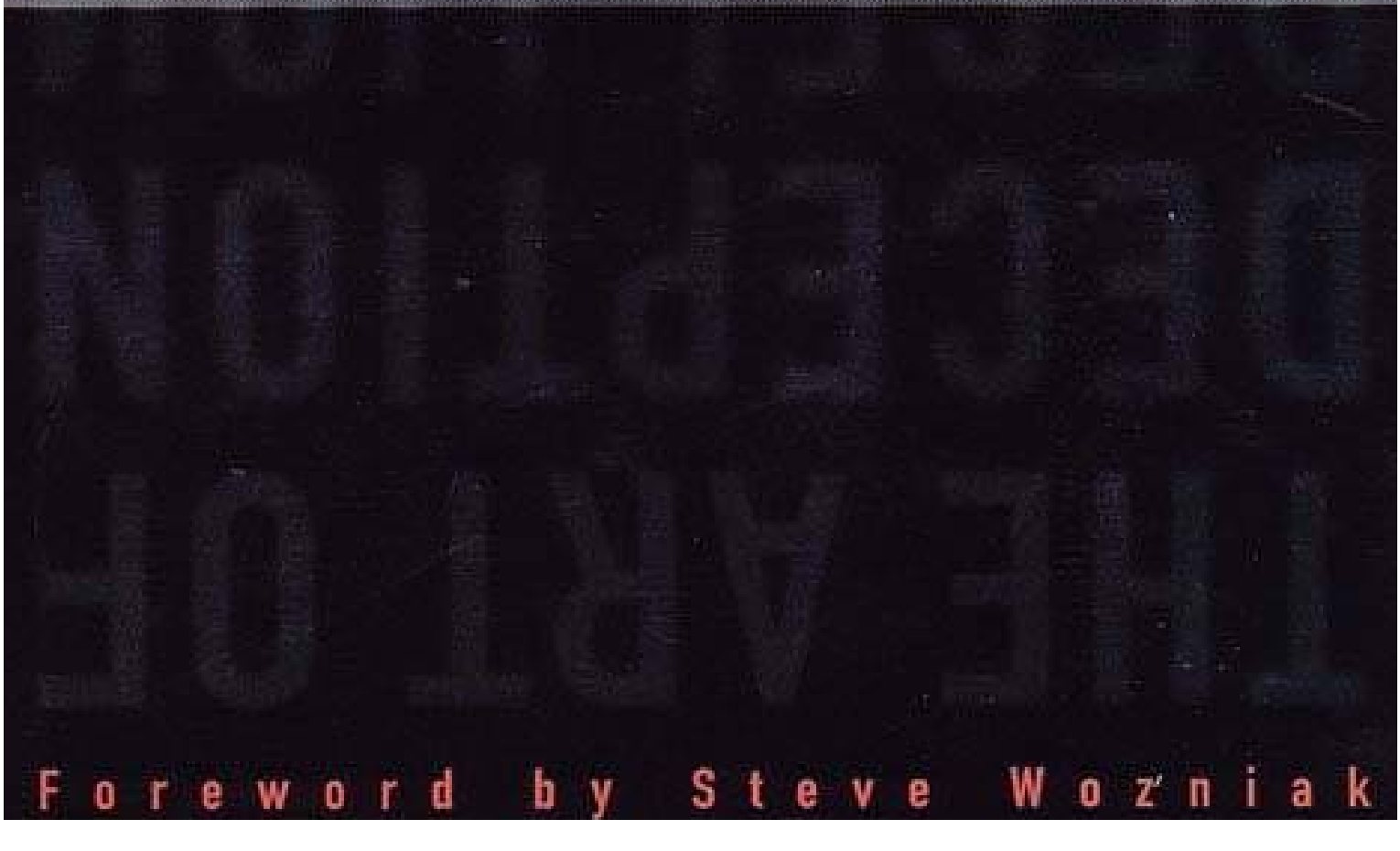
Controlling the Human Element of Security

THE ART OF DECEPTION

KEVIN D. MITNICK

& William L. Simon



Foreword by Steve Wozniak

EL ARTE DEL ENGAÑO

Controlar el elemento humano de la seguridad

KEVIN D. MITNICK
& William L. Simon
Prólogo de Steve Wozniak

ANALIZADOS POR KINETICSTOMP, REVISADO Y AMPLIADO POR SWI

Para Reba Vartanian, Shelly Jaffe, pollito Leventhal y Mitchell Mitnick y para la tarde Alan Mitnick, Adam Mitnick y Jack Biello

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

Ingeniería social

Ingeniería social utiliza influencia y persuasión para engañar a las personas por convencerlos de que el ingeniero social es alguien que no es o por manipulación. Como resultado, el ingeniero social es capaz de tomar ventaja de las personas para obtener información con o sin el uso de tecnología.

Contenido

Prólogo

Los seres humanos nacemos con una unidad interior para explorar la naturaleza de nuestro entorno. Como jóvenes, fueron intensamente curiosos tanto Kevin Mitnick y sobre el mundo y con ganas de demostrar a nosotros mismos. Fuimos galardonados con frecuencia en nue intenta aprender cosas nuevas, resolver acertijos y ganar en los juegos. Pero al mismo tiempo, el mundo nos enseña las reglas de comportamiento que limitado nuestro interior nos instar a hacia la exploración libre. Para nuestros más audaces científicos y tecnológicos empresarios, así como para personas como Kevin Mitnick, siguiendo este impulso interior ofrece la mayor emoción, permitirnos realizar cosas que otros creen que no se puede hacerse.

Kevin Mitnick es uno de las mejores personas que conozco. Le pido, y él dirá enérgicamente que solía hacer - ingeniería social – entrana estafar gente. Pero Kevin ya no es un ingeniero social. Y aun cuando fue su motivación nunca fue a enriquecerse o dañar a otros. Eso no quiere para decir que no peligrosos y destructivos criminales por ahí que utilizan la ingeniería social para causar daño real. De hecho, eso es exactamente por eso Kevin escribió este libro - para advertirle acerca de ellos.

El arte del engaño muestra cuán vulnerables somos - Gobierno, negocios, y cada uno de nosotros personalmente - a las intrusiones del ingeniero social. En este era consciente de la seguridad, nos gastan enormes sumas en tecnología para proteger nuestra datos y redes informáticas. Este libro señala lo fácil que es engañar a personas con información privilegiad y eludir toda esta protección tecnológica.
Si trabaja en la empresa o el Gobierno, este libro proporciona un camino poderoso Mapa para ayudarle a comprender cómo funcionan los ingenieros sociales y lo que puede hacer para frustrarles. Con historias de ficción entretenida y reveladora, Kevin y coautor Bill Simon dar vida a las técnicas de lo social Ingeniería inframundo. Después de cada historia, ofrecen directrices prácticas para ayudar a prevenir las violaciones y amenazas a que están descritos.

Seguridad tecnológica deja lagunas importantes que las personas como Kevin nos puede ayudar Cerrar. Lee este libro y finalmente puede darse cuenta que todos tenemos que recurrir a la De Mitnick entre nosotros para orientación.

Steve Wozniak

Prefacio

Algunos piratas informáticos destruyen popular archivos o discos duros enteros; llamamos galletas
o vándalos. Algunos piratas informáticos novato no te molestes en aprendizaje de la tecnología, sino simp
Descargar herramientas de hackers de irrumpir en los sistemas informáticos; llamamos script
kiddies. Los hackers más experimentados con conocimientos de programación desarrollan hacker
programas y publicarlos en la Web y a los sistemas de tablón de anuncios. Y, a continuación
son personas que no tienen ningún interés en la tecnología, pero usan la computadora
simplemente como una herramienta para ayudarlos en robar dinero, bienes o servicios.

A pesar del mito creado por medio de Kevin Mitnick, yo no soy un hacker malintencionado.

Pero me estoy poniendo por delante de mí.

SALIDA

Mi camino probablemente se estableció temprano en la vida. Yo era un niño despreocupado, pero aburrid
Después mi padre cuando yo tenía tres años, mi madre trabajó como camarera a
nos apoyan. A ver me luego - un sólo niño ser criado por una madre que puso en
durante mucho tiempo, atosigar días puntualmente a veces errático - habría sido ver un
jovencita en sus propio casi todas sus horas vigilia. Era mi niñera.

Creció en una comunidad del Valle de San Fernando me dio la totalidad de Los
Angeles para explorar y por la edad de los doce que había descubierto una manera de viajar gratis
en toda la zona de L.A. todo mayor. Me di cuenta un día mientras viajaba en el bus
que la seguridad de los traslados en autobús que había comprado dependía del inusual patrón
de la perforadora de papel, que los controladores se utilizan para marcar el día; tiempo y ruta en el
resguardos de transferencia. Me dijo un conductor amable, responder a mi pregunta cuidadosamente planta
Dónde comprar ese tipo especial de punch.

Las transferencias se supone que le permiten cambiar autobuses y continuar un viaje a su
destino, pero trabajó cómo utilizarlos para viajar a cualquier lugar que quería ir
de forma gratuita. Obtener transferencias en blanco fue un paseo por el Parque.

Los contenedores de basura en las terminales de autobús siempre estaban llenas de libros sólo-parcialme
de las transferencias que los controladores arrojó lejos del final de los turnos. Con una almohadilla de
espacios en blanco y el puñetazo, pude Marcar mis propias transferencias y viajar a cualquier lugar que
Autobuses de L.A. fueron. En poco tiempo, pero todo había memorizado los horarios de autobuses de la
todo el sistema. (Esto fue un ejemplo temprano de mi memoria sorprendente para determinados
tipos de información; Aún así, hoy, puedo recordar números de teléfono, contraseñas, y
otros detalles aparentemente triviales como en mi infancia).

Otro interés personal que surgieron en una edad temprana fue mi fascinación
realizar magia. Una vez que aprendí cómo funcionaba un truco nuevo, sería práctica,

practicar y practicar algunos más hasta que lo domina. En una medida, fue a través de magia que descubrí el disfrute en adquirir conocimiento secreto.

Desde teléfono venía de Hacker
Mi primer encuentro con lo que sería eventualmente aprendo llamar ingeniería social surgió durante mis años de secundaria cuando conocí a otro estudiante que fue atrapados en un hobby llamado teléfono phreakin. Teléfono phreaking es un tipo de hacking le permite explorar la red telefónica mediante la explotación de los sistemas telefónicos y empleados de la compañía de teléfono. Me mostró aseados trucos que podía hacer con una teléfono, como obtener cualquier información de la compañía telefónica en cualquier el cliente y utilizando un número de prueba secreta para hacer llamadas de larga distancia gratis. (En realidad era libre sólo a nosotros. Descubrí mucho más tarde que no era una prueba secreta número en absoluto. Las llamadas fueron, de hecho, se facturan a MCI algunos pobres empresa cuenta.)

Fue mi introducción a la ingeniería social-mi jardín de infantes, por así decirlo. Mi amigo y otro phreaker de teléfono que conocí poco después me deja escuchar que cada uno hace las llamadas de pretexto a la compañía telefónica. He escuchado las cosas dijeron les hizo sonar creíble; Aprendí sobre las oficinas de la empresa de teléfono diferente, jerga y procedimientos. Pero que la \"formación\" no duró mucho; no tuve que. Pronto me fue haciendo que todos en mi propia, aprendiendo como fui, haciendo incluso mejor que mi primera profesores.
Se ha creado el curso de que mi vida seguiría durante los próximos quince años. En alto escuela, uno de mis bromas favoritas de todos los tiempos fue obtener acceso no autorizado a la conmutador telefónico y cambiar la clase de servicio de un compañero por teléfono phreak. Cuando él intentó hacer una llamada desde su casa, obtendría un mensaje diciéndole que depósito un centavo porque había recibido el conmutador de la compañía de teléfono de entrada indicó que estaba llamando desde un teléfono público.

Me convertí en absorbida en todo lo relacionado con teléfonos, no sólo de la electrónica, switches y equipos, sino también la organización empresarial, los procedimientos, y la terminología. Después de un tiempo, probablemente sabía más sobre el sistema de teléfono que cualquier empleado solo. Y había desarrollado mis habilidades de ingeniería social para el punto de que, a los diecisiete años, fui capaz de hablar a la mayoría empleados de telecomunicaciones casi nada, si yo estaba hablando con ellos en persona o por teléfono.

Mi publicitada piratas carrera realmente comenzado cuando estaba en la escuela secundaria. Mientras que no puedo describir el detalle aquí, baste decir que uno de la conducción fuerzas en mis primeros hacks era ser aceptada por los chicos en el grupo de piratas informáticos.

Entonces usamos el hacker de plazo a una persona que pasaba gran parte de tiempo de trastear con hardware y software, ya sea para desarrollar más eficiente programas o para omitir los pasos innecesarios y hacer el trabajo más rápidamente. El

término se ha convertido en un peyorativo, llevando el significado de \"delincuente malicioso\". En estas páginas utilizo el término de la manera que siempre he utilizado-en su anterior, más sentido benigno.

Después de la escuela secundaria estudié equipos en el centro de aprendizaje del equipo en Los Ángeles. Dentro de unos meses, manager del equipo de la escuela se dio cuenta de que tenía vulnerabilidad encontrada en el sistema operativo y administrativo obtuvo lleno privilegios en su minicomputadora de IBM. Los mejores expertos en informática en sus personal docente no se ha podido averiguar cómo lo había hecho. En lo que pudo haber sido uno de los primeros ejemplos de \"alquiler del hacker\", me dio una oferta que no podía rechazar: hacer un proyecto de honores para mejorar la seguridad del equipo de la escuela, o en la cara suspensión para hackear el sistema. Por supuesto, he decidido hacer el proyecto de honores, y terminó graduándose cum laude con honores.

Convertirse en un ingeniero Social
Algunas personas levantarse de la cama cada mañana horrorizado su rutina diaria de trabajo en las minas de sal proverbiales. He tenido la suerte de disfrutar de mi trabajo. n particular, Usted no puede imaginar el desafío, la recompensa y el placer tuve el tiempo que pasé como un investigador privado. Yo estuve afilando mis talentos en el arte de performance llamado social Ingeniería (sacar a la gente a hacer cosas que normalmente no hacen por un extraño) y ser pagado por ello.

Para mí no fue difícil convertirse en experto en ingeniería social. Mi padre parte de la familia había sido en el campo de ventas durante generaciones, por lo que el arte de influencia y persuasión podrían haber sido un rasgo heredado. Cuando se combinan ese rasgo con una inclinación para engañar a las personas, tiene el perfil de un típico ingeniero social.

Se podría decir que hay dos especialidades dentro de la clasificación de puestos del estafador. Alguien que estafas y trampas de gente de su dinero pertenece a una Sub-Specialty, el grifter. Alguien que utiliza el engaño, influencia, y persuasión contra las empresas, generalmente dirigidas a su información, pertenece a la otro sub-specialty, el ingeniero social. Desde el momento de mi truco de traslados en autobús, Cuando yo era demasiado joven para saber que no había nada malo con lo que estaba haciendo, Había comenzado a reconocer un talento para descubrir los secretos que no se supone que tienen. Construí sobre ese talento mediante engaño, conociendo la jerga y desarrollo una habilidad de manipulación.

Una forma he trabajado en el desarrollo de las habilidades de mi oficio, si puedo llamarlo un oficio, fue destacar algún dato realmente no importa y ver si me alguien podría hablar en el otro extremo del teléfono en proporcionar, sólo para mejorar mis habilidades. De la misma manera que solía practicar mis trucos de magia, practicado

pretexting. A través de estos ensayos, pronto descubrí que podía adquirir prácticamente cualquier información que dirigido.

Como describí en su testimonio del Congreso ante senadores Lieberman y Thompson años:

He ganado acceso no autorizado a sistemas informáticos en algunos de los más grandes corporaciones del planeta y han penetrado con éxito algunos de los más sistemas informáticos resistentes jamás desarrollaron. He usado tanto técnicos como no-medios técnicos para obtener el código fuente para varios sistemas operativos y dispositivos de telecomunicaciones para estudiar sus vulnerabilidades y su interior funcionamiento.

Toda esta actividad fue realmente satisfacer mi curiosidad; para ver qué podía hacer; y encontrar información secreta acerca de sistemas operativos, teléfonos celulares, y cualquier otra cosa que despertó mi curiosidad.

REFLEXIONES FINALES
He reconocido desde mi detención que las acciones que tomó fueron ilegales ya compromiso de invasiones de privacidad.

Mis fechorías estaban motivados por la curiosidad. Quería saber como podría sobre el funcionamiento de redes de telefonía y los-y-entresijos de la seguridad informática. ME pasó de ser un niño que le encantaba realizar trucos de magia para convertirse en el mundo hacker más notorio, temido por las corporaciones y el Gobierno. Como reflejan volver a mi vida durante los últimos 30 años, admito que hice algunos extremadamente pobres decisiones, impulsadas por mi curiosidad, el deseo de aprender acerca de la tecnología y la necesidad de un buen reto intelectual.

Ahora soy una persona cambiada. Me estoy volviendo mi talento y los conocimientos He reunido sobre tácticas de ingeniería social y la seguridad de información para ayudar a Gobierno, empresas y particulares prevención, detectan y responden a amenazas de seguridad de la información.

Este libro es una forma más que puedo utilizar mi experiencia para ayudar a otros a evitar la esfuerzos de los ladrones de información malintencionada del mundo. Creo que encontrará el historias agradables, reveladora y educativas.

Introducción

Este libro contiene una gran cantidad de información sobre seguridad de la información y social Ingeniería. Para ayudarle a encontrar su camino, aquí un rápido vistazo a cómo este libro es organizado:

En la parte 1 te revelan el eslabón más débil de seguridad y mostrar por qué usted y su empresa están expuestos a ataques de ingeniería social.

En la parte 2 verá cómo los ingenieros sociales de juguete con su confianza, su deseo de ser útil, su simpatía y su credulidad humana para obtener lo que quieren. Historias de ficción de ataques típicos demostrará que los ingenieros sociales pueden llevar muchos sombreros y muchas caras. Si crees que nunca ha encontrado uno, eres probablemente equivocado. Reconocerá un escenario que has experimentado en estos ¿historias y se preguntan si tuvieras un pincel con ingeniería social? Usted muy bien podría. Pero una vez que haya leído los capítulos 2 a 9, sabrás cómo obtener el mano superior cuando el ingeniero social siguiente trata de llamada.

Parte 3 es la parte del libro donde se ve cómo el ingeniero social aumenta la apuesta, en inventado historias que muestran cómo puede avanzar en sus instalaciones corporativas, robar el tipo de secreto que puede hacer o quebrar tu empresa y frustrar su alta tecnología medidas de seguridad. Los escenarios en esta sección le hará consciente de las amenazas que van desde la venganza de simple empleado para el terrorismo cibernético. Si usted valora la información que mantiene su negocio funcionando y la privacidad de sus datos, usted ¿desea leer capítulos 10 al 14 de principio a fin.

Es importante señalar que, salvo indicación contraria, las anécdotas en este libro son puramente ficticio.

En la parte 4 hablar la charla corporativa sobre cómo evitar el éxito social Ingeniería ataques contra su organización. Capítulo 15 proporciona un modelo para un exitoso programa de formación en seguridad. Y capítulo 16 sólo puede guardar tu cuello- es una política de seguridad completa que se puede personalizar para su organización y implementar inmediatamente para proteger a su empresa y la información.

Por último, he proporcionado una seguridad en una sección de resumen, que incluye listas de comprobació tablas y gráficos que resumen la información clave que puede utilizar para ayudar a su empleados de frustrar un ataque de ingeniería social en el trabajo. Estas herramientas también proporciona valiosa información que puede utilizar en la elaboración de su propio programa de formación en segurida

En todo el libro también encontrará varios elementos útiles: cuadros de Lingo proporcionar definiciones de ingeniería social y terminología hacker informática; Mensajes de Mitnick ofrecen breves palabras de sabiduría para ayudar a reforzar su seguridad

estrategia; y notas y barras laterales dan interesantes antecedentes adicionales o información.

Parte 1
Detrás de las escenas

Capítulo 1
Eslabón de seguridad

Una empresa puede que haya adquirido las mejores tecnologías de seguridad que puede el dinero comprar, formado su gente tan bien que ellos encierran todos sus secretos antes de casa por la noche y contratado guardias de construcción de la mejor empresa de seguridad en el negocio.

Esa empresa es aún totalmente Vulnerable.

Las personas pueden seguir todas seguridad mejor las prácticas recomendadas por los expertos, servilmente instalar cada producto de seguridad recomendada y estar completamente alerta acerca de la configuración correcta del sistema y aplicar parches de seguridad.

Las personas siguen siendo completamente vulnerables.

EL FACTOR HUMANO
Testimonio ante el Congreso no hace mucho tiempo, explicó de que a menudo pude obtener las contraseñas y otras piezas de información confidencial de las empresas por fingiendo ser otra persona y acaba pidiendo.

Es natural que anhelan una sensación de absoluta seguridad, llevando a muchas personas a resolver para un falso sentido de seguridad. Considerar el propietario responsable y amoroso que ha instalado un Medico, una cerradura de tambor conocida como pickproof, en su parte frontal puerta para proteger a su esposa, sus hijos y su casa. Ahora es cómodo que él ha hecho su familia mucho más seguro contra intrusos. Pero qué pasa con el intruso - ¿Quién rompe una ventana, o grietas el código para la apertura de la puerta de garaje? ¿Qué ¿instalación de un sistema de seguridad sólido? Mejor, pero todavía ninguna garantía. Bloqueos de caros o no, el dueño de casa sigue siendo vulnerable.

¿Por qué? Porque el factor humano es verdaderamente el eslabón más débil de seguridad.

Demasiado a menudo, la seguridad es sólo una ilusión, una ilusión hecha a veces peor Cuando la credulidad, ingenuidad o ignorancia entran en juego. Del mundo más respetado científico del siglo XX, Albert Einstein, es citado diciendo,
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
sobre el primero.\" Al final, los ataques de ingeniería social pueden tener éxito cuando las personas son tontos o, más comúnmente, simplemente ignorantes sobre buenas prácticas de seguridad.
Con la misma actitud como nuestros propietarios conscientes de la seguridad, mucha información profesionales de tecnología (IT) tienen la idea errónea que ha realizado sus empresas en gran medida inmunes a atacar porque ha implementado la seguridad estándar productos - firewalls, sistemas de detección de intrusiones o autenticación más sólida

tarjetas inteligentes dispositivos tales como tokens basados en tiempo o biométricos. Quien piense que es resolver solo oferta verdadera seguridad de productos de seguridad. la ilusión de seguridad. Se trata de vivir en un mundo de fantasía: será inevitablemente, más tarde si no antes, sufren un incidente de seguridad.

Como señaló el consultor de seguridad Bruce Schneier lo pone, \"la seguridad no es un producto, es un proceso\". Además, la seguridad no es un problema de tecnología, es un pueblo y problema de gestión.

Como los desarrolladores inventan continuamente mejores tecnologías de seguridad, lo que cada vez más difícil de explotar las vulnerabilidades técnicas, los atacantes se convertirán más y mucho más para explotar el elemento humano. Craqueo del servidor de seguridad humana es a menudo fácil, no requiere de ninguna inversión más allá del costo de una llamada telefónica e implica riesgo mínimo.

UN CASO CLÁSICO DE ENGAÑO

¿Cuál es la mayor amenaza para la seguridad de los activos de su empresa? Eso es fácil: el ingeniero social--un mago sin escrúpulos que le viendo su mano izquierda mientras que con su derecha roba tus secretos. Este personaje es a menudo tan amigable, glib, y obligar a que estás agradecido por haber encontrado en él.

Analicemos un ejemplo de ingeniería social. No mucha gente aún hoy Recuerde al joven llamado Stanley Mark Rifkin y su aventura poco con la ahora extinta seguridad Pacífico Banco Nacional en Los Ángeles. Cuentas de variar su escapada, y Rifkin (como yo) nunca ha contado su propia historia, por lo que la a continuación se basa en informes publicados.

Separación de código

Un día en 1978, Rifkin moseyed sobre seguridad Pacífico autorizado-personal - Sala de transferencia única, donde el personal enviados y recibidos que suman un total de transferencias varios millones de dólares cada día.

Él estaba trabajando para una empresa bajo contrato para desarrollar un sistema de copia de seguridad pa en caso de que su equipo principal nunca bajó de alambre datos de la sala. Ese papel le dio acceso a los procedimientos de transferencia, incluyendo cómo funcionarios del Banco dispuestos para un transferencia para ser enviado. Había aprendido ese banco oficiales que fueron autorizados para orden de transferencias se dará un código diario celosamente cada mañana para utilizar al llamar a la habitación de alambre.

En la sala de alambre los secretarios sí guardan la molestia de intentar memorizar código de cada día: el código escrito en una hoja de papel y lo publicado donde

puede ver fácilmente. Este día especial de noviembre Rifkin tenía un específico motivo de su visita. Quería obtener un vistazo a ese documento.

Al llegar a la sala de alambre, tomó algunas notas sobre procedimientos operativos, supuestamente para asegurar el sistema de copia de seguridad sería malla correctamente con el sistemas regulares. Mientras tanto, leyó subrepticiamente el código de seguridad de la publicado el deslizamiento del papel y lo memorizado. Unos minutos más tarde caminó. Como él dijo después, sintió como si sólo había ganado la lotería.

Existe esta cuenta bancaria suiza...
Dejando la habitación sobre 3 de la tarde, se dirigió directamente a la teléfono público en el lobby de mármol del edificio, donde depositó una moneda y marcado en la sala de transferencia bancaria. Luego cambió de sombreros, transformando a sí mismo de Stanley Rifkin, asesor del Banco, en Mike Hansen, miembro de la Ribera Departamento Internacional.

Según una fuente, la conversación fue algo así:

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
contestó el teléfono.
Pide el número de oficina. Ese fue el procedimiento estándar, y fue preparado: \"286\" él dijo.
Luego pidió la chica, \"Está bien, ¿qué es el código?\"

Rifkin ha dicho que su latido impulsados por adrenalina \"recogió su ritmo\" en este punto. Suavemente, respondió \"4789.\" Luego se dirigió a dar instrucciones para cableado \"diez millones de dólares - doscientos mil exactamente\" a la confianza de Irving Empresa en Nueva York, para el crédito del Banco Wozchod Handels de Zurich, Suiza, donde ya había establecido una cuenta.

La chica entonces dijo, \"está bien, tengo. Y ahora necesito el asentamiento interoffice número\".

Rifkin estalló en un sudor; se trata de una cuestión que no había previsto, algo había escapado a través de las grietas en su investigación. Pero se las arregló para permanecer en carácter, actuado como si todo estaba bien y al instante respondió sin falta un ritmo, \"Let me check; Llamaré le derecha atrás.\" Una vez cambió de sombreros volver a llamar a otro departamento en el Banco, esta vez alegando que un empleado en la sala de transferencia bancaria. Obtuvo el número de asentamientos y llamado la niña Atrás.

Ella tomó el número y dijo: \"Gracias\". (Dadas las circunstancias, su agradecimiento él tiene que ser considerada altamente irónico.)

Logro de cierre
Unos días más tarde Rifkin voló a Suiza, recogió su efectivo y entregado
8 millones de dólares a una agencia rusa para un montón de diamantes. Voló hacia atrás, pasando
a través de aduanas de Estados Unidos con las piedras escondidas en un cinturón de dinero. Él había tirad
el Banco más grande atraco en la historia--y hacerlo sin usar un arma, incluso sin una
equipo. Curiosamente, su alcaparra finalmente lo hizo en las páginas de la Guinness
Libro de Records mundiales en la categoría de \"fraude informático más grande.\"

Rifkin Stanley había utilizado el arte del engaño--las habilidades y técnicas que son
hoy llama ingeniería social. Planificación detallada y un buen regalo de gab es todo lo
realmente tuvo.

Y eso es lo que este libro--acerca de las técnicas de ingeniería social (en el que
realmente lo tuyo es experto) y cómo defenderse contra utilizados en su
empresa.

LA NATURALEZA DE LA AMENAZA
La historia de Rifkin aclara perfectamente cómo engañar a nuestro sentido de seguridad puede
ser. Incidentes como éste - muy bien, quizás no 10 millones de dólares heists, pero los incidentes perjudici
No obstante - están ocurriendo cada día. Puede estar perdiendo dinero ahora mismo, o
alguien puede estar robando nuevos planes de producto, y aún no sabes. Si se
no ha sucedido ya a su empresa, no es una cuestión de si ocurrirá,
pero cuando.

Una creciente preocupación
El Instituto de seguridad del equipo, en su informe de 2001 sobre delitos informáticos, informó
que el 85 por ciento de las organizaciones respondieron había detectado seguridad informática
brechas en los doce meses anteriores. Que es un número asombroso: sólo
quince de cada cien organizaciones responder fueron capaces de decir que ellos
no había una brecha de seguridad durante el año. Igualmente asombroso fue el
número de organizaciones que informaron que experimentaron pérdidas financieras
debido a las violaciones de equipo: 64 por ciento. Habían también más de la mitad de las organizaciones
sufrió financieramente. En un solo año.
Mis propias experiencias me llevan a creer que los números en los informes como este son
un poco inflado. Soy sospechoso de la agenda del pueblo llevando a cabo la
encuesta. Pero eso no quiere para decir que el daño no es extenso; es. Quienes incumplan
para planificar un incidente de seguridad están planeando para el fracaso.

Productos de seguridad comercial implementados en la mayoría de las empresas están encaminados prin
proporcionando protección contra el intruso equipo aficionado, como los jóvenes
conocidos como script kiddies. De hecho, estos piratas wannabe con descargado
software en su mayoría son sólo una molestia. Las mayores pérdidas, las amenazas reales, vienen
desde los sofisticados intrusos con objetivos bien definidos que están motivados por

ganancia financiera. Estas personas centrarse en un destino cada vez más que, como el aficionados, intentando infiltrarse en sistemas tantas como sea posible. Mientras los aficionados los intrusos equipo simplemente ir por cantidad, destino de los profesionales de la información de calidad y valor.

Tecnologías como dispositivos de autenticación (para probar identidad), control de acceso (para administrar el acceso a los archivos y recursos del sistema) y detección de intrusiones sistemas (el equivalente electrónico de alarmas antirrobo) son necesarios para una empresa programa de seguridad. Sin embargo, es hoy en día típico para una empresa a gastar más dinero en café que implementar medidas para proteger la organización contra ataques a la seguridad.

Igual la mente criminal no puede resistir la tentación, es impulsada por la mente de hacker a encontrar formas de eludir la seguridad potente salvaguardias de tecnología. Y en muchos casos, lo hacen por dirigidas a las personas que utilizan la tecnología.

Prácticas engañosas

Hay un dicho popular que un equipo seguro es aquél que está apagado. Inteligente, pero falsa: la pretexter simplemente alguien habla en entrar en la Oficina y encender el equipo. Puede obtener un adversario que quiere su información que, normalmente en cualquiera de varias formas diferentes. Es sólo una cuestión de tiempo, paciencia, personalidad y persistencia. Es donde entra en juego el arte del engaño.

Para derrotar a las medidas de seguridad, un atacante, un intruso o un ingeniero social debe encontrar un forma de engañar a un usuario de confianza para que revelen información o engañar a un incauto marcar en le da acceso. Cuando se engaña, empleados de confianza influenciados, manipulados en revelar información confidencial o realizar acciones que crea un agujero de seguridad para el atacante se deslice a través de ninguna tecnología en el mundo puede proteger un negocio. Al igual que a veces son capaces de criptoanalistas revelar el texto de un mensaje codificado por encontrar una debilidad que les permite omitir la tecnología de cifrado, los ingenieros sociales usar engaño practicado en sus empleados para omitir la tecnología de seguridad.

ABUSO DE CONFIANZA

En la mayoría de los casos, los ingenieros sociales exitosos tienen habilidades de gente fuerte. Son encantador, amable y fácil como--rasgos sociales necesarios para el establecimiento rápidos RapPort y confianza. Un experimentado ingeniero social es capaz de acceder a información de prácticamente cualquier destino mediante el uso de las estrategias y tácticas de su oficio.

Tecnólogos experimentados laboriosamente han desarrollado soluciones de seguridad de la información para minimizar los riesgos relacionados con el uso de computadoras, pero dejó sin resolverse la vulnerabilidad más importante, el factor humano. A pesar de nuestro intelecto, nos

los seres humanos - tú, yo y todos los demás - siguen siendo la amenaza más grave a cada uno seguridad de los demás.

Nuestro carácter nacional

No somos conscientes de la amenaza, especialmente en el mundo occidental. En los Estados Unidos La mayoría de Estados, no estamos capacitados para sospechar uno del otro. Nos enseñan \"Amarás a tu prójimo\" y tener confianza y fe en sí. Considerar cómo difícil que es para que las organizaciones de reloj de barrio para que la gente para bloquear su Casas y automóviles. Este tipo de vulnerabilidad obvio, y sin embargo, parece ser ignorado por muchos de los que prefieren vivir en un mundo de ensueño - hasta que se quemaron.

Sabemos que no todas las personas son amables y honestos, pero demasiado a menudo vivimos como si s fueron. Esta encantadora inocencia ha sido el tejido de la vida de los estadounidenses y doloroso renunciar a ella. Como nación hemos construido en nuestro concepto de libertad que los mejores lugares para vivir son aquellos donde los bloqueos y las claves son las menos necesarias.

Mayoría de la gente ve en el supuesto de que no va ser engañados por otros, basados en la creencia de que la probabilidad de ser engañados es muy baja; el atacante, comprender esta creencia común, hace su petición de sonido tan razonable que no plantea ninguna sospecha, explotando todo el tiempo la confianza de la víctima.

Inocencia organizacional

Que la inocencia que es parte de nuestro carácter nacional fue evidente cuando copia equipos en primer lugar se estaban conectados remotamente. Recordemos que ARPANet (el Agencia de proyectos de investigación avanzada de defensa departamento Red), el predecesor 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 tecnológica adelanto. Muchos instituciones educativas establecidas principios sistemas informáticos con poca o ninguna seguridad. Uno señaló libertario de software, Richard Stallman, incluso se negó a Proteja su cuenta con una contraseña.

Pero con el Internet se utiliza para el comercio electrónico, los peligros de la débil seguridad en nuestro mundo por cable han cambiado drásticamente. Implementar más la tecnología no va a resolver el problema de la seguridad humana.

Basta con mirar nuestros aeropuertos hoy. La seguridad se ha convertido en primordial, sin embargo esta por informes de los medios de viajeros que han sido capaces de burlar la seguridad y llevar potencial pasados los puestos de control de armas. ¿Cómo es esto posible durante un tiempo ¿Cuando nuestros aeropuertos están en estado de alerta? ¿Están fallando los detectores de metales? Lol El problema no está en las máquinas. El problema es el factor humano: la gente manejar las máquinas. Funcionarios del aeropuerto pueden calcular las referencias de la Guardia Nacional

instalar detectores de metales y sistemas de reconocimiento facial, pero educando a la vanguardia personal de seguridad sobre cómo correctamente la pantalla a pasajeros es mucho más probable ayudar.

El mismo problema existe en Gobierno, negocio y educación instituciones en todo el mundo. A pesar de los esfuerzos de profesionales de la seguridad, información en todo el mundo sigue siendo vulnerable y continuará a ser visto como una madura destino por atacantes con técnicas de ingeniería social, hasta 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 ilusiones y convertirse en más consciente de las técnicas que están siendo utilizadas por aquellos que intentan atacar la confidencialidad, integridad y disponibilidad de nuestros sistemas informáticos y redes. Nosotros hemos llegado a aceptar la necesidad de conducción defensiva; es el momento de aceptar y apre la práctica de la informática defensiva.

La amenaza de un allanamiento que viole su privacidad, su mente o su empresa sistemas de información no parezca reales hasta que sucede. Para evitar una costosa dosis de realidad, que todos necesitan ser conscientes, educados, atentos y agresiva protección de nuestros activos de información, nuestra propia información personal y nuestro infraestructuras críticas de la nación. Y debemos aplicar las precauciones hoy.

LOS TERRORISTAS Y ENGAÑO

Por supuesto, el engaño no es una herramienta exclusiva del ingeniero social. Física terrorismo hace la noticia más importante, y nos hemos dado cuenta como nunca antes que el mundo es un lugar peligroso. Después de todo, la civilización es sólo una chapa delgada.

Infusión en los ataques contra Nueva York y Washington, D.C., en septiembre de 2001 tristeza y miedo en los corazones de cada uno de nosotros - no sólo los estadounidenses, pero bueno- gente de significado de todas las Naciones. Ahora nos estamos alertó sobre el hecho de que hay terroristas obsesivos situados alrededor del mundo, bien - entrenados y espera lanzar nuevos ataques contra nosotros.

El esfuerzo intensificado recientemente por nuestro Gobierno ha aumentado los niveles de nuestro conciencia de seguridad. Tenemos que estar alerta, en guardia contra todas las formas de terrorismo. Tenemos que comprender cómo los terroristas traición crean falsos identidades, asumen roles como estudiantes y vecinos y fundirse en la multitud. Ellos ocultar sus verdaderas creencias mientras que trazan contra nosotros - practicando trucos de engaño similar a aquellos que leerá acerca en estas páginas.

Y mientras, a lo mejor de mi conocimiento, los terroristas han aún no utilizado social Ingeniería ardides para infiltrarse en las empresas, plantas de tratamiento de aguas, eléctricas instalaciones de generación, o de otros componentes vitales de nuestra infraestructura nacional, la potencial está ahí. Es demasiado fácil. La conciencia de seguridad y políticas de seguridad

que espero será poner en marcha y aplicada por los directivos corporativos debido a este libro saldrá ninguno demasiado pronto.

SOBRE ESTE LIBRO

Seguridad corporativa es una cuestión de equilibrio. Hojas de seguridad muy poco su empresa vulnerable, pero con un énfasis excesivo en la seguridad se obtiene en la forma de atendiendo a empresas, inhibe el crecimiento y la prosperidad de la empresa. El desafío es lograr un equilibrio entre seguridad y productividad.

Otros libros sobre seguridad de la empresa se centran en la tecnología de hardware y software, y no debidamente cubierta la amenaza más grave de todos: engaño humano. El propósito de este libro, por el contrario, es para ayudarle a comprender cómo usted, co - se están manipulando a los trabajadores y otras personas de su empresa y las barreras pueden levantar para dejar de ser víctimas. El libro se centra principalmente en la técnica métodos que utilizan los intrusos hostiles para robar información, poner en peligro la integridad de la información que se cree que es seguro pero no es., o destruir el trabajo de la empresa producto.

Mi tarea se hace más difícil por una simple verdad: cada lector habrá sido manipulado por los grandes expertos de todos los tiempos en la ingeniería social - sus padres. Encontraron maneras para ayudarle - \"por tu propio bien\", hacer lo pensaron mejores. Los padres se convierten en grandes narradores de la misma manera que social ingenieros desarrollar hábilmente muy historias plausibles, razones, y justificaciones para lograr sus objetivos. Sí, todos estábamos moldeadas por nuestros padres: ingenieros sociales benevolentes (y a veces no tan benévolos).

Condicionada por esa formación, nos hemos vuelto vulnerables a la manipulación. Nos viviría una vida difícil, si tuviéramos que estar siempre en guardia, desconfía de otros, cuestión que nosotros fuésemos dpdo de alguien que intenta tomar ventaja de nosotros. En un mundo perfecto sería implícitamente confiamos otros seguros que la gente que nos encontramos va a ser honesto y confiable. Pero hacemos no vivimos en un mundo perfecto, y por eso tenemos que ejercer un nivel de vigilancia repeler los esfuerzos engañosos de nuestros adversarios.

Las partes principales de este libro, partes 2 y 3, se componen de historias que muestran que los ingenieros sociales en acción. En estas secciones se podrá leer sobre:

- Qué teléfono phreaks descubrió hace años: un ingenioso método para obtener un número de teléfono están ocultos de la compañía telefónica.
- Diferentes métodos utilizados por los atacantes para convencer incluso alerta, sospechoso empleados para revelar sus contraseñas y nombres de equipo.
- Cómo un administrador de operaciones Centro cooperó en permitiendo a un atacante roban información de producto más secreta de su empresa.

• Los métodos de un atacante que engañó a una dama en la descarga de software
hace espías en cada pulsación de tecla y los detalles de los correos electrónicos que le.
• Cómo investigadores privados obtener información acerca de su empresa y sobre TI
Personalmente, que prácticamente puedo garantizar enviará un escalofrío por la columna vertebral.

Se podría pensar como leen algunas de las historias en las partes 2 y 3 que no son posible, que nadie podría realmente triunfar en getting away with las mentiras, sucias Trucos y de esquemas, inscritos en estas páginas. La realidad es que en cada caso, estas historias representan eventos que pueden suceder; muchos de ellos están ocurriendo cada día en algún lugar en el planeta, tal vez incluso a su negocio mientras lees esto libro.

El material en este libro será una verdadera revelación a la hora de proteger su empresa, 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 me cambio cursos. Mi objetivo aquí es para ayudarle a crear el las políticas del negocio necesario y conciencia de capacitación para minimizar las posibilidades de sus empleados nunca ser engañados por un ingeniero social. Comprensión de la estrategias, métodos y tácticas del ingeniero social ayudará a prepararte para implementar controles razonables para salvaguardar sus activos de TI, sin menoscabar su productividad de la empresa.

En definitiva, he escrito este libro para elevar su conciencia sobre la amenaza planteados por la ingeniería social y que le ayudarán a asegurarse de que su empresa y su empleados tienen menos probabilidades de ser explotados de esta manera.

O tal vez debo decir, es mucho menos probable que pueda ser aprovechada nunca más.

Parte 2
El arte del atacante

Capítulo 2
Cuando no está información inocua

¿Qué opinas mayoría de la gente es la verdadera amenaza de ingenieros sociales? Lo que debe ¿hacer que su guardia?

Si el objetivo es capturar algunos altamente valioso Premio--digamos, un componente vital de la la empresa capital intelectual - y tal vez lo que se necesita es, figuradamente, sólo un bóveda más fuerte y guardias más fuertemente armados. ¿Verdad?

Pero en realidad penetrar la seguridad de la empresa a menudo comienza con el malo obtener algún dato o algún documento parece tan inocente,
tan cotidiana y sin importancia, que no vea la mayoría de la gente en la organización razón para el elemento debe ser protegido y restringido

VALOR OCULTO DE LA INFORMACIÓN
Mucha de la información aparentemente inocua en posesión de una empresa es apreciado
un atacante de ingeniería social porque puede desempeñar un papel vital en su esfuerzo por vestir a sí mismo en un manto de credibilidad.

A lo largo de estas páginas, voy a mostrarle cómo los ingenieros sociales hagan lo que lo hacen por alquiler que \"testigo\" los ataques por sí mismo--a veces presenta la acción desde el punto de vista del pueblo siendo víctima, lo que le permite poner en sus zapatos y medidor de cómo usted mismo (o tal vez de su empleados o compañeros de trabajo) que han respondido. En muchos casos también tendrás la experiencia de los mismos acontecimientos desde la perspectiva del ingeniero social.

La primera historia mira una vulnerabilidad en el sector financiero.

CREDITCHEX
Durante mucho tiempo, los británicos acondicionar con un sistema bancario muy tapada. Como un ciudadano ordinario, verdadero, usted no podía caminar en frente a la calle y abrir un banco cuenta. No, el Banco no considera le acepte como cliente a menos que algunos persona ya bien establecida como un cliente le proporcionó una carta de recomendación.

Una diferencia, por supuesto, en el mundo de la banca aparentemente igualitaria de en la actualidad. Y nada más en evidencia que nuestra moderna facilidad de hacer negocios en América amistoso, democrática, donde casi nadie puede caminar en un banco y ¿fácilmente abrir una cuenta de cheques, derecho? Bueno, no exactamente. La verdad es que los bancos comprensiblemente tienen una resistencia natural a abrir. una cuenta para alguien que

sólo podría tener una historia de escribir cheques malas--que serían unos como bienvenidas
como una hoja de rap de los cargos de robo o malversación de fondos del Banco. Por lo tanto es una prá
en muchos bancos para obtener una rápida pulgares arriba o abajo de pulgares sobre un posible nuevo
cliente.

Una de las principales empresas que bancos contratación con esta información es una
traje llamaremos CreditChex. Ofrecen un valioso servicio a sus clientes, pero
como muchas empresas, también sin saberlo pueden proporcionar un servicio útil para saber
ingenieros sociales.

La primera llamada: Kim Andrews
Banco Nacional, se trata de Kim. ¿Desea abrir una cuenta hoy en día?
Hola, Kim. Tengo una pregunta para usted. ¿Ustedes utilizan CreditChex?
Sí.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
es un 'ID comerciante'?\"

Una pausa; ella pesaba la cuestión, pensando en lo que se trataba y
Si ella debe responder.

El llamador rápidamente continuado sin faltar un ritmo:

Porque, Kim, estoy trabajando en un libro. Se trata de Investigaciones privadas.
There was an error deserializing the object of type System.String. Encountered unexpected character 's'.
ayudando a un escritor.
¿Por lo que se llama un ID comerciante, derecho?
Uh huh.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Gracias por tu ayuda. Adiós, Kim.\"

La segunda llamada: Chris Talbert
Banco Nacional, nuevas cuentas, se trata de Chris.
There was an error deserializing the object of type System.String. The token 'true' was expected but foun
CreditChex. Estamos haciendo una encuesta para mejorar nuestros servicios. Puede me sobra un
par de minutos?\"

Alegró, y salió de la llamada:

There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
siguió respondiendo a su cadena de preguntas.
¿Cuántos empleados en su sucursal de utilizan nuestro servicio?
¿Con qué frecuencia usted llamarnos con una investigación?

