POLÍTICAS DE SEGURIDAD FÍSICA

Aunque los ingenieros sociales tratan de evitar a aparecer en persona en un lugar de trabajo que desea orientar su campaña, hay momentos en los que se viole su espacio. Estas políticas le ayudará a mantener su espacio físico seguro de la amenaza.

18-1 de identificación para los empleados que no

Política: La gente de entrega y otros empleados que no deben entrar en la empresa locales sobre una base regular deben tener un distintivo especial u otra forma de identificación de acuerdo con la política establecida por la seguridad corporativa.

Explicación / Notas: los empleados que necesitan para no entrar en el edificio con regularidad (por ejemplo, para hacer las entregas de alimentos o bebidas en la cafetería, o reparación de las fotocopiadoras o los teléfonos de instalación) debe emitir una forma especial de insignia de identificación de la empresa para este fin. Otros que necesitan para entrar en sólo de vez en cuando o en una sola vez deben ser tratados como visitantes y se debe acompañados en todo momento.

18-2 visitantes de identificación

Política: Todos los visitantes deben presentar una licencia de conducir válida o cualquier otra imagen
de identificación para ser admitido en las instalaciones.

Explicación / Notas: El personal de seguridad o recepcionista debe hacer una fotocopia de el documento de identificación antes de emitir una tarjeta de visitante. La copia debe ser mantuvo con el registro de los visitantes. Por otra parte, la información de identificación puede registrado en el registro de los visitantes por el recepcionista o el guardia, los visitantes no deben ser
permite escribir la información de identificación propio.

Ingenieros sociales que luchan por ganar la entrada a un edificio siempre va a escribir información falsa en el registro. A pesar de que no es difícil obtener una identificación falsa y conocer el nombre de un empleado que él o ella puede decir que es de visita, que exige que el empleado responsable debe registrar la entrada añade un nivel de seguridad a la proceso.

18-3 visitantes Acompañamiento

Política: Los visitantes deben ser escoltados o en compañía de un empleado en todo momento.

Explicación / Notas:. Un truco popular de los ingenieros sociales es el de organizar a visitar a un empleado de la compañía (por ejemplo, visitar a un ingeniero de producto en el pretexto de ser el empleado de un socio estratégico). Después de haber sido acompañado a la primera reunión, el ingeniero social asegura a su anfitrión que no puede encontrar su propia camino de vuelta al vestíbulo. De este modo se obtiene la libertad para vagar por el edificio y, posiblemente, tener acceso a información sensible.

18-4 placas temporales

Política: Los empleados de la compañía de otro lugar-que no la tienen
tarjetas de empleado con ellos deben presentar una licencia de conducir válida o cualquier otra imagen
Identificación y se emitirá una tarjeta de visitante temporal.

Explicación / Notas: Los atacantes a menudo se hacen pasar por empleados de una oficina diferente o
sucursal de una empresa para ganar la entrada a una empresa.

18-5 de evacuación de emergencia

Política: En cualquier situación de emergencia o de simulacro, personal de seguridad debe asegurarse de que

todo el mundo ha evacuado las instalaciones.
Explicación / Notas: El personal de seguridad debe comprobar que no existen rezagados que pueden ser
dejó en los baños o áreas de oficina. Según lo autorizado por el departamento de bomberos o otra autoridad a cargo de la escena, la fuerza de seguridad tiene que estar alerta
para cualquier persona de salir del edificio poco después de la evacuación.
Espías industriales o intrusos informáticos sofisticados pueden causar una desviación de la ganancia
acceso a un edificio o un lugar seguro. Una derivación se utiliza para liberar un inofensivo químicos conocidos como butil mercaptano en el aire. El efecto es la creación de la impresión de que hay una fuga de gas natural. Una vez que el personal de iniciar una evacuación procedimientos, el atacante utiliza esta atrevida diversión para robar información o de que acceder a los sistemas informáticos de la empresa. Otra táctica usada por la información implica permanecer detrás de los ladrones, a veces en un baño o un armario, en el momento de un simulacro de evacuación previsto, o después de salir una bengala de humo u otro dispositivo
a causa de una evacuación de emergencia.
18-6 Los visitantes en la sala de correo electrónico
Política: No se debe permitir a los visitantes en la sala de correo sin la supervisión de un trabajador de la empresa.
Explicación / Notas: La intención de esta política es evitar que una persona ajena a el intercambio, el envío, o el robo de correo dentro de la compañía.
18-7 números de placas de vehículos
Política: Si la empresa cuenta con un aparcamiento vigilado, el personal de seguridad deberá registro de vehículos
números de matrícula de cualquier vehículo de entrar en la zona.
18-8 contenedores de basura
Política: contenedores de basura deben permanecer en las instalaciones de la empresa en todo momento y
debe ser inaccesible al público.
Explicación / Notas: los atacantes informáticos y espías industriales puede obtener valiosa información de los contenedores de basura de la empresa. Los tribunales han sostenido que la basura es
consideran propiedad en abandono legal, por lo que el acto de basurero de buceo es perfectamente
legal, siempre y cuando los receptáculos de basura están en la propiedad pública. Por esta razón, es
importante que los recipientes de basura se encuentra en
propiedad de la compañía, donde la compañía tiene el derecho legal de proteger a los contenedores
y su contenido.
POLÍTICAS PARA RECEPCIONISTAS
Los recepcionistas están a menudo en primera línea cuando se trata de lidiar con la social ingenieros, sin embargo, rara vez se da la formación suficiente seguridad para reconocer y detener
un invasor. Instituto de estas políticas para ayudar a su recepcionista proteger mejor a su empresa y sus datos.
19-1 directorio interno
Política: La revelación de información en el directorio interno de la empresa debe ser limitado a las personas empleadas por la empresa.
Explicación / Notas: Todos los títulos de los empleados, los nombres, números de teléfono y direcciones
contenidos en el directorio de la empresa deben ser considerados internos
información, y sólo debe ser revelada de acuerdo con las políticas relacionadas con la clasificación de los datos y la información interna.

Además, cualquier persona que llama debe tener el nombre o la extensión de la persona que están tratando de ponerse en contacto. Aunque la recepcionista puede poner una llamada a través de un
persona cuando una persona no sabe la extensión, diciendo a la persona que llama número de extensión debe ser prohibido. (Para aquellos curiosos que la gente siga por ejemplo, puede experimentar este procedimiento llamando a cualquier gobierno de los EE.UU. la agencia y pedir al operador que facilite una extensión.)

19-2 Los números telefónicos de los departamentos específicos / grupos

Política: Los empleados no deberán proporcionar los números de teléfono directo para la empresa help desk, telecomunicaciones departamento, las operaciones de computadora, o sistema de personal del administrador, sin verificar que el solicitante tiene una necesidad legítima ponerse en contacto con estos grupos. La recepcionista, al transferir una llamada a estos grupos, debe anunciar el nombre del llamante.

Explicación / Notas: Aunque algunas organizaciones pueden encontrar esta política demasiado restrictiva, esta regla se hace más difícil para un ingeniero social para hacerse pasar por un empleado por engañar a los demás empleados en la transferencia de la llamada de su de extensión (que en algunos sistemas de teléfono hace que la llamada a comparecer a su origen dentro de la empresa), o demostrar conocimiento de estas extensiones a la víctima con el fin de crear un sentido de autenticidad.

19-3 transmisión de información

Política: los operadores telefónicos y los recepcionistas no deben tomar mensajes o relé información en nombre de cualquiera de las partes, personalmente, no sabe que es un activo de los empleados.

Explicación / Notas: Los ingenieros sociales son expertos en engañar a los empleados sin querer dar fe de su identidad. Un truco de ingeniería social para obtener el número de teléfono de la recepcionista y, con un pretexto, pedir a la recepcionista para tener los mensajes que puedan venir por él. Luego, durante una llamada a la víctima, el atacante se hace pasar por un empleado, le pide información sensible o realizar una tarea, y le da el número de la centralita como un número de devolución de llamada. El atacante más tarde vuelve a llamar a la recepcionista y se le da ningún mensaje de la izquierda para
él por la víctima inocente.

19-4 artículos que se dejen para la recolección

Política: Antes de lanzar cualquier objeto a un mensajero o cualquier otra persona sin verificar, la recepcionista o guardia de seguridad deben obtener una identificación con foto y entrar en el información de identificación en el registro de recolección como lo requiere la aprobación procedimientos.

Explicación / Notes. "Una de las tácticas de ingeniería social para engañar a un empleado en la liberación de materiales sensibles a otro empleado, supuestamente autorizado por dejar a estos materiales en el recepcionista o el mostrador de recepción para su recogida. Naturalmente, el guardia de seguridad recepcionista o asume que el paquete está autorizado para su liberación. El ingeniero social o bien se presenta a sí mismo o tiene un mensajero servicio de recoger el paquete.

POLÍTICAS PARA EL GRUPO DE INFORMES DE INCIDENTES

Cada empresa debe crear un grupo central que debe ser notificado cuando cualquier forma de ataque a la seguridad de la empresa se identifica. Lo que sigue son algunas directrices para la creación y estructuración de las actividades de este grupo.

Incidente 20-1 grupo de informes

Política: Un individuo o grupo debe ser designado y los empleados deben ser instruidos para reportar incidentes de seguridad para ellos. Todos los empleados deben estar provistos
con la información de contacto del grupo.

Explicación / Notas: Los empleados deben entender la forma de identificar una amenaza a la seguridad,
y ser capacitados para informar de cualquier amenaza a un grupo de notificación de incidentes

específicos. También es
importante que una organización establecer procedimientos específicos y la autoridad para
un grupo para actuar cuando una amenaza se informa.
20-2 Los ataques en curso
Política: Cada vez que el grupo de notificación de incidentes ha recibido informes de un curso
ataque de ingeniería social que se iniciará inmediatamente los procedimientos de alerta
todos los empleados asignados a los grupos objetivo.
Explicación / Notas: El grupo de notificación de incidentes o gerente responsable debe
También tomar una determinación sobre si se debe enviar una alerta en toda la compañía. Una vez que el
persona responsable o un grupo tiene una creencia de buena fe que un ataque puede ser en
el progreso, la mitigación del daño debe ser una prioridad, notificando la empresa
personal para estar en guardia.
La seguridad de un vistazo
Las listas y las tablas de referencia de la versión siguiente proporcionar una rápida social
métodos de ingeniería en los Capítulos 2 a 14, y los procedimientos de verificación
detallada en el capítulo 16. Modificar esta información para su organización, y hacer
a disposición de los empleados para referirse a cuando una cuestión de seguridad de información surge.
IDENTIFICACIÓN DE UN ATAQUE DE SEGURIDAD
Estas tablas y listas de verificación le ayudará en la detección de un ataque de ingeniería social.
El ciclo de la Ingeniería Social
Proceso / descripción
Investigación
Puede incluir información de fuente abierta, tales como la SEC y los informes anuales,
folletos de marketing, las solicitudes de patentes, recortes de prensa, revistas del sector,
Contenido del sitio web. También basurero de buceo.
El desarrollo de una relación de confianza
El uso de información privilegiada, tergiversación de identidad, citando los conocidos
víctima, la necesidad de ayuda, o la autoridad.
La explotación de la confianza
Pedir información o una acción por parte de la víctima. En picadura inversa,
manipular la víctima para pedir atacante en busca de ayuda.
Utilizar la información
Si la información obtenida es sólo un paso a la meta final, vuelve atacante antes
pasos en el ciclo hasta que se alcance el objetivo.
Métodos comunes de ingeniería social
Haciéndose pasar por un compañero de trabajo
Haciéndose pasar por un empleado de una aplicación de proveedor, empresa asociada, o la ley
Haciéndose pasar por alguien con autoridad
Haciéndose pasar por un nuevo empleado solicitando ayuda
Haciéndose pasar por un vendedor o el fabricante sistemas de llamada a ofrecer una revisión del sistema o
actualización
Ofreciendo ayuda si surge algún problema, entonces lo que se produce el problema, lo que
la manipulación de la víctima para pedir ayuda
Envío de software libre o parche para las víctimas de instalar
El envío de un caballo de virus o un troyano en un archivo adjunto de correo electrónico
El uso de un falso pop-up ventana pidiendo que ingrese de nuevo o firmar con
contraseña
La captura de las pulsaciones de teclado víctima con el sistema informático consumible o
programa
Dejando a un disquete o CD en todo el lugar de trabajo con el software malicioso en el que
Usando la jerga de información privilegiada y la terminología para ganarse la confianza
Ofreciendo un premio por registrarse en un sitio web con nombre de usuario y contraseña

Borrado de un documento o archivo en la sala de la empresa de correo para la entrega intraoffice
Modificación de la máquina de fax de dirigirse a parecen provenir de un lugar interno
Pidiendo recepcionista para recibir luego reenviar un fax
Pedir que un archivo sea transferido a un lugar aparentemente interno
Obtención de un buzón de voz configurado para devolver la llamada perciben como atacante interno
Haciéndose pasar por las oficinas remotas y pidiendo acceso al correo electrónico a nivel local
Señales de advertencia de un ataque
La negativa a dar de nuevo llamar al número de
Fuera de lo común solicitud
Afirmación de la autoridad
Hace hincapié en la urgencia
Amenaza a las consecuencias negativas del incumplimiento
Muestra molestia cuando se le preguntó
Nombre cayendo
Elogios o adulaciones
Coqueteando
Los objetivos comunes de los ataques
Tipo de destino / EJEMPLOS
Sin darse cuenta del valor de la información
Recepcionistas, telefonistas, auxiliares administrativos, guardias de seguridad.
Privilegios especiales
Mesa de ayuda o soporte técnico, administradores de sistemas, operadores de computadoras, los administradores del sistema telefónico.
Fabricante / proveedor
Hardware, los fabricantes de software, sistemas de correo de voz vendedores.
Departamentos específicos
Contabilidad, recursos humanos.
Factores que las empresas sean más vulnerables a los ataques
Gran número de empleados
Varias instalaciones
Información sobre el paradero de los empleados a la izquierda en los mensajes de correo de voz
La información del teléfono de extensión disponible
La falta de capacitación de seguridad
Falta de un sistema de clasificación de datos
No hay reporte de incidentes / plan de respuesta en el lugar
VERIFICACIÓN DE LA CLASIFICACIÓN DE DATOS D
Estas tablas y gráficos le ayudarán a responder a las solicitudes de información o acción que pueden ser ataques de ingeniería social.
Verificación de identidad de Procedimiento
Proceso / descripción
Identificador de llamadas
Verifique llamada es interna, y el número de nombre o la extensión coincide con la identidad de la persona que llama.
De devolución de llamada
Busque en el directorio de la empresa solicitante y volver a llamar la extensión de la lista.
Avalando
Pregunte a un empleado de confianza para dar fe de la identidad del solicitante.
Secreto compartido común
Solicitud de toda la empresa secreto compartido, como una contraseña o código al día.
Supervisor o gerente
Supervisor inmediato los empleados de contacto y la solicitud de verificación de la identidad y situación laboral.
Correo electrónico seguro
Solicitud de un mensaje firmado digitalmente.

Reconocimiento de voz personal
Para un interlocutor sabe que los empleados, validar con la voz de quien llama.
Contraseñas dinámicas
Verificar frente a una solución contraseña dinámicos como Secure ID o fuertes otros autenticación de dispositivos.
En persona
Requieren solicitante de presentarse en persona con una credencial de empleado o de otro tipo identificación.
Verificación de Procedimiento Situación laboral
Proceso / descripción
Directorio de empleados cheque
Solicitante compruebe que está en la lista en el directorio en línea.
Solicitante de verificación de gerente
Llame al solicitante gerente de utilizar el número de teléfono que aparece en el directorio de la empresa.
Solicitante del departamento o grupo de trabajo de verificación
Llame al departamento solicitante o el grupo de trabajo y determinar que la solicitante es todavía empleados por empresa.
Procedimiento para determinar la necesidad de saber
Proceso / descripción
Consulte la marea empleo / trabajo / lista de responsabilidades
Revise las listas publicadas de que los empleados tienen derecho a determinadas clasificado de la información.
Obtener autorización del gerente
Comuníquese con su gerente o el director de la solicitante, la autoridad para cumplir con la solicitud.
Obtener autorización del propietario o la persona designada información
Solicitar al dueño de la información en caso de solicitante haya una necesidad de saber.
Obtener la autorización con una herramienta automatizada
Compruebe la base de datos de software propietario para el personal autorizado.
Criterios para la Verificación de personas no empleadas
CRITERIO / ACCIÓN
Relación
Verificar que la empresa solicitante tiene un proveedor, socio estratégico, o de otro tipo adecuadas
relación.
Identidad
Verificar la identidad del solicitante y la situación laboral en la firma de vendedor / socio.
De confidencialidad
Verificar que el solicitante ha firmado un acuerdo de confidencialidad en el archivo.
Acceso
Remitir la solicitud a la administración cuando la información se clasifica por encima de Interno.
Datos de la Clasificación
CLASIFICACIÓN / DESCRIPCIÓN / PROCEDIMIENTO
Público
Pueden ser libremente a disposición del público
No hay necesidad de verificar.
Interno
Para su uso dentro de la empresa
Verificar la identidad del solicitante como empleado activo o verificar el acuerdo de confidencialidad
en el archivo y la aprobación de la gestión de los empleados no.
De clasificación de datos (continuación)
CLASIFICACIÓN / DESCRIPCIÓN / PROCEDIMIENTO

Privado
Información de carácter personal para uso exclusivo dentro de la organización
Verificar la identidad del solicitante como empleado activo o sólo dentro de los empleados no con la organización, la autorización. Consulte con el departamento de recursos humanos
revelar información privada a los empleados autorizados o solicitantes externos.
Confidencial
Compartida sólo con las personas con una necesidad absoluta de saber dentro de la organización
Verificar la identidad del solicitante y la necesidad de saber a partir de la información calificada
Propietario. Versión sólo con el consentimiento previo por escrito de gerente, o la información
Propietario o la persona designada. Compruebe si hay acuerdo de confidencialidad en el archivo.
Sólo
gestión de personal puede revelar a personas no empleadas por la empresa.
FUENTES
CAPÍTULO 1
BloomBecker, Buck. 1990. Delitos espectacular Equipo: qué son y
¿Cómo cuestan la mitad American Business mil millones de dólares Dar. Irwin
Publicación profesional.
Littman, Jonathan. 1997. El juego de Fugitivos: En línea con Kevin Mitnick. Poco
Brown & Co.
Penenberg, Adam L. 19 de abril 1999. "La demonización de un hacker". Forbes.
CAPÍTULO 2
La historia de Stanley Riflдn se basa en las siguientes cuentas:
Equipo Insituto de Seguridad. Sin fecha. "Las pérdidas financieras debido a las intrusiones de Internet,
robo de secretos comerciales y otros delitos cibernéticos se disparan. "Comunicado de prensa.
Epstein, Edward
Jay. Sin publicar. "El diamante de la invención." Holwick, Rev. David. Inédito
cuenta.
El propio Sr. Rifkin fue muy amable en el reconocimiento de que las cuentas de su hazaña difieren porque ha protegido su anonimato al negarse a ser entrevistado.
CAPÍTULO 16
Cialdini, Robert B. 2000. Influencia: Ciencia y Práctica, 4 ª edición. Allyn y
Bacon.
Cialdini, Robert B. febrero de 2001. "La ciencia de la persuasión." Científico
Estadounidense. 284:2.
CAPÍTULO 17
Algunas políticas en este capítulo se basan en las ideas contenidas en: Madera, Charles Cresson. 1999. "Políticas de Seguridad de la Información Made Easy". Software de base.
Reconocimientos
DE Kevin Mitnick
La verdadera amistad se ha definido como una mente en dos cuerpos, no muchas personas en la vida de alguien puede ser llamado un verdadero amigo. Jack Biello era un amor y cariño persona que habló en contra de los malos tratos extraordinarios que he sufrido en el manos de los periodistas poco éticos y fiscales exceso de celo del gobierno. Él era un voz clave en el movimiento Free Kevin y un escritor que tuvo una extraordinaria talento para escribir artículos convincente exposición de la información que el gobierno no quiere que usted sepa. Jack siempre estaba allí para hablar sin miedo en mi nombre y para trabajar junto con mi preparación de discursos y artículos, y, en un momento dado, me representaba como un enlace con los medios.
Este libro está dedicado con amor por lo tanto, a mi querido amigo Jack Biello, cuya muerte reciente de cáncer de la misma manera que terminó el manuscrito me ha dejado sensación de un gran sentido de pérdida y tristeza.
Este libro no habría sido posible sin el amor y el apoyo de mi
de la familia. Mi madre, Shelly Jaffe, y mi abuela, Reba Vartanian, han
me ha dado amor y apoyo incondicional durante toda mi vida. Me siento muy afortunado de

han planteado como una madre amorosa y dedicada, que también considero mi mejor amigo. Mi abuela ha sido como una mañana de mi segundo, dándome con la misma educación y el amor que sólo una madre puede dar. Como el cuidado y personas compasivas, me han enseñado los principios de preocuparse por los demás y echando una mano a los menos afortunados. Y o, imitando el patrón de dar y cuidar, que en cierto sentido, seguir los caminos de sus vidas. Espero que perdón por poner en segundo lugar durante el proceso de escribir este libro, dejando pasar oportunidades de verlos con la excusa de trabajo y los plazos para cumplir. Este libro no habría sido posible sin su continuo amor y el apoyo que siempre va a tener cerca de mi corazón.

¡Cómo me gustaría que mi padre, Alan Mitnick, y mi hermano, Adam Mitnick, habría vivido lo suficiente para romper una botella de champán conmigo en el día de esta El primer libro aparece en una librería. Como vendedor y propietario de un negocio, mi padre me enseñó muchas de las cosas buenas que nunca voy a olvidar. Durante los últimos meses de la vida de mi papá tuve la suerte de poder estar a su lado para consolarlo lo mejor que pude, pero fue una experiencia muy dolorosa de la que todavía no he recuperado.

Mi tía Chickie Leventhal siempre tendrá un lugar especial en mi corazón; a pesar de que estaba decepcionado con algunos de los errores estúpidos que he hecho, sin embargo, ella siempre estaba allí para mí, que ofrece su amor y apoyo. Durante mi devoción intensa a escribir este libro, he sacrificado muchas oportunidades para unirse a ella, mi primo, Mitch Leventhal, y su novio, el doctor Robert Berkowitz, por nuestra celebración semanal de Shabat.

También tengo que dar mi más sincero agradecimiento al novio de mi madre, Steven Knittle, que estaba allí para llenar para mí y para ofrecer a mi madre con amor y apoyo.

El hermano de mi padre claramente merece muchos elogios, se podría decir que heredé de mi oficio de la ingeniería social del tío Mitchell, que sabía cómo manipular el mundo y su gente de manera que yo ni siquiera la esperanza de entender, mucho menos maestro. Por suerte para él, nunca tuvo mi pasión por la tecnología informática durante los años que utilizó su personalidad encantadora influenciar a nadie que él deseaba. Él siempre tendrá el título de ingeniero de Gran Maestro social.

Y mientras escribo estos agradecimientos, me doy cuenta de que tanta gente para agradecer y expresar su agradecimiento a la oferta de su amor, la amistad y apoyo. Yo No puedo empezar a recordar los nombres de todas las personas amables y generosas que he se reunieron en los últimos años, pero basta con decir que se necesita una computadora para almacenarlas todos. Ha habido tanta gente de todo el mundo que han escrito a me con palabras de aliento, elogios y apoyo. Estas palabras han significado un mucho para mí, sobre todo en los momentos que más lo necesitaba.

Estoy especialmente agradecido a todos mis seguidores que estuvo a mi lado y pasó su valioso tiempo y energía correr la voz a cualquiera que quisiera escuchar, manifestar su preocupación y oposición sobre mi trato injusto y la hipérbole de la creado por aquellos que buscaban sacar provecho de la "El mito de Kevin Mitnick."

He tenido la extraordinaria fortuna de estar asociado con el autor más vendido Bill Simon, y hemos trabajado diligentemente juntos a pesar de nuestras diferentes los patrones de trabajo. Bill está muy organizado, se levanta temprano y trabaja en una deliberada y bien planificada de estilo. Estoy agradecido de que Bill tuvo la amabilidad de dar cabida a mi tarde en la noche el horario de trabajo. Mi dedicación a este proyecto y largas horas de trabajo me mantuvo despierto hasta bien entrada la mañana que entraba en conflicto regular con Bill horario de trabajo.

No sólo estaba la suerte de estar asociado con alguien que podría transformar mis ideas en frases dignas de un lector sofisticado, pero también es Bill (sobre todo) una muy

el hombre paciente que aguantar a mi estilo de programador de centrarse en los detalles.
De hecho nos hizo pasar. Sin embargo, quiero pedir disculpas
a Bill en estos reconocimientos que siempre se arrepentirá de ser el uno, porque
de mi orientación a la precisión y el detalle, que le hizo llegar tarde a un plazo
para la primera y única vez en su carrera como escritor de largo. Él tiene el orgullo de un escritor que yo
finalmente han llegado a comprender y compartir, y esperamos hacer otros libros juntos.
El placer de estar en la casa de Simón en Rancho Santa Fe para trabajar y ser
mimado por la esposa de Bill, Arynne, podría ser considerado un punto culminante de este escrito
del proyecto. Arynne conversación y la cocina se enfrentarán en la memoria de la primera
su lugar. Ella es una dama de la calidad y la sabiduría, llena de diversión, que ha creado un hogar de
calidez y belleza. Y nunca voy a beber un refresco de dieta de nuevo sin audiencia
Arynne voz en el fondo de mi mente me amonestar a los peligros de la
El aspartamo, Stacey Kirkland significa mucho para mí. Ha dedicado muchos
horas de su tiempo ayudando a mí en el Macintosh para diseño de las tablas y gráficos
que ayudó a dar a la autoridad visual a mis ideas. Admiro sus cualidades maravillosas;
Ella es realmente una persona amorosa y compasiva que sólo merece las cosas buenas
en la vida. Ella me dio la motivación como un buen amigo y es alguien que me importa
profundamente. Quiero darle las gracias por todo su apoyo amoroso, y por estar ahí
para mí cada vez que lo necesitaba.
Alex Kasper, Nexspace, no sólo es mi mejor amigo, sino también un socio de negocios
y su colega. Juntos hemos organizado una charla popular programa de radio de Internet conocido como
"El lado oscuro de Internet" en la FKI AM 640 en Los Angeles bajo la hábil
orientación del Programa Director David G. Hall. Alex gentilmente ofrecido su
inestimable ayuda y asesoramiento a este proyecto de libro. Su influencia siempre ha
sido positivo y útil, con una amabilidad y generosidad que a menudo se extendía mucho más
más allá de la medianoche. Alex y yo recientemente completó una película / vídeo para ayudar a las empresas
capacitar a su gente en la prevención de ataques de ingeniería social.
Pablo Dryman, tomar una decisión informada, es un amigo de la familia y más allá. Esta muy
respetada y de confianza investigador privado me ayudó a entender las tendencias y
procesos de realización de investigaciones de fondo. El conocimiento de Pablo y
la experiencia me ayudó a resolver los problemas de seguridad personal calificado en la parte 4 de
este libro.
Uno de mis mejores amigos, Layman Candi, ha ofrecido apoyo y me
el amor. Ella es realmente una persona maravillosa que merece el mejor de la vida. Durante el
trágicos días de mi vida, Candi ofrecido siempre apoyo y amistad. Estoy
afortunados de haber conocido a un ser humano maravilloso, atento y compasivo,
y quiero darle las gracias por estar ahí para mí.
Seguro que mi cheque de regalías primero iré a mi compañía de teléfonos celulares para todos los
tiempo que pasé hablando con Erin Finn. Sin lugar a dudas, Erin es como mi alma gemela.
Nos parecemos en muchos sentidos que da miedo. Los dos tenemos un amor
para la tecnología, los mismos gustos en comida, música y películas. AT & T Wireless es
definitivamente perdiendo dinero por haberme dado todo el "huir de noches y fines de semana" las llamadas a
su casa en Chicago. Al menos yo no estoy usando el plan de Kevin Mitnick más.
Su entusiasmo y la fe en este libro impulsado mi espíritu. Lo afortunado que soy al
tiene ella como un amigo.
Estoy ansioso por dar las gracias a aquellas personas que representan a mi carrera profesional y se
dedicado de forma extraordinaria. Mis charlas son administrados por Amy