¿Que de nuestros números 800 hemos hemos asignado le para llamar a nosotros?
¿Nuestros representantes siempre han sido Cortés?
¿Cómo es nuestro tiempo de respuesta?
¿Cuánto tiempo llevas con el Banco?
¿Qué ID comerciante utiliza actualmente?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
usted?\"
¿Si tuviera alguna sugerencia para mejorar nuestro servicio, lo que podría ser?

Y:

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
rama?\"

Estuvo de acuerdo, charlamos un poco, el llamador sonó y Chris volvió a trabajar.

La llamada tercera: Henry McKinsey
CreditChex, se trata de Henry McKinsey, ¿cómo puedo ayudarle?

El llamador dijo que estaba en el Banco Nacional. Dio el ID comerciante adecuado y luego le dio el nombre y número de seguridad social de la persona que estaba buscando información sobre. Enrique pide la fecha de nacimiento, y el llamador dio demasiado.

Después de unos momentos, Henry Lee el anuncio desde su pantalla de ordenador.

There was an error deserializing the object of type System.String. End element 'root' from namespace "
fondos suficientes - es el familiar bancario jerga para controles que se han escrito cuando no hay suficiente dinero en la cuenta para cubrirlas.
¿Cualquier actividad desde entonces?
No hay actividades.
¿Ha habido alguna otra consulta?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Chicago.\" Él tropezó sobre el nombre del siguiente, las inversiones mutuas de Schenectady, y tuvo que explicarlo. \"Eso es en el estado de Nueva York\", añadió.

Investigador privado en el trabajo
Tres de esas llamadas fueron hechas por la misma persona: un investigador privado que veremos llamar a Oscar Grace. Grace tuvo un nuevo cliente, una de sus primeras. Un policía hasta unos pocos meses antes, se encontró que algunos de este nuevo trabajo vinieron naturalmente, pero algunos ofrecen un reto a sus recursos e inventiva. Este uno se vino abajo firmemente en la categoría de desafío.

Angelo privado ojos de ficción - la picas de Sam y el Philip Marlowes
-pasar mucho tiempo de noche horas sentado en autos esperando a coger un cónyuge infiel. PIs de la vida real lo mismo. También hacen menos escrito acerca, pero no menos importante tipo de espionaje para los cónyuges beligerantes, un método que se inclina más fuertemente en lo social conocimientos de ingeniería que en combates fuera el aburrimiento de vigilias de tiempo de la noche.

Nuevo cliente de Grace fue una señora que parecía como si ella tenía una forma bastante cómoda presupuesto de ropa y joyería. Ella entraba a su Oficina un día y toma asiento en la silla de cuero, el único que no tiene papeles amontonados en él. Ella se instaló su gran bolso de Gucci en su escritorio con el logotipo volvió a enfrentarse a él y anunció que planeaba decirle a su marido que ella quería un divorcio, pero admitió que \"sólo es un problema muy poco.\"

Parecía que su maridito era un paso por delante. Él ya había sacado el dinero de su cuenta de ahorros y una cantidad aún mayor de su cuenta de corretaje. Ella quería saber donde sus bienes habían sido squirreled lejos y su divorcio abogado no ayuda en absoluto. Gracia conjeturó que el abogado fue uno de los Uptown, altos consejeros que no ensuciarse la manos sobre algo como el dinero dónde desordenado.

¿Podría ayudar gracia?

Ella aseguró que sería una brisa, citada una cuota, gastos facturados al costo, y recogió un cheque para el primer pago.

Luego se enfrentó a su problema. ¿Qué haces si no has manejado nunca un pedazo de trabajar como antes y bastante no sabe cómo localizar un ¿rastro de dinero? Avanzar por los pasos del bebé. Aquí, es mg de acuerdo a nuestra fuente, Historia de Grace.

Supe CreditChex y cómo los bancos utilizan el traje - mi ex esposa solía trabajar en un banco. Pero no sabía la jerga y procedimientos y tratando de pedir mi ex - sería una pérdida de tiempo.

Paso 1: obtener la terminología recta y averiguar cómo hacerlo la solicitud suena como que sé lo que estoy hablando. Llamado en el Banco, el primero joven Dama, Kim, era sospechosa preguntado sobre cómo identifican a sí mismos Cuando teléfono CreditChex. Ella vaciló; no sabía si me dijera.
¿Me echan atrás por? No un poco. De hecho, las dudas me dieron una pista importante, una señal de que tenía que suministrar una razón ella encontraría creíble. Cuando trabajé en el con en ella, haciendo investigación para un libro, alivió sus sospechas. Dices que eres un autor o un escritor de la película y todo el mundo se abre.

Ella tenía otros conocimientos que habría ayudado - cosas como qué reforma CreditChex requiere para identificar a la persona que está llamando acerca de qué información puede pedir, y una grande, lo que fue Kim banco número ID comerciante. ME estaba dispuesto a pedir a esas preguntas, pero su vacilación enviado hasta la bandera roja. Ella compró la historia de investigación del libro, pero ya tenía algunas sospechas odiosas. Si ella había sido más dispuesta derecho cierto, habría pedido a revelar más detalles acerca de sus procedimientos.

JERGA
MARCA: Víctima de una estafa.
QUEMAR la fuente: Un atacante se dice que han quemado la fuente cuando él permite a una víctima a reconocer que ha producido un ataque. Una vez que la víctima se convierte en consciente y notifica a otros empleados o administración de la tentativa, se se vuelve extremadamente difícil de explotar la misma fuente en futuros ataques.

Tienes que ir en instinto de tripa, escuchar cerca de la marca de lo que está diciendo y cómo ella está diciendo. Esta señora sonaba lo suficientemente inteligente como para campanas de alarma em
Si preguntas demasiados inusuales. Y a pesar de que ella no sabía que me fue o qué número estaba llamando, aún en este negocio de que nunca desea alguien poniendo la palabra que busque fuera alguien llamar para obtener información sobre el negocio. Eso es porque no lo hace Quiero quemar la fuente - quizá desee llamar misma Oficina volver otra vez.

Estoy siempre en el reloj de signos poco que me dan una lectura en forma cooperativa un es la persona, en una escala que va desde \"sonido desea a una persona agradable y creo todo lo que está diciendo\"para\"llamar a los policías, alerta a la Guardia Nacional, este tipo hasta no sirve\".

Leí a Kim como un poco de borde, así que llamé simplemente a alguien a una rama diferente. Mi segunda llamada con Chris, el truco de la encuesta jugó como un encanto. La táctica aquí es para deslizar las preguntas importantes entre los inconsecuentes que son se utiliza para crear una sensación de credibilidad. Antes he bajado la pregunta acerca de la Mercante ID número CreditChex, corrió una prueba poco de último minuto por pidiendo su una pregunta personal acerca de cuánto tiempo había estado con el Banco.

Una pregunta personal es como una mina terrestre - algunas personas paso derecho sobre él y nunca aviso; para otras personas, sopla y les envía corriendo para seguridad. Así que si me pedir una pregunta personal y ella respuestas a la pregunta y el tono de su voz no cambia, eso significa que probablemente no es escéptica sobre la naturaleza de la solicitud. Puedo con seguridad pido las buscadas después de la pregunta sin despertar le sospechas y ella será probablemente me dan la respuesta que estoy buscando.

Sabe una cosa más que un buen PI: nunca terminar la conversación después de obtener el información clave. Otro dos o tres preguntas, charla un poco y luego s bien decir adiós. Más tarde, si la víctima recuerda nada de lo que le pregunte, será probablemente el último par de preguntas. Normalmente se olvidará el resto.

Así que Chris me dio su número de ID del comerciante y el número de teléfono llaman a realizar solicitudes. Habría sido más feliz si me había metido a algunas preguntas acerca de cuánta información puede obtener de CreditChex. Pero no fue mejor para empujar mi suerte.

Es como tener un cheque en blanco a CreditChex. Ahora pude llamar y obtener información cada vez que quería. Incluso no tuve que pagar por el servicio. Tal como se resultó, la rep CreditChex estaba feliz de compartir exactamente la información quería: dos lugares marido de mi cliente había solicitado recientemente para abrir una cuenta. ¿Hasta donde estaban los activos que su para ser ex esposa estaba buscando? Donde otra cosa pero ¿en las instituciones bancarias en la lista el tipo de CreditChex?

Analizando el timo
Este ardid todo se basó en una de las tácticas fundamentales sociales Ingeniería: acceso a la información que se trata de un empleado de la empresa como inocua, cuando no lo es.

El primer empleado de Banco confirmó la terminología para describir la identificación número que se utiliza al llamar a CreditChex: el ID del comerciante. La segunda siempre el número de teléfono para llamar a CreditChex y la pieza más importante de la información, número de ID del comerciante del Banco. Toda esta información apareció a la dependienta que inocuo. Después de todo, el empleado de Banco pensaba que ella estaba hablando con alguien de ¿Creditchex-así lo que podría ser el daño en revelar el número?

Todo esto sentó las bases para la tercera convocatoria. Grace tenía todo lo que necesitaba al teléfono CreditChex, pasar como representante de uno de sus bancos de clientes, Nacional y simplemente pedir la información que fue después.

Con tanta habilidad en robar información como un buen estafador tiene a robar su dinero, Grace tenía un talento para la lectura de las personas. Sabía que el común táctica de enterrar las preguntas claves entre inocentes. Sabía que un personal pregunta probaría a voluntad del segundo empleado cooperar, antes inocentemente pidiendo el número de ID del comerciante.

Error del empleado primero confirmar la terminología para el ID de CreditChex número sería casi imposible para protegerse. La información es tan ampliamente conocido en el sector bancario que parece ser poco importante - la modelo muy de los inocuos. Pero el segundo empleado, Chris, no debería haber sido

tan dispuestos a responder preguntas sin comprobar positivamente que el llamador era realmente quien afirmaba ser. Ella debería, al menos, han tomado su nombre y número y llamado de este modo, si cualquier pregunta surgió más tarde, ella puede tener mantiene un registro de qué número de teléfono que había utilizado la persona. En este caso, haciendo un llame como hubiera hecho mucho más difícil para el atacante hacerse pasar por un representante de CreditChex.

MENSAJE DE MITNICK

Un ID del comerciante en esta situación es análogo a una contraseña. Si el personal del Banco lo tratan como un PIN de ATM, podrían apreciar la naturaleza sensible de la información. Existe un código interno o número de la organización que las personas ¿no tratar con suficiente atención?

Mejor aún, habría sido una llamada a CreditChex usando un banco de monja ya tenía registro - no es un número proporcionado por el llamador: para verificar la persona realmente trabajó allí, y que la empresa realmente estaba haciendo un estudio de clientes. Teniendo en cuenta los aspectos prácticos del mundo real y las presiones de tiempo que funcionan la mayoría de la gente bajo hoy, sin embargo, este tipo de llamada de teléfono de verificación es mucho esperar, salvo Cuando un empleado es sospechoso que se está realizando algún tipo de ataque.

LA TRAMPA DE INGENIERO

Es ampliamente conocido que empresas de head hunter usan ingeniería social para contratar talento empresarial. Este es un ejemplo de cómo puede suceder.

A finales de 1990, una agencia de empleo no muy ética firmado un nuevo cliente, un empresa busca ingenieros eléctricos con experiencia en el teléfono industria. Honcho en el proyecto fue una dama dotada de una voz ronco y manera sexy que ella había aprendido a usar para desarrollar confianza inicial y relación sobre el teléfono.

La dama decidió etapa una redada en un teléfono celular servicio proveedor para ver si ella podría ubicar algunos ingenieros que podrían verse tentados a cruzar la calle a un competidor. Ella no podía llamar exactamente a la Junta de conmutador y decir \"Déjame hablar cualquiera con cinco años de experiencia en ingeniería\". En su lugar, por razones que convertido en claro en un momento, comenzó el asalto de talento buscando una pieza de información que parecía no tener ninguna sensibilidad en absoluto, información empresa personas dan a casi nadie que pide.

La primera llamada: La recepcionista

El atacante, usando el nombre Didi Arenas, coloca una llamada a las oficinas corporativas de el servicio de teléfono celular. En parte, la conversación fue así:

Recepcionista: Buenas tardes. Se trata de Marie, ¿cómo puedo ayudarle?
¿Didi: Puede conectarme al departamento de transporte?

R: no estoy seguro que si tenemos uno, miraré en mi directorio. ¿Quién está llamando?
D: es Didi.
¿R: Estás en el edificio, o...?
D: no, estoy fuera del edificio.
¿R: Didi que?
D: Didi Arenas. Tuve la extensión para el transporte, pero me olvidé lo que era.
R: Un momento.

En este punto para disipar sospechas, Didi pidió a un casual, haciendo sólo conversación pregunta para establecer que estaba en el \"interior\" familiarizado con ubicaciones de la empresa.

D: ¿qué edificio Estás en - Lakeview o lugar principal?
R: Principal lugar. (pausa) Es 805 555 6469.

Para proporcionar a sí misma con una copia de seguridad en caso de no proporciona la llamada al transport lo que ella estaba buscando, Didi dijo que ella también quería hablar con bienes raíces. El recepcionista le dio ese número. Cuando Didi pide estar conectado a el número de transporte, la recepcionista intentó, pero la línea estaba ocupada.

En ese momento Didi pidieron un tercer número de teléfono, cuentas por cobrar, ubicado en un centro corporativo en Austin, Texas. La recepcionista le pidió que espere un momento y salió fuera de la línea. Informar a la seguridad de que ella tenía un sospechoso ¿llamada telefónica y pensamiento allí era algo sospechoso pasa? En absoluto y Didi no tienen menos poco de preocupación. Ella estaba siendo un poco de una molestia, pero a la Recepcionista era parte de una jornada típica. Después de aproximadamente un minuto, el Recepcionista volvió sobre la línea, que miraron hacia arriba el número de cuentas por cobrar, lo probé y poner Didi a través.

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 ya haciendo?
P: muy bien.

Didi, a continuación, utiliza un término familiar en el mundo corporativo que describe la carga código para la asignación de gastos contra el presupuesto de una organización específica o Grupo de trabajo:

D: excelente. Tengo una pregunta para usted. ¿Cómo puedo saber el centro de coste para una ¿Departamento en particular?
P: usted tendría que obtener una suspensión de la analista de presupuesto para el departamento.

D: sabes quién sería el analista de presupuesto para ¿Thousand Oaks - sede? Estoy tratando de llenar un formulario y no sé el centro de coste adecuado.
P: Sólo sé cuando y ' All necesita un número de centro de costo, llamar a su presupuesto analista.
D: ¿tienes un centro de coste para su departamento hay en Texas?
P: tenemos nuestro propio centro de coste, pero no nos dan una lista completa de ellos.
D: ¿cuántos dígitos es el centro de coste? Por ejemplo, ¿cuál es su centro de coste?
¿P: bien, gusta, eres con 9WC o con la SAT?

Didi no tenía ni idea qué departamentos o grupos de éstos que se refiere, pero no lo hizo asunto. Ella contestó:

D: 9WC.
P: entonces es usualmente cuatro dígitos. ¿Quien dijo que fuiste con?
D: Sede--Thousand Oaks.
P: bien, aquí está uno de Thousand Oaks. Es la 1A5N, que como n en Nancy.

Sólo colgando fuera mucho tiempo suficiente con alguien dispuesto a ser útil, Didi había el costo del centro número necesitaba - uno de esos fragmentos de información que no uno piensa en proteger porque parece que algo que no podía ser de cualquier valor a un forastero.

La llamada tercera: Un número incorrecto ayudo
Paso de Didi sería parlay el número de centro de coste en algo real valor usando como un chip de póquer.

Comenzó llamando al departamento de bienes raíces, pretendiendo que ella había alcanzado un número incorrecto. Empezando con un \"perdona que moleste, pero.... \"ella afirmaba ella un empleado que había perdido su directorio de la empresa y pidió que fueron se supone que llame para obtener una nueva copia. El hombre dice que la copia impresa es obsoleta ya estaba disponible en el sitio de intranet de la empresa.

Didi dijo que prefería usar una copia impresa, y el hombre le dijo a llamar Publicaciones y luego, sin piden - tal vez sólo para mantener el sexy -

Dama de sonar el teléfono un poco más - servicialmente buscó el número y le dio a ella.

La llamada cuarta: Bart en publicaciones

En publicaciones, habló con un hombre llamado Bart. Didi dijo que ella estaba de Thousand Oaks y tuvieron un nuevo consultor que necesitaba una copia de la Directorio de la empresa. Ella le dijo una copia impresa funcionaría mejor para la consultor, aunque era un poco anticuado. Bart le dijo que ella tendría que llenar un formulario de pedido y enviar el formulario sobre él.

Didi dijo ella estaba fuera de forma y era una fiebre, y Bart sería un cariño ¿y rellena el formulario para ella? Concuerda con demasiado entusiasmo, y Didi le dio los detalles. Para la dirección del contratista ficticio, ella drawled el número de los ingenieros sociales llaman una gota de correo, en este caso un casillas de correo Etc.-tipo de actividad comercial donde su empresa alquiló cuadros para situaciones igual a ésta.

El anterior lingüisticas ahora vinieron mano: habrá un cargo por el costo y envío del directorio. Bien - Didi dio el centro de coste de Thousand Oaks:

IA5N, que como n en Nancy.

Unos días más tarde, cuando llegó el directorio corporativo, Didi encontrado fue e incluso recompensa más grande que ella esperaba: no sólo muestran el nombre y teléfono los números, pero también demostró que trabajaba para quien - la estructura corporativa de la toda la organización.

La dama de la voz ronca estaba lista para comenzar a hacer su head-hunter, personas-incursiones llamadas telefónicas. Ella había estafado a la información que necesitaba para lanzar le RAID mediante el regalo de gab perfeccionado un polaco alto por cada ingeniero social especializada. Ahora ella estaba lista para la recompensa.

JERGA
MAIL DROP: Término del ingeniero social para un buzón de alquiler, normalmente alquilado bajo un nombre supuesto, que se utiliza para entregar documentos o paquetes de la víctima ha sido engañado en enviar

MENSAJE DE MITNICK
Al igual que piezas de un rompecabezas, cada pieza de información puede ser irrelevante por sí. Sin embargo, cuando las piezas se ponen juntos, emerge un panorama claro. En este

Caso, la imagen de la Sierra de ingeniero social fue toda la estructura interna de la empresa.

Analizando el timo

En este ataque de ingeniería social, Didi iniciado por obtener números de teléfono para tres departamentos de la compañía de destino. Esto fue fácil, porque los números era pidiendo no fueron ningún secreto, especialmente a los empleados. Un ingeniero social aprende a sonido como un insider y Didi era experto en esto juego. Uno de los números de teléfono que le llevó a un número de centro de costo, luego que ella se utiliza para obtener una copia del directorio de empleados de la empresa.

Las principales herramientas que necesitaba: sonando amistosa, utilizando algunos jerga corporativa y, con la última víctima, tirar un poco y bateo verbal de pestaña.

Y uno más herramienta, un elemento esencial no fácilmente adquirida - la manipuladora habilidades del ingeniero social, refinado a través de la extensa práctica y las no escritas lecciones de antaño generaciones de hombres de confianza.

MÁS INFORMACIÓN DE \"INÚTIL\"

Además de un número de centro de coste y las extensiones de teléfono interno, qué otro aparentemente inútil información puede ser muy valioso a tu enemigo?.

Llamada de Peter Abel

There was an error deserializing the object of type System.String. The token 'true' was expected but foun
Tus entradas a San Francisco están listos. ¿Quieres a entregarlos, o hacer desea recogerlo?\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'P'.
Abels?\"
Sí, pero no tengo ningún acuerdo sobre los ADPIC proximamente.
There was an error deserializing the object of type System.String. The token 'true' was expected but foun
San Francisco?\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'P'.
conversación amigable.
There was an error deserializing the object of type System.String. The token 'true' was expected but foun
arreglos bajo el número de empleado. Tal vez alguien utiliza mal número. ¿Cuál es tu número de empleado?\"

Peter descifrará recita su número. Y ¿por qué no? Va casi todos formulario de personal rellena, mucha gente en la empresa tiene acceso a ella - recursos humanos, nóminas y, obviamente, la Agencia de viajes fuera. No se trata un número de empleado como algún tipo de secreto. ¿Qué diferencia haría?

La respuesta no es difícil de averiguar. Podrían ser dos o tres piezas de información basta para montar una representación eficaz - el ingeniero social ocultación a sí mismo en la identidad de otra persona. Conseguir el nombre del empleado, su teléfono

número, su empleado número--y tal vez, de buena medida, su manager nombre y teléfono número--y una mitad - ingeniero social competente está equipado con la mayoría de lo que es probable que deba sonido auténtico para el próximo objetivo llamadas.

Si alguien que se dice fue de otro departamento en su compañía tuvo llamó ayer, dada una razón plausible y pidieron su número de empleado, ¿habría tenido alguna reticencia en dárselo a él?

Y por cierto, ¿cuál es su número de seguridad social?

MENSAJE DE MITNICK
Es la Moraleja de la historia, no dar ninguna empresa personal o interna información o identificadores a nadie, a menos que su voz es reconocible y el solicitante tiene una necesidad de saber.

PREVENIR LA CON
Su empresa tiene la responsabilidad de hacer empleados conscientes de cómo un grave error puede producirse de mal manejo de información no pública. Un meditado política de seguridad de la información, combinada con la debida educación y capacitación, será aumentar considerablemente la conciencia de los empleados sobre el manejo adecuado de las empresas información del negocio. Una política de clasificación de datos le ayudará a implementar controles adecuados con respeto Pararevelación 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 versión de aparentemente información inocua:

El departamento de seguridad de la información que necesita para llevar a cabo la formación de la concien detallando los métodos utilizados por los ingenieros sociales. Un método, como se describió anteriormente es obtener información aparentemente no confidencial y utilizarla como un chip de póquer para ganar confianza a corto plazo. Cada empleado debe ser consciente de que cuando una persona que llama tiene conocimiento sobre identificadores internos, jerga y procedimientos de la empresa que hace de ninguna manera, forma o formulario autenticar el solicitante o autorizar a él o ella como una necesidad de saber. Un llamador podría ser un ex empleado o contratista con la información privilegiada necesaria. En consecuencia, cada empresa tiene un responsable de determinar el método de autenticación adecuado para utilizarse Cuando los empleados interactúan con personas que no reconocen en persona o a través de la Telefónica.

La persona o personas con el papel y la responsabilidad de redactar una de datos política de clasificación debe examinar los tipos de datos que pueden utilizar para obtener

acceso para empleados legítimos que parece inocuo, pero podría llevar a información, sensible. Aunque nunca daría a los códigos de acceso su tarjeta de cajero automático, le diría alguien qué servidor se usa para desarrollar ¿productos de software de la empresa? Esa información podría ser usada por una persona ¿fingiendo ser alguien que tiene acceso legítimo a la red corporativa?

A veces sólo saber dentro de terminología puede hacer el ingeniero social aparecen autorizada y bien informados. El atacante se basa a menudo en este común idea errónea a engañando a sus víctimas en cumplimiento de las normas. Por ejemplo, un ID comerciante es un identificador que la gente en el departamento de cuentas nuevas de un Banco casualmente utilizar cada día. Pero tal un identificador exactamente lo mismo que un contraseña. Si cada empleado comprende la naturaleza de este identificador- que se utiliza para autenticar positivamente un solicitante--podría tratarlo con más respeto.

MENSAJE DE MITNICK
Como va el viejo adagio - paranoicos incluso reales probablemente tienen enemigos. Debemos Supongamos que cada negocio tiene sus enemigos, también - los atacantes que se dirigen a la red infraestructura para comprometer secretos comerciales. No terminan siendo una estadística sobre delitos informáticos - ya es hora para apuntalar las defensas necesarias por implementar controles adecuados a través de políticas de seguridad bien pensado fuera y procedimientos.

Ninguna empresa - bien, muy pocos, al menos, dar los números de teléfono de discado directo de su Presidente CEO o Junta. Mayoría de las empresas, sin embargo, no tiene preocupación sobre dar números de teléfono para la mayoría de los departamentos y grupos de trabajo de la, Organización - especialmente a alguien que es, o parece ser, un empleado. A respuesta posible: una política que prohíbe dar teléfono interno número de empleados, contratistas, consultores y temps a los forasteros. Más lo importante es desarrollar un procedimiento paso a paso para identificar positivamente si una pidiendo números de teléfono que llama es realmente un empleado.

Códigos de contabilidad para grupos de trabajo y departamentos, así como copias de la directorio corporativo (si copia impresa, archivo de datos o teléfono electrónico libro sobre la Intranet) son blancos frecuentes de ingenieros sociales. Cada empresa necesita un escrito, Karadzic política sobre la divulgación de este tipo de información. Las salvaguardias debe incluir el mantener un registro de auditoría instancias de registros cuando sensibles la información es divulgada a personas fuera de la empresa.

Información, como un número de empleado, por sí mismo, no debe utilizarse como cualquiera tipo de autenticación. Cada empleado debe estar formado para verificar no sólo la identidad del solicitante y el solicitante del necesita saber.

En su formación en seguridad, considere la posibilidad de enseñanza empleados este enfoque: siempre una pregunta o pide un favor por un extraño, primero aprender a rechazar educadamente hasta que la solicitud puede ser verificada. -Antes de ceder ante el deseo natural de ser Sr. o Sra. útiles - siga las políticas de empresa y procedimientos con respecto a verificación y divulgación de información no pública. Este estilo puede ir en contra nuestra tendencia natural a ayudar a los demás, pero un poco paranoia sana puede ser necesario para evitar ser dpdo próximo del ingeniero social.

Como han demostrado las historias en este capítulo, aparentemente inocuo información puede ser la clave para los secretos más preciados de su empresa.

Capítulo 3
El ataque directo: Pidiendo sólo se

Muchos ataques de ingeniería social son complejos, que implican una serie de pasos y saben elaborar planificación, combinando una mezcla de manipulación y tecnológico-Cómo.

Pero siempre me parece sorprendente que un hábil ingeniero social a menudo consigue su objetivo con un ataque directo, simple y sencillo. Sólo pidiendo abiertamente la información puede ser todo lo que necesitan - como verá.

UN RAPIDITO MLAC
¿Quiere saber el número de teléfono están ocultos de alguien? Un ingeniero social puede decirle formas una docena (y encontrará algunos de ellos descritos en otras historias en estas páginas), pero probablemente la hipótesis más simple es aquella que utiliza un teléfono único llamar, como esta.

Número, por favor
El atacante marcó el teléfono de empresa privada para el MLAC, la Centro de asignación de línea mecanizada. A la mujer que respondieron, dijo:

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele frito en un incendio. Policias pensar algunos sobrante intentó incendiar su casa para la seguro. Me salió aquí solo intentando rewire este dos todo cien- par terminal. Realmente pude utilizar alguna ayuda ahora. ¿Qué instalaciones deben ser trabajando en Main sur 6723?\"

En otras partes de la compañía telefónica, la persona que llama sabría inversa información de búsqueda en el pub no números (no publicado) se supone que dará a sólo a la compañía de teléfonos autorizados MLAC se supone que sólo conocer empleados de la empresa. Y si bien nunca se daría información al público, quien quisiera rechazar ayuda un poco a un hombre de empresa afrontar pesados- asignación de destino?. Siente pena por él, ella ha tenido días malos en el trabajo y ella te
doblar las reglas un poco para ayudar a un compañero empleado con un problema. Ella da él el cable y pares y cada número de trabajo asignado a la dirección.

MENSAJE DE MITNICK
Es naturaleza humana para confiar en nuestro prójimo, especialmente cuando la solicitud cumple la prueba de ser razonable. Los ingenieros sociales usar este conocimiento para explotar sus las víctimas y para lograr sus objetivos.

Analizando el timo
Como observará repetidamente en estas historias, conocimiento de la jerga de la empresa, y de su estructura corporativa - en sus diferentes oficinas y departamentos lo que cada uno hace y información que cada uno tiene - es parte de la esencial bolsa de trucos de los exitosos ingeniero social.

YOUNG MAN ON THE RUN
Un hombre denominaremos Frank Parsons había estado huyendo durante años, aún buscados por el Gobierno Federal para ser parte de un grupo antiguerra clandestino en la década de 1960. En los restaurantes se sentó frente a la puerta y tenía una forma de echar un vistazo sobre su asumir cada de vez en cuando que otras personas encuentran desconcertante. Se trasladó cada pocos años.

En una de punto de Frank, aterrizó en una ciudad no saber y establecer sobre caza de trabajo. Para alguien como Frank, con sus habilidades de equipo bien desarrollada (y social habilidades de ingeniería, así como, incluso, aunque él nunca figuran los de un trabajo aplicación), encontrar un buen trabajo normalmente no era un problema. Excepto en momentos cuando la economía está muy apretada, personas con conocimientos de buen equipo técnico suelen encontrar sus talentos de alta demanda y tienen poco problema aterrizando en sus pies. Frank encuentra rápidamente un pozo – pagando oportunidad laboral en una gran Centro de atención a largo plazo, lujo cerca de donde vivía.

Sólo el billete, pensó. Pero cuando comenzó a andar su camino a través de la formularios de solicitud, llegó a un uh-AH: el empleador exige al solicitante para proporcionar una copia de su récord de historia criminal del Estado, que tuvo que obtener propio de la policía del Estado. La pila de documentos de empleo incluye un formulario para solicitar este documento, y la forma tenía una pequeña caja para proporcionar una huella digital. A pesar de que ellos estaban pidiendo una impresión de sólo el dedo índice derecho, si se coincide su impresión con uno en base de datos del FBI, habría probablemente pronto a trabajar en el servicio de comida en un resort financiado por el Gobierno Federal.

Por otro lado, se produjo a Frank que quizás, sólo quizás, podría seguir capaz de llegar lejos con esto. Tal vez el Estado no enviar que las muestras de huellas digitales el FBI en absoluto. ¿Cómo podría averiguar?

¿Cómo? ¿Fue un ingeniero social--cómo crees descubrió? Colocó un llamada telefónica a la patrulla del Estado: \"Hola. Estamos haciendo un estudio del departamento de Esta de la justicia. Nosotros estamos investigando los requisitos para implementar una nueva huella sistema de identificación. Puedo hablar allí alguien que realmente conoce lo que estás haciendo que quizás podría ayudarnos a?\"

Y cuando el experto local llegó en el teléfono, Frank le pidió una serie de preguntas acerca de lo que estaban utilizando los sistemas y las capacidades para buscar y almacenar datos de huellas digitales. Tuvo problemas de equipo? Ataron en el Centro Nacional de información de crimen de búsqueda de huellas dactilares (NCIC) o solo dentro de la ¿Estado? ¿Fue bastante fácil para todos aprender a usar el equipo?

Astutamente, él furtivamente la pregunta clave en el resto.

La respuesta fue música para sus oídos: No no estaban atados en el NCIC, que sólo protegido contra el estado Penal información índice (CII).

MITNICK MESSGAE

Experto información estafadores no tengan ningún reparo en sonar hasta federal, estatal, o funcionarios del gobierno local para obtener información sobre los procedimientos de aplicación de la ley. Con esa información en la mano, puede ser capaz de sortear el ingeniero social comprobaciones de seguridad estándar de la empresa.

Eso era todo que Frank necesitaba saber. No tenía ningún registro en ese Estado, por lo que él presentó su solicitud, fue contratado para el trabajo y nadie nunca apareció en su escritorio un día con el saludo, \"estos señores son de FBI y les gustaría tener una pequeña charla con usted.\"

Y, de acuerdo con él, demostró ser un empleado modelo.

EN LA MISMA PUERTA

A pesar del mito de la Oficina sin papeles, las empresas continúan imprimir resmas de papel cada día. Información de impresión de su empresa puede ser vulnerable, incluso si utiliza precauciones de seguridad y acabar con ella confidencial.

Aquí es una historia que muestra cómo los ingenieros sociales podría obtener la mayoría documentos secretos.

Bucle alrededor de engaño

Cada año la compañía telefónica publica un volumen llamado el número de prueba Directorio (o al menos solían, y porque estoy todavía en libertad supervisada, No voy a preguntar si todavía lo hacen). Este documento fue muy apreciado por teléfono phreaks porque estaba repleto de una lista de todos los teléfonos celosamente números utilizados por artesanos de la empresa, técnicos, a otros para cosas como tronco pruebas o controles de números que siempre suena ocupado.

Uno de estos test números, conocida en la jerga como un bucle alrededor, fue particularmente útil. Phreaks teléfono utilizado como una manera de encontrar otros phreaks de teléfono para conversar co sin costo alguno para ellos. Teléfono phreaks también usó una forma de crear un número de llamada de vu para dar a, digamos, un banco. Un ingeniero social diría a alguien en el Banco el número de teléfono para llamar al llegar a su oficina. Cuando el Banco llamado de vuelta a la prueba número (bucle-alrededor) el teléfono venía sería capaz de recibir la llamada, pero él tenía la protección de haber utilizado un número de teléfono que no pudo se remonta a él.

Un directorio de número de Test proporciona mucha información ordenada que podría utilizarse por cualquier teléfono hambriento de información, testosteroned, phreak. Así que cuando el nuevo directorios fueron publicados cada año, eran codiciados por un montón de jóvenes cuya afición estaba explorando la red telefónica.

MENSAJE DE MITNICK
Formación en seguridad con respecto a la política de la empresa diseñada para proteger la información debe ser para todos en la empresa, no cualquier empleado que tiene activos acceso físico o electrónico a la empresa de TI de activos.

Estafa de Stevie
Naturalmente, las empresas de telefonía no hacen estos libros fáciles de conseguir, así que teléfono phreaks tiene que ser creativo para obtener uno. ¿Cómo pueden hacer esto? Un joven ansioso con una mente bent en adquirir el directorio podría promulgar un escenario como este.

Tarde de un día, una noche suave en el otoño del sur de California, un chico llamo le Stevie teléfonos un pequeño Teléfono Oficina central, que es la empresa la edificio desde el que ejecutan las líneas de teléfono a todos los hogares y empresas en el área de servicio establecidos.

Cuando el guardarrail en servicio responde a la llamada, Stevie anuncia que él es de la División de la compañía telefónica que publica y distribuye impreso materiales. \"Tenemos su nuevo directorio número de prueba\", dice. \"Pero para seguridad razones, no podemos entregamos la copia hasta que recogemos antiguo. Y la entrega Guy retrasados. Si quieres deja tu copia justo fuera de su puerta, él puede Swing por recoger tuyo, colocar uno nuevo y en su camino.\"

El guardarrail confiado parece pensar que suena razonable. Lo hace tal y como pidió, apagando en la puerta del edificio su copia de la Directorio, su portada claramente marcado en grandes letras rojas con la empresa\" CONFIDENCIAL - CUANDO YA NO ES NECESARIO ESTE DOCUMENTO DEBE SER PURGADOS.\"

Stevie unidades por y mira cuidadosamente para detectar cualquier policias o compañía de teléfono gente de seguridad que podría estar acechando detrás de árboles o mirando para él desde coches aparcados. Nadie a la vista. Casualmente recoge el directorio codiciado y unidades de distancia.

Aquí es sólo un ejemplo más de lo fácil que puede ser de un ingeniero social obtener lo que quiere, siguiendo el principio simple de \"pregunte por ello.\"

ATAQUE CON GAS

Activos de la empresa no sólo están en riesgo en un escenario de ingeniería social. A veces es quienes una empresa son las víctimas.

Trabajo como empleado de servicio al cliente trae su cuota de frustraciones, su cuota de se ríe y su cuota de errores inocentes - algunos de los cuales pueden tener infeliz consecuencias para los clientes de la empresa.

Historia de Janie Acton

Janie Acton había dotación un cubículo como un cliente servicio rep f ciudad natal Energía eléctrica, en Washington, D.C., para poco más de tres años. Ella fue considerado como uno de los empleados mejores, conscientes e inteligentes

Fue cuando esta una llamada particular llegó en la semana de Thanksgiving. El llamador, dijo,
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
Secretaria en las oficinas ejecutivas que funciona para uno de los vice presidentes, y ella está pidiendo información y no puedo utilizar mi ordenador recibí un correo electrónico de esta chica que dice 'ILOVEYOU.' y cuando abrí los recursos humanos el archivo adjunto, no podía usar mi máquina más. Un virus. Me pille un virus estúpido. De todas formas, podría buscar alguna información de cliente para mí?\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'J'
Sí.
There was an error deserializing the object of type System.String. Encountered unexpected charac

Aquí el atacante llamado en la información de su investigación avance para hacer el propio sonido auténtico. Había aprendido que él quería era almacenados en algo llamado el sistema de información de facturación de clientes, y tenía descubrió cómo empleados contemplados para el sistema. Preguntó, \"puede aparezca un cuenta el CBIS?\"

Sí, ¿cuál es el número de cuenta.?
No tengo el número; Te necesito para traerlo hasta por su nombre.
Está bien, ¿cuál es el nombre?
There was an error deserializing the object of type System.String. Encountered unexpected character 'H

Vale, lo tengo.
Gran. ¿Es la cuenta actual?
Uh huh, es actual.
There was an error deserializing the object of type System.String. Encountered unexpected characte
¿Tienes un lápiz?
Listo para escribir.
Cuenta número BAZ6573NR27Q.
Lee el número nuevo y luego dijo, \"Y ¿cuál es la dirección de servicio?\"
Ella le dio la dirección.
Y ¿cuál es el teléfono?
Janie descifrará Lee esa información, demasiado.

El llamador le agradeció, dijo adiós y colgó. Janie pasó a la siguiente
llamada, nunca pensando en otra cosa.

Proyecto de investigación de arte de Sealy
Sealy de arte había dado un trabajo como editor independiente para pequeñas editoriales
Cuando se encontró con él podría ganar más dinero haciendo investigación para escritores y
empresas. Él pronto averiguado que la tarifa que podría cobrar subió
Cómo cerrar la asignación lo llevó a la línea a veces borrosa la proporción
entre el legal y el ilegal. Sin nunca saberlo, sin duda alguna vez
dándole un nombre, Art fue un ingeniero social, utilizando técnicas conocidas a todos
corredor de información. Resultó tener un talento nativo para el negocio
averiguar por sí mismo técnicas que la mayoría de los ingenieros sociales tuvo que aprender de
otros. Después de un tiempo, cruzó la línea sin la pospuesta menos de culpabilidad.

Un hombre contactó conmigo que estaba escribiendo un libro sobre el gabinete en el Nixon
años y fue en busca de un investigador que se pudo obtener el interior primicia en
William E. Simon, quien había sido Secretario del Tesoro de Nixon. Sr. Simon había
murió, pero el autor tenía el nombre de una mujer que había sido en su personal. Fue
bastante seguro que ella todavía vivía en D.C., pero no había podido obtener una dirección. Ella
no tenía un teléfono a su nombre, o al menos ninguno que se enumeran. Por lo que de
Cuando me llamó. Yo le dije, claro, no hay problema.

Este es el tipo de trabajo generalmente puede traer en una llamada telefónica o dos, si usted
Sé lo que estás haciendo. Cada empresa de servicios públicos locales se cuentan generalmente con
para regalar la información. Por supuesto, tienes a BS un poco. Pero lo que tiene un
¿Little white mentira ahora y después - derecho?

Me gusta utilizar un enfoque diferente cada vez, sólo para mantener las cosas interesantes. \"Esto
es Fulano en las oficinas ejecutivas\"siempre ha trabajado bien para mí. Por lo tanto tiene \"I ' ve
tiene alguien en la línea de su cargo de Vicepresidente alguien\"que trabajó
Esta vez, demasiado.

MENSAJE DE MITNICK
Nunca piensa en todos los ataques de ingeniería social deben ser elaborados ardides de tan complejos que son probables a ser reconocido antes de que pueda completarse. Algunos son en- ataques y-out, huelga y desaparecen, muy simples que son no más..., bueno, sólo solicitarlo.

Tienes que tipo de desarrollar el instinto del ingeniero social, hacerse una idea de cómo Cooperativa la persona en el otro extremo va a estar con ustedes. Esta vez me tocó con una dama agradable y útil. En una sola llamada telefónica, tuve la dirección y número de teléfono. Misión cumplida.

Analizando el timo
Ciertamente Janie sabía que la información del cliente es sensible. Ella sería nunca discutir cuenta de un cliente a otro cliente, o dar información privada al público.

Pero, naturalmente, para la persona que llama desde dentro de la empresa, aplican reglas diferentes. Para u compañero empleado es todo acerca de ser un jugador de equipo y ayudando a cada otro obtener el trabajo realizado. El hombre de facturación podría se buscaron los detalles a sí mismo si su equipo hubiera sido abajo con un virus, y ella estaba contenta de poder ayudar a una co- trabajador.

Arte construido gradualmente a la información clave que él estaba realmente después, pidiendo preguntas en el camino las cosas realmente necesitó, tales como la número de cuenta. Pero al mismo tiempo, la cuenta número información proporciona un respaldo: si el empleado se había convertido en sospechoso, llamaría u tiempo y una mejor oportunidad de éxito, porque conociendo la cuenta número le haría sonido más auténtico a la dependienta siguiente llegó.

Nunca se ocurrió Janie que alguien realmente podría mentir sobre algunos cosa como esta, que la llamada no puede ser realmente desde el departamento de facturación todos. Por supuesto, la culpa no encuentran a los pies de Janie. Ella no era versada en la la regla sobre asegurándose de que usted sabe que usted está hablando antes de examinar información en el archivo del cliente. Nunca nadie había dicho sobre el peligro de un llamada telefónica como el de arte. No era en la política de la empresa, no era parte de su formación, y nunca había mencionado su supervisor.

PREVENIR LA CON
Un punto para incluir en su formación en seguridad: sólo porque sabe un llamador o visitante los nombres de algunas personas en la empresa, o conoce algunas de la jerga corporativa o procedimientos, no significa que él es quien dice ser. Y definitivamente no

establecer le alguien autorizado para dar información interna o el acceso a su sistema informático o red.

Necesidades de formación de seguridad destacar: en caso de duda, verificar, comprobar, verificar.

En épocas anteriores, el acceso a la información dentro de una empresa fue una marca de rango y privilegio. Los trabajadores avivado los hornos, corrió las máquinas, ha escrito las letras, y presentó los informes. El capataz o jefe les dijo qué hacer, cuándo y cómo. Se fue el capataz o jefe que sabía cómo muchos widgets cada trabajador debe ser producir un cambio, cuántos y en qué colores y tamaños de la fábrica es necesaria para activar esta semana, la próxima semana y a finales de mes.

Los trabajadores manejan máquinas y herramientas y materiales y jefes manejadas información. Los trabajadores necesarios sólo la información específica de sus puestos de trabajo especí

La imagen es un poco diferente hoy, ¿no? Muchos trabajadores de la fábrica utilizan algunos formulario de equipo o máquina impulsada por el equipo. Una gran parte de la fuerza de trabajo, información crítica se empuja hacia abajo a los escritorios de los usuarios para que pueda cumplir con la responsabilidad de hacer su trabajo. En el entorno actual, casi todo lo hacen empleados implica el manejo de la información.
Es por eso la política de seguridad de una empresa debe ser distribuido toda la empresa, independientemente de la posición. Todo el mundo debe entender que no es sólo de los jefes y ejecutivos que tienen la información de que un atacante podría ser después. Hoy, los trabajadores en todos los niveles, incluso aquellos que no usar una computadora, son susceptibles de ser dirigidos. El recién contratado representante en el grupo de servicio al cliente puede ser sólo los débiles enlace que rompe un ingeniero social para lograr su objetivo.
Formación en seguridad y políticas de seguridad corporativas necesitan reforzar enlace.

Capítulo 4
Fomento de la confianza

Algunas de estas historias podrían llevarle a pensar que creo que todos en el negocio es un completo idiota, listo, incluso ganas, regalan cada secreto en su posesión. El ingeniero social sabe no es verdad. ¿Por qué la ingeniería social ¿ataques tanto éxito? No es porque las personas son estúpidas o falta de sentido común. Pero, como seres humanos todos somos vulnerables a ser engañados porque la gente puede ha extraviado su confianza si manipulado en ciertas maneras.

El ingeniero social anticipa sospecha y resistencia, y siempre está dispuesto para activar la desconfianza en confianza. Un buen ingeniero social planea su ataque como un ajedrez juego, anticipando las preguntas podría pedir su destino para que él pueda estar listo con el respuestas adecuadas.

Una de sus técnicas comunes implica construir un sentimiento de confianza por parte de sus víctimas. ¿Cómo hace un estafador que le confía en él? Confía en mí, él puede.

CONFIANZA: LA CLAVE DEL ENGAÑO
Más un ingeniero social puede hacer que su contacto parece negocio como de costumbre, la más él disipa sospecha. Cuando las personas no tienen una razón para sospechar, tiene fácil para un ingeniero social ganar su confianza.

Una vez que tiene su confianza, se baja el puente levadizo y la puerta del castillo iniciada abrir por lo que puede entrar y tomar toda la información que quiere.