Gris (una persona honesta y solidaria a quien admiro y adoro) David Fugate, de Producciones orillas del agua, es un agente literario que fue a batear por mí en muchos ocasiones antes y después de que el contrato se firmó libro, y Los Ángeles el abogado Gregory Vinson, que estaba en mi equipo de la defensa durante mis años de duración batalla con el gobierno. Estoy seguro de que puede relacionarse con la comprensión de Bill y la paciencia de mi atención a los detalles, sino que ha tenido la misma experiencia de trabajo conmigo en informes jurídicos que ha escrito en mi nombre.

He tenido demasiadas experiencias con abogados, pero estoy ansioso por tener un lugar para expresar mi agradecimiento por los abogados que, durante los años de mi negativa interacciones con el sistema de justicia penal, se acercó y se ofreció a ayudar a cuando yo estaba en situación desesperada. De las palabras amables con profundo compromiso con mi caso, conocí a muchos que no en todos encajan en el estereotipo del abogado centrado en sí mismo. Yo han llegado a respetar, admirar y apreciar la bondad y generosidad de espíritu que me ha dado tan libremente por muchos. Cada uno de ellos merecen ser reconocidos con un párrafo de las palabras favorables, yo por lo menos mencionarlos a todos por su nombre, por cada uno de ellos vive en mi corazón rodeado de apreciación: Greg Aclin, Bob Carmen, Juan Dusenbury, Ellison Sherman, Omar Figueroa, Hagin Carolyn, Rob Hale, Alvin Michaelson, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Richard Sherman, Skip Pizarras, Karen Smith, Richard Steingard, el Honorable Robert Talcott, Barry Tarlow, John Yzurdiaga, y Gregory Vinson.

Agradezco mucho la oportunidad que John Wiley & Sons me ha dado al autor de este libro, y por su confianza en un autor por primera vez. Quiero dar las gracias las siguientes personas Wiley quien hizo posible este sueño: Ellen Gerstein, Bob Ipsen, Carol Long (mi editor y diseñador de moda), y Nancy Stevenson.

Otros miembros de la familia, amigos personales, compañeros de trabajo que han dado me asesoramiento y apoyo, y han alcanzado en muchos aspectos, son importantes para reconocer y agradecer. Ellos son: J. J. Abrams, David Agger, Bob Arkow, Stephen Barnes, el doctor Robert Berkowitz, Dale Coddington, Eric Corley, Delin Cormeny, Ed Cummings, Davis Arte, Michelle Delio, Sam Downing, John Draper, Paul Dryman, Duva Nick, Eskapa Roy, Alex Fielding, Lisa Flores, Brock Frank, Steve Gibson, Jerry Greenblatt, Greg Grunberg, Bill Mango, David G. Alto, Dave Harrison, Herman Leslie, Jim Hill, Dan Howard, Steve Hunt, Rez Johar, Knittle Steve, Gary Kremen, Krugel Barry, Earl Krugel, Adrian Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, Little CJ, Jonathan Littman, Mark Maifrett, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Muñoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Poulsen Kevin, Scott prensa, Linda y Pryor Arte, Jennifer Reade, Israel y Rachel Rosencrantz, Mark Ross, William Royer, Irv Rubin, Ryan Russell, Neil Saavedra, Schwartu Wynn, Pete Shipley, Tamizar Joh, Dan Sokol, Spector Trudy, Spergel Matt, Eliza Amadea Sultan, Douglas Thomas, Roy "Ihcker, Turbow Bryan, Wetzel Ron, Don David Wilson, Darci Wood, Kevin Wortman, Steve Wozniak, y todos mis amigos en el W6NUT (147.435 MHz) repetidor en Los Angeles.

Y mi agente de libertad condicional, Larry Hawley, merece un agradecimiento especial por haberme dado permiso para actuar como asesor y consultor en asuntos relacionados con la seguridad de autor de este libro.

Y, finalmente, he de reconocer que los hombres y mujeres de hacer cumplir la ley. Yo simplemente no tienen ninguna malicia hacia estas personas que están haciendo su trabajo. Creo firmemente que poner el interés del público por delante de uno mismo y dedicar su vida al servicio público es algo que merece respeto, y

mientras yo he sido arrogante a veces, quiero que todos ustedes sepan que me encanta este país, y hará todo lo que esté a mi alcance para ayudar a que sea el lugar más seguro el mundo, que es precisamente una de las razones por las que he escrito este libro.
DE BILL SIMON
Tengo esta idea de que hay una persona ideal para todo el mundo, es sólo que algunas personas no tienen la suerte de nunca encontrar su Sr. o la Sra. derecho. Otros se suerte. Tuve suerte con suficiente antelación en la vida para pasar un buen número de años ya (y contar con el gasto de muchos más) con uno de los tesoros de Dios, mi esposa, Arynne .. Si Yo olvidarme de lo afortunado que soy, sólo tengo que prestar atención a la cantidad de personas buscar y cuidar a su empresa. Arynne - Le doy las gracias por caminar por la vida con mí.
Durante la redacción de este libro, he contado con la ayuda de un grupo fiel de amigos que proporcionan la seguridad de que Kevin y yo estábamos conseguir nuestro objetivo de la combinación de realidad y fascinación en este libro inusual. Cada una de estas personas representa un verdadero valor y leal y sabe que él o ella puede ser llamado como me meto en mi proyecto de escritura siguiente. En orden alfabético: Jean-Claude Beneventi, Linda Brown, Walt Brown,. Gral. Don Johnson, Ryan Dorothy, Stark Guri, Chris Empinada, empinada Michael y John Votaw.
Reconocimiento especial a John Lucich, presidente de la Red de Seguridad Grupo, que estaba dispuesto a tomar tiempo para que un amigo de un amigo-solicitud, y Atuendo de Gordon, quien amablemente envió numerosas llamadas telefónicas acerca de las operaciones de TI.
A veces en la vida, un amigo se gana un lugar exaltado mediante la introducción de usted a alguien otra persona que se convierte en un buen amigo. En la literatura Producciones agencia de agua, en Cardiff, California, el agente David Fugate fue el responsable de concebir la idea para este libro, y por ponerme junto con el co-autor que se convirtió en amigo de Kevin. Gracias, David. Y a la cabeza de Ribera, el proyecto de ley Gladstone incomparable, que se las arregla para mantenerme ocupado con el proyecto de libro, uno tras otro: Estoy contento de tienen ustedes en mi esquina.
En nuestra casa y mi oficina en casa, Arynne es ayudado por un personal capaz que incluye asistente administrativo Dudgeon Jessica y ama de casa Josie Rodríguez.
Agradezco a mis padres Marjorie y Simon IB, que me gustaría estuviera aquí en la tierra para disfrutar de mi éxito como escritor. También agradezco a mi hija, Victoria. Cuando estoy con ella me doy cuenta de lo mucho que admiro, respeto, y estamos orgullosos de lo que es.

Analizados por kineticstomp

_____
_____
Suplemento
por rápida
[Capítulo 1-Banned Edition]
Historia de Kevin
Por Kevin Mitnick
Yo me resistía a escribir esta sección, porque estaba seguro de que el sonido selfserving. Bueno, está bien, es su propio beneficio. Pero he estado en contacto con, literalmente, cientos de personas que quieren saber "quién es Kevin Mitnick?". Para los que no les importa, por favor, a su vez con el capítulo 2. Porque todo el mundo aquí, por lo que vale la pena, es mi historia.
Kevin habla un poco de hackers destruir los archivos de las personas o unidades de todo el bardo, sino que son

llamados crackers o vándalos. Algunos hackers novatos no se molestan en aprender el tecnología, sino que basta con descargar las herramientas de hacker para irrumpir en los sistemas informáticos;
se llaman script kiddies. Hackers más experimentados con conocimientos de programación desarrollar programas de hacker y publicarlas en la web y tablón de anuncios
sistemas. Y luego hay personas que no tienen interés en la tecnología,
pero el uso de la computadora sólo como una herramienta que les ayuda en el robo de dinero, bienes o
los servicios. A pesar del mito creado por los medios de Kevin Mitnick, yo no soy un malintencionado
hacker. Lo que hice no fue ni siquiera contra la ley, cuando empecé, pero se convirtió en un crimen
después de la nueva legislación fue aprobada. Seguí todos modos, y fue capturado. Mi tratamiento por el gobierno federal no se basó en los crímenes, sino en hacer
un ejemplo de mí. Yo no merecía ser tratado como un terrorista o violento
penal: Después de haber buscado mi residencia con una orden de allanamiento en blanco, siendo lanzado en solitario durante meses, les niegan los derechos constitucionales fundamentales garantiza a toda persona acusada de un delito, se les niega no sólo la libertad bajo fianza, pero una libertad bajo fianza
audiencia, y se ven obligados a pasar años luchando por obtener del gobierno
pruebas por lo que mi abogado designado por el tribunal podría preparar mi defensa.
¿Qué pasa con mi derecho a un juicio rápido? Durante años me dieron una opción cada seis meses: firmar un documento renunciando a su derecho constitucional a un juicio rápido o ir a juicio con un abogado que no está preparado, me eligió para firmar. Pero me estoy adelantando mi historia. Iniciando mi camino se hizo probablemente temprano en la vida. Yo era un feliz golucky
niño, pero aburrido. Cuando mi padre se separaron cuando yo tenía tres años, mi madre trabajaba como camarera para que nos apoyen. Para ver conmigo entonces un hijo único criado por una madre, que puso en largos días, acosado en un horario a veces errático habría
ido a ver a un joven en su propia casi todas las horas de vigilia. Yo era mi propio
niñera. Al crecer en una comunidad del Valle de San Fernando me dio todo
de Los Angeles para explorar, y por la edad de doce años que había descubierto una manera de viajar gratis a lo largo de toda la zona de mayor Ángeles. Me di cuenta un día mientras se conduce
el autobús que la seguridad de la transferencia de autobuses que había comprado se basó en la inusual
patrón del papel golpe que los controladores utilizados para conmemorar el día, hora y ruta en la transferencia se desliza. Un conductor amable, respondiendo a mi pregunta cuidadosamente plantados, dijo
me dónde comprar ese tipo especial de ponche. Las transferencias están destinadas a permitir cambiar de autobús y continuar un viaje a su destino, pero he trabajado la manera de
los utilizan para viajar a cualquier parte que quería ir de forma gratuita. Realizar transferencias en blanco
Fue un paseo en el parque: los cubos de basura en las terminales de autobuses estaban llenos siempre con
sólo los libros-en parte-de las transferencias que utilizan los controladores tiró al final de su cambios. Con una capa de blanco y el punzón, pude marcar mi propia y las transferencias
viajar a cualquier parte que los autobuses de Los Ángeles se fue. En poco tiempo, que casi había memorizado el
horarios de los autobuses de todo el sistema. Este fue un primer ejemplo de mi sorpresa
de memoria para ciertos tipos de información, aún hoy puedo recordar teléfono
números, contraseñas y otros objetos ya en mi infancia. Otro
interés personal que surgió a temprana edad fue mi fascinación con la realización de
magia. Una vez que aprendió un nuevo truco funcionó, me gustaría practicar, practicar, y
la práctica hasta que lo domina. Hasta cierto punto, fue a través de la magia que he descubierto

el disfrute de la gente engañando. Desde Phreak teléfono, a mi primer Hacker
encuentro con lo que finalmente aprender a llamar a la ingeniería social fue
durante mis años de escuela secundaria, cuando me encontré con otro estudiante que fue capturado
en un hobby llamado phone phreaking. Phone phreaking es un tipo de piratería que
le permite explorar la red telefónica mediante la explotación de los sistemas telefónicos y
los empleados de la compañía telefónica. Él me mostró truquitos que podía hacer con un
teléfono, como la obtención de cualquier información de la compañía telefónica había en cualquier
cliente, y el uso de un número secreto para hacer la prueba de larga distancia las llamadas gratis
realmente libre sólo para nosotros - me enteré mucho más tarde que no era un número de prueba secreta
En absoluto: las llamadas fueron de hecho, se facturarán a la cuenta un poco de compañía pobres MCI).
Esa fue mi introducción a la ingeniería social de mi jardín de infantes, por así decirlo. Él
y otro phreaker teléfono conocí poco después que me escuche, ya que en cada
pretexto hizo llamadas a la compañía telefónica. He oído las cosas que dijo que hizo
que suenen creíbles, he aprendido acerca de las diferentes oficinas de la compañía telefónica, la jerga
y los procedimientos. Pero que "la formación" no duró mucho tiempo, no tenía que hacerlo. Pronto se
hacerlo todo por mi cuenta, a medida que iba aprendiendo, haciendo que sea aún mejor que los primeros
los profesores. El curso de mi vida seguiría para los próximos quince años se había establecido.
Uno de mis bromas de todos los tiempos favorito era el acceso no autorizado a los
conmutador telefónico y el cambio de la clase de servicio de un phreaker compañeros.
Cuando se hubo intento de realizar una llamada desde su casa, se ponía un mensaje diciéndole que
depositar una moneda de diez centavos, porque el interruptor de la compañía telefónica recibida de entrada que
indicó que estaba llamando desde un teléfono público.
Yo se absorbió en todo lo relacionado con los teléfonos, no sólo de la electrónica,
interruptores y equipos, sino también la organización de la empresa, los procedimientos, y
la terminología. Después de un tiempo, probablemente sabía más sobre el sistema telefónico
que cualquier otro empleado.
Y, ya había desarrollado mis habilidades de ingeniería social hasta el punto que, a los diecisiete años
años de edad, fue capaz de hablar la mayoría de los empleados Telco en casi cualquier cosa, ya sea
Yo estaba hablando con ellos en persona o por teléfono. Mi carrera comenzó a la piratería
cuando yo estaba en la escuela secundaria. En ese entonces se utilizó el término hacker para referirse a una persona
que pasó una gran cantidad de pequeños ajustes de tiempo con el hardware y software, ya sea para
desarrollar programas más eficientes o pasar por alto los pasos innecesarios y terminar el trabajo
de forma más rápida. El término se ha convertido en algo peyorativo, que lleva el significado
de "criminal malicioso". En estas páginas el término de la forma en que he utilizado siempre
que en su anterior, el sentido más benigno. A finales de 1979, un grupo de tipos colega hacker
que trabajaba para el diario Los Angeles Unified School District me atreví a intentar hackear
en el arca, el sistema informático en Digital Equipment Corporation utiliza para
el desarrollo de sus RSTS / software E del sistema operativo. Yo quería ser aceptado por
los chicos de este grupo de hackers para que pudiera recoger sus cerebros para aprender más sobre
sistemas operativos. Estos nuevos "amigos" habían logrado tener en sus manos la
el número de marcación en el sistema informático diciembre Pero ellos sabían el número de acceso telefónico

no me sirve de nada: sin un nombre de cuenta y contraseña, que nunca sería
capaz de entrar Estaban a punto de descubrir que cuando se subestiman los demás,
puede volver a morder en el culo. Resultó que, para mí, incluso en ese
temprana edad, la piratería en el sistema de diciembre fue una presa fácil. Que dice ser Anton
Chernoff, uno de los principales desarrolladores del proyecto, puesto que una simple llamada telefónica a la
el Administrador del sistema. Yo decía que no podía acceder a uno de "mis" cuentas, y se
lo suficientemente convincente como para hablar del hombre en darme acceso y que me permite
seleccionar una contraseña de mi elección. Como un nivel adicional de protección, siempre que sea
cualquier marcado en el sistema de desarrollo, el usuario también ha de proporcionar un acceso telefónico
contraseña. El administrador del sistema me dijo la contraseña. Se trataba de "bufón"
que creo que describe lo que debe haber sentido como más adelante, cuando se encuentran descubierto
lo que había sucedido. En menos de cinco minutos, yo había tenido acceso a Digital
RSTE / E el desarrollo del sistema. Y yo no estaba registrado como tal como un usuario normal,
sino como alguien con todos los privilegios de un desarrollador de sistemas. Al principio, mi nuevo
así llamados amigos se negaron a creer que había ganado el acceso a The Ark Uno de ellos
marcado por el sistema y empujó el teclado delante de mí con un desafío
expresión de su rostro. Su boca se abrió como la materia de manera casual en una sesión
cuenta con privilegios. Más tarde me enteré que se fueron a otro lugar y,
El mismo día, comenzó a descargar el código fuente de los componentes de la DEC
del sistema operativo. Y entonces me llegó el turno a piso. Después de haber
descargar todo el software que quería, llamaron a la seguridad de la empresa
departamento de diciembre y les dijo que alguien había hackeado en la compañía
red corporativa. Y le dieron mi nombre. Mis supuestos amigos utilizado por primera vez mi
acceso para copiar el código fuente de alta sensibilidad, y luego me dio vuelta pulg
No fue una lección aquí, pero no una me las arreglé para aprender con facilidad. A través de los años
venir, en repetidas ocasiones se meten en problemas porque confiaba en la gente que me
pensaba que eran mis amigos. Después de la secundaria, estudié las computadoras en la computadora
Centro de Aprendizaje en Los Angeles.
En pocos meses, el gerente de la escuela de la computadora me di cuenta que había encontrado un
vulnerabilidad en el sistema operativo y ha ganado todos los privilegios administrativos en
su minicomputadora IBM. El mejor equipo de expertos en su personal docente
No podía entender cómo había hecho esto. En lo que pudo haber sido uno de los primeros
ejemplos de "contratar a los hacker", me llegó una oferta que no podía rechazar: ¿Es una
honra a los proyectos para mejorar la seguridad de la escuela de computación, o la suspensión de la cara
hackear el sistema. Por supuesto que me eligió para hacer el proyecto honores, y terminó
Cum Laude con honores. Convertirse en un ingeniero social que algunas personas
levantarse de la cama cada mañana temiendo su rutina de trabajo diario en la proverbial
minas de sal. He tenido la suerte de disfrutar de mi trabajo. En particular, no se puede
imaginar el desafío, la recompensa y el placer que tenía en el tiempo que pasé como una organización privada
investigador. Yo estaba afilando mis talentos en el arte de performance llamado social
ingeniería-que la gente haga cosas que normalmente no haría para un strangerand
paguen por ello. Para mí no fue difícil convertirse en experto en el desarrollo social
ingeniería. Parte de mi padre de la familia había estado en el campo de las ventas de
generaciones, por lo que el arte de la influencia y la persuasión podría haber sido una enfermedad hereditaria
rasgo. Cuando se combina una inclinación para engañar a la gente con el talento de los

influencia y persuasión que llegue al perfil de un ingeniero social. Es posible que
decir que hay dos especialidades dentro de la clasificación del puesto de artista de la estafa.
Alguien
que estafa a la gente y los tramposos de su dinero pertenece a una sub-especialidad,
el estafador. Alguien que utiliza el engaño, la influencia y la persuasión contra
empresas, por lo general dirigidas a la información, pertenece a la otra sub-especialidad,
el ingeniero social. Desde el momento de mi truco de traslado en autobús, cuando yo era
demasiado joven
saber que había algo malo con lo que estaba haciendo, había comenzado a
reconocer un talento para descubrir los secretos que no se supone que tiene. He construido en
que el talento mediante engaño, a sabiendas de la jerga y el desarrollo de un bien afinado
habilidad de manipulación.
Una forma en que solía trabajar en el desarrollo de las habilidades de mi oficio (si se me permite
llamarlo un
artesanales) fue a recoger a algún tipo de información que realmente no se preocupan por ver y
si yo pudiera hablar a alguien en el otro extremo del teléfono en su prestación, sólo para
mejorar mis talentos. De la misma manera que solía practicar mis trucos de magia, me
practicado pretextos. A través de estos ensayos, pronto me di cuenta de que podían adquirir
prácticamente toda la información que objetivo. En testimonio ante el Congreso antes de
Senadores
Lieberman y Thompson años más tarde, les dije, "he ganado no autorizado
el acceso a los sistemas informáticos de algunas de las corporaciones más grandes del planeta, y
han penetrado con éxito en algunos de los sistemas informáticos cada vez más resistentes
desarrollados. He utilizado los medios tanto técnicos como no técnicos para obtener la
código fuente para varios sistemas operativos y dispositivos de telecomunicaciones para
estudiar sus vulnerabilidades y su funcionamiento interno. "Todo esto fue realmente
satisfacer mi propia curiosidad, ver qué podía hacer, y descubrir información secreta
sobre los sistemas operativos, los teléfonos celulares, y cualquier cosa que agita mi curiosidad.
La serie de acontecimientos que cambiaría mi vida comenzó cuando se convirtió en el tema
de 04 de julio 1994 en primera plana, por encima de la doble historia en el New York Times.
Durante la noche, que la historia de una vuelta a mi imagen de una molestia poco conocida de un
hacker en enemigo público número uno del ciberespacio. John Markoff, el
Grifter medios de comunicación

"La combinación de magia técnica con la astucia años de edad, de un estafador, Kevin
Mitnick es un programador de computadoras fuera de control. "(The New York Times, 07/04/94).
Combinando el deseo de las edades de edad para alcanzar la fortuna inmerecida con el poder de
publicar historias falsas y difamatorias sobre sus súbditos en la primera página de la
New York Times, John Markoff fue verdaderamente un periodista de tecnología fuera de control.
Markoff fue para ganarse más de $ 1 millón por sí sola la creación de lo que
etiqueta de "El mito de Kevin Mitnick." Se hizo muy rico a través de la muy
Yo misma técnica utilizada para comprometer los sistemas y redes en todo el
mundo: el engaño. En este caso, sin embargo, la víctima del engaño no era un
usuario de la computadora sola o administrador del sistema, que era toda persona que confió en
el
noticias publicadas en las páginas del New York Times.Cyberspace 's Most
Quería artículo Markoff Times fue claramente diseñado para conseguir un contrato para un
libro sobre la historia de mi vida. Nunca he conocido a Markoff, y sin embargo, se ha convertido,
literalmente,
un millonario a través de su calumniosa y difamatoria "informes" acerca de mí en el
Momento y en su libro de 1991, Cyberpunk. En su artículo, que incluye algunas decenas
de las acusaciones sobre mí que declaró como un hecho sin citar sus fuentes, y que
incluso un proceso mínimo de comprobación de los hechos (que me pareció todo de primer nivel
periódicos requeridos a sus reporteros a hacer) habría revelado como falso o
no probadas. En ese mismo artículo falsas y difamatorias, Markoff me etiquetados como

"Ciberespacio más buscados," y como "un equipo de los más buscados del país criminales ", sin evidencia de la justificación, la razón o de apoyo, con no más discreción de un escritor para un tabloide. En su artículo contra ella, Markoff falsamente que había escuchas telefónicas del FBI (no había), que había dividido en las computadoras de NORAD (que ni siquiera están conectados a cualquier red en el exterior), y que yo era un equipo "vandalismo", a pesar de que Yo nunca había dañado intencionalmente cualquier equipo que he accedido. Estos, entre otras denuncias escandalosas, eran completamente falsas y diseñadas para crear una sensación de miedo acerca de mis capacidades. En otra violación de la ética periodística, Markoff no dio a conocer en dicho artículo, y en todas sus posteriores artículos-a preexistente relación conmigo, una animosidad personal basada en mi haber se negó a participar en el libro Cyberpunk Además, yo le había costado un montón de los ingresos potenciales por la no renovación de una opción para una película basada en la libro. Artículo de Markoff fue claramente diseñado para burlarse de la ley de Estados Unidos organismos de aplicación.

"... Las fuerzas del orden", Markoff, escribió, "parece que no puede ponerse al día con él ...." La el artículo se enmarca deliberadamente para echarme como el número del ciberespacio Public Enemy Uno con el fin de influir en el Departamento de Justicia para elevar la prioridad de mi caso. Unos meses más tarde, Markoff y su cohorte Tsutomu Shimomura se ambos participan como agentes de gobierno de facto de mi detención, en violación de los la ley federal y la ética periodística. Ambos serían cercanos al tres en blanco órdenes fueron utilizados en un allanamiento ilegal de mi residencia, y estar presente en mi arresto. Y, durante la investigación de mis actividades, los dos también violaría la ley federal mediante la interceptación de una llamada telefónica personal mío. Mientras me lo a ser un villano, Markoff, en un artículo posterior, creado Shimomura como el número uno del héroe del ciberespacio. Una vez más estaba violando la ética periodística al no la divulgación de una relación preexistente: este héroe, de hecho, había sido amigo personal de Markoff durante años. Mi primer encuentro con Markoff había llegado a finales de los años ochenta, cuando él y su esposa Katie Hafner me contactaron mientras estaban en el proceso de la escritura cyberpunk, que iba a ser la historia de tres hackers: un Chico alemán conocido como Pengo, Robert Morris y yo.