NOTA
Puede que observe que me refiero a los ingenieros sociales, teléfono phreaks y con juego operadores como \"él\" a través de la mayoría de estas historias. Esto no es chauvinismo; es simplemente refleja la verdad que la mayoría de los profesionales en estos campos son hombres. Pero aunque hay no muchas mujeres ingenieros sociales, el número está creciendo. Hay suficiente mujeres ingenieros sociales por ahí que usted no debería bajar su guardia sólo porque se oye la voz de la mujer. De hecho, los ingenieros sociales femeninos tienen una clara ventaja porque pueden utilizar su sexualidad para obtener cooperación. Encontrará un pequeño número de los llamados sexo suave representado en estas páginas

La primera llamada: Andrea Lopez
Andrea Lopez contestó el teléfono en la tienda de alquiler de video donde trabajaba, y en un momento estaba sonriendo: siempre es un placer cuando un cliente tiene la problemas para decir que él está feliz acerca del servicio. Este llamador dijo que había tenido una muy buena experiencia con la tienda y él querían enviar el administrador de un Carta sobre ella.

Preguntó por el nombre del administrador y la dirección de correo, y ella le dijo que era Tommy Allison y le dio la dirección. Como él se acerca para colgar, tuvo otra idea y dijo: \"podría escribir en su sede de la empresa, también. ¿Cuál es su número de tienda?\" Ella le dio esa información. Dijo Gracias, añadió algo agradable sobre cómo ayuda había sido y dijo Adiós.

There was an error deserializing the object of type System.String. Encountered unexpected character 's'.
lindo sería si gente hacía más a menudo.\"

La segunda llamada: Ginny
Gracias por llamar a Video Studio. Se trata de Ginny, ¿cómo puedo ayudarle?
There was an error deserializing the object of type System.String. The token 'true' was expected but found
cada semana, más o menos. \"Es Tommy Allison, Gerente del Parque forestal, tienda 863. Nos tiene un cliente aquí que quiere alquilar 5 Rocky y estamos todos de copias. Puede usted comprobar en qué tienes?\"
Ella volvió en la línea después de unos momentos y dijo: \"sí, tenemos tres copias\".
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
ayuda de nuestra tienda, acabo de llamar y preguntar por Tommy. Alegrará hacer todo posible para usted.\"

Tres o cuatro veces durante el próximo par de semanas, Ginny recibió llamadas de Tommy para obtener ayuda acerca de una cosa u otra. Eran aparentemente legítimas peticiones, y siempre fue muy amable sin sonar como estaba tratando de llegar a su. Fue un poco chatty en el camino, así como - \"te enteraste el grande ¿fuego en Oak Park? Manojo de calles cerradas por allí\"y similares. Las llamadas fueron un poco descanso de la rutina del día y Ginny siempre alegró oír desde él.

Un día Tommy llamado sonda subrayado. Preguntó, \"chicos llevan ¿tiene problemas con sus equipos?\"

There was an error deserializing the object of type System.String. Encountered unexpected charac
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
reparador dice que todo parte de la ciudad perderá sus teléfonos e Internet conexión hasta consiguen esto fijo. \"
Oh, no. ¿Fue herido el hombre?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
un cliente suyo aquí que quiere alquilar el Padrino II y no tiene su tarjeta con él. Puede comprobar su información para mí?\"
Sí, seguro.

Tommy dio nombre y dirección del cliente, y Ginny lo encontró en el
equipo. Ella dio a Tommy el número de cuenta.
There was an error deserializing the object of type System.String. Encountered unexpected character
Nada que mostrar.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
base de datos más tarde cuando los equipos volver. Y él quiere poner
este cargo en la tarjeta Visa usa en tu tienda, y él no lo tiene con él.
¿Qué es la tarjeta número y fecha de vencimiento?\"

Le dio a él, junto con la fecha de caducidad. Tommy dijo: \"Hey, gracias por
la ayuda. Hablar con usted pronto,\"y colgado arriba.

Historia de Doyle Lonnegan
Lonnegan no es un joven que desea encontrar esperando al abrir
la puerta delantera. Un hombre de la colección una sola vez por deudas de juegos malas, él sigue
un favor ocasional, si no ponerlo fuera mucho. En este caso, fue
ofrece un paquete considerable de dinero en efectivo por poco más de hacer algunas llamadas telefónicas
una tienda de video. Suena bastante fácil. Es sólo que sabía que ninguno de sus \"clientes\"
Cómo ejecutar este con; que necesitaban a alguien con el talento de Lonnegan y saber-
Cómo.

Personas no escriben cheques para cubrir sus apuestas cuando son mala suerte o estúpido en el
Mesa de póker. Todo el mundo lo sabe. ¿Por qué mantuvo estos amigos míos
¿jugando con un truco que no tiene verde fuera de la tabla? No preguntar. Tal vez
son un poco de luz en el departamento de IQ. Pero son amigos míos--lo que puede
¿hacer?
Este chico no tenía el dinero, por lo que tomaron una verificación. Pido! Debe de condujo
él a un cajero, es lo que debe de hacer. Pero no, una verificación. Para
$3.230.
Naturalmente, rebotó. ¿Qué cabría esperar? Así que me llamen; ¿puedo ayudar?
No cierro puertas en los nudillos de las personas más. Además, hay mejores maneras
hoy en día. Les dije, 30 por ciento de Comisión, que quisiera ver qué podía hacer. Por lo tanto se
me da su nombre y dirección, y subir en el equipo para ver lo que tiene el
videoclub más cercano a él. Yo no estaba en un gran apuro. Llamadas a acogedora hasta cuatro telefónic
el Gerente de la tienda y luego, bingo, I've got número de tarjeta Visa de tramposo.
Otro amigo mío es propietario de un bar de topless. Cincuenta de los Bucks, puso poker de guy
dinero a través de un encargado de Visa desde la barra. Explico el truco que a su
esposa. ¿Cree que él podría intentar contar Visa no es su cargo? Se equivoca. Él
sabe que sabemos quien es. Y si pudimos conseguir su número de Visa, él te figura nos
se puede obtener mucho más aparte. Sin preocupaciones en este sentido.

Analizando el timo
Llamadas iniciales de Tommy a Ginny eran simplemente construir confianza. Cuando llegó el momento
el ataque, ella dejarla guardia Tommy abajo y aceptado para que él
afirmó que, el administrador en otra tienda de la cadena.
Y ¿por qué no ella aceptarlo--ella ya lo sabía. Sólo le había conocido
por teléfono, por supuesto, pero habían establecido una amistad de negocios que
es la base para la confianza. Una vez ella lo había aceptado como una figura de autoridad, un administrado
en la misma empresa, se había establecida la confianza y el resto fue un paseo en la
Parque.

MENSAJE DE MITNICK
La técnica de picadura de confianza es uno de lo social más eficaz
tácticas de ingeniería. Tienes que pensar si realmente sabes la persona eres
hablando. En algunos casos raros, la persona no sea quien dice ser.
En consecuencia, todos tenemos que aprender a observar, pensar y cuestionar la autoridad.

VARIACIÓN SOBRE UN TEMA: CAPTURA DE TARJETA
Construir un sentido de confianza no necesariamente exige una serie de llamadas telefónicas con
la víctima, como sugiere el artículo anterior. Recuerdo un incidente que fue testigo de
en cinco minutos fue todo que lo llevó.

Sorpresa, papá
Una vez me senté en una mesa en un restaurante con Enrique y su padre. En el curso de
conversación, Henry regañó a su padre para dar su número de tarjeta de crédito como si
se tratara de su número de teléfono. \"Seguro, tienes que darle el número de su tarjeta cuando usted
\"comprar algo, dijo. \"Pero dando a un almacén que archivos tu número en su
Records - es tonto real.\"

El único lugar que hago en Video de estudio,\"Sr. Conklin dijo, la misma denominación
cadena de tiendas de vídeo. \"Pero voy en mi factura de Visa cada mes. Si ha iniciado
ejecución de gastos, que lo sé.
\"Seguro, dijo Henry,\"pero una vez que tengan su número, es muy fácil para alguien que
roban\"

Te refieres a un empleado torcido\".
No, nadie - no sólo un empleado. \"
\"Está hablando a través de su sombrero, dijo el Sr. Conklin.
Puedo llamar ahora y que me diga su número de Visa,\"Henry disparo
Atrás.
No, no, \"dijo su padre.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
la tabla\".

Sr. Conklin parecía apretado alrededor de los ojos, la mirada de alguien sintiéndose seguro de
Sí, pero no querer mostrarlo. \"Digo que no sabes que está hablando
acerca de,\"él corteza, sacar su billetera y bofetadas billete de cincuenta dólares en la
tabla. \"Si puedes hacer lo que dices, que
tuyo.
There was an error deserializing the object of type System.String. Encountered unexpected characte
Sacó su teléfono celular, preguntó qué rama usó y llamó a su padre
Asistencia de directorio para el número de teléfono, así como el número de la tienda en
cerca de Sherman Oaks.

Entonces llamó a la tienda de Sherman Oaks. Con prácticamente el mismo enfoque
se describe en el artículo anterior, rápidamente obtuvo el nombre del administrador y la tienda
número.

Entonces llamó a la tienda donde su padre tenía una cuenta. Él sacó el viejo
suplantar la-administrador de truco, según su propia y dando el nombre del administrador
el número de almacén que sólo había obtenido. Luego utilizó el mismo truco: There was an error dese
¿equipos trabajando bien? Nuestra han estado arriba y abajo\". Escuchaba su respuesta
y luego dijo, \"pues mira, yo tengo uno de sus clientes aquí que quiere alquilar
un video, pero nuestros equipos están ahora hacia abajo. Te necesito para buscar el
cliente cuenta y asegúrese de que él es un cliente en su rama. \"
Henry le dio el nombre de su padre. A continuación, utilizando sólo una ligera variación en
técnica, hizo la solicitud para leer la información de la cuenta: dirección,
número de teléfono y fecha de que la cuenta fue abierta. Y entonces dijo: \"Hey, escucha,
Estoy levantando de una larga línea de clientes aquí. ¿Cuál es el número de tarjeta de crédito y
fecha de caducidad?\"
Henry celebró el teléfono celular a su oreja con una mano mientras que escribió sobre un
servilleta de papel con la otra. Como terminó la llamada, él deslizó la servilleta en
frente a su padre, quien Miró con la boca abierta de suspensión. El pobrecito a
parecía totalmente sorprendido, como si sólo hubiera salido todo su sistema de confianza el
drenaje.

Analizando el timo
Pensar en su propia actitud cuando alguien que no conoces te pide para
algo. Si un extraño cutre llega a tu puerta, no es probable que le
en; Si un extraño llega a su puerta bien vestidos, zapatos brilló, cabello perfecto,
con forma amable y una sonrisa, es probable que sea mucho menos sospechosos. Tal vez
realmente es Jason desde las películas de viernes 13, pero que estás dispuesto a comenzar
confiar en esa persona mientras él se ve normal y no tiene un cuchillo
su mano.
Lo que es menos obvio es que juzgamos personas por teléfono de la misma manera. Hace
¿Este sonido de persona como él está tratando de venderme algo? Él es amable y
¿saliente o presiento algún tipo de hostilidad o presión? ¿Él o ella tiene el

¿discurso de una persona educada? Nosotros juzgar estas cosas y tal vez una docena a los demás inconscientemente, en un instante, a menudo en los primeros momentos de la conversación.

MENSAJE DE MITNICK

Es naturaleza humana pensar que es poco probable que usted está siendo engañado en cualquier particula transacción, por lo menos hasta que haya alguna razón para creer lo contrario. Nos pesan los riesgos y, a continuación, la mayor parte del tiempo, dar a la gente el beneficio de la duda. Es decir el comportamiento natural de gente civilizada..., por lo menos civilizadas personas que nunca han sido estafado, manipulado o engañado por una gran cantidad de dinero.
Como los niños nuestros padres nos enseñaron no a confiar en extraños. Quizás nos deberíamos todos escu Este principio milenario en el trabajo de hoy.

En el trabajo, gente que pide de nosotros todo el tiempo. ¿Tienes una dirección de correo electrónico ¿para este chico? ¿Dónde está la versión más reciente de la lista de clientes? Quien tiene la ¿subcontratista en esta parte del proyecto? Por favor, envíe la actualización más reciente del proyecto. Necesito la nueva versión del código fuente.

Y adivinen qué: a veces son personas que hacen esas peticiones su personalmente no sé, gente que trabaja por parte de la empresa, o afirman que lo hacen. Pero si la información que dan, se retira, y parecen ser en el saber (\"Marianne dijo...\";\"Es en el servidor de K-16... \"; \"... revisión 26 de los nuevo producto planes\"), extendemos nuestro círculo de confianza para incluir en ellos, y alegremente darles lo que está pidiendo.

Sin duda, nos podemos tropezar un poco, preguntarnos \"por qué alguien el Planta de Dallas necesita ver los nuevos planes de producto?\"o\"podría duele nada ¿dar el nombre del servidor es\"? Así que pedimos otra pregunta o dos. Si la respuestas aparecen razonables y forma de la persona es tranquilizador, dejamos abajo nuestra guardia, retorno a nuestra inclinación natural a confiar en nuestro colega hombre o mujer, y hacer (con razón) lo que nos estamos les pide que hagan.

Y no creo que por un momento que el atacante sólo tendrá como objetivo las personas ' ho utilizar sistemas de informáticos de la empresa. ¿Qué pasa con el tío en la sala de correo? \"Vas a hacer ¿me un favor rápido? Colocar esto en la valija de correo intra empresa?\" El correo empleado de la sala sabe que contiene un disco con un programita especial para la ¿Secretario del CEO? Ahora ese atacante obtiene su propia copia personal del CEO Correo electrónico. WoW! ¿Puede realmente ocurre en su empresa? La respuesta es, absolutamente.

EL CELULAR DE UNO CIENTO

Muchas personas miran a su alrededor hasta la); encontrar un mejor trato; los ingenieros sociales no mirar para un mejor trato, encuentran una manera de hacer un trato mejor. Por ejemplo, a veces un

empresa lanza una campaña de marketing que es por lo que difícilmente puede llevar a pasarlo arriba, mientras que el ingeniero social analiza la oferta y se pregunta cómo puede endulzar el acuerdo.

No hace mucho tiempo, una empresa inalámbrica nacional tuvo una importante promoción en marcha ofreciendo un flamante teléfono para un céntimo cuando te registrado en uno de sus planes de llamadas.

Como muchas personas han descubierto demasiado tarde, hay una buena muchas preguntas una comprador prudente debe preguntar antes de inscribirse en un plan de llamadas de celular Si el servicio es analógico, digital o una combinación; el número de en cualquier momento minutos que se puede utilizar en un mes; Si se incluyen tarifas de itinerancia.. y, y sucesivamente. Especialmente importante comprender desde el principio es el término del contrato de ¿compromiso--cuántos meses o años tendrá que comprometerse a?

Imagen de un ingeniero social en Filadelfia que se siente atraída por un modelo de teléfono barato ofrecidos por una compañía de teléfono celular en suscripción, pero odia el llamado plan que va con él. No es un problema. Esta es una forma que podría manejar la situación.

La primera llamada: Ted
En primer lugar, el ingeniero social marca una cadena de tiendas de electrónica en Occidente Girard.

Ciudad de electrones. Esta es Ted.
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
acerca de un teléfono celular. Dijo que sería llamarlo cuando me decidí por el plan que buscaba, y me olvidé de su nombre. ¿Quién es el chico que trabaja en ese departamento en la noche ¿cambio?
Hay más de uno. ¿Fue William?
There was an error deserializing the object of type System.String. Encountered unexpected character '\'". flaco.\"
There was an error deserializing the object of type System.String. Unexpected end of file. Followin
Hadley. H--UNA--D--L--E--Y.
Sí, eso suena bien. ¿Cuando él va a estar?
No sé su agenda esta semana, pero el pueblo de noche viene en unas cinco.
Buena. Lo probaré esta noche, entonces. Gracias, Ted.

La segunda llamada: Katie
La siguiente llamada es una tienda de la misma cadena en North Broad Street.

Hola, ciudad de electrones. Katie hablando, ¿cómo puedo yo ayudarte?

There was an error deserializing the object of type System.String. Unexpected end of file. Following el hoy en día?\"

Algo lento, ¿qué pasa?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
conocer el uno que me refiero?\"
Derecho. He vendido un par de esos la semana pasada.
¿Todavía tiene algunos de los teléfonos que van con ese plan?
Tengo una pila de ellos.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
él hasta en el contrato. Revisé el inventario maldito y no tenemos ninguna
teléfonos de izquierda. Estoy tan avergonzada. ¿Me pueden hacer un favor? Lo envío le sobre a
tu tienda para recoger un teléfono. Le Vendemos el teléfono para un céntimo y escribir
¿él hasta un recibo? Y supone que me llaman una vez lo tiene el teléfono
puede hablar le a través de cómo el programa de TI\".
Sí, seguro. Le enviara más.
Esta bien. Su nombre es Ted. Ted Yancy.

Cuando el chico que se llama a sí mismo Ted Yancy se muestra en la
Tienda de North Broad St., Katie redacta una factura y le vende
el teléfono celular de un céntimo, tal como ella había pedida al hacer
por su \"trabajador co\". Ella cayó el con anzuelo, line, y sedal.

Cuando es el momento de pagar, el cliente no tiene ningún centavos en su bolsillo, de tan él
alcanza en el plato pequeño de peniques al mostrador del cajero, toma uno, y
le da a la niña en el registro. Llega el teléfono sin pagar siquiera una
ciento para ella.

A continuación, es libre para ir a otra empresa inalámbrica que utiliza el mismo modelo de
teléfono y seleccionar cualquier plan de servicio que le gusta. Preferiblemente uno en un mes a mes
base, sin ningún compromiso requerido.

Analizando el timo
Su natural para las personas a tener un mayor grado de aceptación para cualquier persona que
pretende ser un empleado de sus compañero, y quien sabe procedimientos de la empresa, d lingo.
El ingeniero social en esta historia aprovechó por encontrar los detalles
de una promoción, identificándose como una empresa
empleado y pidiendo un favor de otra sucursal. Esto sucede
entre ramas de tiendas y servicios en una empresa, la gente
están físicamente separados y lidiar con compañeros de trabajo tienen realmente nunca
conoció el día y día.

PIRATERÍA EN LA FEDS
Personas a menudo no se detenga a pensar acerca de qué materiales está haciendo su organización
disponible en la Web. Para mi show semanal sobre KFI Talk Radio 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 de la delincuencia. Más tarde se encontró co el manual NCIC real sí en línea, un documento confidencial que da todos los instrucciones para recuperar la información de base de datos nacional de crimen del FBI.

El manual es un manual para los organismos encargados de hacer cumplir la ley que da el formato y códigos para recuperar información sobre delincuentes y delitos de la nacional base de datos. Pueden buscar en la misma base de datos para agencias de todo el país 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 diferentes tipos de Tatuajes, para cascos de barcos diferentes, a denominaciones de dinero robado y bonos.

Cualquier persona con acceso al manual puede buscar la sintaxis y los comandos para extraer información de la base de datos nacional. A continuación, siguiendo las instrucciones de la Guía de procedimientos, con un poco nerviosas, nadie puede extraer información de la base de datos. El manual también ofrece números de teléfono para pedir apoyo en utilizando el sistema. Puede haber manuales similares en su empresa ofrece códigos de producto o códigos para recuperar información confidencial.

El FBI casi ciertamente nunca ha descubierto que su manual confidencial y instrucciones de procedimiento están disponibles para cualquier persona en línea, y no creo que sean muy contentos si sabían. Una copia fue publicada por un Gobierno Departamento en Oregón, el otro por una agencia policial en Texas. ¿Por qué? En cada caso, alguien probablemente consideraba la información sin valor y registrarlo, no podía hacer ningún daño. Tal vez alguien publicado en su intranet sólo como una conveniencia a sus propios empleados, nunca darse cuenta de que se hizo la información disponible para todos en Internet que tiene acceso a una buena búsqueda motor como Google - incluyendo el justo-llanura-curioso, la CP wannabe, el hacker y el jefe de la delincuencia organizada.

Aprovechando el sistema

El principio de utilizar esa información para engañar a alguien en el Gobierno o una configuración de negocios es la misma: porque un ingeniero social sabe cómo tener acceso a bases de datos específicas o aplicaciones, o sabe los nombres de equipo de la empresa servidores o similares, gana credibilidad. Credibilidad lleva a confiar. Una vez social Ingeniero tiene esos códigos, obtener la información que necesita es un proceso fácil. En este ejemplo, puede comenzar por llamar a un empleado en un local Oficina de teletipo de policía del Estado y una pregunta acerca de uno de los códigos en la manual - por ejemplo, el código de la ofensa. Podría decir algo como, \"cuando lo hago una investigación OFF en el NCIC, estoy recibiendo un \"sistema está inactivo ' error. ¿Eres ¿obtener lo mismo cuando haces un OFF? ¿Usted probarlo para mí?\" O tal vez diría que estaba tratando de buscar una wpf - policía habla de una persona buscada archivo.

El empleado de teletipo en el otro extremo del teléfono sería recoger el taco
que el llamador estaba familiarizado con los procedimientos operativos y los comandos para
consulta la base de datos NCIC. Quien mas que alguien capacitado en utilizando NCIC
¿Quisiera saber estos procedimientos?

Después de que el empleado ha confirmado que su sistema está funcionando muy bien, la conversación
puede pasar algo como esto:
There was an error deserializing the object of type System.String. Encountered unexpected character
Necesito hacer un comando OFF Reardon, Martin. DOB 10118\/66.
There was an error deserializing the object of type System.String. Encountered unexpected character '('.
número de seguridad social como la sosh.)
700-14-7435.
Después de mirar para el anuncio, ella podría volver con algo parecido,
Tiene un 2602.
El atacante sólo tendría que mirar el NCIC en línea para buscar el significado de
el número: el hombre tiene un caso de estafa en su registro.

Analizando el timo
Un ingeniero social logrado no parar durante un minuto para reflexionar sobre maneras de
irrumpir en la base de datos NCIC. ¿Por qué debería él, cuando una simple llamada a su local
la policía de departamento y algunos hablar suave así suena convincente como una
¿información privilegiada, es todo lo que se tarda en obtener la información que quiere? Y la próxima ve
llama a una agencia de policía diferente y utiliza el mismo pretexto.

JERGA
SOSH: Argot de aplicación de ley para un número de seguridad social

Usted podría preguntarse, no es riesgoso para llamar a un departamento de policía de la estación del algu
¿una Oficina de la patrulla de carreteras? ¿No el atacante corre un gran riesgo?

La respuesta es no... y por una razón específica. Como la gente en hacer cumplir ley-miento,
las personas en las fuerzas armadas, han arraigado en ellos desde el primer día en la Academia un
respeto de rango. Como el ingeniero social está haciéndose pasar por un sargento o
Teniente--un rango superior de la persona está hablando - será la víctima
regirá esa lección well-learned que dice que no cuestionar las personas
en una posición de autoridad sobre usted. Rango, en otras palabras, tiene sus privilegios, en
particular el privilegio de no ser desmentidos por personas de rango inferior.

Pero no creo que la aplicación de la ley y los militares son los únicos lugares donde esto
el respeto de rango puede ser aprovechada por el ingeniero social. A menudo los ingenieros sociales
utilizar la autoridad o rango en la jerarquía corporativa como un arma en sus ataques contra
las empresas - como un número de las historias de estas páginas demuestran.

PREVENIR LA CON

¿Cuáles son algunos pasos que su organización puede tomar para reducir la probabilidad de que los ingenieros sociales aprovechará para confiar en el instinto natural de sus empleados ¿las personas? Aquí tiene algunas sugerencias.

Proteger a sus clientes

En esta era electrónica, muchas empresas que venden al consumidor mantén las tarjetas de crédito en el archivo. Hay razones para ello: el cliente ahorra la molestia de tener que proporcionar la información de tarjeta de crédito cada vez que visita la tienda o el sitio Web para realizar una compra. Sin embargo, la práctica debe ser desalentada.

Si debe mantener los números de tarjeta de crédito en archivo, ese proceso debe ser acompañado por las disposiciones de seguridad que van más allá de cifrado o mediante el acceso control. Los empleados necesitan estar capacitados para reconocer estafas de ingeniería social como los que en este capítulo. Ese empleado de compañero que nunca has conocido en persona pero no puede ser que se ha convertido en un amigo de Telefónica que pretende ser. Él no se puede tener la \"necesidad de conocer\" información confidencial de clientes de acceso, porque él no realmente funcionen para la empresa en absoluto.

MENSAJE DE MITNICK

Todos deben ser conscientes del modus operandi del ingeniero social: reunir como mucha información sobre el destino de lo posible y utilizar esa información para obtener confianza como un insider. A continuación, ir a la yugular!

Confianza sabiamente

No es sólo las personas que tienen acceso a información confidencial claramente - el ingenieros de software, la gente en r
defensivo contra las intrusiones. Casi todos los miembros de su organización necesitan capacitación para proteger a la empresa de espías industriales y ladrones de información.

Sentando las bases para ello debe comenzar con un estudio de toda la empresa los activos de información, mirando por separado cada sensible, crítica, o valioso, y preguntando qué métodos un atacante podría utilizar para comprometer los activos mediante el uso de tácticas de ingeniería social. Caso de capacitación para las personas que han confiado en el acceso a dicha información debe diseñarse alrededor de las respuestas a estas preguntas.

Cuando alguien que no conozco personalmente pide alguna información o material, o le pide que realice alguna tarea en el equipo, tiene sus empleados preguntar sí algunos. preguntas. Si dio esta información a mi peor enemigo, podría ¿se utiliza para herir a mí o a mi empresa? Entender completamente el potencial ¿efecto de los comandos que me pide para entrar en mi ordenador?

No queremos ir por la vida siendo sospechoso de cada nueva persona encuentro. Aún más confianza estamos, más probable que la próxima social Ingeniero en llegar a la ciudad será capaz de engañarnos en renunciar a nuestra empresa información propietaria.

¿Lo que pertenece en la Intranet?
Partes de la intranet pueden estar abiertas al mundo exterior, otras partes restricción a empleados. Cuidado de cómo está su empresa en la toma de información seguro ¿no está publicado sea accesible al público pretende protegerlo de? Cuando es la última vez que alguien en su organización comprueba para ver si cualquier sensible información sobre la intranet de su empresa sin darse cuenta se hicieron disponible ¿a través de las áreas de acceso público del sitio Web?

Si su empresa ha implementado servidores proxy como intermediarios para proteger la empresa frente a amenazas de seguridad electrónica, han sido esos servidores comprueba ¿recientemente para asegurarse que están configurados correctamente?

¿De hecho, nadie nunca comprobó la seguridad de la intranet?

Capítulo 5
Permítame ayudarle

Estamos todos agradecidos cuando nos estamos plagadas por un problema y alguien con la conocimiento, habilidad y voluntad viene ofreciendo a nosotros echar una mano. El ingeniero social entiende y sabe cómo sacar provecho de ella.

También sabe cómo plantear un problema para usted..., entonces te hacen agradecido cuando él resuelve el problema... y finalmente jugar en su gratitud para extraer algunas información o un pequeño favor de usted que dejará su empresa (o tal vez ustedes, individualmente) mucho peor para el encuentro. Y es no posible que nunca saben que has perdido algo de valor. Aquí hay algunas formas típicas que social paso de ingenieros para \"ayudar\".

LA INTERRUPCIÓN DE LA RED
Día y hora: el lunes, 12 de febrero, 15:25
Lugar: Oficinas de construcción naval de estribor

La primera llamada: Tom Delay
Tom DeLay, teneduría de libros.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
solucionar un problema de red del equipo. ¿Sabes si hay alguien en tu
Grupo ha estado teniendo problemas para mantenerse en línea?\"
UH, no que i know de.
Y no tienes ningún problema usted mismo.
No, parece bien.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
importante nos avisa inmediatamente si pierde la conexión de red.\"
No suena bien. ¿Cree que puede pasar?
¿Esperamos que no, pero llamaremos si, derecho?
Mejor creerlo.
There was an error deserializing the object of type System.String. Unexpected end of file. Following e
problema para usted...\"
Apuesta sería.
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
Usted puede llegarme directamente si es necesario\".
Sería genial. Adelante.
Es 555 867 5309.
555 867 5309. Entiendo. Oye, gracias. ¿Cuál era su nombre de nuevo?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
conectado a. Echa un vistazo en tu equipo y ver si hay una pegatina
en algún lugar dice algo así como \"Número de puerto\".

There was an error deserializing the object of type System.String. Unexpected end of file. Follo
Vale, entonces en el fondo del equipo, puede usted reconocer el cable de red.
Sí.
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
enchufado.\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
cierre lo suficiente como para leerlo. Está bien - dice puerto 6 guión 47.\"
Bueno - es lo que teníamos le abajo como, simplemente haciendo seguro.

La segunda llamada: El chico de TI
Dos días más tarde, una llamada vino a través de operaciones de red de la misma empresa
Centro.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
solucionar un problema de cableado. Te necesito para desactivar el puerto 6 47.\"

El chico de TI dijo que se haría en pocos minutos y para hacerles saber
cuando estaba listo para tenerlo activado.

La llamada tercera: Cómo obtener ayuda del enemigo
Aproximadamente una hora más tarde, el chico que se llama a sí mismo Eddie Martin fue comprando en
Circuit City cuando sonó su teléfono celular. Comprueba el ID del llamador, vio que la llamada fue
de la empresa de construcción naval y se apresuró a un lugar tranquilo antes de contestar.

Help Desk, Eddie.
Ah, bueno, Eddie. Tienes un eco, ¿dónde estás?
There was an error deserializing the object of type System.String. Unexpected end of file. Follow
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
¿me llamó el otro día? Mi conexión de red bajó justo como lo dijiste
podría y estoy un poco de pánico aquí.\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
cuidado de al final del día. Que bien?\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
para mí?\"
Presionado ¿cómo estás?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
en media hora?\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
y ver si puedo abordarlo para usted.
Bueno, realmente aprecio que, Eddie.

La llamada cuarta: Gotcha!
Cuarenta y cinco minutos más tarde...

¿Tom? Es Eddie. Seguir adelante y probar la conexión de red.

Después de un par de momentos:

Ah, bueno, está trabajando. Eso es simplemente genial.
Bueno, contento que pude tener cuidado de para usted.
¡ Sí, muchas gracias.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
algunos programas que oughta ejecutando. Eche un par de minutos\".
Ahora no es el mejor momento.
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
problema pasa\".
Bueno... Si es tan solo unos minutos.
Aquí es lo que haces...

Eddie tomó entonces Tom a través de los pasos de descargar una pequeña aplicación de un Sitio Web. Después había descargado el programa, Eddie dijo Tom al hacer doble clic en . Trató, pero informó:

No está funcionando. No está haciendo nada.
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
de la misma, podemos tratar otra vez.\" Y habló a Tom a través de los pasos de eliminar el programa para que no se pudo recuperar.

Tiempo total transcurrido, doce minutos.

Historia del atacante
Bobby Wallace siempre pensé que era ridículo cuando recogió un buen asignación como éste y su cliente pussyfooted alrededor de la treta, pero pregunta obvia de por qué querían la información. En este caso sólo podía pensar en dos razones. Quizás representaban algún traje que estaba interesado en compra la empresa de destino, Starboard naval y quería saber lo que tipo de forma financiera estaban realmente en - especialmente todas las cosas del destino que desee mantener oculto de un comprador potencial. O tal vez representaban el dinero era de inversores que pensaban que había algo sospechoso acerca de la forma ser manejados y quería averiguar si algunos de los ejecutivos tenían un caso de mano en la cookie-jar.

Y tal vez su cliente también quería decirle que la verdadera razón porque, si Bobby sabía cómo valiosa la información era, probablemente desee más dinero para hacer el trabajo.

Hay muchas maneras de crack en los archivos más secretos de la empresa. Bobby pasó un unos días dándole vueltas las opciones y haciendo un poco comprobar todo antes de que él se decidió por un plan. Se radicó en que pidieron un enfoque especialmente le gustaba, donde el objetivo está configurado para que el atacante le pide ayuda.

Para empezar, Bobby recogió un celular de $39.95 en una tienda de conveniencia. Él realizó una llamada al hombre había elegido como su destino, pasar a sí mismo como desde la empresa Atencin y configurar las cosas para que el hombre llamaría de Bobby teléfono celular cualquier momento encontró un problema con su conexión de red.

Dejó una pausa de dos días para no ser demasiado obvio y luego hizo una llamada a el centro de operaciones de red (NOC) de la empresa. Afirmó que tenía problemas- Tiro un problema para Tom, el destino y pidió tener red de Tom conexión desactivada. Bobby sabía que esto era la parte más complicada del conjunto Escapada - en muchas empresas, la labor de personas de mesa de ayuda estrechamente con el NOC; de hecho, sabía que la mesa de ayuda es a menudo parte de la organización de TI. Pero el indiferente NOC guy habló con consideran a la llamada de rutina, no pedí la nombre de la persona de mesa de ayuda que supuestamente estaba trabajando en la creación de redes problema y acordados para desactivar el puerto de red de destino. Cuando haya terminado, Tom sería totalmente aislados de la intranet de la empresa, no se puede recuperar archivos desde el servidor de archivos de intercambio con sus compañeros, Descargar su correo electrónico, o incluso envi página de datos a la impresora. En el mundo de hoy, es como vivir en una cueva.

Como Bobby se esperaba, no mucho antes de su teléfono celular sonó. Por supuesto que hizo el propio sonido deseosos de ayudar a este pobre \"compañero empleado\" en apuros. Entonces él llamado el NOC y tuvo el hombre de la conexión de red tuvo que volver. Por último, llamó al hombre y lo manipuló nuevamente, esta vez haciéndole sentir culpable por haber dicho que no después Bobby le había hecho un favor. Tom accedió a la solicitud que descargar una pieza de software en su equipo.

Por supuesto, accedió a no exactamente lo que parecía. El software que Tom le dijo que mantendría su conexión de red de bajando, fue realmente un Caballo de Troya, una aplicación de software que hizo para el equipo de Tom lo que la engaño original se hizo para los troyanos: trajo el enemigo dentro del campamento. Tom informó que nada ocurrió cuando él hizo doble clic sobre el icono del software; el hecho fue que, por diseño, él no podía ver nada sucede, aunque la pequeña aplicación fue instalar un programa secreto que permitiría el infiltrado encubierta acceso a equipo de Tom.

Con el software que se ejecuta, Bobby se prestó con control completo sobre Equipo de Tom, un acuerdo conocido como un shell de comandos remotos. Cuando Bobby accede a equipo de Tom, él podría buscar archivos de contabilidad

podría ser de su interés y copiarlos. Luego, en su tiempo libre, él podría examinarlas para la información que daría a sus clientes lo que estaban buscando.

JERGA
CABALLO de Troya: Un programa que contiene código malicioso o dañino, diseñado para dañar el equipo o los archivos de la víctima, u obtener información de la víctima equipo o red. Algunos troyanos están diseñados para ocultar dentro de la computadora sistema operativo y espía en cada pulsación de tecla o acción, o aceptar instrucciones sobre una conexión de red para realizar alguna función, todo esto sin la víctima siendo consciente de su presencia.

Y no era todo. Podría volver en cualquier momento para buscar a través del correo electrónico mensajes y notas privadas de ejecutivos de la compañía, un texto de búsqueda palabras podría revelar cualquier cositas interesantes de información.

Tarde en la noche que estafó a su destino en instalar el caballo de Troya software, Bobby lanzó el teléfono móvil en un contenedor de basura. Por supuesto tuvo cuidado para borrar la memoria primero y extraiga la batería antes de él, arrojó el último lo que quería era alguien que llame al número del teléfono celular por error y tiene el timbre de inicio de teléfono!

Analizando el timo
El atacante gira una web para convencer el destino que tiene un problema que, de hecho, realmente no existe - o, como en este caso, un problema que no ha sucedido aún, pero que el atacante sabe sucederá porque él va a causar. Él entonces se presenta a sí mismo como la persona ¿Quién puede proporcionarla solución.

La instalación de este tipo de ataque es particularmente jugosa para el atacante:
Debido a la semilla plantada por adelantado, cuando el destino descubre que tiene un problema, él mismo hace la llamada telefónica para pedir ayuda. El atacante sólo se sienta y espera a que el teléfono suena, una táctica conocida cariñosamente en el mercado como ingeniería social inversa. Un atacante puede hacer que el destino le llaman Gana credibilidad instantánea: si hacer una llamada a alguien creo que está en la mesa de ayuda, No voy a empezar pidiéndole que probar su identidad. Es entonces cuando el atacante ha hecho.

JERGA
SHELL de comando remoto: Una interfaz no gráfica que acepta texto base de comandos para realizar ciertas funciones o ejecutar programas. Un atacante que aprovecha las vulnerabilidades técnicas o es capaz de instalar un programa caballo de Troya en el equipo de víctimas puede ser capaz de obtener acceso remoto a un shell de comandos

Ingeniería SOCIAL inversa: Un ataque de ingeniería social en la que la atacante configura una situación donde la víctima encuentra con un problema y contactos el atacante para obtener ayuda. Otra forma de ingeniería social inversa convierte las tablas sobre el atacante. El destino reconoce el ataque y utiliza psicológico principios de influencia para extraer tanta información como sea posible de la atacante que puede salvaguardar el negocio había concentrado en activos.

MENSAJE DE MITNICK

Si un extraño no es un favor, y le pide un favor, no corresponder sin pensar cuidadosamente sobre lo que él está pidiendo.

En una estafa como esta, intenta elegir un destino que es probable que el ingeniero social tienen un limitado conocimiento de computadoras. Cuanto más sabe, más probable que él obtendrá sospechoso o figura simplemente fuera que él está siendo manipulada. Lo que me llaman a veces el trabajador desafiado por el equipo, que tiene menos conocimiento sobre tecnología y procedimientos, es más probable que cumplir. Él es más probable que caen de una artimaña como \"Sólo Descargar este pequeño programa,\" porque él no tiene ni idea de los posibles daños que puede infligir un programa de software. Además, hay una posibilidad mucho más pequeña a comprender el valor de la información sobre la red de informática que está poniendo en riesgo.

UN POCO DE AYUDA PARA LA NUEVA GAL

Nuevos empleados son un destino maduro para los atacantes. Sin embargo, no saben muchas personas no saben los procedimientos o el correcto e incorrecto de la empresa. Y, en el nombre de hacer una buena primera impresión, están ansiosos por mostrar cómo cooperativa y rápida respuesta pueden ser.

Andrea útil
Recursos humanos, Andrea Calhoun.
Andrea, Hola, esto es Alex, con la seguridad de la empresa.
¿Sí?
¿Cómo estás haciendo hoy?
Esta bien. ¿Qué le puedo ayudar?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
a algunas personas a probarlo la ronda. Quiero obtener el nombre y número de teléfono
de las nuevas contrataciones el mes pasado. Me puedes ayudar con eso?\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following
¿Cuál es su extensión?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
cuando estoy en mi Oficina, probablemente después de cuatro\".

Cuando Alex llama acerca de 4:30, Andrea tenía la lista listo y le lee los nombres y extensiones.

Un mensaje para Romero

Rosemary Morgan estaba encantada con su nuevo trabajo. Nunca había trabajado para una revista antes y fue encontrar a la gente mucho más amigable que ella esperaba, un sorpresa debido a la incesante presión de la mayoría del personal fue siempre bajo para obtener otro tema terminado antes del plazo mensual. La llamada que recibió un jueves por la mañana volvió a confirmar esa impresión de amabilidad.

¿Es Rosemary Morgan?

Sí.

Hola, Romero. Bill Jorday, esto es con el grupo de seguridad de la información.

¿Sí?

¿Nadie de nuestro Departamento ha examinado las mejores prácticas de seguridad con usted?

No creo.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el

en desde fuera de la empresa. Eso es porque no queremos ninguna responsabilidad para uso sin licencia del software. Y para evitar cualquier problema con el software que podría tiene un virus o un gusano\".

Esta bien.

¿Son conscientes de nuestras políticas de correo electrónico?

Lol

There was an error deserializing the object of type System.String. Encountered unexpected character '\

¿Iniciar sesión bajo el nombre de usuario Rosemary?

No, es subrayado R Morgan.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el

abrir cualquier archivo adjunto de correo electrónico que no está esperando. Obtener lotes de virus y gusa

Enviado alrededor y vienen en los correos electrónicos que parecen ser de gente que conoces. Así que si usted recibe un correo electrónico con un archivo adjunto que no estaban esperando que debe siempre

Compruebe que la persona que aparece como remitente realmente le ha enviado el mensaje. Le comprender?\"

Sí, he escuchado acerca de eso.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el

Cuándo última cambias tu contraseña?\"

Sólo he estado aquí tres semanas; Sigo usando el uno que primero establecer.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el

seguro que las personas están utilizando contraseñas que no son demasiado fáciles de adivinar. ¿Está util

contraseña que esté formada por letras y números?\"

No.

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

Es nombre de mi hija - Annette.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el

basado en información familiar. Bueno, vamos a ver..., que podría hacer lo mismo que hago.

Está bien utilizar lo que está utilizando ahora como la primera parte de la contraseña, pero luego cada vez que se modifique, agregue un número para el mes actual.\"
Así que si hice eso ahora, para marzo, se utilizan tres, o AH-tres.
Depende de usted. ¿Que estaría más cómodo con?
Supongo que Annette-tres.
Bellas. ¿Desea que le muestre cómo hacer el cambio?
No, yo sé cómo.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
en el equipo y es importantes mantenerlo actualizado. Usted no debe nunca desactivar la actualización automática, incluso si el equipo se ralentiza cada vez en un al mismo tiempo. Okay?\"
Seguro.
There was an error deserializing the object of type System.String. Unexpected end of file. Following
por lo tanto puede llamarnos si tienes problemas al equipo?\"
Ella no. Le dio el número, ella escribió cuidadosamente y se volvió para trabajar, una vez más, se complace en lo bien cuidado de ella sentía.

Analizando el timo

Esta historia refuerza un tema subyacente que encontrará a lo largo de este libro: la información más común que un ingeniero social quiere de un empleado, independientemente de su objetivo final, es las credenciales de autenticación del destino. Con un nombre y contraseña de cuenta en la mano de un único empleado en el área derecha del la compañía, el atacante tiene lo que necesita acceder al interior y encontrar lo que información que es después. Esta información es como encontrar las claves de la Reino; con ellos en la mano, puede moverse libremente alrededor del paisaje corporativo y encontrar el tesoro que se busca.

MENSAJE DE MITNICK

Antes de que nuevos empleados pueden acceder a los sistemas informáticos de empresa, deben ser entrenados para seguir buenas prácticas de seguridad, especialmente las políticas sobre Nunca revele sus contraseñas.

NO SEGURO COMO CREES

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
sólo llanura negligente.\" 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 protegen confidencial información puede estar en grave peligro.

Aquí es una historia que ilustra una vez más cómo las empresas engañar a sí mismos cada día en pensando en sus prácticas de seguridad, diseñados por experimentados, competentes, profesionales, no puede eludirse.

Historia de Steve Cramer

No fue un gran césped, no uno de esos pliegos costosa clasificados. Obtuvo no envidia. Y sin duda no era lo suficientemente grande como para darle una excusa para comprar un sit-abajo mower, que estaba bien, porque él no habría utilizado uno de todas formas. Steve disfrutó de cortar el césped con un cortacéspedes de mano porque tomó más tiempo y la quehacer proporciona una conveniente excusa para centrarse en sus propios pensamientos en lugar de escuchando a Anna contándole historias de la gente en el banco donde ella trabajado o explicando recados para él. Las odiaba listas de miel-do que se había convertido en parte integrante de su fin de semana. Aunque brilló su mente que 12 - Pete años era joder listo para unirse al equipo de natación. Ahora tendría que estar en práctica o un encuentro cada sábado por lo que no quedas atascado con las tareas del sábado.

Algunas personas podrían pensar trabajo de Steve diseñar nuevos dispositivos para GeminiMed Productos médicos fue aburrido; Steve sabía que él era salvar vidas. Steve pensó a sí mismo como estar en una línea creativa del trabajo. Artista, compositor, ingeniero - en Vista de Steve corren el mismo tipo de desafío que hizo: crearon algo que nadie había hecho antes. Y su más reciente, un Intrigantemente inteligente nuevo tipo de stent de corazón, sería su logro enorgullezco aún.

Era casi de 11:30 este sábado particular y Steve estaba molesto porque había casi terminó cortando el césped y no había hecho ningún progreso real en averiguar cómo reducir el requerimiento de energía en el corazón de stent, el último hurdle restante. Un problema perfecto a mull sobre siega, pero ninguna solución había llegado.

Anna apareció en la puerta, sus cabellos cubiertos en el pañuelo rojo vaquero paisley ella siempre llevaba al polvo. \"Llamada telefónica\", gritó a él. \"Alguien de trabajo.\"

There was an error deserializing the object of type System.String. Encountered unexpected chara

Ralph algo. Creo.

¿Ralph? Steve no podía recordar a nadie en GeminiMed llamado Ralph quien podría llamar a un fin de semana. Pero Anna probablemente tenía el nombre equivocado.

There was an error deserializing the object of type System.String. Encountered unexpected character 'R'.

Anna obtener desde un nombre hispano a Ralph, preguntaba Steve.

There was an error deserializing the object of type System.String. Encountered unexpected character 'T'.