¿Cuál sería mi compensación sea por participar? Nada. Yo no podía ver el punto de darles mi historia si ellos se benefician de ella y yo no, así que se negó a ayudar. Markoff me dio un ultimátum: o entrevista con nosotros o cualquier cosa que escuchar desde cualquier fuente será aceptado como la verdad. Era evidente que estaba frustrado y molesto que no iba a cooperar, y me dejaba saber que tenía los medios para que me arrepiento. Decidí mantenerme firme y no cooperar a pesar de sus tácticas de presión. Cuando se publicó, el libro me presenta como "El Hacker Darkside". Llegué a la conclusión de que los autores han incluido intencionadamente afirmaciones no, falsa con el fin de vengarse de mí por no cooperar con ellos. Al hacer mi personaje parece más siniestro y la fundición de mí en un falso la luz, es probable que el aumento de las ventas del libro. Un productor de cine por teléfono con una gran noticia: Hollywood estaba interesado en hacer una película sobre la Hacker Darkside representado en Cyberpunk. Señalé que la historia estaba llena de inexactitudes y mentiras acerca de mí, pero aún estaba muy entusiasmado con la del proyecto. He aceptado 5.000 dólares por una opción de dos años, en contra de un adicional de $ 45,000 si fueron capaces de llegar a un acuerdo de producción y seguir adelante. Cuando la opción expirado, la productora solicitó una prórroga de seis meses. En este momento me tenía un empleo remunerado, y por lo tanto había poca motivación para ver una película producida que me mostró de un modo tan desfavorable y falsa. Yo me negué a ir junto con la extensión. Que mató a la oferta de cine para todos, incluyendo a Markoff, quien

había esperado, probablemente para hacer una gran cantidad de dinero del proyecto. Aquí se una razón más para John Markoff a ser vengativo hacia mí. Todo el tiempo Cyberpunk fue publicado, Markoff tuvo correspondencia por correo electrónico en curso con su Shimomura amigo. Ambos estaban interesados extraña en mi paradero y lo que estaba haciendo. Sorprendentemente, un mensaje de correo electrónico contiene información que habían aprendido asistía a la Universidad de Nevada, Las Vegas, y tenido el uso del laboratorio de computación del estudiante. ¿Podría ser que Markoff y Shimomura estaban interesados en hacer otro libro acerca de mí? De lo contrario, ¿por qué se preocupan lo que estaba haciendo? Markoff en persecución Dar un paso atrás a finales de 1992. Yo estaba a punto de Al final de mi libertad supervisada por comprometer la Digital Equipment Red corporativa de la Corporación. Mientras tanto, me di cuenta de que el gobierno estaba tratando de armar un caso contra mí, esta vez para llevar a cabo contra-inteligencia para averiguar por qué escuchas telefónicas habían sido colocados en las líneas telefónicas de una empresa de Los Angeles P. II. En mi excavación, me confirmó mi sospecha: el Pacífico Bell personal de seguridad eran de hecho la investigación de la empresa. Así que fue un crimen informático subdirector del Departamento del Sheriff del Condado de Los Angeles es. (Que el diputado se convierte ser, co-dicho sea de paso, el hermano gemelo de mi co-autor en este libro. Pequeño mundo). En este tiempo, los agentes federales establecer un informante criminal y lo envió a atrapar a mí. Ellos sabían que yo siempre traté de mantener control sobre cualquier organismo de investigación mí. Por lo que tenían amistad con este informante mí y me fuera de punta que estaba siendo monitoreados. También me contó los detalles de un sistema informático utilizado en Pacific Bell que me permite hacer contra-vigilancia de sus controles. Cuando He descubierto su trama, que se convirtió rápidamente las tablas en él y lo expuso a la tarjeta de crédito el fraude se estaba llevando a cabo mientras trabajaba para el gobierno en un informante de la capacidad. Estoy seguro de que los federales apreciar que! Mi vida cambió en Día de la Independencia de 1994, cuando mi pager me despertó temprano en la mañana. La persona que llamó dijo que de inmediato debe recoger un ejemplar del New York Times. Yo No lo podía creer cuando vi que Markoff no sólo había escrito un artículo sobre mí, pero el Times había colocado en la primera página. El primer pensamiento que vino a mente por mi seguridad personal, ahora el gobierno se vería sustancialmente aumentando sus esfuerzos para encontrarme. Me sentí aliviado de que en un esfuerzo para demonizar me, el Times había utilizado una imagen impropia de muy. Yo no tenía miedo de ser reconoció que había elegido una imagen tan anticuada que no se parecía en nada como yo! Cuando comencé a leer el artículo, me di cuenta de que Markoff se estaba poniendo a sí mismo para escribir el libro de Kevin Mitnick, tal como él siempre había querido. Yo Simplemente no podía creer lo que el New York Times correría el riesgo de la impresión de la declaraciones notoriamente falsas que había escrito sobre mí. Me sentía impotente. Aunque Yo había estado en condiciones de responder, yo ciertamente no tendría una audiencia igual el New York Times s para refutar escandalosas mentiras de Markoff. Mientras que yo puedo estar de acuerdo había sido un dolor en el culo, yo nunca había destruido información, ni utilizados o revelada a terceros toda la información que había obtenido. Las pérdidas reales de las empresas de mis actividades de hacking ascendieron al coste de las llamadas telefónicas que había hecho en teléfono, la empresa los gastos, el dinero gastado por las empresas para conectar la seguridad vulnerabilidades que mis ataques había revelado, y en algunos casos posiblemente empresas que causan que volver a instalar sus sistemas operativos y aplicaciones por miedo podría haber modificado el software de una manera que me permita acceder en el futuro. Aquellos

las empresas tendrían que seguía siendo vulnerable a un daño mucho peor si mis actividades no había hecho consciente de los puntos débiles de su cadena de seguridad. A pesar de que había
causaron algunas pérdidas, mis acciones y la intención no era maliciosa ... y luego John Markoff cambió la percepción del mundo sobre el peligro que representaba. El poder
de un periodista poco ético de un periódico influyente como para escribir un falso y historia difamatoria sobre cualquier persona debe perseguir todos y cada uno de nosotros. El próximo
objetivo podría ser usted.
Después de mi detención fui trasladado a la cárcel del condado de Smithfield, North Carolina, donde los EE.UU. Servicio de Alguaciles Federales ordenó carceleros que me coloque en el `
hole'-confinamiento solitario. Dentro de una semana los fiscales federales y mi abogado llegado a un acuerdo que no podía rechazar. Podría ser retirados de aislamiento en
la condición de que renunciar a mis derechos fundamentales y acordó: a) sin derecho a fianza audiencia; b) no la audiencia preliminar, y, c) nada de llamadas, excepto con mi abogado
y dos miembros de la familia. Firmar, y yo podía salir de la soledad. Yo signed.The
los fiscales federales en el caso de jugar todos los trucos sucios en el libro hasta que se lanzado casi cinco años después. Me vi obligado en repetidas ocasiones a renunciar a mis derechos en
para ser tratado como cualquier otro acusado. Sin embargo, este fue el caso de Kevin Mitnick: No había reglas. No hay obligación de respetar los derechos constitucionales de los acusado. Mi caso no se trataba de la justicia, pero sobre el gobierno
determinación de ganar a toda costa. Los fiscales habían hecho muy exagerada reclamaciones ante el tribunal sobre el daño que había causado y la amenaza que yo representaba,
y los medios de comunicación se había ido a la ciudad citando las declaraciones sensacionalistas y ahora se
demasiado tarde para que los fiscales a dar marcha atrás. El gobierno no podía permitirse el lujo de
perder el caso Mitnick. El mundo estaba mirando.
Yo creo que los tribunales han comprado en el miedo generado por la cobertura de los medios de comunicación, ya que
muchos de los periodistas más ética había recogido los "hechos" de los estimados New York Times y las repitió. El mito generado por los medios al parecer, incluso
miedo agentes del orden. Un documento confidencial obtenido por mi
abogado puso de manifiesto que los EE.UU. Servicio de Alguaciles Federales emitió una advertencia a todas las leyes
los agentes del orden de no revelar ninguna información personal para mí, de lo contrario, que podrían encontrar sus vidas destruidas por vía electrónica. Nuestra Constitución exige
que el acusado se presume inocente antes del juicio, con la garantía de todos los ciudadanos de la
derecho a una audiencia de fianza, cuando el acusado tiene la oportunidad de ser representado por
un abogado, presentar pruebas y contrainterrogar a los testigos. Increíblemente, el gobierno había sido capaz de eludir estas protecciones basadas en la falsa
histeria generada por los periodistas irresponsables como John Markoff. Sin
precedente, que se llevó a cabo como un pre-juicio-detenido a una persona en prisión preventiva o
condena por más de cuatro años y medio. El juez se niega a concederme una libertad bajo fianza audiencia se debatió todo el camino hasta la Corte Suprema de los EE.UU.. Al final, mi
del equipo de defensa me aconsejó que me había propuesto otro precedente: yo era el único federal
detenido en la historia de EE.UU. negó una audiencia de fianza. Esto significaba que el gobierno nunca

tenía que cumplir con la carga de probar que no había condiciones de la liberación que razonablemente asegurar mi presencia en la corte. Al menos en este caso, federal los fiscales no se atreven a alegar que podría iniciar una guerra nuclear por silbar en un teléfono público, como otros fiscales federales lo habían hecho en un caso anterior. La mayoría de los graves acusaciones en mi contra eran que yo había copiado el código fuente propiedad de varios terminales de telefonía celular y sistemas operativos populares. Sin embargo, el Los fiscales alegaron públicamente y ante el tribunal que había causado pérdidas colectivas más de $ 300 millones a varias empresas. Los detalles de los importes de las pérdidas se aún bajo el sello de la corte, supuestamente para proteger a las empresas involucradas, mi del equipo de defensa, sin embargo, cree que la petición fiscal de sellar la información se inició para encubrir su mala conducta grave, en mi caso. También vale la pena señalando que ninguna de las víctimas en mi caso habían presentado pérdidas en el Comisión de Valores de conformidad con la ley. Cualquiera de varias empresas multinacionales violan la ley federal en el proceso de engañar a la SEC, accionistas y analistas - o las pérdidas atribuibles a mi hacking, de hecho, demasiado trivial como para ser reportado. En su libro Juego de Fugitivos, Jonathan Li wan informes que dentro de una semana de The New York Times de primera plana, el agente de Markoff había "Negoció un acuerdo global" con el editor Walt Disney Hyperion para un libro sobre la campaña para localizar a mí. El avance era de un estimado de US $ 750.000. Según Littman, no iba a ser una película de Hollywood, así, Miramax con la entrega de 200.000 dólares para la opción y "un total de $ 650.000 a ser pagar a inicio del rodaje. "Una fuente confidencial recientemente me informó que se ocupan de Markoff fue de hecho mucho más que Littman había se pensaba originalmente. Así que John Markoff tiene un millón de dólares, más o menos, y se me cinco años. Un libro que examina los aspectos legales de mi caso fue escrito por un hombre que se había sido fiscal en el Los Angeles de Fiscal de Distrito oficina, un colega de los abogados que me procesados. En su libro Espectacular Delitos Informáticos, Buck Bloombecker escribió: "Me duele tener que escribir acerca de mis antiguos colegas en menos de términos halagadores .... Estoy obsesionado por Ingreso fiscal federal adjunto James Asperger que gran parte de la argumento utilizado para mantener a Mitnick tras las rejas se basa en rumores que no resultan. "Él va a decir:" Fue lo suficientemente malo que los fiscales los cargos hizo en la corte se extendió a millones de lectores de periódicos de todo el país. Pero es mucho peor que estas acusaciones falsas fueron una gran parte de la base para mantener a Mitnick tras las rejas sin posibilidad de fianza? "El continúa con cierta extensión, al escribir sobre las normas éticas que los fiscales debe vivir, y luego escribe: "El caso de Mitnick, sugiere que las falsas acusaciones utiliza para mantenerlo bajo custodia también prejuicios consideración de la corte de una feria sentencia. "En su artículo de 1999 de Forbes, Adam L. Penenberg describió elocuentemente mi situación de esta manera:. "crímenes de Mitnick fueron curiosamente inocua rompió en equipos de la empresa, pero no hay evidencia indica que destruyó los datos. O vendidos cualquier cosa que copiar. Sí, hurtado de software, pero, al hacerlo, dejó atrás. "El El artículo dijo que mi delito era "burlarse de la seguridad informática costoso sistemas empleados por las grandes corporaciones. "Y, en el libro El juego de Fugitivos autor Jonathan Littman señaló: "La codicia del gobierno podía entender. Sin embargo, un hacker que ejerció el poder por su propio bien ... era algo que no podían . comprender "En otras partes del mismo libro, Littman escribió: EE.UU. El abogado James Sanders admitió al juez Pfaelzer que el daño de Mitnick de diciembre no fue el 4 dólares millones de dólares que habían hecho los titulares, pero 160.000 dólares. Incluso esa cifra no se daños causados por Mitnick, pero el coste aproximado de trazar la debilidad en la seguridad de que sus incursiones habían traído a la atención de DEC. El gobierno reconoció

no tenía pruebas de las afirmaciones salvajes que había ayudado a mantener Mitnick sin fianza y en confinamiento solitario. No hay prueba de Mitnick había comprometido nunca la seguridad de los
la NSA. No hay prueba de que Mitnick había emitido nunca un comunicado de prensa falso para la Seguridad
Pacific Bank. No hay prueba de que Mitnick cambiado alguna vez el informe de crédito de TRW juez. Pero el juez, tal vez influenciado por los terribles medios de comunicación,
rechazó la declaración de culpabilidad y Mitnick sentenciado a un largo plazo, entonces incluso el gobierno quería. A lo largo de los años que pasó como un hacker aficionado, he
ganó notoriedad no deseada, ha escrito en numerosos informes de prensa y
artículos de revistas, y tenía cuatro libros escritos por mí. Markoff y
Libro difamatorio de Shimomura fue hecho en un largometraje llamado Takedown. Cuando
el guión encontrado su camino en Internet, muchos de mis partidarios protestaron
Miramax Films para llamar la atención del público a la caracterización inexacta y falsa
de mí. Sin la ayuda de muchos tipos y gente generosa, la película
seguramente habría falsamente me presenta como el Hannibal Lecter del ciberespacio.
Presionado por mis seguidores, la compañía de producción acordado para resolver el caso en términos confidenciales para mí evitar la presentación de una demanda por difamación en contra de ellos.

Consideraciones finales

A pesar de las descripciones de escandaloso y difamatorio John Markoff de mí, mi
crímenes fueron simples delitos de delito informático y hacer llamadas telefónicas gratuitas.
He reconocido desde mi arresto que las acciones que tomé fueron ilegales, y que
las invasiones de la privacidad comprometidos. Pero sugerir, sin justificación, la razón o prueba, al igual que los artículos Markoff, que había privado a los demás de su dinero o propiedad por ordenador o fraude electrónico, simplemente no es verdad, y sin el apoyo de la pruebas. Mis delitos fueron motivados por la curiosidad: quería saber tanto
como pude sobre cómo las redes de teléfono funcionaba, y las entradas y salidas de la computadora
la seguridad. Pasé de ser un niño al que le encantaba realizar trucos de magia a convertirse en hacker más famoso del mundo, temido por las corporaciones y el gobierno.
A medida que reflexiono sobre mi vida durante los últimos treinta años, admito que me hizo algunas
decisiones de extrema pobreza, impulsado por la curiosidad, el deseo de aprender acerca de tecnología, y un buen desafío intelectual. Soy una persona diferente ahora. Estoy
convertir mis talentos y el amplio conocimiento que he reunido acerca de la información tácticas de seguridad y de ingeniería social para ayudar a gobiernos, empresas y
las personas para prevenir, detectar, y responder a las amenazas a la seguridad de la información. Este
libro es una forma más que puedo utilizar mi experiencia para ayudar a otros a evitar el los esfuerzos de los ladrones de información maliciosa del mundo. Creo que se encuentra la historias agradables, abrió los ojos y la educación.
Kevin Mitnick

_____

El capítulo perdido de Mitnick encontrados
Por Michelle Delio
wired.com, 05 de noviembre 2002
Un capítulo que falta del libro de reciente hacker Kevin Mitnick se ha publicado
a través de Internet.
El capítulo fue originalmente programado para ser el primer capítulo en el nuevo libro de Mitnick, El arte del engaño, pero no fue incluido en la versión publicada del libro.
Capítulo Primero apareció únicamente en alrededor de 300 ejemplares sin unir la cocina que la publicación
Wiley empresa distribuida a los medios de comunicación varios meses antes de soltar el libro, de acuerdo con un portavoz de Wiley.

El editor decidió suprimir el capítulo poco antes de soltar el libro.
Wiley representantes no pudieron comentar de inmediato sobre por qué el capítulo
fue retirado.
El capítulo contiene los primeros recuento de Mitnick de su vida como un pirata y un
fugitivo, así como su detención, el juicio y la vida en la cárcel.
El capítulo también incluye acusaciones de que John Markoff Mitnick, la tecnología
reportero de The New York Times, impreso infundios sobre Mitnick durante
del hacker años como fugitivo.
El capítulo que falta se hizo por primera vez a disposición del público la noche del sábado en Yahoo
grupo de discusión llamado "Kevin es historia". Desde entonces ha aparecido en otros sitios web.
Mitnick dijo que no sabía que había fijado el capítulo online. E-mails a la
yahoo.com dirección que aparece con el mensaje original no obtuvo respuesta.
"Me siento muy bien sobre el capítulo que se está disponible", dijo Mitnick. "Por un largo
momento en que fue presentado como el Osama bin Laden de la Internet y yo quería realmente
para poder decirle a mi lado de la historia. Yo quería ser capaz de explicar exactamente lo que
Lo hice y lo que no hacen a la gente que pensaba que me conocía ".
Gran parte del material en la "falta el capítulo" detalles Mitnick relaciones con
Markoff.
La principal preocupación de Mitnick es que Markoff "no reconoció una preexistente
relación "con Mitnick en una historia de 04 de julio 1994, que apareció en la
primera página de The New York Times.
Historia de Markoff se describe como un hacker Mitnick muy peligroso capaz de
intrusión en los ordenadores gubernamentales críticas e insistió en que Mitnick había hasta el momento
eludirse fácilmente las fuerzas del orden.
Mitnick las acusaciones de que Markoff estaba enojado con él debido a un reparto de la película no
basado en el libro de Markoff 1991, Cyberpunk: Forajidos y hackers en el
Equipo de Frontera.
En el momento de su publicación, Mitnick disputa la veracidad del libro, pero más tarde aceptó
5.000 dólares de una oferta total de 50.000 dólares para actuar como consultor para la película basada en la
libro porque necesitaba el dinero.
Dos años más tarde, cuando el estudio quería renovar el contrato, Mitnick, para entonces
empleados, se negó a renovar. Esta negativa, de acuerdo con Mitnick y dos fuentes
familiarizado con el incidente, hizo que el acuerdo para morir.
Mitnick dijo Markoff debería haber mencionado el acuerdo comercial fracasó en su
artículos subsiguientes sobre Mitnick. También sostiene que muchos de los hacks
que se le atribuyen por Markoff nunca sucedió.
"Pero tratar de demostrar que no hackear algo es imposible si la gente
creo que está lo suficientemente capacitado para evadir la detección ", dijo Mitnick.
Markoff se negó rotundamente a comentar cualquiera de las acusaciones de Mitnick en el capítulo Una.
Mitnick dijo que deseaba que el capítulo podría haber sido publicado con el libro, pero
que respetaba la decisión de su editorial.
"Pero, obviamente, el Internet es una excelente manera de filtrar sin censura,
información a todo el mundo ", agregó Mitnick." Estoy contando los días hasta que pueda
ir en línea otra vez. "
Mitnick se le ha prohibido el uso de Internet como una condición de su supervisión
puesta en libertad. Él es libre de ir de nuevo en línea el 21 de enero de 2003, después de cerca de ocho
años fuera de línea.
El primer sitio que visitamos es el blog de su novia.

"Ella me dice que ha estado documentando nuestra línea de relación con el" Mitnick , dijo. "Me encantaría saber lo que ella ha estado diciendo sobre mí."

Introducción

Kevin Mitnick (alias "Cóndor") es sin dudas el hacker más conocido. Movido por una curiosidad insaciable sobre la tecnología de las computadoras y los teléfonos, se especializó en phreaking y en ingeniería social. Sus actividades llevaro el tema del hacking a los medios en forma masiva y fue objeto de durísima reprimenda. Ha cumplido condena y recuperó su libertad pero le ha sido vedado el acercarse a ordenador alguno.

En esta página se presenta el capítulo número uno, no publicado, del libro de Kevin Mitnick "The Art of Deception" ("El Arte del Engaño"). Este capítulo obtenido en formato pdf de algún sitio que ahora no recuerdo, ha sido arreglado por un compilador anónimo que explica en la últmia página su origen. De acuerdo a lo que se dice en un informe de la revista Wired, parece que Kevin escribió esto para el libro pero fue cortado por el editor poco antes de salir a la venta, por razones hast el momento desconocidas. Sin embargo sin más que leer me doy cuenta que Kevin hace su descargo y habla, más allá de su culpabilidad, sobre la manipulación y tergiversación de la información por parte de los medios y sobre la igualdad de derechos en un país, Estados Unidos, que se jacta de la libertad ciudadana.

Como la idea es siempre difundir la información, y el compilador del capítulo insta a ello, me pareció adecuado realizar una traducción del material y presentarla aquí, obviamente junto con el original en pdf. Así aquellos que puedan leer inglés o simplemente prefieran la versión original, no tienen más que bajarlo desde aquí.

Kevin Mitnick - The Art Of Deception - Unpublished Chapter 1 [traducción]

Capítulo 1
La historia de Kevin
Por Kevin Mitnick

Estaba un poco reacio a escribir esta seccion debido a que seguramente sonaría algo autocomplaciente. Bien, ok, es autocomplaciente. Pero he sido contactado por cientos de personas que querían saber "¿quién es Kevin Mitnick?". Para aquellos a quienes no importa, por favor sigan con el capítulo dos. Para todos los demás, esta es mi historia.

Kevin habla

Algunos hackers destruyen los archivos de la gente o discos rigidos enteros; son los llamados crackers o vándalos. Algunos hackers novicios no se preocupan siquiera de aprender la tecnología, tan solo se dedican a bajar herramientas de hacker para irrumpir en sistemas informáticos; son los llamados "script kiddies". Hackers más experimentados con conocimientos de programación desarrollan software que postean en la web y en BBS's. Son individuos sin un interés particular en la tecnología, pero que utilizan las computadoras simplemente como herramientas para ganar dinero, bienes o servicios.
Mas allá del mito de Kevin Mitnick, creado por los medios, no soy un hacker malicioso. Lo que yo hice incluso no era contra la ley al momento de comenzarlo, sino que se volvió un crimen al surgir nueva legislación. Yo continué y fui atrapado. El trato que se me dio por parte del gobierno federal se basó no en los crímenes, sino en hacer de mí un ejemplo. No merezco ser tratado como un terrorista o un criminal violento: registrando mi residencia sin autorización, aislado por meses, siéndome denegados derechos constitucionales fundamentales garantizados a cualquiera acusado de un crimen, negándose la fianza y una apelación para ella, forzándome a emplear años en peleas legales para obtener la evidencia gubernamental que le permitiera a mi abogado preparar mi defensa.
¿Qué hay acerca de mi derecho a un juicio rápido? Por años se me dio una chance cada seis meses: firmar un papel renunciando a mi derecho constitucional de un juicio rápido o ir a juicio con un abogado no preparado del todo; elegí firmar. Pero me estoy adelantando en mi historia.

Comenzando

Mi ruta fue probablemente establecida desde temprano. En aquel entonces era un chico feliz, pero aburrido. Luego de que mi padre partió cuando tenía tres años, mi madre trabajó de camarera para mantenernos. Me veo como un niño mantenido por una madre sometida a horarios erráticos, que luego pasó a ser un joven teniéndoselas que vérselas por sus propios medios todo el tiempo.Yó fui mi propio babysitter.
Crecer en una comunidad de San Fernando Valle significó explorar todo Los Angeles, y para la edad de doce había descubierto una manera de viajar gratis a través de la gran área de L.A. Mientras corría el autobus un día caí en cuenta que la seguridad del transfer que había comprado residía en el inusual patrón del punzón que los conductores utilizan para marcar el día, tiempo y la ruta en dichos transfers. Un amigable chofer, al cual pregunté en forma muy cuidadosa, me dijo donde podía comprar ese tipo especial de punzón. Los transfers cumplían la función de permitir el trasbordo de bus y continuar viaje a destino, pero yó elaboré un plan para utilizarlos de forma que me permitiesen viajar a donde quisiese sin pagar. Obtener transfers en blanco fue fácil: los tachos de basura en las terminales estaban llenos de libros con transfers parcialmente usados que eran arrojados por los choferes al final de sus recorridos. Con una plancha de esos y el punzón fui capaz de marcar mis propios transfers y viajar a cualquier parte donde los buses de LA. Llegaban. Luego de algún tiempo tenía memorizados todas las rutinas del sistema de transporte.

Este es solo un ejemplo de mi sorprendente memoria para ciertos tipos de información; aún hoy puedo recordar números de teléfono, passwords y otras cosas que datan de mi niñez.

Otro interés personal que emergió en mí a temprana edad fue mi fascinación con la magia. Una vez que aprendía como funcionaba un truco, lo practicaba, lo practicaba y lo practicaba hasta dominarlo. Por extensión, fue a través de la magia que descubrí el placer de engañar gente.

De Phreaker a Hacker

Mi primer encuentro con lo que eventualmente aprendería a llamar "ingeniería social" fue en mis años de High School cuando me encontré con otro estudiante que estaba metido en un hobby llamado "phone phreaking". Este es un tipo de hackeo que permite explorar la red telefónica explotando los sistemas telefónicos y a los empleados de las empresas que brindan estos servicios.El me mostró algunos trucos que pudo hacer con un teléfono, como por ejemplo obtener de la compañía teléfonica cualquier información que esta tuviera acerca de un cliente en particular, y utilizar un número secreto de prueba para realizar llamadas de larga distancia en forma gratuita (mucho mas tarde descubrí que no era un número secreto después de todo: las llamadas estaban facturándose a una cuenta MCI de alguna compañia). Esta fue mi introducción a la ingeniería social, mi jardín de infantes, para decirlo de cierto modo.