Pensamos que tal vez un gusano, y tenemos que limpiar las unidades y restaurar de copia de seguridad. Deberíamos poder tener funcionando por los archivos El miércoles o Jueves. Si tenemos suerte.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
encima. ¿Cómo podrían estas personas ser tan estúpido? Realmente piensan que pudo
¿administrar sin acceso a sus archivos de fin de semana todos y la mayor parte de la próxima semana? \
Voy a sentarse en mi casa terminal en sólo dos horas y voy a necesitar
acceso a Mis archivos. Yo hago esto claro?\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Dio hasta mi fin de semana para venir y trabajar en ello y no es divertido tener
todo el mundo hablo para obtener cabreado me.\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
hecho esta tarde. ¿Qué parte de esto ¿no entiendes?\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'R'.
¿Qué decimos que tendrás tus archivos por el martes?
There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
iba a llamar si él no podía conseguir su punto a través del cráneo grueso de este chico.
There was an error deserializing the object of type System.String. Encountered unexpected character 'R'.
molestia. \"Déjame ver qué puedo hacer para que pueda ir. Utilice la RM22
servidor correcto?\"
RM22 y el GM16. Ambos.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
y la contraseña.\"
UH AH, Steve pensó. ¿Lo que está sucediendo aquí? ¿Por qué él necesitaría mi contraseña?
¿Por qué pediría de todas las personas, pues?
There was an error deserializing the object of type System.String. Encountered unexpected character '\'".
Perez. Mira, te digo lo que, cuando fueron contratados, hubo una forma que tenías que
Llene los datos para obtener su cuenta de usuario, y tenías que poner una contraseña. He podido
Buscar y mostrar que tenemos en archivo aquí. Okay?\"
Steve ver que durante unos instantes, luego acordado. Colgó con creciente
impaciencia mientras que Ramón fue para recuperar documentos de un archivador. Finalmente
en el teléfono, Steve podía oírle arrastrándose a través de una pila de documentos.
There was an error deserializing the object of type System.String. Encountered unexpected character 'R'.
Steve pensó. Es el nombre de su madre, y de hecho a veces había utilizado como
una contraseña. Él podría muy bien han presentado su contraseña al rellenar
con sus papeles de nuevo empleado.
There was an error deserializing the object of type System.String. Encountered unexpected characte
There was an error deserializing the object of type System.String. Unexpected end of file. Following
el acceso directo y obtener copia de sus archivos con prisa, te re vas a tener a Ayuda me
aquí.\"
Mi ID es s, d, subrayado, cramer--c-r-a-m-e-r. La contraseña es 'pelícano 1.'
There was an error deserializing the object of type System.String. Encountered unexpected character 'R'.
horas.\"
Steve terminó el césped, almorzó y por el tiempo que obtuvo su equipo encontró
que de hecho habían restauradas sus archivos. Complacido consigo mismo para manejo

que tio tan enérgicamente, y espera Anna había oído cómo asertiva
él fue. Sería bueno darle el chico o su jefe un attaboy, pero él sabía que
fue una de esas cosas que él nunca conseguiría a hacerlo.

Historia de Craig Cogburne

Craig Cogburne había sido un vendedor de una empresa de alta tecnología y hecho bien en
. Después de un tiempo comenzó a darse cuenta de que tenía una habilidad para la lectura de un cliente,
comprender que la persona era resistente y reconociendo
algunos debilidad o vulnerabilidad que hizo fácil cerrar la venta. Comenzó a
pensar en otras formas de usar este talento, y la ruta eventualmente lo llevó a una
campo mucho más lucrativo: espionaje corporativo.

Esta fue una asignación de caliente. No buscar que me lleve mucho tiempo y vale la pena
suficiente para pagar un viaje a Hawaii. O tal vez Tahití.

El chico que me contrató, él no me diga al cliente, por supuesto, pero lo imaginé que
algunas empresa que quería ponerse al día con la competencia en un rápido, grande,
salto fácil. Todo lo tengo que hacer es conseguir los diseños y productos Especificaciones para un nuevo
Gadget llamado un stent de corazón, independientemente que fue. La empresa se llamaba
GeminiMed. Nunca oído hablar de ella, pero fue un traje de Fortune 500 con oficinas en la mitad
una docena de lugares - que hace el trabajo más fácil que una pequeña empresa donde
hay una oportunidad justa del chico que está hablando sabe al tio está reclamando ser
y sabe que no eres él. Esto, como pilotos dicen acerca de una colisión en el aire, puede arruinar
todo el día.

Mi cliente me envió un fax, un poco de revista de algún médico que dice GeminiMed
estaba trabajando en un stent con un radical nuevo diseño y serían llamados el algo -
IO0. For crying out loud, algún reportero ya ha hecho un buen pedazo de la
Misión para mí. Tuve una cosa necesitaba incluso antes de que me empecé a, el nuevo
nombre del producto.

Primer problema: obtener los nombres de las personas en la empresa que trabajaba en el algo-100
o que necesite ver los diseños. Por lo que he llamado al operador de panel de control y dijo, \"me
prometió una de las personas en su grupo de ingeniería que sería ponerse en contacto con él
y no recuerdo su apellido, pero su nombre comenzó con una S.\" Y ella
dijo: \"tenemos un arquero Scott y un Sam Davidson\". Tomé un tiro largo. \"Que
uno trabaja en el grupo de STH100?\" Ella no sabía, así que elegí sólo Scott Archer
al azar, y ella sonó su teléfono.

Cuando contestó, dije, \"bueno, esto es Mike, en la sala de correo. Tenemos un FedEx aquí que es para el equipo del proyecto corazón algo Stent-100. Cualquier idea que ¿debe ir a\"? Me dio el nombre del líder del proyecto, Jerry Mendel. Yo incluso lo llevó a buscar el número de teléfono para mí.

Llamé. Mendel no estaba allí, pero su mensaje de correo de voz dijo que estaría de vacaciones hasta el siglo XIII, lo que significaba que tenía otra semana para esquiar o lo que sea, y cualquiera que necesita algo entretanto debe llamar a Michelle en 9137. Muy útil, estas personas. Muy útil.

Colgó y llamada a Michelle, le recibió en el teléfono y dijo, \"este es Bill Thomas. Jerry me dijo que debo llamarle cuando tuve el preparado especificaciones que él quería que los chicos en su equipo para revisar. Trabaja en el corazón stent, derecho?\" Dijo que eran.

Ahora estábamos tratando la parte sudorosa de la estafa. Si comenzó a sonar sospechosa, estaba listo para jugar la Carta sobre cómo sólo intentaba hacer un favor que Jerry me había pedido. Dije, \"sistema que estás en?\"
¿El sistema?
¿Qué servidores de computadora utiliza su grupo?
There was an error deserializing the object of type System.String. Encountered unexpected character 's'.
y fue una pieza de información que pude obtener de ella sin hacerla sospechosas. Que le suavizado para el siguiente bit, hecho tan casualmente como pude administrar. \"Jerry dijo que podría darme una lista de direcciones de correo electrónico para las personas equipo de desarrollo,\"dijo y había celebrado mi aliento.
Seguro. ¿La lista de distribución es demasiado larga para leer, puedo yo lo le por correo electrónico?

Perdón. Sería cualquier dirección de correo electrónico que no terminaron en GeminiMed.com una enorme bandera roja. \"¿Qué fax a mí?\" He dicho.
No tenía ningún problema con ello.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el usted en un bit,\"dijo y colgó.

Ahora, podría pensar estaba saddled con un pegajoso problema aquí, pero es sólo otro truco de rutina del comercio. Esperé un rato para que mi voz no suena familiar a la recepcionista, y luego la llamó y dijo: \"Hola, es Bill Thomas, nuestro fax máquina no funciona aquí, puedo tener un fax enviado al equipo?\" Dijo seguro y me dio el número.

¿Luego simplemente caminar en y recoger el fax, correcto? Por supuesto que no. Primera regla: nunca visita los locales a menos que usted debe absolutamente. Tienen un tiempo duro te identificar si eres sólo una voz en el teléfono. Y si no se identifican

usted, ellos no pueden detener le. Es difícil poner esposas alrededor de una voz. Así que llamé a ¿la recepcionista después de un rato y le preguntó, llegó mi fax? \"Sí\", ella dijo.

There was an error deserializing the object of type System.String. End element 'root' from namespace " e enviarla para mí?\" Estuvo de acuerdo. Y por qué no--¿cómo podría cualquier recepcionista ¿espera reconocer datos confidenciales? Mientras ella envió el fax a la
There was an error deserializing the object of type System.String. End element 'root' from namespace " e
me uno con el signo por delante \"Faxes enviados\/Rcvd.\" Se suponía que mi fax llegar antes de que lo hice, y como se esperaba, estaba allí esperándome cuando caminaba en. Seis páginas en $1.75. Para un proyecto de ley de $10 y cambio, tuve toda la lista del grupo de nombres y direcciones de correo electrónico.

Obtener dentro de
Está bien, así que tuve por ahora habló con tres o cuatro personas diferentes en sólo unas horas y ya era un gigante paso a obtener dentro de equipos de la empresa.
Pero necesitaría un par más piezas antes de se casa.

Número uno fue el número de teléfono para marcar en el servidor de ingeniería desde fuera. Llamé a GeminiMed otra vez y pidieron que el operador de panel de control Departamento y pidió que el chico que contestó a alguien que pudiera darme alguna ayuda de equipo. Me pasó, y pongo en un acto de confusión y tipo de estúpida sobre todo técnica. \"Estoy en casa, sólo compré un nuevo portátil ya que deba configurarlo o puedo llamar desde fuera. \"

El procedimiento era obvio pero pacientemente le dejo me habla a través de él hasta que consiguió al número de teléfono de acceso telefónico. Me dio el número como si fuera simplemente otro rutina pieza de información. Entonces le hice esperar mientras lo probé. Perfecto.

Así que ya me había pasado el obstáculo de la conexión a la red. Marcado en y encontrados que fueron configurados con un servidor de terminal server que dejaría un llamador conectar cualquier equipo de su red interna. Después de un montón de intentos me tropecé del alguien equipo que tenía una cuenta de invitado con no se requiere contraseña. Algunos sistemas operativos, cuando instaló por primera vez, dirigir al usuario a configurar un ID y contraseña, pero también proporcionar una cuenta de invitado. El usuario se supone para establecer su propia contraseña para la cuenta de invitado o desactivarlo, pero la mayoría de la gente no sabe sobre esto, o simplemente no se moleste. Probablemente sólo fue establecido este sistema y el propietario no hubiera molestado a deshabilitar la cuenta invitado.

JERGA
PASSWOPRD HASH: Una cadena de galimatías que resulta del procesamiento de una contraseña a través de un proceso de cifrado unidireccional. El proceso es supuestamente

irreversible; es decir, su considera que no es posible reconstruir la contraseña desde el hash

Gracias a la cuenta de invitado, ahora tuve acceso a una computadora, que resultó que se esté ejecutando una versión anterior del sistema operativo UNIX. En UNIX, el sistema operativo mantiene un archivo de contraseña que el cifrado de con lluvias contraseñas de todo el mundo autorizado a acceder a ese equipo. El archivo de contraseñas contiene el hash unidireccional (es decir, una forma de cifrado que es irreversible) de contraseña de cada usuario. Con un sentido único hash una contraseña actual como, digamos, There was an error deserializing the object of type System.String. Encountered unexpected character 'w'. UNIX podría convertir a trece caracteres alfanuméricos.

Cuando Billy Bob abajo el Salón quiere transferir archivos a un equipo, él ha necesario para identificarse proporcionando un nombre de usuario y una contraseña. El sistema programa que\"comprueba su autorización cifra la contraseña entra y luego compara el resultado con la contraseña cifrada (hash) contenido en el archivo de contraseñas; Si los dos coinciden, ha dado acceso.

Porque las contraseñas en el archivo estaban cifradas, hizo el propio archivo disponible para cualquier usuario sobre la teoría de que no hay ninguna manera conocida para descifrar la contraseñas. Que es una carcajada - he descargado el archivo, tuvo un ataque de diccionario sobre ella (consulte el capítulo 12 para obtener más información acerca de este método) y encontró que uno de los el equipo de desarrollo, de un chico llamado Steven Cramer, tiene actualmente una cuenta en el equipo con la contraseña \"Janice.\" Sólo en la oportunidad, traté de entrar su cuenta con esa contraseña en uno de los servidores de desarrollo; Si tuviera trabajó, se habría guardado me algún tiempo y un poco riesgo. No lo hizo.

Eso significaba que tendría que engañar al tio me dice su nombre de usuario y contraseña. Por eso, yo esperaría hasta el fin de semana. 70 Ya sabes el resto. El sábado me llamado Cramer y le cruzaron una artimaña sobre un gusano y los servidores tener que restaurar desde la copia de seguridad para superar sus sospechas.

¿Qué pasa con la historia, le dije, uno sobre anuncio una contraseña cuando llenó ¿con sus papeles de empleado? Estaba contando sobre él no recordar que nunca había sucedió. Un nuevo empleado rellena así muchas formas que, años más tarde, que ¿recuerda? Y de todos modos, si había ponchó con él, todavía tenía esa larga lista de otros nombres.

Con su nombre de usuario y contraseña, me metí en el servidor, pescan alrededor de un pequeño mientras y, a continuación, encuentra los archivos de diseño para algo-100. No estaba exactamente seguro cuáles eran la clave, por lo que simplemente transferir todos los archivos a un descenso muerto, un FTP gr sitio en China, donde podría almacenarse sin nadie recibiendo sospechosas. Permiten el cliente ordene a través de la basura y encontrar lo que quiere.

JERGA
DROP DEAD un lugar para dejar información donde es improbable que se encuentran por otros. En el mundo de los espías tradicionales, esto puede estar detrás de una piedra suelta en una pared; en el mundo de los hackers de computadora, es comúnmente un sitio de Internet un país remoto.

Analizando el timo
Para el hombre que estamos llamando Craig Cogburne, o alguien como él igualmente cualificados en las Artes larcenous-pero-no-siempre-ilegal de la ingeniería social, el desafío presentado aquí fue casi de rutina. Su objetivo era buscar y descargar archivos almacenados en un equipo corporativo seguro, protegido por un cortafuegos y todos los habituales tecnologías de seguridad.

La mayor parte de su obra fue tan fácil como la captura de agua de lluvia en un barril. Comenzó haciéndose pasar por alguien de la sala de correo y proporciona una mayor sensación de urgencia diciendo que era un paquete de FedEx a la espera de ser entregado. Esto engaño producido el nombre del líder del equipo de la ingeniería de corazón-stent Grupo, que estaba de vacaciones, pero - conveniente para cualquier ingeniero social tratando de robar información - servicialmente había abandonado el nombre y número de teléfono de su Asistente. Llamándola, Craig desactivadas las sospechas diciendo que estaba respondiendo a una solicitud del líder del equipo. Con el líder del equipo fuera de la ciudad, Michelle no tenía ninguna forma de comprobar su afirmación. Ella aceptó como la verdad y no tenía problema proporcionando una lista de personas en el grupo - por Craig, necesaria y altamente apreciado conjunto de información.

Ella incluso no llegar sospechosa cuando Craig quería la lista enviada por fax en lugar de por correo electrónico, normalmente es más conveniente en ambos extremos. ¿Por qué fue ella tan crédul Como muchos empleados, quería que su jefe para volver al pueblo y encontrar tuvo obstruida un llamador que estaba intentando hacer algo que el jefe le había pedido para. Además, el llamador dijo que el jefe no sólo autorizó la petición, pero pidieron su ayuda. Una vez más, aquí es un ejemplo de alguien mostrando la fuerte deseo de ser un jugador de equipo, que hace que las personas más susceptibles a engaño.

Craig evita el riesgo de entrar físicamente en el edificio simplemente por tener la Fax enviado a la recepcionista, sabiendo que es probable que sea útil. Recepcionistas Después de todo, son, generalmente elegidos por su personalidad encantadora y su capacidad de hacer una buena impresión. Hacer pequeños favores como recibir un fax y enviarlo por viene con el territorio de la recepcionista, un hecho que Craig fue capaz de tomar ventaja de. Lo que ella estaba terminando que pasó a ser la información que podría han planteado alarmas con nadie conoce el valor de la información - pero ¿Cómo podría la recepcionista espera saber qué información es benigna y ¿que tengan en cuenta?

Con un estilo diferente de manipulación, Craig actuaba confundido y ingenuo convencer el tio en operaciones de equipo para proporcionarle el acceso telefónico número en servidor terminal de la empresa, el hardware utilizado como una conexión apuntan a otros sistemas informáticos dentro de la red interna.

MENSAJE DE MITNICK

La primera prioridad en el trabajo es realizar el trabajo. Bajo esa presión, prácticas de seguridad a menudo segundo lugar y son pasados por alto o ignoradas. Social los ingenieros confían en esto cuando practicar su oficio.

Craig fue capaz de conectar fácilmente probando una contraseña predeterminada que nunca había sido cambiado, una de las brechas abiertas, evidentes que existen a lo largo de muchos internos redes que confían en la seguridad del cortafuegos. De hecho, las contraseñas predeterminadas para mucho sistemas operativos, enrutadores y otros tipos de productos, incluyendo PBX, son disposición en línea. Cualquier ingeniero social, hacker o espionaje industrial, así como la llanura simplemente curiosa, puede encontrar la lista en http:\/\/www.phenoelit.de\/dpl\/dpl.html. (Es absolutamente increíble cómo fácil el Internet hace que la vida para quien sepa Dónde buscar. Y ya sabes, también.)

Cogburne realmente consiguió convencer un cauteloso, sospechoso hombre (\"¿Qué dijo que era su apellido? ¿Quién es su supervisor?\") divulgar su nombre de usuario y contraseña para que él pudiera acceder a los servidores utilizados por el equipo de desarrollo. Esto fue como dejar Craig con una puerta abierta para examinar la la mayor parte de la empresa estrechamente vigilado secretos y descarga los planes para el nuevo producto.

¿Qué sucede si Steve Cramer había seguido a sospechar sobre convocatoria de Craig? Era poco probable que él haría cualquier cosa acerca de los informes de sus sospechas hasta que mostró en el trabajo el lunes por la mañana, que habría sido demasiado tarde Para prevenir el ataque.

Una de las claves para la última parte de la estratagema: Craig al principio hizo sonido displicente y desinteresados en preocupaciones de Steve, entonces ha cambiado su melodía y sonaba como si estaba tratando de ayudar para que Steve podría hacer su trabajo. La mayoría de los tiempo, si la víctima cree que intenta ayudarlo o le hacen algunos tipo de favor, él parte con información confidencial que han de lo contrario protegido cuidadosamente.

PREVENIR LA CON

Uno de los más poderosos trucos del ingeniero social consiste en convertir las tablas. Eso es lo que ha visto en este capítulo. El ingeniero social crea el problema, y luego mágicamente resuelve el problema, engañando a la víctima en proporcionar acceso a la compañía del vigilado más secretos. Caerían sus empleados para ello

¿tipo de artimaña? Te ha molestado a redactar y distribuir las reglas de seguridad específicas que ¿podría ayudar a prevenirlo?

Educar, educar y educar...
Hay una vieja historia sobre un visitante de Nueva York que se detiene a una hombre en la calle y pregunta, \"¿Cómo obtengo al Carnegie Hall?\" El hombre responde, \"práctica, práctica, práctica.\" Todo el mundo es así ingeniería vulnerable social que ataca un la compañía sólo eficaz de defensa es educar y capacitar a la gente, dándoles la práctica que necesitan para detectar un ingeniero social. Y, a continuación, seguir recordando a persona sobre una base consistente de lo aprendido en el entrenamiento, pero son todos demasiado apto para olvidar.

Todos los miembros de la organización deben ser entrenados para ejercer un grado apropiado de sospecha y precaución cuando contactada por alguien, que él o ella no personalmente saber, especialmente cuando alguien está pidiendo algún tipo de acceso a un equipo o red. Es naturaleza humana querer confiar en otros, pero como la Japoneses dicen que el negocio es la guerra. Su empresa no puede permitirse bajar su guardia. Directiva de seguridad corporativa debe definir claramente apropiado e inapropiado comportamiento.

La seguridad no es única. Personal de negocios suelen tener diferentes roles y responsabilidades y cada posición tiene asociados a las vulnerabilidades. Allí debe ser un nivel básico de capacitación que todos en la empresa es necesario para completa, y, a continuación, debe también ser capacitados de acuerdo a su perfil de trabajo a adherirse a ciertos procedimientos que reduzcan la posibilidad de que se conviertan en parte del problema. Personas que trabajan con información confidencial o se colocan en posiciones de confianza deben recibir entrenamiento especializado adicional.

Mantener segura la información confidencial
Cuando se acercó gente por un extraño que se ofrece a ayudar, como se ve en las historias en este capítulo, tienen que recurrir a la política de seguridad de la empresa que se adapta según corresponda a las necesidades del negocio, el tamaño y la cultura de su empresa.
NOTA
Personalmente, no creo que cualquier empresa debe permitir cualquier intercambio de contraseñas. Su mucho más fácil establecer una regla dura que prohíbe personal nunca compartir o intercambio de contraseñas confidenciales. Su más seguro, demasiado. Pero cada empresa debe evaluar sus propia cultura y problemas de seguridad en esta elección

Nunca cooperar con un desconocido que le pide a buscar información, escriba comandos desconocidos en un equipo, hacer cambios en la configuración de software o - más potencialmente desastrosa de todos - abrir un archivo adjunto de correo electrónico o Descargar software de marcada. Cualquier programa de software - incluso uno que parece no hacer nada -no se puede ser tan inocente como parece ser.

Hay ciertos procedimientos que, sin importar qué bueno nuestro entrenamiento, tendemos a crecen descuidada acerca con el tiempo. Entonces nos olvidamos de que el entrenamiento en tiempo de cri sólo cuando lo necesitamos. Uno pensaría que no da su nombre de cuenta y contraseña es algo que casi todo el mundo sabe (o debería saber) y apenas necesita ser dijo: es simple sentido común. Pero de hecho, cada empleado debe ser recordado con frecuencia que dar el nombre de cuenta y contraseña su equipo de oficina, su equipo doméstico o incluso la máquina de franqueo de la Sala de correo es equivalente a repartir el número PIN de su tarjeta de cajero automático.

En ocasiones, muy ocasionalmente - hay una circunstancia muy válida cuando ha es necesario, incluso importantes, dar a alguien más confidencial información. Por esa razón, no es conveniente hacer una regla absoluta sobre There was an error deserializing the object of type System.String. Encountered unexpected character 'S'. sobre las circunstancias bajo las cuales un empleado puede dar su contraseña y - lo más importante--quién está autorizado para solicitar la información.

Considere la fuente

En la mayoría de las organizaciones, la norma debe ser que cualquier información que posiblemente pueda causar daño a la empresa o a a. compañero empleado puede darse sólo a alguien que se conoce de forma presencial, o cuya voz es tan familiar que te lo reconoce sin lugar a dudas.

En situaciones de alta seguridad, las solicitudes sólo deben concederse son entrega en persona o con una forma fuerte de autenticación--por ejemplo, dos separar los elementos tales como un secreto compartido y un token de tiempo.

Deben designar los procedimientos de clasificación de datos que no se proporciona información de una parte de la organización participan con trabajo sensible a cualquier persona no personalmente conocido o prestación para de alguna manera.

NOTA

Increíblemente, incluso buscar el nombre y número de teléfono de la persona que llama en la base de datos de empleados de la compañía y llamándolo atrás no es una garantía absoluta los ingenieros sociales conocer formas de plantación de nombres en una base de datos corporativa o redirigir llamadas telefónicas.

Entonces, ¿Cómo manejas una sonda legítima solicitud de información del otro empleado de la empresa, tales como la lista de nombres y direcciones de correo electrónico de ¿personas de su grupo? De hecho, ¿cómo usted sensibilizar para que como un elemento Esto, que es claramente menos valiosa que, dicen, una hoja de especificaciones para un producto en ¿desarrollo, se reconoce como algo sólo para uso interno? Una parte importante de la solución: designar empleados en cada departamento que se encargará de todo solicitudes de información ser enviado fuera del grupo. Una seguridad avanzada-

programa de formación, a continuación, debe proporcionar para hacer estos empleados designados consciente de los procedimientos de verificación especial deben seguir.

Nadie olvida

Nadie puede rattle rápidamente fuera de la identidad de las organizaciones dentro de su empresa necesitan un alto grado de protección contra ataques malintencionados. Pero a menudo pasar por alto otros lugares que son menos obvios, pero altamente vulnerables. En uno de estos historias, la solicitud de un fax ser enviado a un número de teléfono dentro de la empresa parecía inocente y suficientemente segura, todavía el atacante aprovechó esta seguridad Laguna. La lección aquí: todos de secretarios y auxiliares administrativos a los ejecutivos de la empresa y las necesidades de los administradores de alto tienen entrenamiento especial de seguridad por lo que pueden ser alerta para estos tipos de trucos. Y no te olvides de guardia de la puerta delantera: recepcionistas, demasiado, a menudo son primos objetivos para los ingenieros sociales y también debe hacerse consciente de la engañosa técnicas utilizadas por algunos visitantes y llamadores.

Seguridad de la empresa debe establecer un único punto de contacto como una especie de central Clearinghouse para empleados que piensan que puedan haber sido el destino de una social Ingeniería treta. Tener un solo lugar a incidentes de seguridad informe proporcionará un sistema eficaz de alerta temprana que querida cuando una coordinada ataque está en marcha, por lo que cualquier daño puede ser controlado de inmediato.

Capítulo 6
¿Me puedes ayudar?

He visto cómo los ingenieros sociales engañar a la gente ofreciendo a ayudar.Otro enfoque favorito vuelve a las tablas: manipula el ingeniero social pretendiendo él necesita la otra persona para ayudarlo. Podemos simpatizar con la gente en un apuro y el enfoque resulta efectivo una y otra vez en lo que permite una ingeniero social para alcanzar su objetivo.

LA SALIDA DE TOWNER

Una historia en el capítulo 3 mostró cómo un atacante puede hablar a una víctima para que revelen sus número de empleados. Éste utiliza un enfoque diferente para lograr el mismo resultado y, a continuación, muestra cómo el atacante puede hacer uso de ese

Mantenerse al día con los Joneses

En Silicon Valley hay cierta empresa global que será anónima. El oficinas de ventas dispersas y otras instalaciones del campo alrededor de la worldare todos conectado a la sede de la empresa sobre una WAN, una red de área amplia. El intruso, un tipo inteligente, eth0 llamado Brian Atterby, sabía que era casi siempre más fácil dividir una red en uno de los sitios remotos donde la seguridad es prácticamente garantizado a ser más laxas que en la sede.

El intruso telefoneó a la Oficina de Chicago y pidió hablar con el señor Jones.
La recepcionista preguntó si sabía el nombre del Sr. Jones; contestó,
There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
Tres. ¿Departamento que él sería en?
Dijo, \"Si me lees los nombres, tal vez voy reconocerlo.\" Por lo que hizo:
Barry, Joseph y Gordon.
There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
Departamento?\"
Desarrollo de negocios.
Bellas. ¿Puede conectarme, por favor?
Ella pone la llamada a través de. Cuando Jones respondió, el atacante dijo: \"Señor.
¿Jones? Hola, esto es Tony en nómina. Sólo ponemos a través de su solicitud Tu cheque depositado directamente a su cuenta de ahorro y crédito\".
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
no aún tienen una cuenta en una cooperativa de crédito\".
Ah, joder, lo ya puse a través de.
Jones fue poco más de un disgusto en la idea de que podría ser su sueldo va a la cuenta de otra persona, y él estaba empezando a pensar el chico en el otro extremo del teléfono debe ser un poco lento. Antes de que incluso podría responder, el

atacante dijo: \"veo mejor lo sucedido. Se introducen cambios de nómina por
número de empleados. ¿Cuál es tu número de empleado?\"
Jones dio el número. El llamador dijo, \"No, tienes razón, no era la solicitud de
usted, entonces.\" Llegan más estúpido cada año, pensó Jones.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
obtendrá su próximo cheque bien,\"el chico dice tranquilizadora.

Un viaje de negocios
No mucho después, el administrador del sistema en las ventas la empresa Austin, Texas,
Oficina recibió una llamada telefónica. \"Esto es Joseph Jones,\" anunció el llamador. \"Estoy en
Desarrollo de negocios corporativos. Estaré en a, para la semana, en el Driskill
Hotel. Me gustaría que me fije con una cuenta temporal por lo que puedo acceder a mi
correo sin hacer una llamada de larga distancia\".

There was an error deserializing the object of type System.String. The token 'true' was expected but foun
dijo. El falso Jones dio el número y salió, tiene usted alguna alta velocidad\"
números de acceso telefónico.

There was an error deserializing the object of type System.String. Encountered unexpected character 'A'.
Joe. Dígame, ¿cuál es tu número de edificio? \" El atacante había hecho su
deberes y tenía la respuesta listo

MENSAJE DE MITNICK
No confíe en salvaguardias de red y servidores de seguridad para proteger su información. Mirar
a su punto más vulnerable. Generalmente encontrará que la vulnerabilidad reside en su
personas.

There was an error deserializing the object of type System.String. The token 'true' was expected but

Fue tan simple como eso. El administrador del sistema ha verificado el nombre Joseph Jones, el
Departamento y el número de empleados y \"Joe\" habían dado la respuesta correcta a
la cuestión de la prueba. \"Su nombre de usuario va a ser la misma que su empresa,
jbjones,\", dijo el administrador del sistema\"y le doy una contraseña inicial de
\"changeme.\" \"

Analizando el timo
Con un par de llamadas telefónicas y quince minutos de tiempo, el atacante había ganado
acceso a la red de área amplia de la empresa. Se trata de una empresa que, al igual que muchos,
tenía lo que me refiero a como seguridad de caramelo, después de una descripción utilizó por primera ve
Investigadores de los laboratorios, Steve Bellovin y Steven Cheswick. Describieron como
seguridad como \"un duro crujiente shell con un centro frecuentemente masticable\" - como una m

La capa exterior, el cortafuegos, argumentaron Bellovin y Cheswick, no es suficiente protección, porque una vez que un intruso puedo eludirlo interno sistemas informáticos tienen seguridad suave y masticable. La mayoría de las veces, son insuficientemente protegidos.

Esta historia se ajusta a la definición. Con un número telefónico y una cuenta, el atacante incluso no tiene que preocuparse tratando de derrotar a un servidor de seguridad de Internet y, una vez den fácilmente pudo poner en peligro la mayoría de los sistemas de la red interna.

A través de mis fuentes, entiendo este ardid exacta fue trabajado en uno de los fabricantes de software de la computadora más grandes del mundo. Uno pensaría que el los administradores de sistemas en una empresa estaría capacitados para detectar este tipo de Ruse. Pero en mi experiencia, nadie está completamente seguro si es un ingeniero social inteligente y suficientemente persuasivo.

JERGA
Término CANDY seguridad a acuñado por Bellovin y Cheswick de Bell Labs para describir un escenario de seguridad en el perímetro exterior, tales como cortafuegos, es fuerte, pero la infraestructura detrás de él es débil. El término se refiere a m tiene un centro blando y duro caparazón exterior.

JERGA
SPEAKEASY seguridad que se basa en saber cuando deseen es información y el uso de una palabra o nombre para tener acceso a esa información o sistema informático.

SEGURIDAD DE SPEAKEASY
En los viejos tiempos de Tabernas - los clubes nocturnos de la época de la prohibición en su llamada gin bañera fluía--un cliente aspirante obtuvo admisión por aparecer en la puerta y golpeando. Después de unos momentos, un pequeño colgajo en la puerta le swing abierto y un duro, de intimidar a cara sería pares fuera. Si el visitante fue en el sabe, él hablaría con el nombre de algún patrón frecuente del lugar (\"Joe enviado \"fue bastante a menudo), con lo cual el gorila dentro que desenganchar la puerta y dejarlo.

El truco real radica en saber la ubicación de la speakeasy porque la puerta estaba sin marcar, y los propietarios no salir exactamente señales de neón para marcar su presencia. En su mayor parte, sólo aparece en el lugar correcto fue sobre todo lo llevó a obtener. El mismo grado de custodia, infelizmente, practica ampliamente en el mundo corporativo, proporcionando un nivel de protección no que llame a speakeasy seguridad.

Lo vi en el cine
Aquí es una ilustración de una película favorita que muchos recordarán. En Tres días del Cóndor el personaje central, Turner (interpretado por Robert Redford), trabaja para una empresa pequeña investigación contratada por la CIA. Un día él regresa de un almuerzo a encontrar que todos los trabajadores de sus co han sido asesinados hacia abajo. Dejó a averiguar lo que ha hecho y por qué, sabiendo todo el tiempo que buscan los chicos malos, quienquiera que sean, para él.

A finales de la historia, Turner logra obtener al número de teléfono de uno de los chicos malos. Pero ¿quién es esta persona, y cómo puede Turner pin abajo su ubicación? Él está de enhorabuena: El guionista, David Rayfiel, felizmente ha dado Turner un fondo que incluye la capacitación como un liniero de teléfono con el Army Signal Corps, haciendo él conoce de técnicas y prácticas de la compañía telefónica. Con número de teléfono del chico malo en mano, Turner sabe exactamente qué hacer. En guión, la escena dice así:

TURNER vuelve a conectar y grifería otro número.

ANILLO! ANILLO! A continuación:

VOZ de (filtro la mujer) CNA, Sra. Coleman hablando.
TURNER (en la prueba de conjunto)

Se trata de Harold Thomas, Sra. Coleman. Servicio al cliente.

CNA en 202-555-7389, por favor.

MUJER s voz (filtro) un momento, por favor. (casi a la vez)

Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland.

Ignorando el hecho de que el guionista erróneamente utiliza un área de Washington, D.C., ¿código para una dirección de Maryland, puede usted detectar lo que acaba de ocurrir aquí?

Turner, debido a su formación como un liniero de teléfono, sabía qué número marcado para llegar a una Oficina de la compañía de teléfono llamada CNA, el nombre del cliente y Oficina de dirección. CNA está configurado para la conveniencia de instaladores y otros personal de la empresa de teléfonos autorizados. Un instalador podría llamar CNA y dar ellos un número de teléfono. El CNA empleado wouldrespond proporcionando el nombre de la persona en que el teléfono pertenece a la dirección andhis.

Engañando a la compañía telefónica
En el mundo real, el número de teléfono para el CNA es un secreto celosamente.

Aunque las compañías telefónicas finalmente y en estos días son menos generoso sobre entregando información tan fácilmente, al tiempo operó en una variación de seguridad speakeasy que llaman a profesionales de la seguridad seguridad a través de la oscuridad. Presume que quien llama CNA y sabía el jerga adecuada (\"servicio al cliente. CNA en 555-1234, por favor, por ejemplo) era un persona autorizada para disponer de la información.

JERGA
SEGURIDAD a través de la oscuridad un método ineficaz de equipo seguridad que se basa en el mantenimiento de secreto de los detalles de cómo funciona el sistema (protocolos, algoritmos y sistemas internos). Depende de la seguridad por oscuridad la falsa suposición de que nadie fuera de un grupo de confianza de la gente será capaz de burlar el sistema.

MITNICK MESSGAE
Seguridad a través de la oscuridad no tiene ningún efecto el bloqueo social ataques de ingeniería. Cada sistema informático en el mundo tiene al menos un humano utilizarlo. 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 para verificar o no identificar a sí mismo, necesidad de dar un empleado número, sin necesidad de una contraseña que se ha cambiado diariamente. Si supieras el número a la llamada y le sonaba auténticos, entonces usted debe tener derecho a la información.

No era una suposición muy sólida por parte de la compañía telefónica. Sus sólo el esfuerzo en seguridad fue cambiar el número de teléfono periódicamente l, en menos una vez al año. Aún así, el número actual en cualquier momento fue muy ampliamente conocido entre teléfono phreaks, que encantado en el aprovechamiento de este fuente conveniente de información y compartir los métodos-a--it con sus phreaks compañeros. El CN' truco de mesa fue una de las primeras cosas que aprendí cuando me fue a la afición de teléfono phreaking como un adolescente.

En todo el mundo de los negocios y el Gobierno, la seguridad de speakeasy. sigue siendo prevalente. Es probable que sobre jerga, personas y departamentos de su empresa. A veces les a que: a veces un número de teléfono interno es basta.

EL ADMINISTRADOR DE EQUIPO DESCUIDADO
Aunque muchos empleados en las organizaciones son negligentes, despreocupados o inconscientes peligros de seguridad, que esperaría alguien con el administrador del título en el equipo Centro de una empresa de Fortune 500 para estar completamente informados sobre mejores ¿prácticas de seguridad, correctas?

No se espera que un administrador de equipo Centro - alguien que es parte de su Departamento de tecnología de la información de la empresa - a la víctima de la caída a una simplista y la ingeniería social evidente con juego. Especialmente no el ingeniero social es apenas más de un niño, apenas de su adolescencia. Pero a veces pueden ser sus expectativas equivocado.

Ajuste

Hace años era un pasatiempo entretenido para muchas personas a mantener un radio sintonizado a la la policía local o bomberos frecuencias, escuchando los ocasionales altamente encargado de las conversaciones acerca de un robo de banco en progreso, un edificio de oficinas en incendio, o una persecución de alta velocidad como el evento desplegado. Las frecuencias de radio utiliza Ley de agencias y departamentos de bomberos solía estar disponible en los libros en la librería de la esquina; hoy está siempre en anuncios en la Web y desde un libro en que se puede comprar en las frecuencias de Radio Shack, Condado, estado local y, algunos casos, incluso federales organismos.

Por supuesto, no sólo los curiosos que estaban escuchando. Ladrones robando una tienda en medio de la noche pudo sintonizar para escuchar si estaba siendo un coche de policía envió a la ubicación. Traficantes de drogas podrían mantener un control sobre las actividades de la agentes de la Agencia de aplicación de drogas locales. Un pirómano podría mejorar su enfermedad placer por la iluminación de un incendio y luego escuchando todo el tráfico de radio mientras bomberos lucharon sacarlo.

En los últimos años avances en informática han hecho posible cifrar los mensajes de voz. Como ingenieros encontraron formas de cram más potencia en un solo microchip informática, comenzaron a construir pequeñas, cifrada Radios para la aplicación de la ley que impidió que los malos y los curiosos escuchando en.

Danny el interceptor

Un escáner entusiasta y experto hacker llamaremos Danny decidió ver si él no se pudo encontrar una manera de conseguir sus manos sobre el software de encriptación supersecreta - 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 sobre derecho aplicación y posiblemente también uso de la tecnología por lo incluso los más poderosos agencias de Gobierno serían difícil seguir sus conversaciones con su amigos.

Dannys del mundo sombrío de los piratas informáticos pertenecen a una categoría especial que cae en algún lugar entre la mera curiosidad pero-totalmente - benigno y la peligroso. Dannys tienen el conocimiento del experto, combinada con la

travieso hacker del deseo de entrar en sistemas y redes para la
desafío intelectual y por el placer de obtener información sobre cómo la tecnología
obras. Pero su ruptura electrónico- y - entrando acrobacias son sólo eso--acrobacias.
Estas personas, estos piratas benignas, entrar ilegalmente en sitios por pura diversión y
euforia de demostrar que pueden hacerlo. No roban nada, no hacen
cualquier dinero de sus hazañas; ellos no destruir todos los archivos, interrumpir cualquier red
conexiones, o bloquear cualquier sistema informático. El mero hecho de estar allí,
atrapando copias de archivos y correos electrónicos para contraseñas a espaldas de la búsqueda
administradores Curity y red, ajustes de las narices de los responsables
mantener a los intrusos como ellos. El plantearnos es una gran parte de la
satisfacción.

En consonancia con este perfil, nuestro Danny quería examinar los detalles de su destino
la compañía más celosamente producto solo para satisfacer su propia grabación curiosidad
y para admirar las innovaciones inteligentes el fabricante podría haber llegado
con.

Los diseños de producto eran, ni que decir tiene, cuidadosamente guardados secretos, como
preciosos y protegido como cosa en posesión de la empresa. Danny
lo sabía. Y importaba un poco. Después de todo, fue sin nombre, sólo algunos grandes
empresa.

Pero ¿cómo obtener el código fuente del software? Como resultó, agarrando la corona
joyas de Secure Communications Group la empresa demostró para ser demasiado fácil,
a pesar de que la compañía fue uno de los que utilizan la autenticación de dos factores,
un acuerdo en virtud del cual las personas deben utilizar independiente no uno sino dos
identificadores para probar su identidad.

Aquí hay un ejemplo que probablemente ya esté familiarizado con. Cuando su renovación
llega la tarjeta de crédito, se le pedirá que la empresa emisora para hacerles saber por teléfono
que la tarjeta está en posesión de los clientes previsto y no alguien que
robaron la envolvente desde el correo. Las instrucciones con la tarjeta de estos días
generalmente digo para llamar desde casa. Cuando llame, software en la tarjeta de crédito
empresa analiza la ANI, la identificación automática de número, que es
proporcionada por el conmutador telefónico de peaje - llamadas gratis el crédito de la tarjeta de empresa
está pagando.

Un equipo de la compañía de tarjeta de crédito utiliza el número de llamada del partido siempre
la ANI, y partidos número contra base de datos de la empresa
tarjetahabientes. Por el momento el empleado viene de la línea, su muestra
información de la base de datos dando detalles acerca del cliente. Por lo que el empleado
ya sabe que la llamada viene desde la casa de un cliente; es una forma de
autenticación.

JERGA
El uso de dos tipos diferentes de autenticación de dos factores de
autenticación para verificar la identidad. Por ejemplo, una persona puede tener que identificar
el propio llamando desde una determinada ubicación identificable y conocer una contraseña.

El empleado, a continuación, escoge un elemento de la información que aparece acerca de usted - la may
a menudo el número de seguro social, fecha de nacimiento, o nombre de soltera de la madre - y pide
que para este dato. Si da la respuesta correcta, es un segundo
forma de autenticación - basada en la información que debe conocer.

En la empresa de fabricación de los sistemas de radio seguro en nuestra historia, cada
empleado con acceso informático tuvo su nombre habitual de cuenta y contraseña, pero
Además se presta con un pequeño dispositivo electrónico llamado Secure ID. Se trata de
lo que ha llamado un token de tiempo. Estos dispositivos vienen en dos tipos: uno es sobre
la mitad del tamaño de una tarjeta de crédito pero un poco más grueso; otra es pequeño suficiente que
personas simplemente adjunta a sus llaveros.

Derivado del mundo de la criptografía, este gadget en particular tiene un pequeño
ventana que muestra una serie de seis dígitos. Cada sesenta segundos, la pantalla
cambia para mostrar un número de seis dígitos diferente. Cuando se necesita una persona autorizada
para acceder a la red desde fuera del sitio, ella debe identificar a sí misma como un autorizado
usuario escribiendo su PIN secreto y los dígitos que aparece en su dispositivo token.
Una vez verificado por el sistema interno, autentica con su cuenta
nombre y contraseña.

El joven hacker Danny para obtener el código fuente que tan codiciado, habría
han comprometer no sólo algunos empleados nombre de cuenta y contraseña (no
mucho de un reto para el experimentado ingeniero social) pero también alrededor de la
token de tiempo.

Derrotando a la autenticación de dos factores de un token de tiempo combinado con un
del usuario secreto PIN código suena un desafío de misión imposible.
Pero para los ingenieros sociales, el desafío es similar al convirtió en un jugador de póker
¿Quién tiene más que la habitual habilidad en la lectura de sus oponentes. Con un poco de suerte,
cuando él se sienta en una mesa sabe que es probable que marchan con un montón de grande
de dinero de otras personas.

Asalto a la fortaleza
Danny comenzó haciendo sus deberes. Mucho tiempo antes había logrado poner
piezas suficientemente juntos a hacerse pasar por un empleado real. Tenía un empleado
nombre, departamento, número de teléfono y número de empleado, así como la
del administrador nombre y número de teléfono.

Ahora era la calma antes de la tormenta. Literalmente. Pasando por el plan que había trabajado Danny necesita algo más antes de que él podría dar el siguiente paso, y fue algo no tenía control sobre: necesitaba una tormenta de nieve. Danny necesita un poca ayuda de la madre naturaleza en forma de clima tan malo que mantendría trabajadores de entrar en la Oficina. En el invierno en Dakota del Sur, donde el la fábrica en cuestión se encontraba, alguien esperando el mal tiempo lo hizo no hay mucho que esperar. El viernes por la noche, llegó una tormenta. Lo que comenzó como nieve convirtió rápidamente a la lluvia helada que, por la mañana, las carreteras estaban recubiertas con un ingenioso, peligrosa capa de hielo. Para Danny, esta era una oportunidad perfecta.

Telefoneó a la planta, pidió sala para los informáticos y alcanzó uno de los abejas obreras de la misma, un operador de equipo que él mismo anunció como Roger Kowalski.

Dando el nombre del empleado real había obtenido, Danny dijo, \"este es Bob Billings. Trabajo en el grupo de comunicación segura. Ahora estoy en casa y Yo no puedo conducir en debido a la tormenta. Y el problema es que necesito acceder a mi estación de trabajo y el servidor de casa y me dejó mi ID segura en mi escritorio. Puede ¿ir a buscar para mí? ¿O puede alguien? Y, a continuación, lee mi código cuando me ¿necesidad de obtener? Porque mi equipo tiene una fecha límite crítica y no hay manera que pueda hacer mi trabajo. Y no hay forma puedo llegar a la Oficina--las carreteras son mucho demasiado peligroso mi camino.

El operador del equipo, dijo, \"No puedo dejar el centro de cómputo\". Danny saltó derecha: \"tiene una identificación segura de ti mismo?.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. operadores en caso de emergencia\".

There was an error deserializing the object of type System.String. Encountered unexpected character 'D ¿en la red, puede me dejas prestado su ID segura? Sólo hasta que esté seguro unidad \".
There was an error deserializing the object of type System.String. Encountered unexpected charact
There was an error deserializing the object of type System.String. Unexpected end of file. Follo
Para Ed Trenton.
Ah, sí, lo conozco.

Cuando él está obligado a afrontar duras trineos, hace un buen ingeniero social más de la cantidad habitual de investigación. \"Estoy en el segundo piso\", Danny fue INH \"Junto a Roy Tucker.\"

Sabía que ese nombre. Danny volvió a trabajar en él. \"Sería mucho más fácil ir a mi escritorio y recuperar mi ID segura para mí.\"

Danny estaba bastante seguro que el chico no compraría en esto. En primer lugar, sería no quiere dejar en la mitad de su turno para ir conociendo a corredores y hasta escaleras a alguna parte distante del edificio. También él desearía no tener que Paw a través de la mesa de alguien, violando el espacio personal de alguien. No, se fue una apuesta segura que él no quiere hacerlo.

Kowalski no quería decir que no a un chico que necesitaba ayuda, pero no lo hizo queremos decir sí y tener problemas, tampoco. Así que él superaba la decisión: vas a tener pedirle a mi jefe. Colgar en\". Puso el teléfono hacia abajo, y Danny podía oírle recoger otro teléfono, poner en la llamada y explicar la solicitud. Luego hizo Kowalski Algo inexplicable: él realmente avalado por el hombre utilizando el nombre de Bob Billings. \"Sé que le\", dijo su manager. \"Trabaja para Ed Trenton. Podemos le permiten utilizar el ID segura en el centro del equipo ' Danny, sosteniendo a la teléfono, se asombró al escuchar este apoyo extraordinario e inesperado para su causa. Él no podía creer sus oídos o su suerte.
Después de un par de momentos, Kowalski volvió sobre la línea y dijo, \"mi el administrador quiere hablar con usted mismo,\"y le dio el hombre nombre y celular número de teléfono.

Danny llamado el administrador y atravesó toda la historia una vez más, agregar detalles sobre el proyecto estaba trabajando o y por qué su equipo de producto necesarios para cumplir un plazo crítico. \"Sería más fácil si alguien sólo va y \"recupera mi tarjeta, dijo. \"No creo el escritorio está bloqueado, debe existir en mi superior izquierdo cajón.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 's'. uno en el centro de cómputo. Te voy a decir los chicos de turno que cuando llames, debe leer en el código de acceso aleatorio para usted\", y le dio el PIN número para usar con ella.

Para el fin de semana entero, cada vez que Danny quería entrar en la empresa sistema informático, sólo tuvo que llamar al centro de cómputo y pedirles que leer frente a los seis dígitos que aparece en el símbolo (token) Secure ID.

Un trabajo interior
Una vez fue dentro de sistema informático de la empresa, entonces ¿qué? ¿Cómo sería ¿Danny encontrar su camino hacia el servidor con el software que quería? Él ya había preparado para esto.

Muchos usuarios de computadoras están familiarizados con los grupos de noticias, ese amplios conjunto de boletines electrónicos donde las personas pueden publicar preguntas que otras personas responder o encontrar compañeros virtuales que comparten un interés en la música, computadoras, o cualquiera de los cientos de otros temas.

Lo que pocas personas se dan cuenta de cuando registre cualquier mensaje en un sitio de grupo de noticia
su mensaje permanece en línea y disponible durante años. Google, por ejemplo, ahora
mantiene un archivo de siete cien millones de mensajes, algunos datan de
veinte años! Danny comenzado dirigiéndose a la dirección Web
http:\/\/Groups.google.com.

Como buscar términos, Danny entró \"comunicaciones de radio de cifrado\" y la
nombre de la empresa y se encuentra un años de mensajes sobre el tema desde una
empleado. Es un registro que se hizo cuando la compañía fue la primera
desarrollo del producto, probablemente mucho antes de que los departamentos de policía y federal
organismos examinó la trepada de señales de radio.
El mensaje contiene la firma del remitente, dando no sólo el nombre del hombre,
Prensa de Scott, pero su número de teléfono e incluso el nombre de su grupo de trabajo, la
Secure Communications Group.

Danny cogió el teléfono y marca el número. Me pareció un disparo largo--
¿estaría él sigue trabajando en la misma organización años después? Estaría en
¿trabajar en tal un fin de semana tormentoso? Sonó el teléfono una vez, dos veces, tres veces, y
Entonces vino una voz en la línea. \"Esto es Scott\", dijo.

Afirmando ser de la empresa del departamento de TI, Danny manipulado (en prensa
una de las formas ahora familiares de capítulos anteriores) para que revelen la
nombres de los servidores que se utilizó para el trabajo de desarrollo. Estos fueron los servidores que
podría esperarse que mantenga el código fuente que contiene el propiedad cifrado
algoritmo y firmware usado en productos de la empresa radio seguro.

Danny estaba moviendo más cerca y más cerca, y fue construyendo su emoción. Fue
anticipando la fiebre, el gran alto siempre sintió cuando sucedió en
podría lograr algo que sabía que sólo un número muy limitado de personas.

Aún así, no era casa libre todavía. Para el resto del fin de semana sería capaz de entrar en
red de la empresa siempre que quería, gracias a esa cooperativa
Administrador de centro del equipo. Y sabía que quería acceder a los servidores. Pero
cuando él marca en, iniciado sesión en terminal server no le permitiría
conectarse a los sistemas de desarrollo del grupo de comunicación segura. Allí debe
un firewall interno o enrutador proteger los sistemas informáticos de se ha
Grupo. Tendría que encontrar otra manera de.

El siguiente paso tuvo nervio: Danny llamado de vuelta a Kowalski en equipo
Operaciones y complained \"mi servidor no me deja conectar,\" y dijo que
chico, \"necesito que me configurado con una cuenta en uno de los equipos en su
Departamento por lo que puedo usar Telnet para conectar con mi sistema.\"

El director ya había aprobado divulgar el código de acceso se muestra en la
según tiempo testigo, por lo que esta nueva solicitud no parece razonable. Configurar Kowalski
una cuenta temporal y la contraseña en uno de los equipos del centro de operación,
y le dijo a Danny para \"volver a llamarme cuando no necesita más y voy a quitar
It\".

Una vez ingresado en la cuenta temporal, Danny fue capaz de conectarse a través de la
red de sistemas informáticos de asegurar las comunicaciones del grupo. Después de una hora
búsqueda en línea para una vulnerabilidad técnica que le daría acceso a un
servidor de desarrollo principal, golpear el bote. Al parecer el sistema o red
administrador no era vigilante en mantenerse al día con las últimas noticias sobre fallos de seguridad
en el sistema operativo que permite el acceso remoto. Pero Danny.

Dentro de poco tiempo había localizado los archivos de código fuente que fue después de
transferirlos de forma remota a un sitio de comercio electrónico que ofrece espacio de almacenamiento g
En este sitio, incluso si nunca fueron descubiertos los archivos, no serían nunca se remonta
volver a él.

Tuvo un paso final antes de la firma: el proceso metódico de borrar su
pistas. Terminó antes de que el show de Jay Leno había ido fuera del aire durante la noche.
Danny figuró esta había sido una obra de muy buen fin de semana. Y él nunca había
tuve que poner él mismo personalmente en peligro. Fue una emoción intoxicante, incluso mejor que
snowboard o paracaidismo.

Danny llegó ebrio esa noche, no en whisky, gin, cerveza o sake, sino en su sentido de
poder y logro cerrar como vierte a través de los archivos que había robado,
en el software de radio esquivo, muy secreto.

Analizando el timo
Como en el artículo anterior, esta treta funcionaba sólo porque los empleados de una empresa
era todo demasiado dispuestos a aceptar a su valor nominal que llama realmente fue el empleado
pretenden ser. Ese afán de ayudar a un trabajador de co con un problema es, por el
una mano, parte de lo que grasas las ruedas de la industria y parte de lo que hace el
empleados de algunas compañías más agradables trabajar con que los empleados de
otros. Pero por otro lado, esta utilidad puede ser una vulnerabilidad mayor que un
ingeniero social intentará explotar.

Un poco de manipulación utiliza Danny estaba delicioso: cuando hizo la solicitud
que alguien Obtenga su ID segura desde su escritorio, él decía que quería
alguien para \"recuperar\" para él. Recuperación es un comando que le das a tu perro. Nadie
quiere ser contada a buscar algo. Con esa palabra, Danny hizo todo el
solución más cierta que denegará la solicitud y algunos otro aceptados
en cambio, que era exactamente lo que quería.

El operador del centro de cómputo, \"Kowalski, fue tomada por Danny soltando el nombres de personas Kowalski ocurrido saber. Pero por qué habría de Kowalski Manager - un Gerente de TI, nada menos - permitir algunos accesos es ajeno a la empresa ¿red interna? Simplemente porque la convocatoria de ayuda puede ser un potente, convincente herramienta en el arsenal del ingeniero social.

MENSAJE DE MITNICK
Esta historia va a mostrar que según tiempo símbolos y formas similares de autenticación no son una defensa contra el astuto ingeniero social. La única defensa es un empleado de conciencia que sigue las directivas de seguridad y entiende cómo otros maliciosamente pueden influir en su comportamiento.

¿Podría algo así como nunca ocurrirá en su empresa? ¿Lo tiene ya?

PREVENIR LA CON
Parece ser un elemento repetido a menudo en estas historias que organiza un atacante para conectarse a una red de equipo desde fuera de la empresa, sin la persona que le ayuda a tomar medidas suficientes para comprobar que el llamador es realmente un empleado y derecho al acceso. ¿Por qué volver a este tema tan a menudo? Porque realmente es un factor de tantos ataques de ingeniería social. Para lo social Ingeniero, es la forma más fácil de alcanzar su meta. ¿Por qué debería gastar un atacante ¿horas tratando de romper, cuando él puede hacerlo en su lugar con una simple llamada de teléfono?

Uno de los métodos más eficaces para el ingeniero social para llevar a cabo esto tipo de ataque es la simple estratagema de pretender necesitar ayuda - un enfoque frecuentemente utilizado por los atacantes. No quieres dejar de ser útil a sus empleados co trabajadores o clientes, por lo que necesita armarlas con verificación específica procedimientos para utilizar con nadie hace una solicitud para el acceso de equipo o información confidencial. De este modo pueden ser útiles a aquellos que merecen ser ayudó, pero al mismo tiempo proteger los activos de información de la organización y sistemas informáticos.

Procedimientos de seguridad de la empresa deben precisar con detalle qué tipo de verificación mecanismos deben utilizarse en diversas circunstancias. Capítulo 17 proporciona un detallada lista de procedimientos, pero aquí hay algunas pautas a tener en cuenta:

Es una buena manera de verificar la identidad de una persona hace una solicitud llamar a la número de teléfono que aparece en el directorio de la empresa para esa persona. Si la persona hace la solicitud es realmente un atacante, la llamada de verificación que cualquiera le permiten hablar con la persona real en el teléfono mientras el impostor está en suspenso, o podrá llegar a correo de voz del empleado, por lo que se puede escuchar el sonido de su voz, y comparar a thespeech del atacante.

Si se utilizan números de empleados en su empresa para verificar la identidad, a continuación, los números deben tratarse como información confidencial, cuidadosamente vigilado y no entregado a los extraños. Lo mismo vale para todo tipo de identificadores internos, como los números de teléfono interno, departamentales de identificadores de facturación e incluso direcciones de correo electrónico.

Capacitación corporativa debe llamar la atención de todos a la práctica común de aceptando desconocido personas como empleados legítimos sobre los motivos sonido autorizada o bien informado. Sólo porque alguien sabe de una empresa práctica o utiliza terminología interna no es ninguna razón para suponer que su identidad no necesita ser verificado en otras formas.

Oficiales de seguridad y los administradores del sistema no deben limitar su enfoque para que son sólo la alerta de seguridad preocupados por cómo todo el mundo está siendo. Ellos también Debemos asegurarnos de que ellos mismos están siguiendo las mismas normas, procedimientos, y prácticas.

Contraseñas y similares no deben, por supuesto, nunca será compartidas, pero la restricción contra compartir es aún más importante con tokens basado en el tiempo y otros seguros formas de autenticación. Debe ser un asunto de común sentido compartir cualquier de estos elementos viola el punto de haber instalado la empresa la sistemas. Compartir significa que no puede haber ninguna responsabilidad. Si un incidente de seguridad se lleva a cabo o algo va mal, no podrá determinar que la es la parte responsable.

Como reitero a lo largo de este libro, los empleados necesitan estar familiarizados con social Ingeniería estrategias y métodos para analizar cuidadosamente las solicitudes que se reciben. Considere el uso de rol como parte estándar de capacitación en seguridad, por lo que empleados pueden llegar a una mejor comprensión de cómo funciona el ingeniero social.

Capítulo 7
Sitios falsos y peligrosos archivos adjuntos

Hay un viejo dicho que nunca obtener algo a cambio de nada,
Aún así, la estratagema de ofrecer algo gratis sigue siendo un gran empate para ambos legítimo (\"pero esperar--allí es más! Llame ahora mismo y te tiramos en un conjunto de cuchillos y un popcorn popper!\") y no-tan - legítima (\"compra un acre de Pantanal en Florida y obtener un segundo acre libre!\") empresas.

Y la mayoría de nosotros estamos tan ansiosos por obtener algo gratis que podemos ser distraídos de pensar claramente sobre la oferta o la promesa.

Sabemos que la advertencia familiar, \"si el comprador tenga cuidado\", pero es hora de escuchar otra Advertencia: cuidado con los adjuntos de correo electrónico come-on y el software libre. El experto atacante usará casi cualquier medio para entrar en la red corporativa, incluyendo apelando a nuestro deseo natural de obtener un regalo. A continuación presentamos algunos ejemplos.

¿NO TE GUSTA UN LIBRE (EN BLANCO)?\"
Igual que los virus han sido una maldición para la humanidad y médicos desde el comienzo del tiempo, así el denominado virus informático representa una maldición similar para los usuarios de la tecnología. Los virus de computadora que obtenga la mayoría de la atención y terminan en el centro de atención, no casualmente, hacer más daño. Estos son los producto de vándalos de equipo.

Novatos del equipo convirtieron malintencionados, vándalos equipo esforzarse por mostrar cómo son inteligentes. A veces sus actos son como un rito de iniciación, significado Para impresionar a los piratas informáticos más antiguos y con más experiencia. Estas personas están motivada crear un gusano o virus pretende infligir daño. Si su trabajo destruye archivos, destruye todos discos duros y sí los correos electrónicos que miles de personas inocentes, vándalos hojaldre con orgullo en su realización. Si el virus causa suficiente caos que periódicos escriban sobre ello y las noticias de red emisiones advierten tanto mejor.

Mucho se ha escrito acerca de vándalos y sus virus; libros, software ofrecer protección y se han creado programas y empresas todos no tratar aquí las defensas contra los ataques de sus técnicos. Nuestro interés en el momento es menor en los actos destructivos de los vándalos que en el más específico esfuerzos de su primo lejano, el ingeniero social.

Llegó en el correo electrónico
Probablemente reciba correos electrónicos no solicitados cada día que llevan publicidad mensajes o una libre oferta algo-o-otros que usted necesita ni desea. Le

conocer el tipo. Prometen asesoramiento, descuentos en equipos, televisores, cámaras, vitaminas o viajes, ofrece tarjetas de crédito no necesita un dispositivo que le permitirá recibir canales de televisión de pago libres, formas de mejorar su salud o su vida sexual y así.

Pero cada vez que en un tiempo una oferta aparece en su buzón de correo electrónico para algo que llama la atención. Tal vez es un juego libre, una oferta de fotos de su estrella favorita, un programa de calendario gratis o compartir barato\"bisutería que Proteja su equipo contra virus. Cualquiera que sea la oferta, el correo electrónico le dirige para descargar el archivo con las golosinas que el mensaje ha convencido a probar.

O tal vez reciba un mensaje con un asunto que Lee Don, te echo de menos \" o \"Anna, por qué usted no ha escrito me,\" o \"de Hola, Tim, aquí la sexy foto I prometió \". Esto no podía ser correo publicitario no deseado, piensa, porque tiene su propio nombre y sonidos tan personales. Así se abre el archivo adjunto para ver la foto o leer el mensaje.

Todas estas acciones--descarga software usted aprendió acerca de un correo electrónico, haga clic en un vínculo que le lleva a un sitio que no ha oído hablar de la publicidad antes, realmente no sabes--están abriendo un archivo adjunto de alguien invitaciones a problemas. Sin duda, la mayor parte del tiempo lo que obtienes es exactamente lo que esperados, o en el peor de los casos algo decepcionante u ofensivo, pero inofensivo. Pero a veces lo que se consigue es obra de un vándalo.

Envío código malintencionado en el equipo es sólo una pequeña parte del ataque. El atacante debe persuadir a descargar el archivo adjunto para el ataque tener éxito.

NOTA
Conocer un tipo de programa en el equipo metro como una rata, o remoto Troyano de acceso, da el atacante pleno acceso al equipo, como si estuviera sentado en su teclado.

Las formas más dañinas de código malicioso - gusanos con nombres como amor Carta, SirCam y Anna Kournikiva, por nombrar algunos - han confiado en lo social Ingeniería técnicas de engaño y aprovechando nuestro deseo de llegar algo para que nada ser distribuida. El gusano llega como un archivo adjunto un correo electrónico que ofrece algo tentador, tales como información confidencial, libre pornografía, o - una artimaña muy inteligente - un mensaje diciendo que el archivo adjunto es el recibo algún elemento costoso que supuestamente ordenó. Este último truco te lleva para abrir el archivo adjunto por temor a su tarjeta de crédito ha sido acusada de un elemento le no orden.

Es asombroso cuántas personas entran por estos trucos; incluso después de que se le dijo y dijo una vez más sobre los peligros de la apertura de archivos adjuntos de correo electrónico, conciencia de peligro se desvanece con el tiempo, cada uno de nosotros dejando vulnerables.

Detección de Software malintencionado

Otro tipo de malware - abreviatura de software malintencionado - pone un programa en el equipo que opera sin su conocimiento o consentimiento, o realiza una tarea sin su conocimiento. Malware puede parecer bastante inocente, incluso puede ser un Documento de Word o presentación de PowerPoint o cualquier programa que tiene macro funcionalidad, pero secretamente se instalará un programa no autorizado. Por ejemplo, malware puede ser una versión del caballo de Troya que se hablaba en el capítulo 6. Vez Este software está instalado en el equipo, se puede alimentar cada pulsación de tecla que se escribe volver al atacante, incluyendo todas las contraseñas y números de tarjeta de crédito.

Hay otros dos tipos de software malintencionado que puede ser chocante. Uno puede alimentar el atacante cada palabra que hablas dentro del alcance del equipo micrófono, incluso cuando crees que el micrófono está desactivada. Peor, si usted tiene una cámara Web conectada al equipo, un atacante con una variación de este técnica puede ser capaz de capturar todo lo que se lleva a cabo en frente de su terminal, incluso cuando piensas que la cámara esté apagada, día o noche.

JERGA

Argot de MALWARE para software malintencionado, un programa de ordenador, tales como virus, gusano o troyano, que realiza tareas perjudiciales.

MENSAJE DE MITNICK

Cuidado con los frikis teniendo regalos, de lo contrario su empresa podría soportar la misma suerte que la ciudad de Troya. En caso de duda, para evitar una infección, use protección.

Un hacker con sentido del humor malicioso podría intentar plantar un pequeño programa diseñado para ser malvadamente molesto en el equipo. Por ejemplo, puede hacer la bandeja de la unidad de CD mantener estallido abierto, o el archivo que se está trabajando en mantener minimizar. O que podría provocar un archivo de audio reproducir un grito a todo volumen en el media de la noche. Ninguno de estos es muy divertido cuando intentas dormir o realizar trabajo.., pero al menos no hacen ningún daño duradero.

MENSAJE DE UN AMIGO

Los escenarios pueden obtener y lo que es peor, a pesar de sus precauciones. Imaginar: Tienes decidió no correr ningún riesgo. Ya no se descargará todos los archivos excepto desde sitios seguros que usted conozca y confíe, como SecurityFocus.com o Ya no hace clic en vínculos de correo electrónico de Amazon.com.

de fuentes desconocidas. No más adjuntos abiertos en cualquier correo que usted no esperaban. Y comprobar la página del navegador para asegurarse de que existe un símbolo de sitio seguro en todos los sitios que visita para transacciones de comercio electrónico o intercambio de información confidencial.

Y entonces un día recibe un correo electrónico de un amigo o una empresa que lleva asociado un archivo adjunto. No podía ser nada dañino si se trata de alguien ¿saben bien, no? Sobre todo porque se sabe quién culpar si tu datos del equipo fueron dañados.

Abrir el archivo adjunto, y... ¡ BOOM! Sólo consiguió golpear con un gusano o un troyano Caballo. ¿Por qué alguien que sabe haría esto a usted? Porque algunas cosas son no como aparecen. Has leído acerca de esto: el gusano que obtiene a alguien equipo y correos electrónicos a sí mismo a todos en la libreta de direcciones de esa persona. Cada de esas personas recibe un correo electrónico de alguien que conoce y confía y cada uno de los correos electrónicos contiene el gusano, que se propaga como las ondas de confianza desde una piedra arrojada en un estanque todavía.

La razón de que esta técnica es tan efectiva es la que sigue la teoría de matar a dos pájaros de un tiro: la capacidad de propagarse a otras víctimas desprevenidas, y el aspecto que se originó de una persona de confianza.

MENSAJE DE MITNICK

Hombre ha inventado muchas cosas maravillosas que han cambiado el mundo y nuestro modo de vida. Pero para cada buen uso de la tecnología, si un equipo, teléfono o Internet, alguien siempre encontrará una forma de abusar de su o sus propios fines.

Es una triste realidad en el estado actual de la tecnología que puede recibir un correo electrónico de alguien cercano a usted y aún tienen que saber si es seguro abrir.

VARIACIONES SOBRE UN TEMA

En esta era de Internet, hay un tipo de fraude que involucra le misdirecting un sitio Web es no lo que esperaba. Esto sucede regularmente, y tarda un variedad de formas. En este ejemplo, se basa en una real estafa perpetrada en el Internet es representante.

Feliz Navidad...

Un ex vendedor de seguros llamado a Edgar recibió un correo electrónico de un día de PayPal, una empresa que ofrece una forma rápida y cómoda de hacer en línea pagos. Este tipo de servicio resulta especialmente útil cuando una persona en una parte del el país (o el mundo, de eso se trata) está comprando un elemento de un individuo

no lo sabe. Gastos de tarjeta de crédito del comprador de PayPal y transfiere el dinero directamente a la cuenta del vendedor. Como un coleccionista de antigüedad vidrio frascos Edgar hiciero de negocios a través de la empresa de subastas on-line eBay. A menudo, usó PayPal a veces varias veces por semana. Así que Edgar estaba interesado cuando recibió un en la temporada de vacaciones de 2001 que parecían ser de PayPal, ofreciéndole un correo electrónico una recompensa para actualizar su cuenta de PayPal. Lea el mensaje:

Fiestas felices valoran al cliente de PayPal;
Cuando se aproxima el año nuevo y como todos nosotros Prepárate avanzar en un año,
PayPal le gustaría darle un crédito de $5 a tu cuenta!
Todo lo que tienes que hacer para reclamar que tu regalo de $5 de nosotros es actualizar la información s
nuestro sitio seguro de Pay Pal antes del 1 de enero, 2002. Un año trae muchos cambios, por
actualizar su información con nosotros permitirá para que nosotros seguir proporcionando
usted y nuestro servicio de cliente con excelente servicio y mientras tanto,
mantener nuestros registros rectos!

Para actualizar su información ahora y recibir $5 en tu cuenta PayPal
al instante, haga clic en este enlace:

http:\\www, paypal-segura. com\cgi bin

Gracias por usar PayPal.com y ayudarnos a crecer para ser el más grande de nuestro
tipo! Sinceramente deseándoles un muy \"Feliz Navidad y feliz año nuevo\"
Equipo de PayPal

Una nota acerca de los sitios Web E.commerce

Probablemente sepa quienes son reacios a comprar productos en línea, incluso desde
nombre de marca empresas como Amazon y eBay o los sitios Web de Old Navy,
Destino, o Nike. En cierto modo, son derecho a sospechar. Si utiliza el navegador
hoy el estándar de cifrado de 128 bits, la información que envíe a cualquiera seguro
sitio sale del equipo cifrado. Estos datos podrían ser descifrados con
un gran esfuerzo, pero probablemente no es rompible en una cantidad razonable de tiempo,
salvo quizás por la Agencia Nacional de seguridad (y la NSA, hasta 98 como
sabemos, no ha mostrado ningún interés en robar números de tarjetas de crédito de América
los ciudadanos o intentar averiguar quién está ordenando cintas sexys o kinky
ropa interior).

Estos archivos cifrados en realidad podían ser divididos por cualquier persona con el tiempo y
recursos. Pero realmente, qué tonto iría a todo ese esfuerzo para robar una tarjeta de crédito
número cuando muchas empresas de comercio electrónico a cometer el error de almacenar todos sus
¿información financiera del cliente sin encriptar en sus bases de datos? Peor aún, un número

de empresas de comercio electrónico utilice un determinado software de base de datos SQL mal compuesto el problema: han nunca cambió la sistema por defecto contraseña del administrador del programa. Cuando tomaron el software de la cuadro, la contraseña es \"nula\", y hoy es todavía \"null\". Por lo tanto el contenido de la base de datos están disponibles para cualquier persona en quien decide intentar conectarse a Internet el servidor de base de datos. Estos sitios están bajo ataque todo el tiempo y hace de la información obtener robado, sin que nadie ser más prudente,

Por otro lado, la misma gente que no compre en Internet porque son miedo de tener su información de tarjeta de crédito robada a no tener ningún problema de compra con esa misma tarjeta de crédito en una tienda de ladrillo y mortero, o pagando para el almuerzo, Cena, o bebidas con la tarjeta incluso en un back street bar o restaurante no toman a su madre. Crédito recibos de tarjeta robadas estos lugares todo el tiempo o pescaban de papeleras en el callejón. Y cualquier empleado sin escrúpulos o camarero puede anotar su nombre y información de la tarjeta, o utilizar un gadget disponible en Internet, un pasar de tarjeta dispositivo que almacena los datos de cualquier tarjeta de crédito pasa a través de él, para su posterior re

Hay algunos riesgos de compras en línea, pero es probablemente tan segura como compras en un almacén de ladrillos y mortero. Y las empresas de tarjetas de crédito ofrecen el mismo protección al utilizar su tarjeta en línea--si obtener cargos fraudulentos a la cuenta, sólo eres responsable de los primeros $50.
Así en mi opinión, miedo de compras en línea es sólo otro extraviado preocuparse.

Edgar no observe alguno de los varios signos reveladores que algo estaba mal con este correo electrónico (por ejemplo, el punto y coma después de la línea de saludo y el texto ilegible sobre \"nuestro servicio de cliente con excelente servicio\"). Él clic en el enlace, entró la información solicitada - nombre, dirección, teléfono crédito y número de la tarjeta de información - y se sentaron. volver a esperar a los cinco dólares crédito aparezca en su próxima factura de tarjeta de crédito. Lo que se mostró en cambio fue una lista de las cargas para los elementos nunca compró.

Analizando el timo
Edgar se tomó por una estafa de Internet comunes. Es una estafa que viene en una variedad de formas. Uno de ellos (detalladas en el capítulo 9) implica un inicio de sesión de señuelo pantalla creada por el atacante que parece idéntico a lo real. La diferencia es que la falsa pantalla no da acceso al sistema informático que el usuario está tratando de alcanzar, pero en su lugar se alimenta su nombre de usuario y contraseña para el hacker.

Edgar había tomado una estafa en la que los ladrones habían registrado un sitio Web con el nombre \"paypal-secure.com\"-que suena como si debería haber sido un

página segura en el sitio de PayPal legítimo, pero no está. Cuando entró información en este sitio, los atacantes tiene justo lo que querían.

MENSAJE DE MITNICK

Aunque no infalible (seguridad no es), cuando visita un sitio que pide información se considera privada, asegúrese siempre de que la conexión es autenticación y cifrado. Y aún más importante, hacer no automáticamente Haga clic en sí en cualquier cuadro de diálogo que puede indicar un problema de seguridad, como un inváli certificado digital ha caducado o ha sido revocado.

VARIACIONES SOBRE LA VARIACIÓN

¿Cuántas otras formas existen para engañar a los usuarios de computadoras a un falso ¿Sitio Web donde ofrecen información confidencial? No supongo que nadie tiene una respuesta válida, precisa, sino que \"mucha y mucho\" le servirá el propósito.

El eslabón perdido

Un truco aparece regularmente: enviar un correo electrónico que ofrece una tentadora razón para visita un sitio y proporciona un vínculo para ir directamente a ella. Excepto que el enlace no llevarle al sitio piensas que vas a, porque el vínculo sólo se asemeja a un enlace de ese sitio. Aquí es otro examen-circular que realmente se ha utilizado en Internet, otra vez caracterizadas por uso indebido del nombre PayPal:

www. PayPai. com

Un vistazo rápido, esto se ve como si dice PayPal. Incluso si la víctima advierte, él puede pensar que es sólo un ligero defecto en el texto que hace la \"I\" de la mirada de Pal como un There was an error deserializing the object of type System.String. Encountered unexpected characte

www. PayPal. com

¿utiliza el número 1 en lugar de una letra minúscula L? Hay bastante gente que Aceptar errores ortográficos y otra distracción para hacer este Gambito continuamente popular con bandidos de la tarjeta de crédito. Cuando la gente va al sitio falso, parece el sitio esperaban ir a, y entran alegremente su tarjeta de crédito información. Para configurar uno de estos sustos, un atacante sólo necesita registrar la nombre de dominio falso, enviar sus correos electrónicos y espere ventosas mostrar, listo al ser engañado.

A mediados de 2002, recibí un correo electrónico, al parecer era parte de una masa de correo 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 utilizarse con precaución.

MSG: eBay Estimado usuario,

Se ha vuelto muy notable que otra parte ha sido corromper a eBay
cuenta y ha violado nuestra política de usuario acuerdo figuran:

4. Pujar y comprar

Estás obligado a completar la transacción con el vendedor si compra un
elemento a través de uno de nuestro precio fijo formatos o es mejor postor descrito
a continuación. Si eres el mejor postor al final de la subasta (reunión de la
la puja mínima aplicable o requisitos de reserva) y su oferta es aceptada por la
vendedor, estás obligado a completar la transacción con el vendedor, o el
transacción está prohibido por ley o por el presente acuerdo.

Ha recibido este aviso de eBay porque ha llegado a nuestra atención que su
cuenta corriente ha provocado interrupciones con otros usuarios de eBay y eBay
requiere verificación inmediata de su cuenta. Por favor, compruebe su cuenta o
la cuenta puede ser deshabilitada. Haga clic aquí para verificar tu cuenta-
http:\/\/error ebay.tripod.com

Marcas y marcas registradas designadas son propiedad de sus respectivos dueños,
eBay y el logotipo de eBay son marcas comerciales de eBay Inc.

Las víctimas que ha hecho clic en el vínculo pasó a una página Web que parecía muy parecido
una página de eBay. De hecho, la página fue bien diseñada, con un logotipo de eBay auténtico,
y \"Examinar\", \"Vender\" y otros enlaces de navegación que, al hacer clic, tomaron al visitante
el sitio de eBay reales. También hubo un logotipo de seguridad en la esquina inferior derecha. Para
disuadir a la víctima más experimentada, el diseñador utilizó incluso codificación HTML para máscara
donde se ha enviado la información proporcionados por el usuario.

Es un excelente ejemplo de una ingeniería social malintencionado de basados en computadoras
ataque. Aún así, no era sin varios fallos.

El mensaje de correo electrónico no fue bien escrito; en particular, el párrafo que comienza
There was an error deserializing the object of type System.String. Encountered unexpected character 'i'.
bulos nunca contratan un profesional para editar su copia, y muestra siempre). También,
cualquiera que estaba prestando mucha atención se hubiera convertido en sospechoso sobre

eBay pidiendo información de PayPal del visitante; no hay ninguna razón eBay sería pida a un cliente esta información privada con una empresa diferente.

Y alguien conocedor de Internet probablemente sería reconocer que la hipervínculo conecta no al dominio de eBay pero para tripod.com, que es un servicio gratuito Servicio de alojamiento Web. Esto fue un regalo muerto que el correo electrónico no es legítimo. Aún así, apuesto a que mucha gente entró su información, incluyendo una tarjeta de crédito número, en esta página.

NOTA
¿Por qué personas pueden registrar engañosa o se los nombres de dominio?.
Debido a que bajo la actual ley y política on-line, cualquier persona puede registrar cualquier nombre de s
que ' ya no está en uso.
Las empresas intentan luchar contra este uso de direcciones de imitación, pero consideran que lo que está
contra. General Motors presentó demanda contra una empresa registrados
f**kgeneralmotors.com (pero sin los asteriscos) y señaló que la dirección URL
Sitio Web de General Motor. GM perdida.

Estar alerta
Como usuarios individuales de Internet, todos tenemos que estar alerta, haciendo un consciente decisión sobre cuando está bien introducir información personal, contraseñas, cuentas números, pasadores y similares.

¿Cuántas personas conoces que podría decirte si un particular Internet ¿página estás mirando cumple los requisitos de una página segura? Cuántos ¿empleados en su empresa saben qué buscar?

Todos los que usan la Internet deben saber que a menudo sobre el pequeño símbolo en algún lugar aparece en una página Web y se ve como un dibujo de un candado. Ellos debe saber que cuando se cierra el hasp, el sitio ha sido certificado como segura. Cuando el hasp está abierto o falta el icono de candado, el sitio Web no es autenticado como auténtica, y cualquier información transmitida es la clara--es decir, sin cifrar.

Sin embargo, un atacante consigue comprometer privilegios administrativos en un equipo de empresa puede ser capaz de modificar o parche para el código del sistema operativo cambiar la percepción del usuario de lo que realmente está sucediendo. Por ejemplo, la instrucciones de programación en el software del explorador que indican un sitio Web certificado digital es válido puede modificarse para omitir la comprobación. O el sistema podrían ser modificadas con algo llamado un kit de raíz, instalar uno o más atrás puertas a nivel de sistema operativo, que son más difíciles de detectar.

Una conexión segura autentica el sitio como auténtica y cifra el
información que se comunica, por lo que un atacante no puede hacer uso de cualquier información que
es interceptado. Puedes confiar en cualquier sitio Web, incluso uno que utiliza un seguro
¿conexión? No, porque el propietario del sitio puede no ser vigilante sobre la aplicación de todos los
parches de seguridad necesarios, o obligando a los usuarios o administradores respeten bueno
prácticas de la contraseña. Así que usted no puede asumir que cualquier sitio supuestamente seguro es
invulnerable a los ataques.

JERGA
PUERTA de atrás un punto de entrada encubierta que proporciona una forma secreta en un usuario
equipo que es desconocido para el usuario. También usado por los programadores, mientras que el desarro
un software programar para que pueden ir 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 autenticación (una
garantía de que se está comunicando con el auténtico sitio Web). Sin embargo, esto
mecanismo de protección no funciona para los usuarios que no prestar atención a
Si el nombre del sitio aparece en la barra de dirección es de hecho la dirección correcta del
el sitio que están intentando acceder.

Otro problema de seguridad, mayormente ignorada, aparece como un mensaje de advertencia que dice
algo así como \"este sitio no es seguro o el certificado de seguridad ha caducado. Hacer
desea ir al sitio de todos modos?\" Muchos usuarios de Internet no entienden la
mensaje, y cuando aparece, simplemente haga clic en OK o sí y continuar con
su trabajo, consciente de que pueden estar en arenas movedizas. Advertencia: en un sitio
no utilicen un protocolo seguro, nunca debe escribir cualquier confidencial
información como su dirección o número de teléfono, tarjeta de crédito o cuenta bancaria
números, o cualquier cosa que desee mantener en privado.

Thomas Jefferson dijo mantener nuestra libertad necesaria \"vigilancia eterna.\"
Mantener la privacidad y la seguridad en una sociedad que utiliza información como moneda
no requiere menos.

Convertirse en experto en Virus
Una nota especial sobre software antivirus: es esencial para la intranet corporativa, pero
También es esencial para cada empleado que utiliza un equipo. Más allá de simplemente tener anti
el software antivirus instalado en sus equipos, los usuarios obviamente necesitan tener la
software de encendido (que mucha gente no gusta porque inevitablemente retrasa
abajo algunas funciones de equipo).

Con antivirus software allí es otro procedimiento importante para mantener

mente, así: mantener definiciones de virus actualizadas. A menos que su empresa es configurar para distribuir software o actualizaciones a través de la red para cada usuario, cada cada usuario debe asumir la responsabilidad de descargar el último conjunto de virus definiciones por su propia cuenta. Mi recomendación personal es que todo el mundo establece la preferencias de software de virus para que se actualicen automáticamente nuevas definiciones de virus Todos los días.

JERGA
SECURE SOCKETS LAYER un protocolo desarrollado por Netscape que proporciona autenticación de cliente y servidor en una comunicación segura en la Internet.

En pocas palabras, eres vulnerable a menos que las definiciones de virus se actualizan periódicamente. Y aun así, todavía no está completamente a salvo de virus o gusanos que los anti las compañías de software de virus aún no conocen o no ha publicado aún una archivo de patrón de detección para.

Todos los empleados con privilegios de acceso remoto desde sus ordenadores portátiles o casa equipos que han actualizado el software antivirus y un firewall personal en los máquinas como mínimo. Un atacante sofisticado a mirar el panorama para buscar el eslabón más débil, y es donde él va a atacar. Recordando a las personas con equipos remotos con regularidad sobre la necesidad de personal firewalls y actualizado, software Active virus es una responsabilidad, porque no puede esperar trabajadores individuales, administradores, personal de ventas y otros alejados de una TI Departamento recordarán los peligros de dejar sus equipos desprotegidos.

Más allá de estos pasos, recomiendo encarecidamente el uso de los menos comunes, pero no menos paquetes de software importante, esa guardia contra ataques de troyanos, llamados software de Anti-Trojan. En el momento de escribir este artículo, dos de las más conocidas los programas son The Cleaner (www.moosoft.com) y barrido de defensa troyano (www.diamondcs.com.au).

Por último, lo que es probablemente el mensaje más importante de la seguridad de todos para las empresas que no buscar correos electrónicos peligrosos en el gateway de la empresa: desde todos tendemos a ser olvidadizo o negligente sobre cosas que parecen periféricas a obtener nuestros trabajos, los empleados necesitan recordar una y otra vez, en diferentes maneras, no abrir archivos adjuntos de correo electrónico a menos que estén seguros de que la fuente es una persona u organización que pueden confiar. Y también las necesidades de administración para recordar a los empleados que deben utilizar Trojan y software active virus software que proporciona protección valiosa contra el aparentemente fiable correo electrónico que puede contener una carga destructiva.

Capítulo 8
Mediante la simpatía, la culpabilidad y la intimidación

Como se explica en el capítulo 15, un ingeniero social utiliza la psicología de la influencia conducir su destino para cumplir con su solicitud. Ingenieros sociales son muy aptas desarrollar una artimaña estimula las emociones, como miedo, excitación o culpabilidad. Hacen esto mediante el uso de disparadores psicológicos--mecanismos automáticos que conducen personas para responder a las solicitudes sin un análisis profundo de todos los disponibles información.

Todos queremos evitar situaciones difíciles para nosotros y para otros. Sobre esta base impulso positivo, el atacante puede jugar en la simpatía de una persona, hacer que su víctima se sienten culpables, o utilizar la intimidación como un arma.

Aquí hay algunas lecciones de la escuela de postgrado en tácticas populares que juegan en el emociones.

UNA VISITA AL ESTUDIO
Has notado alguna vez cómo algunas personas pueden caminar a la guardia en la puerta decir, un salón de hotel donde algunos reunión, fiesta privada o lanzamiento de libro función está en marcha y sólo a pie pasado esa persona sin ser preguntado por su ¿billete o pase?

De la misma manera, un ingeniero social puede hablar en lugares que usted no habría creído posible - como el siguiente relato sobre la industria del cine aclara.

La llamada telefónica
Oficina de Ron Hillyard, se trata de Dorothy.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Desarrollo de animación en el personal de Brian Glassman. Gente segura haces cosas diferentes aquí\".
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Hacer por usted?\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
por la tarde para una sesión de tono y no sabe que estoy que de hablar sobre cada vez le en el lote. La gente aquí en la Oficina de Brian es muy agradable pero Odio a seguir molestando, cómo lo hago, cómo hacer que. Es como yo solo comenzó la secundaria y no puede encontrar mi camino al baño. Ustedes saben lo que significa?\"

Dorothy se rió.
There was an error deserializing the object of type System.String. Unexpected end of file. Following
obtener Lauren, decirle a que Dorothy dice que ella debe tener buena
cuidado de ustedes\".
Gracias, Dorothy. Y si no se encuentra la sala de la de hombres, puedo llamarte atrás!

Sonreí juntos sobre la idea y colgó.

Historia de David Harold
Me encanta el cine y cuando me mudé a Los Angeles, pensé que llegaría a
todo tipo de personas se reúnen en el negocio del cine y me llevaba a lo largo de Para
las partes y que me durante almuerzo en los estudios. Bueno, estuve allí durante un año, me
fue pasando a veintiséis años de edad, y el más cercano conseguí iba en el
Gira de estudios Universal con toda la gente bonita de Phoenix y Cleveland.
Así que finalmente que lo consiguió al punto donde pensé, si ellos no me invitan, te invito
yo mismo. Que es lo que hice.

He comprado una copia de los Angeles Times y lea la columna de entretenimiento
hace un par de días y escribió los nombres de algunos productores en diferentes
estudios. Decidí que sería tratar de golpear primero en uno de los grandes estudios. Así que llamé a la
panel de control y pidió a la Oficina de este productor ya había leído acerca de la
papel. La Secretaria que respondió sonaba el tipo maternal, así que pensé
había conseguido suerte; Si algún joven que estaba allí esperando que ella sería
descubierto, ella probablemente no me habría dado la hora del día.

Pero esta Dorothy, ella sonaba como alguien que tuviera en un gatito callejero,
alguien que podría sentir pena por el chico nuevo que estaba sintiendo un poco abrumado
en el nuevo puesto de trabajo. Y seguro que tengo sólo el toque justo con ella. No es todos los días le
intentar engañar a alguien y te dan más que le pidieron. Fuera de
lástima, ella no sólo me dio el nombre de una de las personas en seguridad, pero dijo
debe decirle a la señora que Dorothy quería ayudarme.

Por supuesto había planeado usar nombre de Dorothy de todos modos. Esto hizo aún mejor.
Lauren abrió bien y nunca siquiera molestado para buscar el nombre dio a
ver si realmente era la base de datos del empleado.

Cuando condujo hasta la puerta de esa tarde, no sólo tenía mi nombre el
lista de visitantes, incluso tuvieron un espacio de estacionamiento para mí. Tuve un almuerzo tardío en el
Comisario y vagó el lote hasta el final del día. Incluso colado en un
par de sonido etapas y visto películas de tiro ellos. No dejar hasta 7
o ' Clock. Fue uno de mis días más emocionantes jamás.

Analizando el timo

Todo el mundo fue una vez un nuevo empleado. Todos tenemos recuerdos de lo que primero día era como, sobre todo cuando éramos jóvenes y sin experiencia. Cuando un nuevo empleado pide ayuda, puede esperar que muchas personas--especialmente básico personas--se recuerdan sus propios sentimientos de new kid on the block y salir de su manera de echar una mano. El ingeniero social lo sabe y entiende puede utilizarlo para jugar en las simpatías de sus víctimas.

Ponemos demasiado fácil para los forasteros estafar a su manera en nuestra empresa plantas y oficinas. Incluso con guardias en las entradas y los procedimientos de inicio de sesión para quien no es un empleado alguno de varias variaciones en el ardid utilizado Esta historia permitirá un intruso obtener tarjeta de visitante y caminar derecho en. Y ¿Si su empresa requiere que los visitantes ser acompañado? Es una buena regla, pero es sólo efectivo si sus empleados son verdaderamente conciencia acerca de detener a alguien con o sin tarjeta de un visitante que se encuentra en su propia y le cuestionan. Y entonces, si las respuestas no son satisfactorias, sus empleados tienen que estar dispuestos a Póngase en contacto con seguridad.

Haciéndolo demasiado fácil para los extranjeros a 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 que se cierne sobre nuestra sociedad, es algo más que información que podría estar en peligro.