El y otro phreaker que conocí mientras tanto me dejaron escuchar las llamadas que realizaban a la compañía telefónica. Escuché las cosas que ellos decían para que sonase convincente, aprendí sobre diferentes oficinas de las telefónicas, el lingo y los procedimientos. Pero ese "entrenamiento" no duró demasiado. Pronto lo estaba haciendo por mi cuenta, haciéndolo incluso mejor que aquellos primeros maestros. El curso que mi vida seguiría en los próximos quince años ya estaba definido.

Una de mis travesuras favoritas era ganar acceso no autorizado al switch telefónico y cambiar el tipo de servicio de algún compañero phreak. Cuando intentase realizar una llamada desde su casa, obtendría un mensaje pidiéndole que deposite diez centavos, debido a que el switch de la compañía telefónica indicaba que estaba llamando desde un teléfono por cobrar.

Me vi absorbido por saber todo sobre teléfonos, no solamente la electrónica, switches y computadoras, sino también la organización corporativa, los procedimientos y la terminología. Luego de un tiempo probablemente sabía más sobre todo el sistema telefónico que cualquier empleado. Asimismo había desarrollado mis habilidades de ingeniero social hasta tal punto que podía, a los diecisiete años, hablar con muchos de los empleados de las Telco acerca de cualquier asunto, ya sea en persona o por teléfono.

Mi carrera hacker comenzó en la secundaria. Entonces el término hacker se utilizaba para cualquier persona que empleaba una gran cantidad de tiempo liando con hardware y software, para desarrollar programas más eficientes o para saltear pasos innecesarios y terminar el trabajo más rápidamente. El término se ha desvirtuado ahora, pasando a cobrar significado de "criminal malicioso". En estas páginas yó utilizo el término en su sentido más benigno de los viejos tiempos.

A fines de 1979 un grupo de compañeros hackers que habían trabajado para el Los Angeles Unified School District me desafiaron para que intentase hackear en The Ark, el sistema computacional en DEC utilizado para desarrollar su sistema operativo RSTS/E. Yó quería ser aceptado por esos tipos en este grupo para poder aprender más sobre sistemas operativos. Ellos se las habían ingeniado para hacerse con el número de dial-up al sistema DEC. Pero ellos sabían que el simple número no me sería de utilidad: sin un nombre de cuenta y un password jamás sería capaz de ingresar. Se darían cuenta luego que cuando uno subestima a los otros, eso te retorna como una mordida en el trasero.

Resultó que, incluso a esa joven edad, hackear el sistema DEC fue pan comido. Clamando ser Anton Chernoff, uno de los desarrolladores del proyecto, simplemente realizé una llamada al administrador del sistema. Le dije que no podía ingresar en una de "mis cuentas", y fui lo suficientemente convincente quea este tipo me permitió ingresar y elegir un password de mi

agrado. Como nivel extra de protección, cada vez que alguien ingresaba en el sistema de desarrollo, el usuario debía proveer un password de dial-up. El administrador del sistema me proveyó del password. Este era "buffoon" lo cual me parece que describe como se debe haber sentido cuando, mucho más tarde, descubrió lo que había sucedido. En menos de cinco minutos había ganado acceso al sistema de desarrollo del RSTS/E de Digital. Y no estaba logeado como un usuario estándar sino como alguien con todos los privilegios de un desarrollador de sistema. En el comienzo mis llamados-amigos rehusaron creer que había ganado acceso a The Ark. Uno de ellos marcó el número de dial-up del sistema y me puso el teclado enfrente con un aspecto desafiante en su rostro. Su boca se quedó abierta cuando me ingresé en una cuenta privilegiada. Supe luego que, desde otro lugar, ese mismo día comenzaron a hacer download de componentes del código fuente del sistema operativo DEC. Entonces llegaría mi turno de ser derribado.

Luego de que hubieron bajado el software que quisieron, llamaron al departamento de seguridad corporativa de DEC y les informaron que alguien había hackeado en la red de la compañía. Incluso les dieron mi nombre. Mis llamados-amigos primero utilizaron mi acceso para copiar código fuente y luego me traicionaron. Había una lección aquí, pero no una de la cual yó pudiera aprender fácilmente.

En el transcurso de los años venideros, repetidamente me metería en problemas debido a que confiaba en gente que pensaba que eran mis amigos. Luego de la secundaria estudie computación en el Computer Learning Center de Los Angeles. Dentro de unos pocos meses el manager del sistema de la escuela se dio cuenta de que yó había hallado una vulnerabilidad en el sistema operativo y ganado privilegios administrativos completos en su minicomputadora IBM. Los mejores expertos en su staff no podían explicarse como lo había hecho. En lo que podría ser uno de los primeros ejemplos de "contraten al hacker" me fue ofrecida una oferta que no pude rechazar: realizar un proyecto para mejorar la seguridad del sistema computacional de la escuela, o afrontar una suspensión por hackear el sistema. Por supuesto elegí realizar el proyecto y terminé graduándome con honores.

Volviéndose un Ingeniero Social

Alguna gente se levanta cada mañama aborreciendo su rutinal trabajo. He sido lo suficientemente afortunado para disfrutar mi trabajo. Particularmente usted no podría imaginarse el desafío, satisfacción y placer obtenido por el tiempo dedicado a hacer de investigador privado. Perfeccionando mis talentos en el arte llamado ingeniería social -haciendo que la gente haga cosas que no harían de ordinario para un extraño- y siendo pagado por ello.

No fue dificil volverme competente en ingeniería social. El lado paterno de mi familia se había dedicado a las ventas por generaciones, con lo cual el arte de la influencia y la persuación pudieron ser una característica inherente. Cuando usted combina una inclinación por engañar gente con los talentos de la influencia y la persuación, se llega al perfil de un ingeniero social. Podríamos decir que hay dos clasificaciones dentro del arte de la estafa. Alguien que engaña gente para apropiarse de su dinero pertenece a la subespecialidad de estafador; mientras que alguien que utiliza el engaño, la influencia y la persuación contras las compañias, usualemente apuntando a su información, pertenece a la otra subespecialidad: el ingeniero social. Desde la época de mi truco del bus, cuando era demasiado joven para saber si lo que estaba haciendo tenía algo de malo, comencé a reconocer en mí un talento para hallar los secretos que se supone no debería hallar. Perfeccioné ese talento utilizando engaño, conociendo el lingo y desarrollando mi destreza para la manipulación.

Una manera en la cual solía trabajar los trucos de mi destreza era seleccionar algún tipo de información, ni siquiera importante, y ver si podía hablar con alguien del otro lado de la línea para que me la proveyese, solo para mejorar mis aptitudes. De la misma manera solía practicar mis trucos de magia, practiqué los pretextos. A través de esos ensayos pronto hallé que podía adquirir virtualmente cualquier información que desease.

Brindando testimonio al Congreso ante los senadores Lieberman y Thompson, años más tarde, les dije: "He ganado acceso no autorizado a sistemas informáticos de algunas de las mayores corporaciones del planeta y he penetrado exitosamente en algunos de los sistemas más protegidos. He utilizado medios técnicos y no-técnicos para obtener el código fueten de varios sistemas operativos y dispositivos de telecomunicaciones para estudiar sus vulnerabilidades y su funcionamiento interno".

Todo esto fue realmente para satisfacer mi propia curiosidad, ver lo que podía hacer y hallar información secreta acerca de sistemas operativos, teléfonos celulares y cualquier otra cosa que satisficiese mi curiosidad. La sucesión de eventos que cambiaría mi vida comenzó cuando me volví el tema de portada de la edición del 4 de julio de 1994 del New York Times.

Así, de la noche a la mañana, cambió mi imagen desde un poco conocido pero molesto hacker en el enemigo número uno del ciberespacio.

John Markoff, el estafador de los medios

"Combinando conocimiento técnico con la astucia de un estafador, Kevin Mitnick es un programador enloquecido" [New York Times 4/7/1994]. Combinando el eterno deseo de alcanzar una fortuna no merecida con el poder de publicar historias falsas y difamatorias en la portada del New York Times, John Markoff fue realmente un reporteero enloquecido. Markoff ganaría más de un millón de dólares simplemente por crear lo que yo llamo "El Mito de Kevin Mitnick".

El se volvió sumamente rico a través de las mismas técnicas que utilicé para comprometer sistemas informáticos y redes mundiales: el engaño. En este caso la víctima del engaño no fue un simple usuario o un administrador de sistemas sino cada una de las personas que confiaron en las historias publicadas en las páginas del New York Times.

El más buscado del cyberespacio

El artículo de Markoff claramente estaba destinado a conseguir un contrato por un libro acerca de mi vida. Nunca he conocido a Markoff, pero aún se ha vuelto literalmente millonario a través de su reporte difamatorio publicado en el Times y de su libro Cyberpunk de 1991. En su artículo él incluye docenas de alegatos sobre mi, que afirma como verdaderos sin citar siquiera las fuentes, y que incluso un chequeo mínimo (el cual pienso que todo periódico de importancia solicita a sus reporteros realizar) hubiese revelado que son falsos o improbados. En este artículo Markoff me caratuló como "El más buscado del cyberespacio" y como "uno de los criminales informáticos mas buscados", sin razón o evidencia válida,. utilizando no más discreción que la de un escritor de tabloides de supermercado.

En su artículo Markoff falsamente dijo que yó había grabado al FBI (no es cierto); que había ingresado en el sistema informático de NORAD (el cual no está siquiera conectado a red alguna exterior) y que era un "vándalo" de la informática, pese al hecho de que yó jamás dañe intencionalemente ninguna de las computadoras a las cuales tuve acceso. Estos, entre otros ultrajantes alegatos, son completamente falsos y estaban diseñados para crear una sensación de miedo acerca de mis capacidades.

En aún otra falta de ética periodística, Markoff no reveló en ese artículo ni en los subsiguientes una relación pre-existente conmigo, una animosidad personal basada en el hecho de haberme negado yó a colaborar en su libro Cyberpunk. Asimismo, he significado la imposibilidad de recibir potenciales ingresos rehusándome a permitir una opción para una película basada en el libro. El artículo de Markoff, fiue también claramente pensado para burlarse de las agencias encargadas de hacer cumplir la ley. Deliberadamente me promocionaba como el Enenigo Publico Numero Uno del cyberespacio, buscando de esa forma que el Departamento de Justicia elevara la prioridad de mi caso. Un par de meses más tarde, Markoff y su cohorte Tsutomu Shimomura participarían

como agentes de facto del gobierno en mi arresto, en violación de la ley federal y la ética periodística.

Ambos estaban cerca cuando tres ordenes en blanco fueron usados en una búsqueda ilegal de mi residencia, y estaban presentes en mi arresto. Y durante su investigación de mis actividades, ambos violarían la ley federal interceptando una llamada personal mía. Mientras hacía de mi un villano, Markoff, en un subsiguiente artículo, estableció a Shimomura como el héroe número uno del cyberespacio.

Otra vez estaba violando la ética periodística al no revelar la relación preexistente: este héroe era en realidad amigo personal de Markoff desde hacía años.

Primer Contacto

Mi primer contacto con Markoff sobrevino a finales de los ochenta, cuando él y sus esposa Katie Hafner me contactaron mientras estaban en el proceso de escribir Cyberpunk. el cual era la historia de tres hackers: un chico alemán conocido como Pengo, Robert Morris y Yó. ¿Cuál sería mi recompensa por participar? Ninguna.

No pude ver el punto en darles a ellos mi historia si ellos lucrarían con ella y yo no recibiría nada, entonces me rehusé. Markoff me dio un ultimátum: les daba mi historia o sería tomado como verdadero cualquier cosa que escuchase de cualquier fuente. Estaba claramente frustado y enfadado de que yo no cooperase, y me dejó saber que tenía los medios para hacerme cambiar de parecer. Yó elegí continuar en mi postura pese a las tácticas de presión que emplease. Cuando fue publicado el libro me pintaba como un "Hacker del Lado Oscuro". Concluí que los autores habían intencionalmente incluído material infundado o falso para perjudicarme en despecho de no haber colaborado con ellos. Haciéndome aparecer más siniestro probablemente incrementaron las ventas de su libro.

Un productor de cine me telefoneó con grandes noticias: Hollywood estaba interesada en hacer una película del oscuro hacker pintado en Cyberpunk. Le señale que la historia estaba llena de imprecisiones y datos falsos, pero aún estaba muy excitado con el proyecto. Yó acepté U$D 5000 por un opción a dos años, contra unos U$D 45000 si ellos eran capaces de llegar a un acuerdo para producción y avanzar.

Cuando la opción expiró, la compañia productora me pidió una extensión de seis meses. Para esta época yó estaba bien empleado y tenía poca motivación para permitir una película sobre mi que me mostrase bajo tal desfavorable y falsa luz. No acepté seguir con la extensión. Eso terminó con el proyecto de la película para todos, incluso Markoff, quien probablemente esperaba hacerse una gran suma de dinero con ella. Aquí hubo otra razón más para que John Markoff se ensañara conmigo.

En el tiempo de la publicación de Cyberpunk, Markoff se comunicaba por correo electrónico con su amigo Shimomura. Ambos estaban estrañamente interesados en mi y en lo que estaba haciendo. Sorprendentemente un email comentaba que ellos sabían que estaba trabajando en la Universidad de Nevada, Las Vegas, y utilizaba el laboratorio informático estudiantil. ¿Pudiera ser que Markoff y Shimomura estuviesen interesados en realizar otro libro sobre mí? Por otro lado, ¿para qué se preocuparían de lo que yó hacía?