HÁGALO AHORA

No todos los que usan tácticas de ingeniería social están un brillante ingeniero social. Alguien con conocimientos de un interno de una empresa determinada puede activar peligroso. El riesgo es aún mayor para cualquier empresa que posee en sus archivos y bases de datos cualquier información personal acerca de sus empleados, que, por supuesto, la mayoría las empresas hacen.

Cuando los trabajadores no educados o entrenados para reconocer los ataques de ingeniería social, gente decidida como la dama jilted en la siguiente historia puede hacer cosas personas más honestas parece imposibles.

Historia de Doug

Cosas no habían ido tan bien con Linda de todas formas, y yo sabía que en cuanto Conocí a Erin que ella fue para mí. Linda es, así, un poco... bueno, algo no exactamente inestable pero ella especie de puede ir en el extremo profundo cuando ella se molesta. Le dije a su como suaves como pude que tenía que salir, y ayudó a su paquete y incluso dejarla tomar un par de los CDs de Queensryche que fuese mia de verdad. Tan pronto como que se había ido me fui a la ferretería de un nuevo bloqueo de Medico poner el puerta de frente y ponerlo en esa misma noche. A la mañana siguiente me llama el teléfono la compañía y había cambiar mi teléfono número y de hecho inédito.

Que me dejaron libre a perseguir a Erin.

Historia de Linda
Yo estaba dispuesto a dejar, de todas formas, sólo no decidió cuándo. Pero a nadie le gusta sentirse rechazado. Así que era sólo una cuestión de, ¿qué podría hacer para hacerle saber qué imbécil ¿fue?

No tarda mucho en averiguar. Tiene que haber otra chica, de lo contrario él no de me envió embalaje con tanta prisa. Así que sería justo esperar un poco y luego iniciar llamándole la tarde. Ustedes saben, todo el tiempo menos desearían a llamarse.

Esperó hasta el próximo fin de semana y llamado alrededor de 11 en la noche del sábado. Sólo había cambiado su número de teléfono. Y el nuevo número fue oculta. Que sólo muestra qué clase de SOB el chico era.

No era tan grande de un revés. Empecé hurgaba entre los papeles que había logró llevar a casa justo antes de que dejé mi trabajo en la compañía telefónica. Y allí fue--había guardado un billete de reparación de una vez cuando hubo un problema con el línea telefónica de Doug y la impresión de la lista el cable y el par de su teléfono. Ver, puede cambiar su número de teléfono todos desea, pero todavía tiene el mismo par de cables de cobre desde su casa a la compañía telefónica Oficina de conmutación, llamadda Central Oficina o CO. El conjunto de cables de cobre desde todas las casas y apartamentos es identificados por estos números, llamados el cable y el par. Y si sabes Cómo la compañía telefónica hace cosas, que hago, sabiendo el cable del destino y es par todo lo que necesita saber el número de teléfono.
Tenía una lista de todos los COs de la ciudad, con sus direcciones y teléfonos números. Busqué el número de CO en el barrio donde ME Solía vivir con Doug jerk y se llama, pero, naturalmente, nadie estaba allí. ¿Dónde está el guardarrail cuando realmente lo necesita? Me llevo todos sobre veinte segundos para idear un plan. Comenzó a llamar alrededor a otro COs y finalmente encuentra a un chico. Pero fue a millas de distancia y fue probablemente sentado allí con los pies arriba. Sabía que no quiere hacer lo que necesitaba. Yo estaba dispuesto con mi plan.
There was an error deserializing the object of type System.String. End element 'root' from namespace ' unidad de paramédico ha disminuido. Tenemos un técnico de campo tratando de restaurar servicio, pero él no se encuentra el problema. Necesitamos que a la unidad sobre la Webster CO inmediatamente y ver si tenemos que salir de la Oficina central de tono de marcado.

Y entonces yo le dije, ' te llamaré cuando llegue allí, \"porque por supuesto ME no podía tenerlo llamando al centro de reparación y preguntando por mí.

Yo sabía que él no quiere abandonar la comodidad de la Oficina central de paquete y vaya raspar hielo frente a su parabrisas y la unidad a través de la para sobornos por la noche. Pero fue una emergencia, por lo que él no podía decir exactamente que estaba demasiado ocupado. Cuando llegué a él cuarenta y cinco minutos más tarde en el Webster CO, le dije Para comprobar cable 29 par demillonesde y él caminaban a la llama y comprueban y dijeron, Sí, hubo tono de marcado. Que por supuesto ya sabía.

Así, entonces que me dijo, \"Está bien, necesito hacer un LV,\" que significa línea de verificación, que se le pedía para identificar el número de teléfono. Lo hace marcado un número especial que Lee atrás el número llamó desde. Él no saber nada acerca de si es un número no cotizado o es justbeen cambiado, por lo que hizo lo pedí y me escuchó el número que se anuncian en conjunto de prueba de su liniero. Hermosa. Todo esto había trabajado como un encanto.

Yo le dije, \"Bueno, el problema debe estar fuera en el campo,\" como ya sabía el,, umber todo junto. Yo le agradeció y le dijo que sería seguir trabajando en él y dijo bueno noche.

MENSAJE DE MITNICK

Una vez que un ingeniero social sabe cómo funcionan las cosas dentro de la empresa de destino, se se convierte en fáciles de usar ese conocimiento para desarrollar la relación con legítimo empleados. Las empresas deben prepararse para ataques de ingeniería social de empleados actuales o anteriores que pueden tener un hacha para moler. Antecedentes puede ser útil para desestimar las perspectivas que pueden tener una propensión hacia esta tipo de comportamiento. Pero en la mayoría de los casos, estas personas será extremadamente difíciles detectar. La salvaguardia sólo razonable en estos casos es aplicar y auditoría procedimientos de verificación de identidad, incluyendo la situación laboral de la persona, previa a divulgar cualquier información a cualquier persona no personalmente sabe que aún con el empresa.

Tanto para Doug y tratando de esconder de mí detrás de un número no cotizado.
La diversión estaba a punto de comenzar.

Analizando el timo

La joven dama en esta historia fue capaz de obtener la información que quería llevar cabo su venganza porque ella tenía dentro de conocimiento: los números de teléfono, procedimientos y la jerga de la compañía telefónica. Con ella no logró sólo averiguar un número de teléfono nuevo, están ocultos, pero fue capaz de hacerlo en medio de un noche invernal, enviando a un guardarrail teléfono persiguiendo a través de la ciudad para ella.

SR. BIGG QUIERE ESTO
Una forma de intimidación--popular en gran medida popular y altamente eficaz
porque es tan simple--se basa en que influyen en el comportamiento humano mediante el uso de la autori

Sólo el nombre del asistente en la Oficina del CEO puede ser valioso. Privada
investigadores y cazadores de cabeza incluso hacen esto todo el tiempo. Te llaman la
operador de panel de control y decir quieren estar conectado a la Oficina del CEO.
Cuando el Secretario o respuestas de asistente Ejecutiva, te dicen que tienen un
documento o paquete para el CEO o si envía un archivo adjunto de correo electrónico,
imprimirlo? O otro te preguntan, ¿cuál es el número de fax? Y por cierto,
¿Cómo te llamas?

A continuación, llaman a la siguiente persona y decir, \"Jeannie en la Oficina del Sr. Bigg me dijo que
llamarle para que me pueda ayudar con algo.\"

La técnica se denomina name-dropping, y generalmente es usado como un método para
rápidamente establecer rapport por influir en el destino de creer que el atacante
conectado con alguien en autoridad. Es más probable que hacer un favor un destino
alguien que conoce a alguien que sabe.

Si el atacante tiene sus ojos en información altamente confidencial, podrá utilizar esta
tipo de enfoque para agitar emociones útiles en la víctima, como el temor de contraer
problemas con sus superiores. Este es un ejemplo.

Historia de Scott
Scott Abrams.

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
y él es más que un poco infeliz. Dice que envió una nota hace diez días
personas fueron obtener copias de todos su investigación de penetración de mercado a nosotros para
análisis. Nunca tuvimos algo.\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following
¿Qué departamento Estás en?\"
There was an error deserializing the object of type System.String. Encountered unexpected character '\'".
Estoy solo en mi camino a una reunión. Permítanme obtener su número de teléfono
y... \"

El atacante ahora sonado a verdaderamente frustrado: \"es que lo que
tú quieres que diga el Sr. Biggley?! Escucha, él espera que nuestro análisis por la mañana
mañana y nos tienen que trabajar con él esta noche. Ahora, quieres que le diga

no podía hacerlo porque no podíamos recibimos el informe de usted, o desea contar lo que usted mismo?. \"

Un enojado CEO puede arruinar su semana. El objetivo es probable que decida que quizá esto es algo que mejor cuidan antes él entra en esa reunión. Otra vez el ingeniero social ha presionado el botón derecho para obtener la respuesta que quería.

Analizando el timo

El ardid de intimidación con referencia a la autoridad funciona especialmente bien si la otra persona está en un nivel bastante bajo en la empresa. El uso de un importante nombre de la persona no sólo supera reticencia normal o sospecha, pero a menudo hace que la persona deseoso de agradar; es el instinto natural de querer ser útil multiplica cuando piensas que la persona que está ayudando es importante o influyente.

Sin embargo, el ingeniero social sabe que lo mejor es cuando se ejecuta este particular engaño a utilizar el nombre de una persona a un nivel superior del jefe de la persona. Y este Gambito es complicado utilizar dentro de una organización pequeña: el atacante no desea que su víctima haciendo una oportunidad de comentar el VP de marketing. \"Enviaron el tenías ese chico me llaman, de plan de marketing de producto\"demasiado fácilmente puede producir un respuesta de \"Qué plan de marketing? ¿Qué chico?\" Y que podría conducir a la descubrimiento de que la empresa ha sido victimizada.

MENSAJE DE MITNICKS

Intimidación puede crear un miedo del castigo, que influyen en la gente a cooperar. Intimidación puede plantear también el temor de la vergüenza o de ser descalificado de esa nueva promoción.

Deben ser capacitados que es no sólo aceptable sino esperado desafío autoridad cuando la seguridad está en juego. Formación de seguridad de información debe incluir enseñanza personas cómo desafiar la autoridad de formas orientado al cliente, sin dañar las relaciones. Además, esta expectativa debe apoyarse en la arriba a abajo. Si un empleado no va a ser copia de seguridad para personas exigentes independientemente de su condición, la reacción normal es parar desafiante--sólo el lo contrario de lo que desea.

¿QUÉ SABE LA ADMINISTRACIÓN DE SEGURIDAD SOCIAL LE

Nos gusta pensar que los organismos gubernamentales con les nos tenga la información bloqueado con seguridad lejos de personas 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.

Puede llamada de Linn
Lugar: Oficina regional de la administración de Seguridad Social
Tiempo: 1 0:1 8 de la mañana el jueves por la mañana

Tres mod. Esto es posible Linn Wang.

La voz en el otro extremo del teléfono sonaba apologético, casi tímido.

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
¿llamar 'Mayo'?
There was an error deserializing the object of type System.String. Encountered unexpected chara
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
el equipo aún y ahora tiene un proyecto prioritario y él está usando minas.
Somos el Gobierno de los Estados Unidos, para cryin'en voz alta, y dicen
no tienen suficiente dinero en el presupuesto para comprar un equipo para este chico a utilizar.
Y ahora piensa que mi jefe estoy quedando atrás y no quiere escuchar las excusas,
sabes?\"

Sé lo que quiere decir, todos los derechos.
There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
el sistema informático para buscar información sobre los contribuyentes.
¿Sin duda, es necesario what'cha?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
04\/07\/69.\" (Alphadent significa que la búsqueda de equipo para una cuenta
alfabéticamente por contribuyente nombre, más identificado por fecha de nacimiento.)

Después de una breve pausa, pregunta:

¿Qué necesita saber?
There was an error deserializing the object of type System.String. Encountered unexpected character 'h
abreviatura para el número de seguridad social. Ella leerlo fuera.
Está bien, te necesito hacer una numident en ese número de cuenta,
dijo que el llamador.

Fue una petición de ella leer los datos básicos del contribuyente y puede Linn
respondió dando lugar del contribuyente de nacimiento, apellido de soltera de la madre, y
nombre del padre. El llamador escuchó pacientemente mientras ella también le dio el mes y
año que se emitió la tarjeta y que fue emitido por la Oficina del distrito.

A continuación pidió un DEQY. (Pronunciado \"DECK-wee\", es corto
para \"consulta detallada ganancias.\")

La solicitud DEQY trajo la respuesta, \"de qué año?\"
El llamador respondió, \"Año 2001\".
Puede Linn dijo, \"el monto era de $190.286, el ordenante fue MicroTech Johnson\".
¿Los otros salarios?
Lol
There was an error deserializing the object of type System.String. Encountered unexpected characte
Luego intentó organizar a llaman cuando necesita información y no podía
llegar a su equipo, utilizando nuevamente el truco favorito de los ingenieros sociales de siempre
tratando de establecer una conexión de modo que él puede seguir volviendo a la misma
persona, evitando la molestia de tener que encontrar una marca nueva cada vez.

There was an error deserializing the object of type System.String. Encountered unexpected character 's'.
boda.» Cualquier otro momento, ella haría lo que pudiera.

Cuando ella pone el teléfono hacia abajo, puede Linn sintió bien que había sido capaz de ofrecer
un poco de ayuda a un funcionario apreciado compañero.

Historia de Keith Carter
Para juzgar de las películas y de delincuencia más vendida novelas, un privado
investigador es corto sobre ética y mucho conocimiento de cómo obtener los hechos jugosos
en las personas. Hacen esto mediante métodos completamente ilegales, mientras que apenas
gestión evitar obtener detenido. La verdad, por supuesto, es que la mayoría PIs
empresas totalmente legítimas. Dado que muchos de ellos empezaron su vida laboral como
juramento agentes del orden, saben perfectamente lo que es legal y lo
no es y más no son tentados a cruzar la línea.

Sin embargo, hay excepciones. De hecho caben algunas Pis - más que unos pocos - el
molde de los chicos en las historias de crimen. Estos chicos son conocidos en el comercio como
agentes de información, un término amable para personas que están dispuestos a romper las reglas.
Saben que pueden obtener cualquier asignación de hecho mucho más rápido y mucho
más fácil si sacan algunos accesos directos. Que estos accesos directos resultan ser potenciales
delitos que se les podrían aterrizar tras las rejas durante unos pocos años no parece disuadir a
los más inescrupulosos.

Mientras tanto el lujo PIs--quienes trabajan fuera de una suite de Oficina de lujo en un
Alquiler de gran parte de la ciudad--no hacer este tipo de trabajo ellos mismos. Simplemente contratan
algunos corredores de información para hacer por ellos.

El chico que llamaremos Keith Carter era el tipo de ojo privado no comprometido por
ética.

Fue un caso típico de \"Donde esconde el dinero?\" O a veces tiene
There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
sabe donde su marido había escondido su dinero (aunque, por qué una mujer con
dinero nunca se casa con un chico sin fue un acertijo Keith Carter pregunta ahora
y, a continuación, pero nunca había encontrado una buena respuesta para).

En este caso el esposo, cuyo nombre era Joe Johnson, fue el mantenimiento de una la
dinero en hielo. \"Era un chico muy inteligente que había comenzado una empresa de alta tecnología
con diez mil dólares que tomados de la familia de su esposa y construido en un
firma de cien - millones de dólares. De acuerdo con su abogado de divorcio, había hecho un
impresionante trabajo de ocultar sus bienes y el abogado quería un resumen completo.

Keith figuró que su punto de partida sería la administración de la Seguridad Social,
dirigidas a sus archivos sobre Johnson, lo cual estaría llena de gran utilidad
información para una situación como ésta. Armados con sus informaciones, Keith podría pretender
el destino y los bancos, las empresas de corretaje y instituciones extraterritoriales para contar
él todo.
Fue su primera llamada telefónica a una Oficina de distrito local, utilizando el mismo 800 número que
utiliza cualquier miembro del público, el número que aparece en la libreta de teléfonos local. Cuando
un empleado entró en la línea, Keith pidió estar conectado a alguien en reclamaciones.
Espera otro y luego una voz. Ahora Keith desplazado engranajes; \"Hola,\" comenzó. \"Esto es
Gregory Adams, Oficina del distrito de 329. Escucha, estoy tratando de llegar a un ajustador de reclamaci
que controles de cuenta de una número termina en 6363, y el número que tengo va a
una máquina de fax\".

There was an error deserializing the object of type System.String. The token 'true' was expected but fou

A continuación llamó Mod 2. Cuando Linn puede responder, cambió de sombreros y fui
a través de la rutina de ser desde la Oficina del Inspector General y la
problema sobre alguien más tener que utilizar su equipo. Ella le dio la
información que estaba buscando y decidieron hacer lo que ella podía cuando él
necesita ayuda en el futuro.

Analizando el timo
Lo que hizo este planteamiento eficaz fue la obra de la simpatía del empleado con
la historia acerca de que otra persona use su equipo y \"mi jefe no está contento con
Me\". Personas no mostrar sus emociones en el trabajo muy a menudo; cuando lo hacen, puede
rollo derecho sobre otra persona ordinaria defensas contra la ingeniería social
ataques. La estratagema emocional de \"estoy en problemas, no me puedes ayudar?\" fue todo lo
llevó a ganar el día.

Inseguridad social
Increíblemente, la administración de la Seguridad Social ha enviado una copia de su entera Manual de operaciones del programa en la Web, atiborrada con información útil para su pueblo, pero también increíblemente valiosos sociales ingenieros. Contiene abreviaturas, jerga e instrucciones de cómo solicitar lo que desee, como se describe en esta historia.

¿Desea obtener más información acerca de la administración de Seguridad Social interna? Simplemente busca en Google o escriba a 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 cuando leas esto, encontrará las instrucciones on-line que incluso dar información detallada sobre los datos que se puede otorgar a un empleado de SSA la comunidad de aplicación de la ley. En términos prácticos, esa comunidad incluye cualquier ingeniero social que puede convencer a un empleado de SSA que él es de una aplicación de la ley Organización. El atacante no podría haber sido exitoso en la obtención de este información de uno de los secretarios que maneja llamadas telefónicas de la general público. El tipo de ataque Keith utiliza sólo funciona cuando la persona en la el extremo receptor de la llamada es alguien cuyo número de teléfono no está disponible para la deben ser público, y que por lo tanto, tiene la expectativa de que nadie llama alguien en el interior--otro ejemplo de seguridad speakeasy'. Los elementos ayudó a este ataque al trabajo incluye:

Conocer el número de teléfono para el Mod.

Conocer la terminología que utilizaban--numident, alphadent y DEQY.

Pretendiendo ser de la Oficina del Inspector General, que cada federal empleado de Gobierno sabe como una agencia de investigación de todo el Gobierno con amplios poderes. Esto da al atacante un aura de autoridad.

Una Pilota interesante: los ingenieros sociales parecen saber cómo hacer solicitudes por lo que casi nadie nunca piensa, \"¿por qué llaman me ' - aun cuando Lógicamente; habría hecho más sentido si la llamada se había ido a algún otro persona en algún departamento completamente diferente. Tal vez simplemente ofrece como una romper la monotonía de la rutina diaria para ayudar a la persona que llama que la víctima descuentos parece inusual forma de la llamada.
Finalmente, el atacante en este incidente, no satisfecho con la obtención de la información sólo para el caso que nos ocupa, querido establecer un contacto podría llamar el regularmente. Él de lo contrario podría haber sido capaz de utilizar una táctica común para el ataque de simpatía-- There was an error deserializing the object of type System.String. Encountered unexpected character 'T'. teclado puede sustituirse en un día.
Por lo tanto utilizó la historia acerca de alguien que otra persona use su equipo, que podía cadena razonablemente por semanas: \"Yep, pensé que iba a tener su propio equipo

llegó ayer, pero uno en y otro chico tirado algún tipo de acuerdo y lo
en su lugar. Así que este joker es todavía aparezca en mi cubículo.\" Y así sucesivamente.

Pobre me, necesito ayuda. Funciona como un encanto.

UNA SIMPLE LLAMADA
Uno de los obstáculos principales del atacante es hacer su petición razonable de sonido
algo típico de pide que vienen hasta en la jornada de trabajo de la víctima, algo
que no ponen a la víctima fuera demasiado. Como con un montón de otras cosas en la vida,
haciendo una solicitud suena lógico puede ser un desafío, que un día, pero la próxima, puede
ser un pedazo de pastel.

Llamada Mary H
Fecha y hora: el lunes, 23 de noviembre, 7:49
Lugar: Mauersby

A la mayoría de la gente, trabajos de contabilidad es número crunching y recuento de frijol,
generalmente visto como unos tan agradable como tener un canal de raíz. Afortunadamente,
no todo el mundo ve el trabajo de este modo. Mary Harris, por ejemplo, encontró su trabajo
como un contable senior absorbente, parte de la razón fue uno de los más
empleados de contabilidad dedicados a ella
empresa.

Sobre este particular lunes, Mary llegó temprano para obtener una ventaja en lo que ella
espera a ser un día largo y se sorprendió al encontrar su timbre de teléfono. Ella
recogí y dio su nombre.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
soporte técnico para su empresa. Hemos iniciado un par de quejas durante el fin de semana
de las personas que tienen problemas con los equipos allí. Pensé que podía
solucionar problemas antes de que todo el mundo entra en trabajo esta mañana. ¿Tiene
cualquier problema con el equipo o la conexión a la red?\"

Ella le dijo que no sabía aún. Ella encendida su equipo y mientras era
arranque, explicó lo que quería hacer.

There was an error deserializing the object of type System.String. End element 'root' from namespace " e
las pulsaciones de tecla que escribe, y queremos seguro van a través de la red
correctamente. Así que cada vez que escriba un trazo, quiero que me diga lo que es, y I'll
ver si la misma letra o número es aparecer aquí. Okay?\"

Con visiones de pesadilla de su equipo no funciona y un día frustrante de no ser capaz de hacer cualquier trabajo, ella estaba más que feliz con la ayuda de este hombre su. Después de unos momentos, ella le dijo: \"tengo la pantalla de inicio de sesión, y voy a Escriba en mi ID. Yo estoy escribiendo ahora--M...A...R....Y...F.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. contraseña pero no me digas lo que es. Nadie no diga nunca su contraseña, ni soporte técnico. Sólo voy a ver asteriscos aquí--es tu contraseña protegido por lo que no puedo ver it ': nada de esto era cierto, pero tenía sentido a María. Y luego dijo, \"Déjame saber una vez que el equipo ha puesto en marcha\".
Cuando dijo que se estaba ejecutando, tuvo su abierto dos de sus aplicaciones y ella informó que lanzaron \"bien\".

Mary se siente aliviada al ver que todo parecía estar funcionando normalmente. Peter dijo: \"me alegro que pude hacer seguro que podrás utilizar tu equipo está bien. Y \"escuchar, añadió,\" acaba de instalar una actualización que permiten a la gente a cambiar sus contraseñas. ¿Estaría dispuesto a tomar un par de minutos conmigo, por lo que puede ¿ver si conseguimos que funcione bien?

Fue agradecido por la ayuda que había dado y fácilmente de acuerdo. Peter habló ella a través de los pasos del lanzamiento de la aplicación que permite al usuario cambiar contraseñas, un elemento estándar del sistema operativo Windows 2000. \"Go por delante e introduzca su contraseña, \"le dijo. \"Pero no olvide decir que fuera fuerte.\"

Cuando ella había hecho eso, Pedro dijo, \"sólo para esta prueba rápida, cuando le pregunta por su nueva contraseña, escriba 'test123'. A continuación, escriba de nuevo en la casilla de verificación, y Haga clic en entrar.\"

Le caminó a través del proceso de desconexión del servidor. Él tuvo su esperar un par de minutos y, a continuación, conectar de nuevo, esta vez intentando iniciar sesión con ella nueva contraseña. Funcionó como un encanto, Pedro parecía muy complacido y le habló a través de cambiar a su contraseña original o elegir uno nuevo--una vez más le advirtió de no decir la contraseña en voz alta.

There was an error deserializing the object of type System.String. Encountered unexpected character 'P'. Si ningún problema, simplemente llame aquí en Arbuckle. Estoy generalmente en proyectos especiales pero alguien que pueden ayudarle a respuestas\". Ella le agradeció a y dijeron adiós.

Historia de Peter
La palabra había metido sobre Peter--un número de personas en su Comunidad que había ido a la escuela con él había oído que convirtió en algún tipo

de un genio de la computadora que a menudo puede encontrar información útil que otras personas no se pudo obtener. Cuando Alice Conrad le vino a pedir un favor, dijo no al principio. ¿Por qué debería él ayudar? Cuando él se topó con ella una vez e intentó pedir una fecha, ella había rechazó fría.

Pero su negativa a ayudar no parecía le sorprende. Dijo que ella no pensaba que era algo que podía hacer de todos modos. Fue como un desafío, porque por supuesto estaba seguro que podía. Y que fue cómo llegó a
de acuerdo.
Alice había ofrecida un contrato para algún trabajo de consultoría para un marketing empresa, pero los términos del contrato no parecían muy bueno. Antes de que ella regresó a piden un mejor trato, ella quería saber qué términos otros consultores en sus contratos.

Se trata de cómo Peter narra la historia.

No digo que Alice pero bajé de la gente que me quiere hacer algo no creo que pudiera, cuando supe que sería fácil. Bueno, no fácil, exactamente, no A esta hora. Sería necesario un poco de hacerlo. Pero que estaba bien.

Podría mostrar su qué inteligente trataba realmente.

Un poco después 7:30 el lunes por la mañana, llamé a las oficinas de la empresa de marketing y obtuvo al recepcionista, dijo que estaba con la empresa que maneja su pensión planes y necesita hablar con alguien en contabilidad. Advirtió si alguno de los ¿Contabilidad personas aún no habían llegado? Ella dijo: \"creo que vi a Mary vienen en unos pocos hace minutos, voy a tratar le para usted.\"

Cuando María recogió el teléfono, le dije mi pequeña historia sobre el equipo problemas, que fue diseñado para darle el nerviosismo por lo que estaría encantado de cooperar. Tan pronto como le había hablado a través de cambiar su contraseña, yo entonces rápidamente registran en el sistema con la misma contraseña temporal había pedido a utilizar, test123.

Aquí es donde la maestría viene--he instalado un pequeño programa que me permitió acceso sistema informático de la empresa, siempre he querido, utilizando un contraseña secreta de mi propia. Después colgaron con Mary, fue mi primer paso para borrar la auditoría camino por lo que nadie sabría incluso había estado en su sistema. Era fácil. Después de elevar mis privilegios de sistema, fui capaz de descargar un libre programa llamado clearlogs que encontré en un seguridad - relacionados sitio Web en www.ntsecurity.nu.

Tiempo para el trabajo real. Corrí a buscar los documentos con el contrato de palabra\" el nombre de archivo y los archivos descargados. Entonces busqué más y llegó la veta madre--el directorio que contiene todos los pagos de consultor informes. Así que me juntar todos los archivos de contrato y una lista de pagos.

Alice podría poros a través de los contratos y ver cuánto estaban pagando otros consultores. Dejarla hacer el donkeywork de exageradas a través de todos esos archivos. Tuve hacer lo que me pregunta.
Desde los discos puse los datos, imprimido por lo que algunos de los archivos ella pudo mostrar la evidencia. Hizo conocerme y comprar la cena. Usted debe han visto su rostro cuando ella thumbed a través de la pila de documentos. \"No way\", ella dijo. \"No way\".

No traigo los discos. Eran el cebo. Dijo que ella tendría que venir para obtenerlos, esperando quizás ella quiere mostrar su gratitud por el favor le hice.

MENSAJE DE MITNICK
Es increíble lo fácil que es para que un ingeniero social para que la gente a hacer cosas basadas sobre cómo estructura la solicitud. La premisa es desencadenar una respuesta automática basado en principios psicológicos y dependen de la toma del pueblo de atajos mentales Cuando perciben el llamador como aliado.

Analizando el timo
Llamada a la empresa de marketing de Peter representa la forma más básica de ingeniería social--un intento simple que necesitan poca preparación, trabajó en el primer intento y tomó sólo unos minutos para que.

Aún mejor, Mary, la víctima no tenía ninguna razón para pensar que cualquier tipo de truco o treta había desempeñado en ella, ninguna razón para presentar una denuncia o plantear un ruckus.

El esquema funcionó a través del uso de Peter de tres tácticas de ingeniería social. Primero obtuvo cooperación inicial de Mary generando miedo--hacerla pensar que ella equipo no sea utilizable. Luego tomó el tiempo para tenerla a abrir dos de ella aplicaciones así que ella podría ser segura estaban trabajando muy bien, fortalecimiento de la relación entre los dos de ellos, un sentido de ser aliados. Finalmente, consiguió que le mayor cooperación para la parte esencial de su tarea jugando con su agradecimiento por la ayuda que había proporcionado en asegurarse de que su equipo estaba bien.

Diciéndole ella no debería nunca revele su contraseña, no debe revelar incluso él, Peter hizo un trabajo exhaustivo pero sutil de convencerla de que le preocupaba

sobre la seguridad de los archivos de su empresa. Esto aumenta la confianza que él debe ser legítimo, porque él era proteger a ella y la empresa.

LA POLICÍA RAID

Imagen esta escena: el Gobierno ha estado tratando de poner una trampa para un hombre llamado Arturo Sánchez, quien ha estado distribuyendo películas gratis por Internet. El Estudios de Hollywood dicen que está violando sus derechos de autor, dice que él está tratando de empujar a reconocer un mercado inevitable por lo que podrá empezar a hacer algo acerca de hacer nuevas películas disponibles para su descarga. (Correctamente) señala Esto podría ser una enorme fuente de ingresos para los estudios que parecen ser ignorando completamente.

Buscar orden, por favor

Casa tarde una noche, él comprueba las ventanas de su apartamento desde a través de la calle y los avisos de las luces están apagados, aunque siempre deja uno en cuando él sale.

Él libras y golpea en la puerta de un vecino, hasta que el hombre despierta y aprende hubo de hecho una redada policial en el edificio. Pero hicieron los vecinos quedarse abajo, y él aún no seguro qué apartamento que entraron. Él sólo sabe dejaron llevar algunas cosas pesadas, sólo ellos estaban envueltos arriba y él no podía decir lo que eran. Y no tener a nadie en esposas.

Arturo comprueba su apartamento. La mala noticia es que existe un documento de la policía que requieren que llame de inmediato y solicitar una cita para una entrevista dentro de tres días. La peor noticia es que sus equipos están desaparecidos.

Arturo se desvanece en la noche, va a quedar con un amigo. Pero la incertidumbre Roe en él. ¿Cuánto sé la policía? Han ellos atrapados con él en ¿por último, pero le dejó una oportunidad de huir? O esto es acerca de algo más completo, ¿algo que puede aclarar sin tener que salir de la ciudad?

Antes de leer sobre, pararse a pensar por un momento: se puede imaginar cualquier forma le ¿puede averiguar lo que la policía sabe sobre usted? Suponiendo que no tienes ninguna hacer contactos políticos o amigos en el departamento de policía o la Fiscalía s, te imaginas que hay alguna forma de que usted, como un ciudadano cualquiera, podría conseguir esto ¿información? ¿O puede que incluso alguien con conocimientos de ingeniería social?

Timos de la policía

Arturo satisfecha su necesidad de saber como esta:, obtuvo el teléfono número de un almacén cercano de copia, llamó y pidieron su número de fax.

Entonces llamó a la Fiscalía y pidieron registros. Cuando tenía
conectado con la Oficina de registros, presentó a sí mismo como un investigador con
Condado de Lake y dijo que necesitaba hablar con el empleado que archivos activos
mandamientos.

There was an error deserializing the object of type System.String. The token 'true' was expected but fou
sospechoso anoche y yo estoy intentando localizar la declaración jurada.\"

There was an error deserializing the object of type System.String. Encountered unexpected characte

Dio su dirección, y ella sonaba casi emocionada. \"Oh, sí,\" ella barbotear, \"me
saber que uno. \"El autor Caper.'\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.

Ah, lo tengo aquí.

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
Servicio en este caso si yo quince minutos. He sido tan despistado últimamente, salí
el archivo en su casa y me no voy nunca hacerla ida y vuelta en el tiempo. Pude obtener copias
de usted?\"

Seguro, no hay problema. Voy a hacer copias; puede venir justo encima y recogerlo.

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
posible usted podría fax les a mí?\"

Que creó un pequeño problema, pero no insuperables. \"No tenemos un fax
aquí en registros,\"dijo. \"Pero tienen uno abajo en la Oficina del empleado
ellos podrían permitirme usar.\"

Dijo, \"Déjame llamar a Oficina del empleado y configurarlo\".

La dama en la Oficina del Secretario dice que alegraría a cuidar de él pero quería
saber \"Quién va a pagar?\" Necesitaba un código contable.

There was an error deserializing the object of type System.String. Encountered unexpected character
Entonces llamó a la Oficina del DA, nuevamente se identificó como oficial de policía y
simplemente pide al recepcionista, \"¿Qué es el código contable para oficina del DA?\"
Sin dudarlo, le dijo.
Llamar a volver a la Oficina del empleado para proporcionar el número de cuentas le dio el
excusa para manipular la dama un poco más: le habló a caminar
arriba para obtener copias de los documentos a ser enviado por fax.

NOTA
¿Cómo sabe un ingeniero social los detalles de operación tantos: policía
departamentos, oficinas de fiscales, prácticas de compañía de teléfono, la organización de
específico las empresas se encuentra mapos útil en sus ataques, tales como
¿telecomunicaciones y equipos? Porque es su negocio para averiguar. Esto
el conocimiento es un stock de ingenieros sociales en el comercio porque la información puede ayudar a
él en sus esfuerzos por engañar.

Cubriendo sus huellas
Arturo todavía tenía un par de pasos a seguir. Siempre existe la posibilidad
que alguien huele algo sospechoso, y podría llegar a la tienda de copia
para encontrar una pareja de detectives, vestida casualmente y tratando de buscar ocupado hasta
alguien apareció pidiendo ese fax particular. Esperó un rato y luego
devolver la llamada Oficina de empleado para verificar que la señora había enviado el fax. Muy bien has

Llamó a otro almacén de copia de la misma cadena a través de la ciudad y utiliza el ardid
acerca de cómo fue \"complacido con su manejo de un trabajo y desea escribir la
Administrador de una carta de felicitación, ¿cuál es su nombre?\" Con esa pieza esencial
de la información, llamada la primera tienda de copia nuevamente y dijo que quería hablar con
el administrador. Cuando el hombre recogió el teléfono, Arturo dijo: \"Hola, esto es Edward
en tienda 628 de Hartfield. Mi jefe, Anna, me dijo que le llamemos. Tenemos un
cliente que es todo molesto--alguien le dio el número de fax de la tienda equivocada.
Aquí está esperando un fax importante, sólo el número le dieron es para tu
tienda.\" El Gerente se comprometió a tener uno de su pueblo busque el fax y enviarlo
a la tienda inmediatamente de Hartfield.

Arturo ya estaba esperando en la segunda tienda cuando el fax llegó allí. Vez
lo tenía en la mano, llamado de vuelta a la Oficina del empleado para decirle a las señora gracias, y
\"No es necesario traer esas copias espalda arriba, sólo puede tirarlos
lejos ahora.\" Entonces llamó el administrador en la primera tienda y le dijo, también,
tirar su copia del fax. De esta manera sería cualquier registro de lo que
había tenido lugar, en caso de que alguien más tarde llegaron alrededor de preguntas.
Los ingenieros sociales saber que nunca puede ser demasiado cuidadoso.

Dispuestas de esta manera, Arturo incluso no tiene que pagar en la primera tienda de copia
para recibir el fax y enviando nuevamente a la segunda tienda. Y si se
resultó que la policía aparezco en la primera tienda, Arturo ya sería
tiene su fax y durante mucho tiempo se ha ido por el momento podría organizar a la gente la
segunda ubicación.

El final de la historia: la declaración jurada y orden demostraron que tenía la policía bien
pruebas documentadas de actividades de copia de la película de Arturo. Eso fue lo que

es necesario saber. Antes de la medianoche, él había cruzado la línea de Estado. Arturo fue en el camino a una nueva vida, con una nueva identidad, lista empezar de nuevo en algún otro en su campaña.

Analizando el timo

Las personas que trabajan en cualquier Oficina del distrito, en cualquier lugar, se encuentran en constante Póngase en contacto con oficiales de policía--respondiendo a preguntas, hacer arreglos, teniendo mensajes. Nadie suficientemente orgulloso para llamar y pretenden ser un oficial de policía, sheriff adjunto, o lo que es probable que se adoptará en su palabra. A menos que sea evidente que él no conoce la terminología, o si está nervioso y tropiezos en sus palabras, o de alguna otra manera no suena auténtico, él puede incluso no pedirá una sola pregunta para verificar su reclamación. Eso es exactamente lo que sucedió aquí, con dos diferentes trabajadores.

MENSAJE DE MITNICK

La verdad del asunto es que nadie es inmune a ser engañado por un bien social ingeniero. Debido a que el ritmo de vida normal, no siempre tomamos el tiempo decisiones reflexivos, incluso sobre cuestiones que son importantes para nosotros. Complicado situaciones, falta de tiempo, el estado emocional o fatiga mental puede fácilmente distraernos. Así que tomamos un atajo mental, tomar nuestras decisiones sin analizar la información cuidadosamente y completamente, un proceso mental conocido como automático responder. Esto es cierto incluso para la aplicación de la ley federal, estatal y local funcionarios. Somos todos humanos.

Obtención de un código de carga necesaria fue manejada con una sola llamada de teléfono. A continuació Arturo jugó la Carta de simpatía con la historia acerca de \"una reunión con el secreto Servicio en quince minutos, he sido chiflado y dejó en casa el archivo. \" Ella Naturalmente sintió lástima por él y salió de su manera de ayudar.

A continuación, utilizando no uno, sino dos tiendas de copia, Arturo hizo extra seguro cuando fue a recoger el fax. Una variación de esto que hace aún más el fax difícil hacer un seguimiento: en lugar de tener el documento enviado a otro almacén de copia, el atacante puede dar lo que parece ser un número de fax, pero realmente es una dirección en un servicio de Internet que recibirá un fax para usted y reenviará automáticamente a gratuito tu dirección de correo electrónico. De este modo se puede descargar directamente al atacante equipo y él nunca tiene que mostrar su cara cualquier sitio donde alguien podría más tarde poder identificarlo. Y la dirección de correo electrónico y número de fax electrónico pueden ser abandonado tan pronto como ha cumplido la misión.

CONVERTIR LAS TABLAS

Un joven llamo Michael Parker fue una de esas personas que averiguado un poco tarde que el los puestos de trabajo van principalmente a personas con títulos universitarios. Él

tuvo la oportunidad de asistir a una universidad local en una beca parcial más educación
préstamos, pero significaba trabajar noches y fines de semana para pagar su alquiler, comida, gas, y
seguro de automóvil. Michael, quien siempre le gustaba encontrar atajos, quizá se pensó
fue otra forma, uno que paga más rápido y con menos esfuerzo. Porque tenía
sido aprendiendo acerca de equipos desde el momento en que llegó a jugar con uno a diez años
y quedó fascinado con averiguar cómo funcionaban, decidió ver si él
podría \"crear\" su propia acelerado licenciatura en Ciencias de la computación.

Graduarse--sin honores

Él pudo haber roto en los sistemas informáticos de la Universidad estatal, se encuentra el
registro de alguien que se había graduado con una bonita B + o a la media, copiadas la
grabar, poner su nombre en ella y añadió que los registros de ese año
clase graduanda. Pensar esto, de alguna manera sentirse incómodo acerca de la idea,
se dio cuenta que debe haber otros registros de un estudiante después de haber sido el campus--
registros de pago de matrícula, la Oficina de vivienda y quién sabe qué más. Crear
sólo el registro de cursos y grados deja demasiadas lagunas.

Conspirar, sintiendo su camino, llegó a lo que podría llegar a su
gol de ver si la escuela tenía un graduado con el mismo nombre que el suyo, que había
obtuvo un título de ciencia de equipo en cualquier momento durante un período adecuado de años. Si
así, podría simplemente poner abajo el número de seguridad social de los otros Michael Parker en
formularios de solicitud de empleo; cualquier empresa que comprueba el nombre y social
seguridad número con la Universidad que se dijo que, sí, tenía la
grado reclamada. (No sería evidente para la mayoría de la gente pero era obvio que le
que él podría poner un número de seguridad social en la aplicación de trabajo y entonces, si
contratado, poner su propio número real sobre las formas de nuevo empleado. Mayoría de las empresas
nunca pensaría comprobar si un nuevo empleado había utilizado un número diferente
anteriormente en el proceso de contratación.)

Registro de problemas

¿Cómo encontrar a un Michael Parker en los registros de la Universidad? Pasó sobre ella como
esto:

Ir a la biblioteca principal en el campus de la Universidad, se sentó en un equipo
terminal, levantó en Internet y acceder a la página Web de la Universidad. Él entonces
llamado Oficina del Secretario. Con la persona que respondió, viajó a través de una
las rutinas de la ingeniería social familiar por ahora: \"estoy llamando desde el
Centro de cómputo, estamos haciendo algunos cambios a la configuración de red y
nosotros queremos asegurarnos de que no
interrumpir su acceso. Servidor que conecta a?\"

There was an error deserializing the object of type System.String. Unexpected end of file. Followi

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
información.

La respuesta, admin.rnu.edu, le dio el nombre del equipo donde estudiante
los registros se almacenan. Esta fue la primera pieza del rompecabezas: ahora conocía su
equipo de destino.

JERGA
TERMINAL tonta un terminal que no contiene su propio microprocesador.
Terminales tontas sólo pueden aceptar comandos simples y mostrar caracteres de texto
y los números.

Él ha escrito la URL en el equipo y no obtuve respuesta--como se esperaba, hubo
un cortafuegos bloqueando el acceso. Así que corrió un programa para ver si se puede conectar a cualquie
de los servicios que se ejecutan en el equipo y encontró un puerto abierto con un Telnet
servicio en ejecución, que permite a una computadora para conectarse remotamente a otro
equipo y acceder a ella como si directamente conectado con una terminal tonta. Todos le
tendría que obtener acceso sería la contraseña e ID de usuario estándar.

Hizo otra llamada a la Oficina del Secretario, este tiempo escuchando cuidadosamente para hacer
seguro que él estaba hablando con una persona diferente. Obtuvo a una dama, y nuevamente afirmó
ser de centro de cómputo de la Universidad. Fueron instalando una nueva producción
sistema de registros administrativos, le dijo. Como un favor, le gustaría a conectar
el nuevo sistema, aún en modo de prueba, para ver si ella podía acceder estudiante académico
registros bien. Él le dio la dirección IP para conectar y hablado le a través de la
proceso.

De hecho, la dirección IP llevó el equipo Michael estaba sentado en el
Biblioteca del campus. Mediante el mismo proceso descrito en el capítulo 8, él había creado un
simulador de inicio de sesión--una señuelo signo en la pantalla--buscando al igual que el uno era
acostumbrados a ver cuando va en el sistema de registros de los estudiantes. \"No es
\"trabajando, le dijo. \"Mantiene diciendo ' Inicio de sesión incorrecto.

Por ahora el simulador de inicio de sesión había alimentado las pulsaciones de su nombre de cuenta y
contraseña para Michael s terminal; Misión cumplida. Le dijo, \"Oh, algunos de
las cuentas aún no se han señalado más aún en este equipo. Me deja configurar tu
cuenta y me voy contactarle.\" Cuidado con Atando cabos sueltos, como cualquiera
experto ingeniero social debe ser, haría un punto de teléfono más tarde a
decir que no funcionaba el sistema de ensayo derecho todavía, y si fue bien con ella,
se llaman volver a ella o de otra gente cuando había averiguado
¿Cuál fue la causa del problema.

El Secretario útil

Ahora Michael sabía qué sistema informático que necesitaba para acceder, y tuvo un ID y contraseña del usuario. Pero él qué comandos sería necesario a fin de buscar el archivos para obtener información sobre Ciencias de la computación gradúan con el nombre correcto y ¿fecha de graduación? La base de datos del estudiante sería una propiedad, creada en campus para satisfacer las necesidades específicas de la Universidad y el Secretario Oficina y tendría una forma única de acceso a la información en la base de datos.

Primer paso en esta última valla de compensación: averiguar quién podía guiar le a través de la Misterios de buscar en la base de datos del estudiante. Llamó a la Secretaría de nuevamente, esta vez llegando a una persona diferente. Fue desde la Oficina del Decano de ingeniería, dijo a la señora, y preguntó, \"que supone que piden rues ayuda cuando tenemos problemas para acceder a la estudiante académico.

Minutos más tarde estaba en el teléfono con el administrador de base de datos de la Universidad, tirando de la ley de simpatía: \"yo soy Mark vendedores, en la Oficina del Secretario. Te apetece ¿teniendo lástima sobre un chico nuevo? Siento que estar llamando usted pero están todos en una reunión por la tarde y no hay nadie alrededor que me ayude. Necesito recuperar una lista de todos graduados con un grado de ciencia de computadora, entre 1990 y 2000. Necesitan al final del día y si no tenerlo, no puedo tener este trabajo por mucho tiempo. Le ¿dispuesto a ayudar a un chico en apuros\"? Ayudar a la gente fue parte de lo que esta Administrador de base de datos, lo que fue paciente adicional como hablaba paso de Michael por hicieron paso a través del proceso.

Por el momento que colgó, Michael había descargado toda la lista de equipo titulados en Ciencias para esos años. Dentro de unos minutos él había ejecutar una búsqueda, encuentran a dos Michael Parkers, elegido uno de ellos y obtuvo social de guy número de la seguridad, así como otra información pertinente que se almacenan en la base de datos.

Sólo se había convertido en \"Michael Parker, Licenciatura en Ciencias de la computación, graduado con honores, 1998.\" En este caso, el \"B.S.\" procedía únicamente.

Analizando el timo

Este ataque utiliza una treta no he hablado antes: el atacante pidiendo la Administrador de base de datos de la organización le caminar los pasos de ejecución no sabía cómo hacer un proceso de equipo. Un potente y eficaz pasando de las tablas, esto es el equivalente de pedir el propietario de una tienda para ayudar a llevas un cuadro que contiene elementos que sólo haya sustraído sus estanterías fuera a su coche.

MENSAJE DE MITNICK

Los usuarios de computadoras son a veces desorientados acerca de las amenazas y vulnerabilidades asociado de ingeniería social que existe en nuestro mundo de la tecnología. Ellos tener acceso a la información, pero falta el conocimiento detallado de lo que podría resultar para ser una amenaza para la seguridad. Un ingeniero social tendrá como objetivo a un empleado que tien comprensión de cómo valiosa la información que se busca es, por lo que es el destino más probable a solicitud del extraño.

PREVENIR LA CON

Simpatía, la culpabilidad y la intimidación son tres disparadores psicológicos muy populares utilizado por el ingeniero social y estas historias han demostrado las tácticas en acción. Pero ¿qué puede hacer para evitar estos tipos de ataques de tu empresa?

Protección de datos

Algunas historias en este capítulo hacer hincapié en el peligro de enviar un archivo a alguien no sabes, aun cuando esa persona es (o parece ser) un empleado y la se envía archivo internamente, con un equipo de dirección o impuestos de correo electrónico dentro de la empresa.

Política de seguridad de la empresa debe ser muy específico sobre las salvaguardias para entrega de datos valiosos a nadie personalmente no conoce al remitente. Exigente procedimientos deben establecerse para transferir archivos con información confidencial. Cuando la solicitud es de alguien conocido no personalmente, deben haber clara pasos a seguir para su verificación, con diferentes niveles de autenticación dependiendo de la sensibilidad de la información.

Aquí están algunas técnicas a tener en cuenta:

Establecer la necesidad de saber (que pueden requerir autorización de la propietario de información designado).

Mantener un registro personal o departamental de estas transacciones.

Mantener una lista de personas que han sido especialmente capacitadas en los procedimientos y que son de confianza para autorizar el envío de información confidencial. Sólo requieren estas personas se puede enviar información a cualquier persona fuera del grupo de trabajo.

Si se realiza una solicitud de los datos por escrito (correo electrónico, fax o correo) complementarias medidas de seguridad para verificar que la solicitud procede realmente de la persona que aparece al provenir.

Acerca de contraseñas

Todos los empleados que son capaces de acceder a cualquier información confidencial--y hoy que significa prácticamente cada trabajador que utiliza un equipo--necesitan entender actos simples como cambiar su contraseña, incluso durante unos instantes, pueden conducir a una infracción de seguridad importantes.

Necesidades de formación de seguridad cubrir el tema de las contraseñas, y que tiene que centrarse en sobre cuándo y cómo cambiar la contraseña, lo que constituye un aceptable contraseña y los peligros de dejar que alguien más se involucren en el proceso. La formación debe transmitir a todos los empleados que deben ser especialmente sospechoso de cualquier solicitud implica sus contraseñas.

En la superficie parece ser un simple mensaje para transmitir a los empleados. Tiene no, porque apreciar esta idea requiere que los empleados entender cómo un simple actúan como cambio de contraseña puede conducir a un compromiso de seguridad. Puede indicar un niño \"Look both ways antes de cruzar la calle,\" pero hasta que el niño comprenda ¿por qué es importante, que usted está confiando en la obediencia ciega. Y normas que requerían ciego obediencia son normalmente ignorado u olvidado.

NOTA

Las contraseñas son esos centro de ataques de ingeniería social que dedicamos un separar la sección el tema en el capítulo 16, donde encontrará específicos políticas recomendadas en la administración de contraseñas.

Un punto Central de informes

Su política de seguridad debe proporcionar una persona o un grupo designado como una central para informes de actividades sospechosas que parecen ser intenta infiltrarse en el punto 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 a hacer estos informes siempre debe cerrar a mano para que empleados no tengan que cavar pues si se convierten en sospechosos que está produciendo un ataque.

Proteja su red

Los empleados necesitan entender que es el nombre de un equipo servidor o red información no trivial, sino puede dar a un atacante conocimientos esenciales que le ayuda a ganar confianza o busque la ubicación de la información que desea.

En particular, personas como administradores de base de datos que trabajan con software pertenecen a esta categoría de personas con experiencia en tecnología, y que necesitan para operan bajo reglas especiales y muy restrictivas sobre la verificación de la identidad de personas que les piden información o asesoramiento.

Personas que ofrecen regularmente cualquiera. tipo de necesidad de ayuda de equipo a ser capacitados en qué tipo de solicitudes deben ser las banderas rojas, sugiriendo que el llamador puede ser el intento de un ataque de ingeniería social.

Cabe señalar, sin embargo, desde la perspectiva del administrador de bases de datos en la última historia en este capítulo, el llamador cumplieron los criterios para ser legítimo: él estaba llamando desde en el campus, y obviamente estaba en un sitio que requiere un nombre de cuenta y contraseña. Esto sólo hace claro una vez más la importancia de tener procedimientos estandarizados para verificar la identidad de alguien que solicita información, especialmente en un caso como este donde el llamador estaba pidiendo ayuda en obtener acceso a los registros confidenciales.

Todo de este Consejo va doble para colegios y universidades. No es una noticia que equipo de hacking es un pasatiempo favorito para muchos de los estudiantes universitarios, y debería también no ser ninguna sorpresa estudiante registros--y a veces facultad, así como-- son un blanco tentador. Este abuso es tan galopante que algunas corporaciones realmente considerar campus un ambiente hostil y crear reglas de cortafuegos que bloquean acceso de las instituciones educativas con direcciones que terminan en. edu.

El largo y corto de él es que todos los registros de estudiantes y personal de cualquier tipo debe considerarse como principales blancos de ataque y deben ser bien protegidos como información confidencial.

Consejos de formación
Mayoría de los ataques de ingeniería social es ridículamente fácil para defenderse... para quien lo que busca sabe.

Desde la perspectiva empresarial, existe una necesidad fundamental para la buena formación. Pero también hay una necesidad de algo más: una variedad de formas para recordar lo que han aprendido.

Utilizar pantallas de bienvenida que aparecen cuando se enciende el ordenador del usuario, con una mensaje de seguridad diferentes cada día. El mensaje debe ser diseñado para que se no desaparecerá automáticamente, pero requiere que el usuario haga clic en algunos tipos de reconocimiento de que ha leído.

Otro enfoque que recomiendo es iniciar una serie de avisos de seguridad. Frecuentes mensajes de aviso son importantes; un programa de sensibilización debe ser constante y interminable. En la entrega de contenido, los avisos no deben ser redactada en la misma en cada instancia. Los estudios han demostrado que estos mensajes son más efectivamente recibido cuando varían en redacción o cuando se utiliza en diferentes ejemplos.

Un método excelente es usar extractos cortos en el boletín de la empresa. Esto
no debe ser una columna completa sobre el tema, aunque sería una columna de seguridad
Sin duda ser valiosa. En su lugar, insertar una dos o tres-columna-todo el diseño,
algo así como un pequeño mostrar anuncios en su periódico local. En cada número de la
Boletín, presentar un nuevo aviso de seguridad de esta manera corta, captura de atención.

Capítulo 9
El aguijón inverso

El aguijón, mencionado en otra parte en este libro (y en mi opinión, probablemente el mejor película que s se han hecho acerca de una operación con), expone su complicado trazado en detalle fascinante. La operación en la película es una representación exacta de cómo timadores superiores ejecutan \"el alambre,\" uno de los tres tipos de principales estafas que se denomina There was an error deserializing the object of type System.String. End element 'root' from namespace '' barriendo en una gran cantidad de dinero en una sola noche, no hay ningún libro de texto mejor.

Pero los inconvenientes tradicionales, cualquiera que sea su truco particular, ejecutar según un patrón. A veces un ardid se trabajó en la dirección opuesta, que se llama un invertir sting. Esto es un giro interesante en el que el atacante configura la situación para que la víctima pide el atacante para obtener ayuda, o un trabajador co ha hecho un solicitud, que responde al atacante.
¿Cómo funciona esto? Vas a averiguar.

JERGA
REVERSO picar una estafa en la que la persona siendo atacada pide el atacante para obtener ayuda

EL ARTE DE LA PERSUASIÓN AMISTOSA
Cuando la persona promedio evoca la imagen de un hacker de computadora, lo que Normalmente viene a la mente es la imagen uncomplimentary de un solitario, introvertida Nerd cuyo mejor amigo es su equipo y que tiene dificultades para llevar a cabo un conversación, excepto por mensajería instantánea. El ingeniero social, que a menudo ha habilidades de hacker, también tiene el don de gentes en el extremo opuesto del espectro--bien desarrollar habilidades para utilizar y manipular a la gente que le permita su manera de hablar en obtener información de maneras usted nunca hubiera creído posible.

Llamador de Angela
Lugar: Rama Valle, Banco Federal Industrial.
Hora: 11:27

Angela Wisnowski respondió una llamada telefónica de un hombre que dijo que estaba casi para recibir una considerable herencia y él querían información sobre los diferentes tipos de cuentas de ahorro, certificados de depósito y cualquier otras inversiones ella podrían sugerir que sería seguro, pero ganar interés decente. Ella explicó que hay varias opciones y preguntó si le gustaría venir y sentarse con ella para discutir sobre ellos. Salía en un viaje tan pronto como la dinero llegó, él dijo y había mucho de arreglos para hacer. Así empezó sugerir algunas de las posibilidades y dándole detalles de los tipos de interés,

¿Qué sucede si vende un CD pronto, y así sucesivamente, al intentar fijar abajo su metas de inversión.

Ella parecía estar haciendo progresos cuando dijo, \"Oh, lo siento, tengo que tomar esto otra llamada. ¿A qué hora puedo terminar esta conversación con ustedes por lo que puedo hacer algunos ¿las decisiones? Cuando sale para el almuerzo?\" Ella le dijo 12:30 y dijo que intentaría para volver a llamar antes de entonces o al día siguiente.

Llamador de Louis
Los bancos grandes usan códigos de seguridad interna que cambian cada día. Cuando alguien de información de las necesidades de una rama de otra rama, demuestra que ha titulado la información, demostrando que sabe código del día. Para un agregado grado de flexibilidad y seguridad, algunos grandes bancos emiten múltiples códigos día. En un traje de costa oeste llamaré Industrial Banco Federal, cada empleado encuentra una lista de cinco códigos para el día, identificado como A E, en su equipo cada mañana.

Lugar: mismo.
Hora: 12:48 '.M., el mismo día.

Louis Halpburn no creo nada de ella cuando en esa tarde, llegó una llamada de un Llame al igual que otros que maneja regularmente varias veces por semana.

\"Hola,\" dijo el llamador. \"Esto es Neil Webster. Estoy llamando desde la rama 3182 Boston. Angela Wisnowski, favor.\"
Ella está en el almuerzo. ¿Puedo ayudar?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el clientes\".

El llamador sonaba como él había había tenido un mal día.

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. pila de ellos hacer, es casi 4 aquí y estoy supone estar fuera de esto lugar para ir a una cita médica en media hora\".

La manipulación--dando todas las razones por qué la otra persona debe sentir pena para él--era parte del ablandamiento de la marca. Continuó, \"quien llevó mensaje de teléfono, el número de fax es ilegible. Es la 213-algo. ¿Qué tiene el resto?\"

Louis le dio el número de fax, y el llamador dijo, \"bien, gracias.
Antes de que yo puedo fax esto, necesito pedirle código B.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
obtendría el mensaje.

Esto es bueno, pensó el llamador. Es tan genial cuando personas no caen en la primera
empujón suave. Si, no resisten un poco, el trabajo es demasiado fácil y podría empezar a recibir
perezoso.

A Luis, dijo, \"tengo un gestor de rama que sólo esté paranoico sobre
obtener verificación antes de enviar nada fuera, es todo. Pero escucha, si no lo hace
nos necesita para enviar por fax la información, es bueno. No hace falta verificar.\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'L'.
atrás.\"
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
identificar esto como una solicitud legítima por darme el código. Si no estoy a enfermos
mañana llamaré le entonces.\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Voy a contar ella trató de enviarlo pero no dio el código, ¿vale?\"

Luis renunció bajo presión. Un suspiro audible de molestia llegó volando
su camino hacia abajo de la línea telefónica.

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
quieres?\"
There was an error deserializing the object of type System.String. The token 'true' was expected
Poner la llamada en espera y luego en un poco recogido la línea otra vez. \"Es la 3184.\"

No es el código correcto.
Sí es--B 3184.
No digo B, dije e.
¡ Oh, maldita. Espera un momento.
Otra pausa mientras miraba nuevamente los códigos.
E es 9697.
9697--derecho. Voy a tener el fax en el camino. ¿Vale?
Seguro. Gracias.

Llamada de Walter
Banco Federal industrial, se trata de Walter.
There was an error deserializing the object of type System.String. The token 'true' was expected but found
necesario para extraer la tarjeta de una sig en una cuenta de cliente y me por fax\". La tarjeta de sig,
o tarjeta de firma, tiene algo más que la firma del cliente también tiene
identificar la información, elementos conocidos como el número de seguridad social, fecha de

nacimiento, apellido de soltera de la madre y a veces incluso el número de licencia de conducir. Muy útil para un ingeniero social.

Sure thing. ¿Qué es código C?

There was an error deserializing the object of type System.String. The token 'true' was expected but found
B y e y recuerdo aquellos. Me preguntan una de las personas.\"

¿Está bien, lo que tiene E?

E es 9697.

Unos minutos más tarde, Walter por fax la tarjeta sig lo solicitado.

Llamada de Donna platija
Hola, esto es el Sr. Anselmo.
¿Cómo puedo yo ayudarle hoy?
There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
se han acreditado todavía?\"
¿Usted es un cliente del Banco?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
escribió.\"
El número es 800-555-nuestro.

Está bien, gracias.

Cuento de Vince Capelli
Hijo de un policía de la calle de Spokane, Vince sabía desde una edad temprana que no era van a pasar su vida esclavista largas horas y arriesgar su cuello para mínimo salario. Sus dos principales objetivos en la vida se convirtió en salir de Spokane y entrar en negocios por sí mismo. Las risas de sus homies a través de secundaria sólo le dispararon hasta más--pensaban era hilarante que él fue tan roto en no iniciar su propio negocio pero tenía idea qué negocio podría ser.

Secretamente Vince sabía que tenían razón. Lo único que fue bueno estaba jugando Catcher en el equipo de béisbol de escuela secundaria. Pero no lo suficientemente bueno como para captur beca universitaria, ninguna manera suficientemente buena para el béisbol profesional. Y qué ¿negocio fue él va a poder iniciar?

Una cosa que los chicos en grupo de Vince nunca bastante averiguados: nada uno de ellos tuvo---un nuevo cuchillo navaja, un ingeniosa par de guantes cálidos, una sexys nueva novia si Vince, había admirado antes durante mucho tiempo el tema era suyo. Él no roba o colar a espaldas de nadie; no tenía a. El chico que tenía que

renunciar voluntariamente, y entonces pregunto después de lo ocurrido. Incluso pidiendo Vince no habría metido usted en cualquier lugar: no sabía él mismo. Personas simplemente parecen dejarle tener lo que quería.

Vince Capelli fue un ingeniero social desde una edad temprana, a pesar de que él nunca había escuchado el término.

Sus amigos detuvo riéndose una vez que todos tenían diplomas de escuela secundaria en la mano. Mientras que los otros semicongelados alrededor de la ciudad en busca de empleos donde no tienes que decir \"Do you want fries con eso?\" Papá de Vince le enviado a hablar con un viejo CP PAL que había abandonado la fuerza para iniciar su propio negocio de investigación privada en San Francisco. Rápidamente había descubierto talento de Vince para el trabajo y lo llevó.

Eso fue hace seis años. Odiaba la parte sobre la obtención de las mercancías infiel los cónyuges, que implicaba arqueadas mitigar horas de sesión y viendo, pero sintió continuamente desafiado por asignaciones desenterrar información de activos para abogados intentando averiguar si algún miserable rígido fue lo suficientemente rico como para ser digno de demanda Estas asignaciones le dieron un montón de posibilidades para utilizar su ingenio.

Como el tiempo tuvo que investigar las cuentas bancarias de un chico llamado Joe Markowitz. Joe había trabajado quizás un negocio turbio en un único amigo suyo, que amigo ahora quería saber, si él demandó, era Markowitz vaciar suficiente que ¿el amigo podría obtener su espalda de dinero?

Primer paso de Vince sería averiguar al menos uno, pero preferiblemente dos, de la códigos de seguridad del Banco para el día. Que suena como un reto casi imposible: Lo que en tierra induciría un empleado de banco para cubrir un tranquilizador en su propio ¿sistema de seguridad? Pregúntese--si quería hacer esto, tendría alguna idea ¿de cómo hacerlo?
Para gente como Vince, es demasiado fácil.

Personas confían en TI si conoces el interior jerga de su trabajo y su empresa. Tiene como muestra pertenece a su círculo íntimo. Es como un apretón de manos secreto.

Gran parte de no era necesario para un trabajo como éste. Definitivamente no es cirugía cerebral. Todos de necesario para empezar era un número de sucursales. Cuando marcan el Beacon Street Oficina en Buffalo, el chico que respondió sonaba como un cajero.

There was an error deserializing the object of type System.String. End element 'root' from namespace '' e hacia abajo. \"¿Cuál es el número de sucursales allí?\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele ¿estúpido porque justo había marcado el número de teléfono, no me? \"Número de sucursal\".

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. Porque no es información confidencial, está escrito en apenas alrededor de cada pedazo de papel utilizan.

Paso dos, llame a la sucursal donde mi destino hizo su banca, obtener el nombre de uno de su gente y Averigüe cuándo sería la persona fuera para el almuerzo. Angela. Sale a las 12:30. Hasta ahora, bien.

Paso tres, devolver la llamada a la misma rama durante almuerzo de Angela, de decir que me llamando desde el número de sucursal tal-y-tal en Boston, Angela necesita esto información por fax, gimme un código para el día. Esta es la parte difícil; es donde el goma cumple el camino. Si estaba haciendo hasta una prueba ser un ingeniero social, pondría algo como esto, donde la víctima obtiene sospechoso--por buena razón-- y sigues palo allí hasta que se le rompe y obtener la información necesidad. No puede hacerlo por recitar las líneas de un guión o una rutina de aprendizaje llegó a ser capaz de leer su víctima, captura su estado de ánimo, le jugar como un pez de inicio donde dejó escapar una pequeña línea y tambores, dejar salir y tambores. Hasta que le llegue la red y el flop le en el barco, splat!

Así lo y tuvo uno de los códigos para el día. Un gran paso. Con la mayoría los bancos, uno es todo que utilizan, por lo que habría sido huir de casa. Banco Industrial de la Federal utiliza cinco, por lo que sólo uno de cada cinco es probabilidades de largo. Con dos de los cinco, tuve tienen una mejor oportunidad de obtener mediante el siguiente acto de este drama poco. ME encanta esa parte de \"no decir b decía e.\" Cuando funciona, es hermosa. Y se trabaja la mayor parte del tiempo.

Conseguir un tercero hubiera sido aún mejor. He logrado obtener tres en una sola llamada--\"B\", \"D\" y \"E\" sonido tanto tanto que te llevarás malinterpreta nuevamente. Pero tienes que estar hablando con alguien que tiene un pushover real. Este hombre no estaba. Me gustaría ir con dos.

Los códigos del día sería mi trump para obtener la tarjeta de firma. He llamado y el chico pide un codigo. C quiere y yo sólo tenemos b y e. Pero no es el final de la Mundial. Consiguió permanecer fresco en un momento como este, sonido seguro, mantener en va Real suave, jugué lo con el sobre, \"alguien está usando mi equipo, me preguntan uno de estos otros.\"

Estamos todos los empleados de la misma empresa, estamos todos en este conjunto, hacen fácil en el hombre--es lo que está esperando que la víctima está pensando en un momento como este. Y tocó lo justo por la secuencia de comandos. Tomó una de las opciones que me ofrecieron, dio él la respuesta correcta, envió el fax de la tarjeta de firma.

Casi casa. Una llamada más me dio el número 800 que utilizan los clientes para la automatizado de servicio donde una voz electrónica le lee a la información piden. De la tarjeta de sig, tenía todos los números de cuenta de mi destino y su PIN número, porque ese banco utiliza los primeros cinco o cuatro últimos dígitos de lo social número de la seguridad. De la pluma en la mano, llamé a los 800 número y tras unos minutos de apretar botones, tenía el último saldo en cuatro cuentas de guy y sólo buena medida, su más reciente depósitos y retiros en cada uno.

Todo lo que había pedido mi cliente y mucho más. Siempre me gusta darle un poco extra buena medida. Mantener a los clientes satisfechos. Después de todo, el negocio es lo que mantiene ¿una operación que va derecho?

Analizando el timo
La clave de todo este episodio fue obtener los códigos de ese día y a hacer que el atacante, Vince, utiliza varias técnicas diferentes.

Comenzó con un poco arm-twisting verbal cuando Louis demostró reacio a dar él un código. Luis tenía razón sospechar--los códigos están diseñados para utilizarse en la dirección opuesta. Sabía que en el flujo normal de las cosas, el desconocido llamador podría estar dándole un código de seguridad. Este fue el momento crítico para Vince, él depender que dependía el éxito completo de su esfuerzo.

Ante la sospecha de Louis, Vince simplemente sentado lo con manipulación, utilizando un llamamiento a la solidaridad (\"ir al médico\") y la presión (\"tengo una pila de do, su casi 4\") y la manipulación (\" decirle no darme la código\"). Inteligentemente, Vince no hace realmente una amenaza, él sólo una implícita: Si usted no me dan el código de seguridad, no enviar la información del cliente que su necesita trabajador co, y te voy a decir ella habría enviarlo pero usted no cooperar.

Aún así, vamos a no ser demasiado apresurada en culpar a Louis. Después de todo, la persona en el teléfo sabía (o al menos parecen saber) trabajador co Angela había solicitado un fax.
El llamador sabía acerca de los códigos de seguridad y sabía que fueron identificados por carta designación. El llamador, dijo su gerente de sucursal requiere para una mayor seguridad. Realmente no parece ninguna razón para no darle la verificación se estaba pidiendo.

Luis no está solo. Empleados del Banco entregar códigos de seguridad para los ingenieros sociales Todos los días. Increíble pero cierto.

Hay una línea en la arena donde técnicas del investigador privado deja de ser legal y ser de comienzo ilegal. Vince se quedó legal cuando obtuvo la rama número. Incluso permaneció legal cuando él estafó a Louis para que le den dos de las

códigos de seguridad del día. Cruzó la línea cuando tenía información confidencial un cliente del Banco por fax a él.

Pero para Vince y su empleador, es un crimen de bajo riesgo. Cuando roba dinero o mercancías, alguien notará que ha pasado. Cuando roba información, la mayoría de los tiempo que nadie notará porque la información es todavía en su poder.

MENSAJE DE MITNICK
Códigos de seguridad verbal son equivalentes a las contraseñas en la prestación de un cómodo y medio fiable de protección de datos. Pero los empleados deben estar bien informadas los trucos que utilizan los ingenieros sociales, y no darle las llaves a la Reino.

POLICIAS COMO DUPES
Un sombrío investigador privado o ingeniero social, hay frecuentes ocasiones cuando sería útil saber el número de licencia del alguien conductor--por ejemplo, Si desea asumir la identidad de otra persona para obtener información sobre sus saldos bancarios.

Levantamiento de la billetera de la persona o asomándose sobre su hombro en un oportuno momento, averiguar el número de licencia del conductor debe ser casi imposible. Pero para alguien con conocimientos incluso modesta ingeniería social, es apenas un desafío. Un ingeniero social particular--Eric Mantini, llamaré a él, es necesario obtener del conductor números de registro de licencia y el vehículo sobre una base regular. Eric figuró fue aumenta innecesariamente su riesgo para llamar al departamento de vehículos automotores (DMV) y pasar por el mismo ardid otra vez cada vez que necesitaba información. Se pregunta si no hay alguna manera de simplificar la proceso.

Probablemente nadie había pensado nunca de antes, pero él descubrió una manera para obtener la información en un abrir y cerrar, cada vez que quería. Lo hizo tomando ventajas de un servicio proporcionado por departamento de automotores del su estado. Muchos Estado DMV (o lo que puede llamarse el departamento en su estado) otra manera privilegiada información sobre ciudadanos disponibles para las empresas de seguros, investigadores privados y algunos otros grupos que tiene la legislatura del Estado considera el derecho a compartir por el bien del comercio y la sociedad en general.

El DMV, por supuesto, tiene limitaciones apropiadas que serán los tipos de datos entregado. La industria de seguros puede obtener ciertos tipos de información de la archivos, pero no en otros. Un conjunto diferente de limitaciones se aplica al PIs y así sucesivamente.

Para los funcionarios encargados de hacer cumplir la ley, generalmente se aplica una regla diferente: será suministrar cualquier información en los registros a cualquier funcionario de paz jurada que correctamente

identifica a sí mismo. En el estado de Eric vivía en, fue la identificación requiere un Código de solicitante expedida por el DMV, junto con conducir carnet del oficial de número. El empleado DMV que compruebe siempre haciendo coincidir el oficial nombre contra el número de licencia de su conductor y una otra pieza de información--normalmente la fecha de nacimiento--antes de dar cualquier información.

¿Qué ingeniero social Eric quería hacer era nada menos que ocultar a sí mismo en el identidad de un oficial de la ley. ¿Cómo lograron? Mediante la ejecución de un invertir sting en los policias!

Eric Sting
Primera llamada información de Telefónica y pidieron el número de teléfono de DMV con sede en el Capitolio. Se le dio el número 503555-5000; que, de curso, es el número de llamadas del público en general. Entonces llamó un cercano estación del alguacil y pidieron teletipo--la oficina donde las comunicaciones son enviados a y recibido de otros organismos de represión de la delincuencia nacional la ley base de datos, órdenes locales y así sucesivamente. Cuando llegó el teletipo, dijo que se buscando el número de teléfono para la aplicación de la ley a utilizar al llamar al DMV cuartel general del Estado.

There was an error deserializing the object of type System.String. The token 'true' was expected but f

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
y en parte un número que extrae del aire; Sin duda el especial conjunto de oficina DMV hasta la aplicación de la ley de tomar llamadas sería en el mismo código de área como el número gtyen cabo para el público a la convocatoria y fue casi como seguro que los próximos tres dígitos, el prefijo, sería la misma. así. Lo único que realmente necesitaba saber era los cuatro últimos.

Sala de teletipo del alguacil no recibe llamadas del público. Y ya el llamador tenía la mayor parte de la serie. Obviamente fue legítimo.

There was an error deserializing the object of type System.String. The token 'true' was expected bu

Así que Eric tenía ahora el número de teléfono especial para agentes del orden llamar el DMV. Pero sólo el uno número no era suficiente para satisfacerle; la Oficina sería tiene un buen muchos más que la línea de teléfono único, y Eric necesitaba saber cómo muchas líneas hubo y el número de teléfono de cada uno.

El conmutador
Para llevar a cabo su plan, que necesitaba para acceder al teléfono conmutador maneja las líneas de teléfono de aplicación de la ley en el DMV. Llamó el Estado Telecomunicaciones Departamento y él afirmaba desde Nortel, el

fabricante del DMS-100, uno de los comerciales más utilizados
conmutadores telefónicos. Dijo, \"puede usted por favor transferirme a uno del conmutador
técnicos que trabaja en el DMS-100?\"

Cuando llegó el técnico, afirmó que con la técnica de Nortel
Centro de soporte de asistencia en Texas y explicó que estaban creando un
base de datos master para actualizar todos los conmutadores con las últimas actualizaciones de software. S
todos no hacerse remotamente--necesidad de ningún técnico de conmutador para participar. Pero ellos
es necesario el número de acceso telefónico al conmutador para que pueda realizar las actualizaciones
directamente desde el centro de soporte.

Sonaba totalmente plausible, y el técnico dio a Eric el número de teléfono.
Ahora él podría marcar directamente en uno de los conmutadores telefónicos del Estado.

Para defenderse de los intrusos externos, interruptores comerciales de este tipo son
protegido con contraseña, al igual que cada red informática corporativa. Cualquier buen social
Ingeniero con un fondo de teléfono phreaking sabe que los conmutadores Nortel proporcionan
un nombre de cuenta predeterminado para actualizaciones de software: NTAS (la abreviatura de Nortel
Asistencia técnica; no muy sutil). Pero ¿qué pasa con una contraseña? Eric
marcado en varias ocasiones, cada vez que se trata de una de las obvias y utilizados
Opciones. Ingresar el mismo nombre de cuenta, NTAS, funcionó. Ninguno hizo
There was an error deserializing the object of type System.String. End element 'root' from names

Luego trató de \"Actualizar\"... y fue en. Típico. Con un evidente, fácilmente
contraseña acertada es sólo muy ligeramente mejor que no tener a todos contraseña.

Ayuda a estar al día en su campo; Eric probablemente sabía tanto sobre
conmutador y cómo programar y solucionar como el técnico. Una vez que fue
capaz de acceder al conmutador como un usuario autorizado, él podría obtener el control total sobre
las líneas telefónicas que fueron su objetivo. Desde su ordenador, preguntó el conmutador
el número de teléfono le había dado para llamadas de aplicación de ley a la DMV,
555-6127. Encontró que hubo 19 otras líneas de teléfono en el mismo
Departamento. Obviamente ellos manejan un alto volumen de llamadas.

Para cada llamada entrante, el conmutador fue programado para \"cazar\" a través de los veinte
líneas hasta que encontró uno que no estaba ocupado.

Eligió la número 18 de la línea en la secuencia y el código que agrega
transferencia a esa línea de llamada. El número de desvío de llamadas, ingresó en el teléfono
número de su teléfono celular nuevo, barato, prepago, el tipo que traficantes de drogas son tan
aficionado porque son lo suficientemente baratas tirar a la basura después de que el trabajo es largo.

Con desvío de llamadas activado ahora en la línea 18, tan pronto como la Oficina tiene bastante ocupado para tener diecisiete llamadas en curso, la siguiente llamada a entrar que no suene en la Oficina DMV, pero en su lugar se remitiría a la celda de Eric teléfono. Atrás se sentó y esperó.

Una llamada al DMV

Poco antes de 8 de la mañana, sonó el teléfono móvil. Esta parte fue la mejor, las más deliciosas. Aquí fue Eric, el ingeniero social, hablando con un policia, alguien con la autoridad para venir y arrestarlo, o conseguir una orden de allanamiento y realizar una RAID para reunir pruebas contra él.

Y no solo CP llamaría, pero una cadena de ellos, uno tras otro. En uno ocasión, Eric estaba sentado en un restaurante almorzando con amigos, envío de una llamada cada cinco minutos o menos, escribir la información en una servilleta de papel mediante un Pluma prestada. Todavía descubre este hilarante.

Pero hablando a los policías no perturba un buen ingeniero social en lo más mínimo. En hecho, la emoción de engañar a estos organismos de represión probablemente agregado a Disfrute de Eric s de la ley.

Según Eric, las llamadas fueron algo parecido a esto:

DMV, ¿puedo yo ayudarlo?

Se trata de Detective Andrew Cole.

Hola, detective. ¿Qué puedo hacer por usted hoy?

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. familiares en aplicación de la ley para pedir una foto--útil, por ejemplo, cuando los oficiales van a salir a arrestar a un sospechoso y quieren saber lo que parece.

There was an error deserializing the object of type System.String. Encountered unexpected character 'E'. su agencia?\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'A'

There was an error deserializing the object of type System.String. Unexpected end of file. Followi

¿Cuál es el número de licencia de su conductor. \"¿Cuál es tu fecha de nacimiento\"

El llamador daría su información de identificación personal. Eric iría a través de algún pretexto de verificar la información y luego dicen que el llamador la información de identificación ha sido confirmada y pedir los detalles de lo que el llamador quería averiguar del DMV. Él se pretende empezar a buscar el nombre, con el llamador capaz de oír el clic de las teclas y luego decir algo así, \"Oh, joder, mi equipo solo bajó de nuevo. Lo sentimos, detectives mi equipo ha estado en un abrir y cerrar, toda la semana. ¿Le importaría llamar a volver y obtener otro empleado para ayudarle?\"

De esta manera terminaría la llamada atando los cabos sueltos sin despertar ninguna sospecha acerca de por qué él no fue capaz de ayudar al oficial con su solicitud. Mientras tanto Eric

tenía una identidad robada--detalles podría utilizar para obtener DMV confidencial
información cada vez que necesitaba.

Después de tomar llamadas durante unas horas y obtener decenas de códigos de solicitante, Eric
marcado en el switch y desactiva el reenvío de llamadas.

Durante meses después de él llevaría sobre las asignaciones de jobbed que le
empresas legítimas de PI que querían saber cómo le estaba poniendo su información.
Cada vez que necesitaba, él podría marcar en el conmutador, activar el reenvío de llamadas,
y reunir otra pila de credenciales de la policía.

Analizando el timo
Vamos a ejecutar una reproducción en los ardides que Eric tirado sobre una serie de personas para hacer es
trabajo de engaño. En el primer paso exitoso, obtuvo a adjunto del alguacil en un teletipo
Sala para dar un número de teléfono DMV confidencial a un completo extraño,
aceptar al hombre como un adjunto sin solicitar cualquier verificación.

A continuación, alguien en el departamento de estado de telecomunicaciones hizo lo mismo, aceptando
Reclamación de Eric que estaba con un fabricante de equipo, y proporcionar el
extraño con un número de teléfono para marcar en el teléfono conmutador servir la
DMV.

Eric fue capaz de meterse en el conmutador en gran medida debido a la débil seguridad
prácticas por parte de los fabricantes de switches en con el mismo nombre de cuenta
en todos los conmutadores. Ese descuido hizo un paseo en el Parque para lo social
Ingeniero de adivinar la contraseña, sabiendo que una vez más que cambiar técnicos, sólo
como casi todos los demás, elegir contraseñas que serán una cincha para ellos
Recuerde.

Con acceso al conmutador, configurar reenvío de llamadas de uno de los teléfono DMV
líneas para la aplicación de la ley a su propio teléfono celular.

Y entonces, tapadora y parte más flagrante, estafó a un cumplimiento de la ley
oficial tras otro para que revelen no sólo su solicitante códigos pero sus propias
información de identificación personal, dando a Eric la posibilidad de les suplantar a.

Si bien hubo conocimiento sin duda técnica que saque este truco,
no han trabajado sin la ayuda de una serie de personas que no tenían clue
estaban hablando a un impostor.

Esta historia fue otra ilustración del fenómeno de por qué no preguntan
There was an error deserializing the object of type System.String. Encountered unexpected character 'W'.
Adjunto del Sheriff no sabía--o, en este caso, un extraño a sí mismo pasando como

Adjunto del alguacil--en lugar de lo que sugiere que obtenga la información de un compañero
¿adjunto o su propio Sargento? Una vez más, la única respuesta que puedo ofrecer es que la gente
rara vez esta pregunta. ¿No se produce les pedir? No quieren sonido
¿desafiante e inútil? Tal vez. Cualquier explicación sólo sería
suposiciones. Pero los ingenieros sociales no importa por qué; sólo les importa el hecho de este pequeño
es fácil obtener información que de lo contrario podría ser un reto para obtener.

MENSAJE DE MITNICK
Si tienes un teléfono conmutador en sus instalaciones de la empresa, lo que sería la persona
¿en hacer cargo si recibió una llamada del proveedor, pidiendo el número telefónico?
Y por cierto, esa persona nunca cambió la contraseña por defecto para la
¿conmutador? ¿Es una palabra fácil de adivinar que se encuentra en cualquier diccionario de esa contrase

PREVENIR LA CON
Un código de seguridad, debidamente utilizado, agrega una valiosa capa de protección. Una seguridad
código mal utilizado puede ser peor que ninguno en absoluto porque da la ilusión
de seguridad donde realmente no existe. Qué buena es códigos si sus empleados
no mantenerlos. ¿secreto?

Cualquier empresa con una necesidad de códigos de seguridad verbal necesita precisar claramente para
sus empleados cuando y cómo se utilizan los códigos. Adecuadamente capacitados, el carácter de
la primera historia en este capítulo no habría tenido que confiar en sus instintos, fácilmente
superar, cuando se le preguntó a dar un código de seguridad a un extraño. Él sintió que él
no debe pedirse esta información en las circunstancias, pero carece de un
claro la política de seguridad--y buen sentido común--dio fácilmente.

Procedimientos de seguridad también deben establecer pasos a seguir cuando los campos de un empleado
una solicitud inadecuada para un código de seguridad. Todos los empleados deben estar capacitados para
informar inmediatamente de cualquier solicitud de credenciales de autenticación, como un diario
código o contraseña, que se hizo en circunstancias sospechosas. También debe informar
Cuando un intento de verificar la identidad de un solicitante no retira.

Por lo menos, el empleado debe registrar el nombre del autor de la llamada, número de teléfono,
y oficina o departamento y luego colgar. Antes de llamar a volver él debe comprobar
que la organización tenga un empleado de ese nombre y que la llamada
número de teléfono de espalda coincide con el número de teléfono en línea o impresos
Directorio de la empresa. La mayor parte del tiempo, esta sencilla táctica será todo lo que necesitan para
Compruebe que el llamador es quien dice que es.

Verificación se vuelve un poco más complicado cuando la empresa tiene un teléfono publicado
directorio en lugar de una versión on-line. Se contrataron a personas; licencia de personas; personas

cambiar de teléfono, departamentos y puestos de trabajo. El directorio de la copia impresa es ya actualizado el día después de que ha publicado, incluso antes de ser distribuidos. Incluso en-directorios de línea siempre no se puede confiar, porque los ingenieros sociales saben cómo modificarlos. Si un empleado no puede verificar el número de teléfono de independiente fuente, ella debe ser instruida para verificar por otros medios, tales como ponerse en contacto con el administrador del empleado.

Parte 3
Alerta de intruso

Capítulo 10
Ingrese en las instalaciones

¿Por qué es tan fácil para un forastero a asumir la identidad de un empleado de la empresa y llevar a una representación tan convincente que incluso las personas que son altamente ¿consciente de la seguridad se toman? ¿Por qué es tan fácil engañando a personas que pueden ser plenamente consciente de los procedimientos de seguridad, sospechosos de personas que no lo hacen ¿saber y protección de los intereses de su empresa?

Reflexionar sobre estas preguntas como usted leer las historias en este capítulo.

EL GUARDIA DE SEGURIDAD AVERGONZADO
Fecha: el martes 17 de octubre, 2:16
Lugar: La fábrica en las afueras de Tucson, Skywatcher Aviation, Inc.
Arizona.

Historia de la Guardia de seguridad
Escuchar sus tacones de cuero haga clic en contra el suelo en los salones de la casi desierta planta hizo Leroy Greene sentir mucho mejor que pasar las horas de la noche de su ver en frente de los monitores de vídeo en la Oficina de seguridad. Allí no era incluso no permite que nada mirar en las pantallas, leer una revista o su Biblia de cuero enlazado. Sólo había que sentarse allí mirando la muestra de que aún imágenes donde nada jamás movida.

Pero caminar los pasillos, al menos fue estirando sus piernas y cuando él recordado a tirar de sus brazos y hombros en el pie, le consiguió un poco ejercicio, demasiado. Aunque no realmente contar mucho ejercicio para un hombre que había jugado el tackle derecho en el equipo de fútbol de secundaria campeón All-City. Aún así, pensaba que un trabajo es un trabajo.

Giró la esquina suroeste y comenzó a lo largo de la galería con vistas a la mitad-planta de producción de millas de largo. Él Miró hacia abajo y vio a dos personas caminando pasado la línea de copters parcialmente construidos. La pareja se detuvo y parece estar apuntando cosas fuera mutuamente. Una extraña visión en este momento de la noche. ' Mejor comprobar, \"pensó.

Leroy encabezada por una escalera que le proporcionaría al piso de la línea de producción detrás de la pareja, y no sienten su enfoque hasta que intervino junto a.
There was an error deserializing the object of type System.String. Encountered unexpected character 'h'. mantener su voz suave en momentos como éste; sabía que el mero tamaño de él podría parece amenazante.

There was an error deserializing the object of type System.String. Encountered unexpected character 'o'.
desde la Oficina de Marketing en empresas en Phoenix. Estoy en la ciudad para reuniones y
quería mostrar mi amigo aquí cómo del más grande el mundo helicópteros obtener construidos. \"

There was an error deserializing the object of type System.String. Encountered unexpected character 'L'.
parecían. El tío de Marketing espera apenas la alta escuela, otro
tenía el pelo hasta los hombros y miró sobre quince años.

Alcanzó el uno con el corte de pelo en su bolsillo para su insignia, entonces comenzado a
acaricia todos los bolsillos. Leroy fue de repente comienzo a tener una mala sensación sobre
esto. \"Joder\", dijo el chico. \"Debe has dejado en el coche. Puedo conseguirlo--tomar solo me diez
minutos para salir al estacionamiento y espalda\".

Leroy tuvo su almohadilla fuera de este tiempo. \"Lo que diría que su nombre era, Sor que preguntó,
y anoté cuidadosamente la respuesta. A continuación, les pidió ir con él a la
Oficina de seguridad. En el ascensor hasta el tercer piso, Tom charlamos acerca de haber sido
con la empresa por sólo seis meses y espera que él no iba a llegar en cualquier
problemas para esto.

En la sala de control de seguridad, los dos otros en la noche desplazan con Leroy
se le unió en cuestionamiento al par. Stilton le dio su número de teléfono y dijo
su jefe fue Judy Underwood y dio su número de teléfono y la
información todos retirados en el equipo. Leroy tomó la seguridad otras dos
gente de un lado y se habló sobre qué hacer. Nadie quería sacar este mal;
los tres acordaron mejor llaman a jefe de guy aunque significaría despertar
ella en medio de la noche.

Leroy llamado Sra. Underwood a sí mismo, explicó que él era y ella tenía una
¿El Sr. Tom Stilton trabajando para ella? Ella sonaba como ella era mitad todavía dormida.
There was an error deserializing the object of type System.String. Encountered unexpected char

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
Gafete.\"
Sra. Underwood dijo, \"Déjame hablar con él\".

Stilton en el teléfono y dijo, \"Judy, siento realmente estos chicos despertar
que hasta en la mitad de la noche. Espero que no te vas a
mantenga esta contra mí.\"

Él escuchó y luego dijo: \"fue simplemente que tenía que estar aquí en la mañana
de todas formas, para esa reunión en el nuevo comunicado de prensa. De todos modos, obtendrá el corre
¿sobre el trato de Thompson? Tenemos que cumplir con Jim hasta el lunes por la mañana nos
no pierda esto. Y todavía tengo almuerzo con ustedes el martes, justo?\"

Escuchado un poco más y dijo adiós y colgó.

Pille Leroy sorpresa; había pensado que conseguiría el teléfono vuelve así la dama
podría decirle que todo estaba bien. Se preguntó si tal vez él debería llamar le
una vez más y preguntar, pero pensó mejor. Él ya había molestado a ella una vez en el
media de la noche; Si él llamó una segunda vez, tal vez ella podría obtener molesta y
quejarse a su jefe. \"Por qué hacer olas?\" pensó.

¿Está bien si muestro a mi amigo el resto de la línea de producción? Stilton pidió Leroy
¿Desea que venga, mantener un ojo en nosotros?

There was an error deserializing the object of type System.String. Encountered unexpected character 'L'.
Seguridad saber si necesita estar en el piso de la planta después de horas--es la regla.\"
Te recuerdo que, Leroy, \"Stilton dijo. Y se marcharon.

Habían pasado apenas diez minutos antes de que sonó el teléfono en la Oficina de seguridad.
Sra. Underwood fue en la línea. \"Quién era ese chico?\" ella quería conocer. Ella
dice ella mantuvo tratando de hacer preguntas, pero él sólo mantuvo hablando acerca de tener
almuerzo con ella y ella no sabe quien es el infierno.

Los chicos de seguridad llamados el vestíbulo y la guardia en la puerta para el estacionamiento.
Ambos informaron que los dos jóvenes habían dejado unos minutos antes.

La historia posterior, Leroy siempre terminó diciendo: \"Lordy, jefe chew
Yo por un lado y por el otro. He tenido suerte que todavía tengo un trabajo\".

Historia de Joe Harper
Solo para ver lo que él podría llegar lejos con diecisiete años Joe Harper había sido
furtivamente en edificios de más de un año, a veces durante el día,
a veces por la noche. El hijo de un músico y una camarera cóctel, tanto trabajo
el turno de noche, Joe tenía demasiado tiempo por él mismo. Su historia de ese mismo incidente
arroja luz instructiva sobre cómo sucedió todo.