Markoff en persecución

Volvamos a Septiembre de 1992. Estaba próximo a finalizar mí período de libertad supervisada por haber comprometido la red corporativa de DEC. Entretanto, debido a que estaba consciente de que el gobierno estaba intentando poner otro caso en mi contra, en esta ocasión por realizar actividades de contrainteligencia para descubrir por qué causa se habían intervenido las líneas

telefónicas de una firma de Los Angeles. En mi pesquisa confirmé mi sospecha: la gente de seguridad de Pacific Bell estaba investigando la firma.
Ese era un deputy del crimen informático de la oficina del sheriff del condado de Los Angeles.(Ese deputy sería, casualmente, el hermano gemelo de mi coautor en este libro. ¡Qué mundo pequeño!). En este tiempo los federales habían establecido un informe criminal y lo enviaban a él para atraparme. Ellos sabían que yo siempre había intentado vigilar cualquier agencia que me estuviera investigando. Entonces ellos tenían a este informante ofreciéndome amistad y advirtiéndome que estaba siendo monitoreado. Él también compartió conmigo los detalles de un sistema informático utilizado en Pacific Bell que me permitiría hacer contraespionaje de su monitoreo.
Cuando descubrí su jugada, rápidamente volví las tables contra él y lo expuse por fraude con tarjeta de crédito, el cual a la sazón se hallaba realizando mientras trabajaba para el gobierno en calidad de informante. ¡Estoy seguro de que los federales apreciaron esto!
Mi vida cambió el día de la independencia de 1994, cuando mi pager me despertó temprano en la mañana. El llamado decía que consiguiese inmediatamente una copia del New York Times. Yo no podía creer cuando vi que Markoff no sólo había escrito un artículo sobre mí, sino que el Times había puesto mi foto en primera plana. Lo primero que se me pasó por la cabeza fue el tema de mi seguridad, ahora el gobierno intensificaría los esfuerzos para encontrarme. Estaba aliviado de que, en un esfuerzo por hacerme aparecer demoníaco, el Times hubiese empleado una fotografía que no era apropiada. No me atemorizó el ser reconocido porque ellos habían utilizado una foto tan poco actual, que ni siquiera lucía como yo.
A medida que leía el artículo concluí que Markoff se estaba preparando para escribir el libro de Kevin Mitnick, como siempre había querido. Simplemente no podía creer que el New York Times se arriesgará a dar prensa a las flagrantes y falsas afirmaciones que él había escrito sobre mí. Me sentí desamparado. Incluso si hubiese estado en posición de responderle, ciertamente no hubiera tenido una audiencia igual a la del New York Times para rebatir las atroces mentiras de Markoff.
Pese a que debo aceptar que yo era un "dolor en el trasero", nunca hube destruido informacion, ni utilizado o divulgado a otros cualquier informacion que obtuve. Las pérdidas de las compañias por mis actividades de hacker se debían al costo de las llamadas que había realizado a sus expensas, el dinero gastado por las compañias para tapar las vulnerabilidades que mis ataques habían revelado, y en algunas pocas circunstancias posiblemente la necesidad de la reinstalacion de sus sistemas operativos y aplicaciones por el miedo de que yo hubiese modificado el software de manera que me permitiése futuro acceso. Esas compañias hubiesen permanecido vulnerables a un daño mucho peor si mis actividades no las hubieran hecho concientes de sus débiles vinculos en su cadena de seguridad. Pese a que he causado algunas pérdidas, mis acciones y motivos no fueron maliciosos ... y entonces John Markoff cambió la percepción del mundo sobre el peligro que yo representaba. El poder de un reportero carente de ética de un periódico tan influyente para escribir un articulo falso y difamatorio acerca de cualquiera debería concientizar a cada uno de nosotros. El próximo podría ser usted.

La Orden

Luego de mi arresto fui transportado a la cárcel del condado en Smithfield, North Carolina, en donde el servicio de Marshals de los Estados Unidos le ordenó situarme en "el hoyo"-confinamiento solitario-. Después de una semana los acusadores federales y mi abogado llegaron a un acuerdo que yo no pude rehusar. Sería retirado del aislamiento en la condicion de que renunciase a mis derechos fundamentales y aceptara que: a) no hablaría de libertad bajo fianza, b) no habría fianza preliminar y c) no realizaría llamadas telefónicas, excepto a mi abogado y a dos familiares. Firmaba y podría salir del confinamiento solitario. Yo firmé. Los federales del caso utilizaron cada truco sucio en el libro hasta que me liberaron cinco años después. Fui repetidamente obligado a renunciar a mis derechos para conseguir ser tratado como cualquier otro acusado.
Así fue el caso de Kevin Mitnick: no hubo reglas. No se respetaron los derechos constitucionales del acusado. Mi caso no fue sobre justicia, sino sobre la determinación del gobierno de ganar a cualquier precio. Los fiscales habían hecho verborrágicos alegatos a la corte acerca del daño que

había inflingido y la amenaza que yo representaba, los medios habían llevado al pueblo las afirmaciones sensacionalistas; era demasiado tarde para que los acusadores se retractasen. El gobierno no se podía permitir perder el caso Mitnick. El mundo estaba observando.
Creí que las cortes habían caído en el temor de la cobertura de los medios, porque muchos de los mas éticos reporteros habían tomado los "hechos" del estimado New York Times y repetido tal cual. El mito generado por los medios aparentemente asustó incluso a los oficiales de la ley. Un documento confidencial obtenido por mi abogado mostraba que el servicio de Marshals de los EE.UU. había emitido una advertencia para todos sus agentes de no reverlarme ninguno de sus datos personales bajo riesgo de ver sus vidas electrónicamente destruídas. Nuestra Constitucion requiere que el acusado se presuma inocente antes del juicio, garantizando a todos los ciudadanos el derecho de una libertad bajo fianza donde el acusado tiene la oportunidad de ser representado por un abogado, presentar evidencia y testigos.
Increíblemente, el gobierno había sido capaz de obviar esas protecciones basados en la falsa histeria generada por los reporteros irresponsables como John Markoff. Sin precedentes fui mantenido como un detenido pre-juicio (persona en custodia pendiente de juicio o de sentencia) por cerca de cuatro años y medio. La decisión judicial de negárseme la libertad bajo fianza fue litigiada todo el camino hasta la Suprema Corte de los EE.UU. Sobre el final mi defensa advirtió que había sentado otro precedente: fui el único detenido federal de la historia de los Estados Unidos al cual se le negó una libertad bajo fianza. Esto significa que el gobierno nunca tuvo que soportar la carga de que no existían condiciones de libertad razonables que hubieran asegurado que apareciese en la corte.
Al menos en esta ocasión, los fiscales federales no se atrevieron a alegar que podría iniciar una guerra nuclear por hacer phreaking en un teléfono, como otros hubieron hecho anteriormente. El cargo más serio en mi contra era que había copiado código fuente propietario de varios teléfonos celulares y sistemas operativos. Incluso los fiscales sostuvieron publicamente y en la corte, que había causado perdidas colectivas a las compañias que excedían los U$D 300 millones. Los detalles de los montos de las pérdidas están aún sellados con la corte, supuestamente para proteger a las compañias implicadas; mi defensa cree que el pedido de la fiscalía de sellar la información fue iniciado para cubrir la deliberada exageración de mi caso.
Es de notar también que ninguna de las víctimas en mi caso haya reportado sus perdidas a la Securities and Exchange Commission, como es requerido por ley. O bien varias compañias multinacionales violaron la ley federal, defraudando en el proceso a la SEC, los accionistas, los analistas, etc, o bien las pérdidas atribuídas a mi hackeo fueron, de hecho demasiado triviales para reportarlas.
En su libro The Fugitive Game, Jonathan Littman decía que a una semana de la historia de tapa del New York Times, el agente de Markoff había concertado un acuerdo con el editor Walt Disney Hyperion para un libro acerca de la campaña para atraparme. El adelanto se estimaba en U$D 750000. De acuerdo a Littman habría una película de Hollywood también, con Miramax destinando unos U$D 200000 para la opción y "un total de U$D 650000 a ser pagados luego de comenzado el rodaje". Una fuente confidencial me ha informado recientemente que el trato de Markoff fue mayor a lo que Littman había sugerido originalmente.
Entonces John Markoff tuvo un millón de dólares, más o menos, y yo tuve cinco años.

Lo que Otros Dijeron

Un libro que examina los aspectos legales de mi caso fue escrito por un hombre que formó parte de la fiscalía en la oficina del distrito de Los Angeles, un colega de quienes me acusaron. En su libro "Spectacular Computer Crimes", Buck Bloombecker escribió, "me aflige tener que escribir acerca de mis anteriores colegas en estos menos que favorecedores términos... yo llegué a la conclusión de que mucho del argumento utilizado para mantener a Kevin Mitnick tras los barrotes fue basado en rumores que no se justificaban", incluso dice que "fue malo que los cargos que los fiscales hicieron en la corte se desaparramaran a millones de lectores de periódicos en todo el país. Pero fue mucho peor que esos alegatos falsos fueran una gran parte de la base que mantuvo a Mitnick tras las barras sin la posibilidad de fianza".
Continúa escribiendo sobre los estándares éticos para los cuales deberían vivir los fiscales, y

luego dice, "el caso de Mitnick sugiere que los falsos alegatos utilizados para mantenerlo bajo custodia también perjudicaron las consideraciones de la corte para una sentencia justa". En el artículo de 1999 en Forbes, Adam L.Penenberg describió elocuentemente mi situación de esta manera: "Los crímenes de Mitnick fueron curiosamente inocuos. El irrumpió en computadoras corporativas, pero no hay evidencia de que haya destruido datos. Ni siquiera de que haya vendido algo de lo que copió. Sí, él robó software pero esa actividad en sí estaba en segundo plano". El artículo decía que mi crimen fue "meter su nariz al costo de los sistemas de seguridad informática empleados por las grandes corporaciones".
Y en su libro The Fugitive Game, el autor Jonathan Littman, notó que: "El gobierno podría entender la codicia. Pero un hacker que tenía el poder de su propia pasión ... era algo que no podían tolerar". En alguna parte del libro Littman escribió: "La agencia de abogados James Sanders admitió al juez Pfaelzer que el daño de Mitnick a DEC no fue el publicado, de U$D 4 millones, sino de U$D 160.000. Incluso ese monto no representaba el daño direco de Mitnick sino el costo de rastrear las vulnerabilidades de seguridad que sus incursiones habían hecho notar a la DEC.
"El gobierno admitió que no tenía evidencia de los salvajes cargos que habían ayudado a mantener a Mitnick sin fianza y en confinamiento solitario. No había prueba de que Mitnick hubiese comprometido la seguridad de la NSA. No había prueba de que Mitnick haya alguna vez emitido un falso comunicado para Security Pacific Bank. No había prueba de que Mitnick alguna vez acmbiase el reporte de credito TRW de un juez. Pero el juez, tal vez influenciado por la terrible cobertura de los medios, rechazó la súplica de la defensa y sentenció a Mitnick por un período incluso mayor que el pretendido por el gobierno."
A través de los años pasados dedicándome al hacking había ganado cierta notoriedad no deseada, se había escrito sobre mí en numerosos reportes de noticias y artículos de revista, y tenía cuatro libros sobre mí. El libro de Markoff y Shimomura fue llevado al cine en un film llamado Takedown. Cuando el guión alcanzó la Internet, muchos de mis seguidores instaron a Miramax Films para llamar la atención pública sobre lo inexacto y falso de la caracterización que de mi se hacía. Sin la ayuda de mucha y generosa gente, la película seguramente me hubiera mostrado en forma falsa como el Hannibal Lecter del cyberespacio. Presionada por mis seguidores, la productora accedió a resolver el caso en términos confidenciales para evitar una acción mía por difamación en contra de ellos.

Pensamientos Finales

Pese a la difamatoria y ultrajante descripción de John Markoff sobre mí, mis crímenes fueron simplemente de intromisón en computadoras y de realizar llamadas telefónicas gratuitas. He aceptado desde mi arresto que las acciones que yo realicé son ilegales, y que hube cometido invasiones de la privacidad. Pero sugerir, sin justificación, razón o prueba, como se hizo en los artículos de Markoff, que hube privado a otros de su dinero, o propiedad por fraude informático o electrónico, es simplemente incorrecto y no confirmado por la evidencia.
Mis fechorías fueron motivadas por la curiosidad: yo quería saber tanto como pudiese sobre como trabajaban las redes de teléfonos, y los vericuetos de la seguridad informática. Pasé de ser un chico que amaba realizar trucos de magia a convertirme en el hacker más notorio, temido por las corporaciones y el gobierno. Cuando miro hacia atrás en mi vida de estos últimos treinta años, debo admitir que he tomado algunas decisiones extremadamente malas, dictadas por la curiosidad, el deseo de aprender acerca de la tecnología, y un buen desafío intelectual.
Soy una persona que ha cambiado ahora. Estoy utilizando mis talentos y el conocimiento que he adquirido sobre seguridad informática y tácticas de ingeniería social para ayudar al gobierno y a los individuos a prevenir, detectar y responder ante amenazas de seguridad. Este libro es una manera más en la cual puedo utilizar mi experiencia para ayudar a evitar a otros los esfuerzos de esos maliciosos ladrones de información del mundo. Pienso que econtrará las historias entretenidas y educacionales.

-Kevin Mitnick