Tengo este amigo Kenny, quien piensa que quiere ser un piloto de helicóptero. Preguntó
me pude meterlo en la fábrica de Skywatcher para ver la línea de producción donde
hacen los helicópteros. Él sabe que he metido en otros lugares antes. Es un
a ver si puede caer en lugares que no se supone que adrenalina.

Pero simplemente no entras en un edificio de la fábrica u oficina. Llegué a pensar
hacer un montón de planificación y hacer un pleno reconocimiento en el destino. Compruebe el
página Web de la compañía de teléfono, nombres y títulos y estructura jerárquica
números. Leer recortes de prensa y artículos en revistas. Investigación meticulosa es mi

marca propia de precaución, por lo que pude hablar con alguien que me desafió, con como mucho conocimiento como cualquier empleado.

¿Hasta dónde empezar? Primero busqué en Internet para ver donde la compañía tenía oficinas y vio que era la sede corporativa en Phoenix. Perfecto. Llamé y pedido de comercialización; cada compañía tiene un departamento de marketing. Una dama respondió, y dijo que estaba con gráficos de lápiz azul y queríamos ver si nos podía interesar en el uso de nuestros servicios y que sería hablar. Ella dijo sería Tom Stilton. Pedí su número de teléfono y dijo que no daba que información pero ella podría ponerme a través. La llamada sonó en el correo de voz, y su mensaje, dijo, \"Esto es Tom Stilton en gráficos, extensión 3147, por favor dejar un mensaje\". Seguro--no dan a las extensiones, pero este chico deja su en su correo de voz. Así fue genial. Ahora tenía un nombre y una extensión.

Otra llamada, volver a la misma oficina. \"Hola, estaba buscando Tom Stilton. Él es no en. Me gustaría pedirle a su jefe una pregunta rápida.\" El jefe fue, también, sino por la tiempo que estaba terminado, que yo sabía el nombre del jefe. Y había ido muy bien su extensión el número de su correo de voz, demasiado.

Podría probablemente conseguir nos pasado la Guardia vestíbulo con sin sudar, pero he impulsado por planta y yo pensaba que recordé una valla alrededor del estacionamiento. Una valla significa un Guardia que le comprueba cuando se intenta impulsar en. Y por la noche, podría ser escribir números de licencia, demasiado, así que tendría que comprar un viejo matrícula en una pulga mercado.

Pero primero tendría que obtener el número de teléfono en la choza del guardia. Esperé un poco por lo qu
Tengo el mismo operador cuando marcado en, ella no reconoce mi voz.
Después de un poco llamó y dijo, \"tenemos una denuncia que el teléfono en la cresta
Choza de guardia de carretera ha reportado problemas intermitentes--son sigue teniendo problemas?\" Ella dice que no sabía pero me conectaría.
El hombre respondido, \"puerta de Ridge Road, Ryan se trata.\" Dije, \"Hola, Ryan, se trata de Ben. Tenían problemas con sus teléfonos allí?\" Es simplemente una seguridad mal pagados Guardia pero supongo que tenía cierta formación porque enseguida dijo: \"Ben quien--
¿Cuál es su apellido?\" Sólo conservé derecha como si no hubiese incluso le escuché.
Alguien reportó un problema anteriormente.

Pude oír lo mantiene lejos el teléfono y llamar, \"Hey, Bruce, Roger, hubo un problema con este teléfono. Se volvió y dijo, \"No, no problemas que conocemos\".

¿Cuántas líneas de teléfono tiene allí?
Se había olvidado de mi nombre. \"Dos\", dijo. \"Que estás en ahora?\"
3140.

Gotcha! ¿\"Y está trabajando bien\"?
Me parece.
Está bien, dijo. Escucha, Tom, si tienes algún problema de teléfono, sólo comuníquese con nosotros Telecom cualquier momento. Estamos aquí para ayudar\".

Mi compañero y yo decidimos visitar la planta de la noche siguiente. Tarde esa tarde Llamé a la cabina de guardia, utilizando el nombre del chico de Marketing. Dije, \"Hola, esto es Tom Stilton en gráficos. Estamos en un plazo de accidente y tengo un par de chicos conduce a la ciudad para ayudar. Probablemente no estará aquí hasta uno o dos en el por la mañana. Seguirán en entonces?\"
Él estaba feliz de decir que no, bajé a la medianoche.
Dije, \"bueno, sólo dejo una nota para el siguiente tio, vale? Cuando aparecen dos chicos y decir que han venido a ver Tom Stilton, sólo onda em en--vale?\"

Sí, dijo que estaba bien. Tomó mi nombre, departamento y extensión número y dijo que tener cuidado de ella.

Nos condujo hasta la puerta un poco después de dos, dio el nombre de Tom Stilton y un sueño Guardia sólo señaló la puerta debemos ir y dónde debo aparcar.

Cuando caminamos hacia el edificio, hubo otra estación de la guardia en el vestíbulo, con el habitual libro de inicios de sesión nocturna. Dijo el guardia tenía un informe que necesario para estar listo en la mañana, y esta amiga mía quería ver el planta. \"Está loco por helicópteros,\" dije \"piensa que quiere aprender a piloto uno\". Me preguntó por mi insignia. Llegó en un bolsillo, y luego palmaditas alrededor y dice que debo haber dejado en coche; Voy a ir a conseguirlo. Dije, \"Te llevará unos diez minutos\". Dijo, no importa, está bien, simplemente identificate.
Caminando por esa línea de producción--lo que un gas. Hasta ese tronco de árbol de un Leroy se nos detuvo.

En la Oficina de seguridad, pensé que se vería alguien que realmente no pertenecen nervioso y asustado. Cuando las cosas se ponen apretadas, solo empiezo a sonar como soy realmente al vapor. Como soy realmente quien decía ser y es molesto no creen Me.

Cuando comenzaron a hablar quizás debería llamar a la señora dijo que era mi Jefe y fui para obtener su número de teléfono del equipo, estaba allí pensamiento, el \"Buen momento para hacer una pausa para ti\". Pero hubo ese estacionamiento puerta--incluso si conseguimos salir del edificio, iba a cerrar la puerta y lo no haríamos nunca divisar.

Cuando llama a la dama que fue jefe de Stilton y luego me dio el teléfono, Leroy la dama comenzó a gritar a mí \"Que es esto, quién eres!\" y me quedé solo hablando como estábamos teniendo una conversación agradable y luego colgó.

¿Cuánto tiempo tarda en encontrar a alguien que te puede dar un teléfono de empresa ¿número en medio de la noche? Pensé que teníamos menos de quince minutos para salir de allí antes de esa dama estaba sonando la Oficina de seguridad y poniendo un error en sus oídos.

Nos salió de allí lo más rápido posible sin mirar como teníamos prisa. Seguro que alegró cuando el chico en la puerta sólo agitó nosotros a través de.

Analizando el timo
Cabe señalar que en el incidente real esta historia se basa, los intrusos en realidad eran adolescentes. La intrusión fue una alondra, solo para ver si podrían obtener distancia con él. Pero si era tan fácil para un par de adolescentes, hubiera sido incluso más fácil para los ladrones adultos, espías industriales o terroristas.

Cómo tres oficiales de seguridad experimentados permiten un par de intrusos sólo caminar ¿distancia? Y no cualquier intruso, pero una pareja tan joven que cualquier persona razonable ¿debe haber sido muy sospechoso?

Leroy fue apropiadamente sospechoso, en un principio. Fue correcto en llevarlos a la Oficina de seguridad y en cuestionamiento el chico que se llama a sí mismo Tom Stilton y comprobación de los nombres y números de teléfono que dio. Era cierto en hacer la llamada al supervisor.

Pero al final fue llevado por aire del joven de confianza y indignación. No es el comportamiento que cabe esperar de un ladrón o un intruso--sólo un empleado real habría actuado ese camino... o lo asumió. Leroy debe han sido entrenados para contar con identificación sólida, no de percepciones.

¿Por qué no él más sospechoso cuando el joven colgó el teléfono sin lo entrega vuelve para que Leroy pudieron escuchar la confirmación directa de Judy Underwood y recibir su garantía de que el niño tenía una razón de ser en el ¿planta tan tarde en la noche?

Leroy fue acogido por una artimaña tan audaz que debería haber sido evidente. Pero considerar el momento desde su perspectiva: un graduado de escuela secundaria, preocupado por su trabajo, incierto si él podría tener problemas para molestar a una empresa administrador por segunda vez en medio de la noche. Si había sido en su ¿zapatos, habría hecho la llamada de seguimiento?

Pero por supuesto, una segunda llamada telefónica fue la única acción. ¿Qué otra cosa ¿podría haber hecho el guardia de seguridad?

Incluso antes de colocar la llamada telefónica, él podría han pedido tanto a la par de mostrar algún tipo de identificación de la imagen; llevaron a la planta, por lo que al menos uno de ellos deben tener una licencia de conducir. El hecho de que originalmente dieron falsos nombres habría sido obvios (un profesional habría llegado equipado con identificación falsa, pero estos adolescentes no han tomado esa precaución). En cualquier caso, Leroy debe han examinado sus credenciales de identificación y escrito la información. Si ambos insistieron que no tenían ninguna identificación, él debe entonces ellos han caminado o el coche para recuperar el gafete de la empresa \"Tom Stilton\"afirmó que había dejado allí.

MENSAJE DE MITNICK
Gente manipuladora suelen tener personalidades muy atractivos. Son típicamente articular bastante y rápido en sus pies. Los ingenieros sociales también están especializados en los procesos de pensamiento de distracción popular que cooperan. Pensar que cualquier una persona no es vulnerable a esta manipulación es subestimar la habilidad y el instinto asesino del ingeniero social.
Por otro lado, un buen ingeniero social, nunca subestima a su adversario.

Tras la llamada telefónica, una de las personas de seguridad debería haberse quedado con el par hasta que abandonaron el edificio. Y, a continuación, les caminó hacia su auto y escrito el número de la placa de la licencia. Si él hubiera sido lo suficientemente atento, tendría señaló que hizo la placa (el uno que el atacante había comprado en un mercadillo) no tienen una pegatina de registro válida - y que debería haber sido motivo suficiente para detienen a la pareja para una mayor investigación.

RECOLECCIÓN URBANA
Recolección urbana es un término que describe el manoseo a través de la basura del destino en búsqueda de información valiosa. La cantidad de información que puede obtener información acerca de ur el objetivo es asombroso.

Mayoría de la gente no mucho pensar en lo que está descartando en casa: teléfono facturas, declaraciones de tarjeta de crédito, botellas de prescripción médica, extractos bancarios, trabajo- materiales relacionados y mucho más.

En el trabajo, deben hacerse conscientes de que la gente mira a través de basura para empleados obtener información que puede beneficiarlos.

Durante mis años de secundaria, solía ir excavando a través de la basura detrás de la teléfono local empresa edificios--a menudo solos pero ocasionalmente con amigos que comparten un interés en conocer más acerca de la compañía telefónica. Una vez que

se convirtió en un buzo experimentado de basurero, aprender algunos trucos, como por ejemplo cómo hac
esfuerzos especiales para evitar las bolsas de los baños y la necesidad de llevar
guantes.

Recolección urbana no es agradable, pero la recompensa fue extraordinaria--interna
la compañía de guías telefónicas, manuales de equipo, listas de empleados, descartadas
impresiones mostrando cómo se programa el equipo de conmutación y más--todo allí por
la toma.

Yo sería programar visitas para noches cuando se publica nuevos manuales, porque la
contenedores de basura tendría mucho de los viejos son ignoradas arrojadas a la basura. Y
Me gustaría ir otras veces impar, buscando cualquier notas, cartas, informes etc.
adelante, podrían ofrecer algunas interesantes joyas de información.

Al llegar quisiera encontrar algunas cajas de cartón, les Tire y dejar de lado. Si
alguien me desafió, que pasó ahora y entonces, yo diría que fue un amigo
mover y yo solo estaba buscando cuadros que le ayude a paquete. La Guardia nunca
observado todos los documentos que me había puesto en los cuadros para llevar a casa. En algunos casos,
Dime a perderse, por lo que sólo sería hacia otra oficina central compañía de teléfono.

JERGA
BASURERO conducir atravesando la basura de la empresa (a menudo en un
Basurero fuera y vulnerable) para encontrar información desechado que bien propio
tiene valor, o proporciona una herramienta para usar en un ataque de ingeniería social, como interna
números de teléfono o de títulos

No sé lo que es hoy, pero atrás entonces fue fácil decirle que bolsas
puede contener algo de interés. La basura de cafetería y barreduras de piso
estaban sueltos en las grandes bolsas, mientras que las papeleras Oficina estaban forrados con
bolsas de basura desechable blanco, que la tripulación de limpieza podría levantar a uno por uno
ajuste y una corbata alrededor.

Una vez, mientras busca con unos amigos, llegamos con unas hojas de
papel rasgado con la mano. Y no sólo rasgadas hasta: alguien había ido a la molestia de
extraer las hojas en trozos pequeños, todos cómodamente echado en un solo cinco-
Bolsa de basura de galón. Tomamos la bolsa a una tienda local de donut, vuelca las piezas fuera de
una tabla y comenzó montaje ellos uno por uno.

Estábamos todos puzzle-hacedores, por lo que esto ofrece el estimulante desafío de un gigante
rompecabezas... pero resultó tener más que una recompensa infantil. Cuando haya terminado,
habíamos monté la lista de nombre y contraseña de cuenta completa para uno de los
sistemas de equipo crítico de la compañía.

¿Eran nuestros ataques buceo contenedor vale la pena el riesgo y el esfuerzo? Te apuesto fueron. Incluso más de lo que parece, porque el riesgo es cero. Es cierto, a continuación, y hoy todavía cierto: como no va violar, discutido a través de alguien de otra basura es 100 por ciento legal.

Por supuesto, los hackers y phreaks de teléfono no son los únicos con sus jefes en latas de basura. Departamentos de policía alrededor de la pata del país a través de la basura con regularid y un desfile de gente de dons de la Mafia a los sobornadores menores han sido condenados basado en parte en pruebas reunidas desde su basura. Agencias de inteligencia, incluyendo nuestros propios, han recurrido a este método durante años.

Puede ser una táctica demasiado baja abajo para James Bond--película asistentes prefieren mucho verlo outfoxing el villano y ropa de cama una belleza que permanente hasta su rodillas en la basura. Espías de la vida real son menos partiendo cuando algo de valor puede ser tapada entre las cáscaras de plátano y café motivos, los periódicos y listas de supermercado. Especialmente si la recopilación de la información no ponerlos en daño forma.

Caja de basura

Las corporaciones jugar el juego de buceo de basurero, demasiado. Periódicos tuvieron un día de campo Junio de 2000, informes que Oracle Corporation (cuyo CEO, Larry Ellison, es probablemente, la nación más de marcadas enemigo de Microsoft) ha contratado una investigación empresa que había sido atrapado con las manos en el tarro de cookie. Parece el los investigadores querido basura desde un traje cabildeo soportadas por Microsoft, ley, pero no quieren que el riesgo de obtener atrapados. Según informes de prensa, la empresa de investigación enviado a una mujer que ofrecía a los conserjes $60 a dejarla han la basura de la ley. Transformó hacia abajo. Ella fue volver la próxima noche, upping la ofrecen $500 para los limpiadores y $200 para el supervisor.

Los conserjes transformó hacia abajo y, a continuación, transformó.

Destacado periodista on-line Declan McCullah, tomando una hoja de literatura, titulado su historia de Wired News en el episodio, \"'Twas Oracle que espió en MS.\" Tiempo revista, clavando Ellison de Oracle, tituló su artículo simplemente \"Peeping Larry\".

Analizando el timo

Basado en mi propia experiencia y la experiencia de Oracle, cabría preguntarse ¿por qué nadie molestar a tomar el riesgo de robar la basura de alguien.

La respuesta, creo, es que el riesgo es nulo y los beneficios pueden ser sustanciales. Vale, quizás tratando de sobornar a los conserjes aumenta la posibilidad de consecuencias, pero para quien esté dispuesto a ensuciarse un poco, sobornos no son necesarias.

Para un ingeniero social, recolección urbana tiene sus ventajas. Él puede conseguir suficiente información para orientar su asalto contra la compañía de destino, incluyendo notas, reunión de agendas, cartas y similares que revelar nombres, departamentos, títulos, teléfono números y las asignaciones del proyecto. Basura puede producir organizativa de la empresa gráficos, información sobre la estructura corporativa, horarios de viaje y así sucesivamente. Todos esos detalles pueden parecer triviales para adentro, pero pueden ser muy valiosos información para un atacante.

Mark Joseph Edwards, en su libro Internet Security con Windows NT, habla acerca de los \"informes todos descartados debido a errores tipográficos, las contraseñas escritas en trozo documento, 'mientras estaba en' mensajes con números de teléfono, carpetas de archivo completo con documentos aún en ellos, disquetes y cintas que no eran borradas o destruidas- -todo lo cual podría ayudar a un intruso aspirante. \"

¿El escritor va a pedir \"Y quiénes son esas personas en su tripulación de limpieza? Has decidido que no la tripulación limpieza [podrá] entrar en el equipo la sala, pero no olvides las otras latas de basura. Si los organismos federales consideran necesario Fondo controles sobre las personas que tienen acceso a sus papeleras y Trituradoras, probablemente debería así.\"

MENSAJE DE MITNICK

Tu basura puede ser el tesoro de su enemigo. No damos mucha consideración a los materiales que descartamos en nuestras vidas personales, así que ¿por qué deberíamos creemos perso ¿tiene una actitud diferente en el lugar de trabajo? Todo se trata de educar a la fuerza de trabajo sobre el peligro (personas sin escrúpulos cavando de valiosos información) y la vulnerabilidad (información confidencial no se destruyen o correctamente borrada).

EL JEFE HUMILLADO

Nadie pensó nada al respecto cuando Harlan Fortis llegó a trabajar el lunes por la mañana como es habitual en el departamento de carreteras del condado y dijo que él había abando prisa y olvidado su insignia. El guardia de seguridad vio a Harlan en y va a salir cada día de la semana durante los dos años que había estado trabajando allí. Ella signo lo hizo para un temporal insignia del empleado, le dio a él, y él salió su camino.

No fue sino hasta dos días después que todos infierno comenzó rompiendo sueltos. El historia se extendió por todo el departamento como reguero de pólvora. Mitad de la gente que escuchado que no podía ser cierto. Del resto, nadie parecía saber si reír fuerte o sentir lástima por el pobre alma.

Después de todo, George Adamson fue una persona compasiva, la cabeza mejor y tipo de departamento habían tenido nunca. Él no merece tener esto suceda a él. Suponiendo que la historia era verdad, por supuesto.

El problema comenzó cuando George llama Harlan en su Oficina de la tarde de un viernes y le dijo, tan suavemente como pudo, que vienen Harlan lunes informará a un nuevo trabajo. Con el departamento de servicios de saneamiento. A Harlan, esto no era como estar despedido. Fue peor; fue humillante. Él no iba a llevarlo acostado.

Esa misma noche él mismo sentado en su porche a ver la vuelta enlazado tráfico. Por fin vio al chico de barrio llamado David que todo el mundo llamado \"The War Games Kid\" pasando su ciclomotor en el camino a casa de alto escuela. Se detuvo a David, le dio un código rojo Mountain Dew había comprado especialmente para el propósito y le ofreció un trato: el más reciente jugador de videojuegos y seis juegos a cambio de alguna ayuda de equipo y una promesa de mantener su cerrar la boca.

Después Harlan explicó el proyecto - sin dar ninguna de la puesta en peligro detalles--David acordado. Describió lo que él quería Harlan hacer. Fue a comprar un módem, entrar en la Oficina, encontrar a del alguien equipo donde había un conector de teléfono cerca de repuesto y conecte el módem. Deje el módem bajo el escritorio donde nadie pueda verlo. Luego vino la parte riesgosa. Harlan tuvo que sentarse en el equipo, instale un paquete de software de acceso remoto y obtener se ejecuta. Cualquier momento podría aparecer el hombre que trabajaba en la Oficina, o alguien podría caminar y verlo en la Oficina de otra persona. Fue tan tenso que él pudo apenas leer las instrucciones el kid había escrito para él. Pero él consiguió hacer y se deslizó fuera del edificio sin ser notado.

Plantar la bomba

David se detuvo después de la cena esa noche. Los dos se sentaron a de Harlan equipo y dentro en pocos minutos el chico había marcado en el módem, obtuvo acceso y la máquina de llegó George Adamson. No muy difícil, desde George nunca tuvo tiempo para cautelares cosas como cambiar contraseñas y siempre estaba pidiendo esta persona o que descargar o enviar por correo electrónico un arch para él. En el tiempo, todos en la Oficina sabían su contraseña. Un poco de caza activado el archivo llamado BudgetSlides2002.ppt, que el muchacho descargado en equipo de Harlan. Harlan dijo entonces el kid a ir a casa y venir Atrás en un par de horas.

Cuando David volvió, Harlan le pidió volver a conectar con la carretera Sistema informático de departamento y colocar el mismo archivo espalda donde tenían pareció, sobrescribir la versión anterior. Harlan mostraron a David el video jugador del juego y prometió que si las cosas iban bien, él tendría al día siguiente.

George sorprendente
¿No crees que hay algo sonando tan aburrido como audiencias de presupuesto
sería de mucho interés para nadie, pero la sala de reunión del condado
Consejo estaba abarrotada, llena de periodistas, representantes de interés especial
grupos, los miembros del público y aún dos tripulaciones de noticias de televisión.

George siempre resultaba mucho en juego para él en estas sesiones. El condado
Consejo celebró las cadenas del bolso, y a menos que George podría poner en un convincente
presentación, las carreteras podría ser reducido presupuesto. A continuación, todo el mundo sería
empezar a quejarse de baches y semáforos pegadas y peligroso
intersecciones y culpar a él y la vida sería capaz de avaro para el conjunto
año próximo. Pero cuando se presentó esa noche, se encontraba un sentimiento
seguros. Había trabajado seis semanas en esta presentación y la presentación de PowerPoint
visuales, que había tratado su esposa, su pueblo de personal superior, y algunos
respetados amigos. Todos estuvieron de acuerdo fue su mejor presentación nunca.

Las tres primeras imágenes de PowerPoint jugaron bien. Para un cambio, cada Consejo
miembros estaba prestando atención. Él estaba haciendo eficazmente sus puntos.

Y, a continuación, a la vez todo comenzó fallando. Fue la cuarta imagen
se supone que una foto hermosa al atardecer de la nueva extensión de carretera abierta
año pasado. En su lugar fue algo más, algo muy embarazoso. A
Fotografía de una revista como Penthouse o Hustler. Podía oír el
audiencia entiendo como apresuradamente golpear el botón en su computadora portátil para pasar a la sigu
imagen.

Este fue el peor. Una cosa no quedaba a la imaginación.

Todavía estaba tratando de haga clic en otra imagen cuando alguien en la audiencia
sacó el enchufe de alimentación del proyector mientras que el Presidente golpeaba ruidosamente con
su gavel y gritó por encima el barullo que se suspendió la reunión.

Analizando el timo
Utilizando la experiencia de un hacker adolescente, un empleado disgustado logró acceder a la
equipo del jefe de su departamento, descargar un importante PowerPoint
presentación y reemplazar algunas de las diapositivas con imágenes determinadas causar grave
vergüenza. Luego puso la presentación en equipo del hombre.

Con el módem conectado a un jack y conectado a uno de la Oficina
equipos, el joven hacker fue capaz de marcar desde el exterior. El chico había fijado
hasta el software de acceso remoto de antemano para que, una vez conectado a la
equipo, él tendría acceso completo a cada archivo almacenado en todo el sistema.
Ya el equipo estaba conectado a la red de la organización y él ya

sabía que el jefe de nombre de usuario y contraseña, puede obtener acceso fácilmente al jefe archivos.
Incluyendo el tiempo para analizar en las imágenes de la revista, había tomado el esfuerzo de todo sólo unas pocas horas. Fue el daño resultante a la reputación de un hombre bueno y más allá imaginando.

MENSAJE DE MITNICK
La mayoría de los empleados que son transferidos, despedido, o dejar ir en un reducción nunca son un problema. Sin embargo sólo tarda uno para hacer una empresa comprender demasiado tarde qué medidas han tomado para prevenir desastres. Experiencia y las estadísticas han mostrado claramente que la mayor amenaza para la empresa es desde adentro. Resulta que las personas que tienen un conocimiento íntimo de donde reside la información valiosa y dónde golpear a la compañía para causar más daño.

EL SOLICITANTE DE LA PROMOCIÓN
Tarde en la mañana de un día de otoño agradable, Peter Milton caminó en el lobby de las oficinas regionales de Denver del Honorable de autopartes, piezas nacionales mayorista para el recambio de automóvil. Esperó en la recepción mientras la joven dama firmó en un visitante, dio indicaciones a un llamador y tratadas con el hombre de UPS, todo más o menos al mismo tiempo.

There was an error deserializing the object of type System.String. Encountered unexpected character 'P'.
tiempo para ayudarlo. Ella sonrió, obviamente complacido había notado. Fue desde Marketing en la Oficina de Dallas, le dije y dijo que Mike Talbott de Las ventas de Atlanta iba a ser reunirse con él. \"Tenemos un cliente a visitar juntos esta tarde \", explicó. Sólo esperaré aquí en el lobby.\"

There was an error deserializing the object of type System.String. Encountered unexpected character 'S'.
escuchar lo que venía. \"Si pude ir a la Universidad, que es lo que tendría\", dijo. Me encantaría trabajar en Marketing.

Él sonrió de nuevo. \"Kaila,\" dijo, leyendo su nombre fuera el signo en el contador,
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
más de Marketing. Eso fue hace tres años, y ahora ella es un asistente Director de marketing, haciendo dos veces lo que tenía.\"
Kaila parecía iluso. Añadió, \"Se puede utilizar un ordenador?\" \"Seguro,\" ella dijo.

There was an error deserializing the object of type System.String. Unexpected end of file. Following e
Ella techado. \"Para eso sería incluso paso a Dallas.\"
There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.
pero voy a ver lo que puedo hacer.\"

Ella pensó que este buen hombre en el traje y corbata y con la prolijamente recortados, Well-combed cabello podría hacer una gran diferencia en su vida laboral.

Pete se sentó en el vestíbulo, abrió su portátil y comenzó a obtener algún trabajo hecho. Después de diez o quince minutos, él intervino hasta el contador. \"Escucha,\" él dijo, \"parece que Mike ha sido celebrado. Hay una sala de conferencias donde me podía sentarse y comprobar mis correos electrónicos mientras estoy esperando?\"

Kaila llamó el hombre quien coordinó la programación de sala de Conferencia y arreglada para que Pete usar uno que no era reservado. Siguiendo un patrón recogió de las empresas de Silicon Valley (Apple probablemente fue el primero en hacerlo) algunos de las salas de conferencias fueron nombradas con personajes de dibujos animados, otros después de restaura cadenas o estrellas de cine o héroes de cómic. Se le dijo que busque la Minnie Sala de ratón. Ella lo hizo firmar y le dio instrucciones para encontrar Minnie Ratón.

Encuentra la sala, que se asentaron en y había conectado a su ordenador portátil al puerto Ethernet.

¿Todavía tienes la imagen?

Derecho--el intruso había conectado a la red detrás del firewall corporativo.

Historia de Anthony
Supongo que podría llamar a Anthony Lake un empresario perezoso. O tal vez \"doblados\" viene más estrecha.
En lugar de trabajar para otras personas, había decidido que quería ir a trabajar para a sí mismo; Quería abrir una tienda, donde él podría estar en un solo lugar todo el día y no tienen que correr todo el campo. Sólo quería tener un negocio que él podría ser tan seguro como sea posible que él podía hacer dinero en.

¿Qué tipo de tienda? No tarda mucho en averiguar. Sabía acerca de cómo reparar coches, por lo que el almacén de piezas de un auto.

¿Y cómo construir una garantía de éxito? La respuesta llegó a él en un Flash: convencer mayorista de auto partes Honorable autopartes para venderlo a todos los mercancía que necesitaba en su costo.

Naturalmente no hacen esto con mucho gusto. Pero Anthony sabía cómo estafar a personas, su amigo Mickey sabía de irrumpir en los ordenadores de otras personas, y Juntos trabajaron un plan inteligente.

Ese día de otoño convincentemente pasó a sí mismo como un empleado llamado Peter Milton y él habían estafado su camino dentro de las oficinas de autopartes Honorable y

ya se había conectado su portátil a su red. Hasta ahora, así que fue bueno, pero que sólo el primer paso. Lo que todavía tenía que hacer no sería fácil, especialmente desde Anthony fijó a sí mismo un límite de tiempo de quince minutos--ya y figuró que el riesgo del descubrimiento sería demasiado alto.

MENSAJE DE MITNICK
Capacitar a la gente a no juzgar un libro únicamente por su portada--sólo porque alguien es bien vestido y atento no debería ser más creíble.

En una anterior llamada pretexting como una persona de apoyo de su equipo proveedor, había puesto en un acto de canto y baile. \"La empresa ha adquirido una plan de apoyo de dos años y nos estamos poniéndole en la base de datos por lo que podemos saber cuando ha salido un programa de software que se utiliza con un parche o un nuevo versión actualizada. Por eso necesito que me diga qué aplicaciones utiliza.\"
La respuesta que le dio una lista de programas y un amigo contador identificaron la uno llamado MAS 90 como destino--el programa que mantendría su lista de proveedores y las condiciones de descuento y pago para cada uno.

Con ese conocimiento clave, luego utilizó un programa de software para identifiy,\"todos los sede de trabajo en la red, y no llevarlo mucho para encontrar la correcta servidor utilizado por el departamento de contabilidad. Desde el arsenal de herramientas hacker su portátil, lanzó un programa y utiliza para identificar todos los autorizados usuarios en el servidor de destino. Con otro, corrió, a continuación, una lista de usados las contraseñas, como \"en blanco\" y \"password\" sí. \"Contraseña\" trabajada. No hay sorpresa. Personas sólo pierden toda creatividad a la hora de elegir contraseñas.

Sólo seis minutos pasados y el juego terminó la mitad. Fue en.

Otro tres minutos para agregar muy cuidadosamente su nueva empresa, dirección, teléfono nombre de contacto y número a la lista de clientes. Y después de la entrada decisiva, el único que podría hacer toda la diferencia, la entrada que dice todos los elementos debían ser vendió a él en un 1 por ciento más costo Honorable autopartes.

En poco menos de diez minutos, que fue realizado. Dejó de suficiente tiempo para indicar Kaila Gracias, fue a través de comprobar su correo electrónico. Y llegó a Mike Talbot, cambio de planes, estaba en el camino a una reunión en la Oficina de un cliente. Y él no olvidar le recomendaba para ese trabajo en Marketing, tampoco.

Analizando el timo
El intruso que se llama a sí mismo Peter Milton utiliza dos subversión psicológica técnicas--uno planeado, el otro improvisado por el improviso por el momento.

Él vestido como un trabajador de la administración ganar buen dinero. Traje y corbata, cabello cuidadosamente el estilo--estas parecen pequeños detalles, pero hacen una impresión. ME descubierto este yo mismo, sin darse cuenta. En poco tiempo como programador en GTE California--una compañía de teléfono importantes ya no en existencia--he descubierto que Si me llegó en un día sin una insignia, prolijamente vestidos pero casual--decir, deportes camiseta, teléfonos y estibadores--sería detenido y cuestionado. ¿Dónde está su distintivo, que son ¿te, donde trabajas? Otro día podría llegar, aún sin una insignia pero en un traje y corbata, mirando muy corporativa. Usaría una variación de la milenaria Piggybacking técnica, mezcla con una multitud de personas que caminan en un edificio o una entrada segura. Gustaría acoplar en algunas personas mientras se acercaban a la entrada principal y paseo en charla con la multitud como si yo era uno de ellos. ME andaba pasado e incluso si los guardias notado que era menos de la insignia, no me molesta porque no me parecía gestión y estuve con personas que fueron luciendo distintivos.

De esta experiencia, reconocí como predecible el comportamiento de seguridad guardias es. Como el resto de nosotros, estaban haciendo juicios basados en apariciones--una grave vulnerabilidad que los ingenieros sociales aprender a aprovechar.

Arma psicológica segundo del atacante entró en juego cuando se dio cuenta de la inusual esfuerzo que estaba haciendo el recepcionista. Manejar varias cosas a la vez, ella no consigue agarrara pero administrado para que todos se sientan tuvieron su plena atención. Esto tuvo como la marca de alguien interesado en tomar la delantera, para demostrar ella misma. Y, a continuación, cuando reclamó a trabajar en el departamento de Marketing, él vigiladas para ver su reacción, buscando pistas indicar si está estableciendo un relación con ella. Él fue. Para el atacante, esto agrega hasta alguien podía manipular a través de una promesa de intentar ayudarla a pasar a un mejor trabajo. (De claro, si ella hubiera dicho que quería entrar en el departamento de contabilidad, él habría demandado que él tenía contactos para llegar a ella un trabajo allí, en su lugar.)

Los intrusos también son aficionados de otra arma psicológica utilizada en esta historia: fomento de la confianza con un ataque de dos etapas. Primero usó esa conversación chatty acerca de el trabajo en la comercialización, y utilizó también \"nombre colocar\"--dando el nombre de otro empleado--una persona real, por cierto, justo como el nombre de él utilizado era el nombre de un empleado real.

Él podría han seguido la conversación de apertura enseguida con una solicitud de entrar en una sala de conferencias. Pero en su lugar se sentó un rato y fingió trabajo, supuestamente a la espera de su socio, otra manera de atenuar cualquier posible sospechas debido a que un intruso no colgar. Él no cuelgan de muy larga, sin embargo; los ingenieros sociales saben mejor que la estancia en la escena de la delincuencia ya que es necesario.

MENSAJE DE MITNICK

Permitir que a un extraño en un área donde él puede conectar un portátil en el corporativo red aumenta el riesgo de un incidente de seguridad. Es perfectamente razonable para un empleado, especialmente uno desde fuera del sitio, para consultar su correo electrónico desde una Sala de conferencias, pero a menos que el visitante se estableció como un empleado de confianza o la red es segmentado para evitar conexiones no autorizadas, esto puede ser el débil enlace que permite que los archivos de la empresa a estar en peligro.

Sólo para el registro: por las leyes en los libros en el momento de este escrito, Anthony no se había cometido un delito cuando entró en el vestíbulo. No había cometido un delincuencia cuando usó el nombre de un empleado real. No había cometido un delito cuando habló de su camino en la sala de conferencias. No había cometido un delito Cuando conectado a la red de la empresa y busca el destino equipo.

No hasta que realmente rompió el sistema del equipo él romper la ley.

ESPIONAJE SOBRE KEVIN

Cuando yo trabajaba en un pequeño negocio, hace muchos años empecé a notar que cada vez que entré en la Oficina que compartí con el tres equipo personas formado por el departamento de TI, esta un chico particular (Joe, llamaré le aquí) sería alternar rápidamente la pantalla de su ordenador en una ventana diferente. ME inmediatamente reconocido como sospechosos. Cuando sucedió dos veces más el mismo día, estaba seguro de que algo pasaba que yo debo conocer. ¿Qué ¿fue este chico hasta que él no quería ver?

Equipo de Joe actuó como un terminal para acceder a minicomputadoras de la empresa, así que me instalado un programa de monitoreo en el sombrero de minicomputadora VAX me permitido espiar en lo que estaba haciendo. El programa ha actuado como si estaba buscando una cámara de TV sobre su hombro, que me muestre exactamente lo que estaba viendo en su computadora.

Mi escritorio fue junto a Joe; Cumplí a mi monitor lo mejor pudo en parte a enmascarar su punto de vista, pero podría haber Miró en cualquier momento y se dio cuenta de ME espiaba a él. No es un problema; fue demasiado cautivado en lo que fue haciendo notar.

Lo que vi hizo que mi mandíbula soltar. Miré, fascinado, como el bastardo llamado arriba Mis datos de nóminas. Él fue buscar mi sueldo! Sólo había estado allí unos pocos meses en el momento y adivinado Joe no podía reposar la idea que yo podría han hecho más de lo que fue.

Unos minutos más tarde vi que él estaba descargando herramientas hacker utilizadas por menos experimentado los hackers que no saben lo suficiente sobre programación para elaborar el

herramientas para sí mismos. Joe estaba despistado y no tenía idea que uno de American los hackers más experimentados estaba sentado junto a él. Pensé que era divertido.

Ya tenía la información acerca de mi salario; por lo tanto es demasiado tarde detenerlo. Además, tener acceso a cualquier empleado con el equipo en el IRS o la Seguridad Social Administración puede buscar su salario. Seguro que no quería mi mano por la punta informan lo que descubrí lo que era hasta. Fue mi principal objetivo en el momento mantener un perfil bajo y un buen ingeniero social no anuncia su habilidades y conocimientos. Siempre desea personas le subestima, no veo usted como una amenaza.

Así que dejarlo ir y se rió a mí mismo que Joe pensó que sabía algún secreto yo, cuando era al revés: yo tenía la mano superior por saber lo que había sido hasta.

En el tiempo he descubierto que tres de mis compañeros de trabajo en el grupo de TI divertido ellos mismos consultando el salario de este o ese Secretario lindo o (para la uno chica en el grupo) buscando neat chico que habían manchado. Y estaban todos averiguar el salario y bonos de nadie en la empresa eran curiosos incluidos los directivos.

Analizando el timo

Esta historia ilustra un problema interesante. Eran accesibles a los archivos de nómina las personas que tenían la responsabilidad de mantener el equipo de la empresa sistemas. Por lo que todo se trata de una cuestión personal: decidir quién puede confiar. En algunos casos, personal de TI puede resultar irresistible a snoop alrededor. Y tienen la capacidad para hacerlo porque tienen privilegios que les permita sortear el acceso controles en esos archivos.

Sería una salvaguardia auditar el acceso a archivos especialmente sensibles, como la nómina. Por supuesto, cualquier persona que tenga los privilegios necesarios podría deshabilitar auditoría o posiblemente eliminar todas las entradas que apuntan hacia ellos, pero cada uno paso adicional lleva más esfuerzo para ocultar por parte de un empleado sin escrúpulos.

PREVENIR LA CON

De manoseo a través de su basura para timar a un guardia de seguridad o recepcionista, social ingenieros físicamente pueden invadir su espacio corporativo. Pero alegrará oír que existen medidas preventivas que puede tomar.

Protección después de horas

Se debe exigir a todos los empleados que llegan para trabajar sin sus insignias parada en la Oficina de recepción o seguridad de lobby para obtener una acreditación 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 de la empresa ha tenido un conjunto específico de pasos a seguir cuando se enfrentan a nadie sin la insignia de empleados requeridos.

Para empresas o áreas dentro de una empresa donde la seguridad no es un alto nivel preocupación, puede no ser importante insistir en que cada persona tiene un distintivo visible en todo momento. Pero en las empresas con zonas sensibles, este debería ser un estándar requisito, cumplir rígidamente. Empleados deben ser entrenados y motivados para hay personas que no tienen un distintivo y empleados de alto nivel de desafío se enseñó a aceptar esos desafíos sin causar vergüenza a la persona que se les detiene.

Política de la empresa, debe informar a los empleados de las penas para aquellos que sistemáticamente no llevar sus insignias; las sanciones pueden incluir enviar la empleado de hogar para el día sin pagar, o una notación en su archivo personal. Algunos empresas de instituir una serie de penas progresivamente más severas que pueden incluir notifica el problema al administrador de la persona y, a continuación, emitir una formal advertencia.

Además, donde hay información confidencial para proteger, la empresa debe: establecer procedimientos para autorizar a personas que necesiten para visitar durante no empresariales horas. Una solución: exigir que se hagan los arreglos a través de empresas seguridad o algún otro grupo designado. Este grupo sería verificar rutinariamente el identidad de cualquier empleado llamando a organizar un período visita mediante una llamada a la supervisor de la persona o algún otro método razonablemente seguro.

Tratamiento de la basura con respeto
La historia de buceo de recolección excavadas en los potenciales inadecuados de tu Papelera corporativa. Las ocho claves de sabiduría con respecto a la basura:

Clasificar toda la información confidencial según el grado de sensibilidad.

Establecer procedimientos de toda la empresa para descartar información confidencial.

Insisten en que toda la información confidencial a descartarse en primer lugar se destruyen y proporcionar de una manera segura para deshacerse de información importante sobre trozos de papel demasiado pequeño para la destrucción. Trituradoras no deben ser el tipo de presupuesto low-end, que su vez con tiras de papel que un atacante decidido, dado la suficiente paciencia, puede volver a montar. En cambio, deben ser del tipo llamado Cruz-trituradoras, o aquellos que procesar la salida en pulpa inútil.

Proporcionar una manera para representar inutilizable o borrar completamente equipo multimedia--disquetes, discos Zip, CDs y DVDs utilizados para almacenar archivos, cintas extraíbles, antiguos discos duros y otros soportes informáticos--antes de que se descartan. Recuerde

eliminar archivos que no realmente eliminarlos; aún pueden ser recuperados--como Ejecutivos de Enron y muchos otros han aprendido a su consternación. Simplemente colocando los soportes informáticos en la basura están una invitación a su basurero amistoso local buzo. (Véase capítulo 16 de directrices específicas sobre la disposición de medios y dispositivos).

Mantener un nivel adecuado de control sobre la selección de personas en su limpieza de tripulaciones, utilizando el fondo comprueba si procede.

Recordar a los empleados periódicamente para reflexionar sobre la naturaleza de los materiales son tirando a la basura.

Bloquear los contenedores de basura.

Utilizar contenedores de disposición separada para materiales sensibles y el contrato para tener la materiales resueltas por una empresa de servidumbre que se especializa en este trabajo.

Diciendo adiós a los empleados
Se ha señalado anteriormente en estas páginas sobre la necesidad de ironclad procedimientos cuando un empleado saliente ha tenido acceso a información confidencial, contraseñas, números de acceso telefónico y similares. Los procedimientos de seguridad que deba proporcionan una forma para realizar un seguimiento de quién tiene autorización para diversos sistemas. ser difícil de mantener un ingeniero social determinado resbale pasado su seguridad barreras, pero no hacerlo fácil para un ex-empleado.

Otro paso fácilmente pasar por alto: cuando un empleado que estaba autorizado a recuperar las cintas de backup de hojas de almacenamiento, debe llamar a una política escrita para la empresa de almacenamiento de información que se le notifique inmediatamente para quitar su nombre de lista de autorización.

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

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

Una política de terminación de equipo del empleado acceso inmediato--preferiblemente antes de que la persona ha dejado incluso el edificio.

Un procedimiento para recuperar el gafete de la persona, así como las claves o electrónicos dispositivos de acceso.

Disposiciones que requieren guardias de seguridad ver foto ID antes de admitir a cualquiera empleados que no tienen su pase de seguridad, y para comprobar el nombre contra una lista para comprobar que la persona aún es empleada por la organización.

Algunos pasos más parecerá excesiva o demasiado caros para algunas empresas, pero son adecuados a los demás. Entre estos seguridad más estrictas las medidas son:

Acreditaciones electrónicos combinados con escáneres en entradas; cada empleado robaba su insignia mediante el analizador electrónico una instantánea determinación de que la persona sigue siendo un empleado actual y derecho a entrar en el edificio. (Sin embargo, tenga en cuenta que guardias de seguridad aún deben ser entrenados para estar en alerta para piggybacking--una persona no autorizada que se desliza por la estela de un empleado legítimo).

Un requisito que todos los empleados del mismo grupo de trabajo como la persona que abandone (especialmente si la persona es ser despedida) cambiar sus contraseñas. (Hace este parecer ¿extremo? Muchos años después de mi breve tiempo trabajando en General teléfono, me aprendí que la gente de seguridad Pacific Bell, cuando escucharon teléfono General había contratado me, \"rodó en el suelo de risa\". Pero en General teléfono crédito cuando se dieron cuenta que tenían un reputado hacker trabajando para ellos después de me despidió, entonces se exige que se cambie las contraseñas para todos en el empresa!)

No desea que sus instalaciones para sentirse como cárceles, pero al mismo tiempo necesita defender contra el hombre que fue despedido ayer pero es intención volver hoy de hacerlo daños.

No se olvide nadie

Las políticas de seguridad tienpasar por alto el nivel de entrada trabajador, la gente le gusta recepcionistas que no manejan información corporativa confidencial. Hemos visto en otros lugares que los recepcionistas son un objetivo práctico para los atacantes y la historia de la robo en la empresa de piezas de auto proporciona otro ejemplo: una persona amistosa, vestido como un profesional, que pretende ser un empleado de la compañía de otro instalación puede no ser lo que parece. Recepcionistas deben ser capacitados sobre pidiendo educadamente ID compañía cuando sea apropiado y las necesidades de capacitación que no sólo para la recepcionista principal sino también para todos los que se asienta como un alivio a la recepción durante la hora del almuerzo o pausas.

Para los visitantes de fuera de la empresa, la política debe exigir que una identificación con foto se muestra y la información registrada. No es difícil conseguir ID falso, pero por lo menos exigentes ID dificulta grado pre-texto, uno para el atacante.

En algunas empresas, tiene sentido seguir una política que requiere que los visitantes ser acompañado desde el lobby y de reunión en reunión. Procedimientos, es necesario la escolta que claro al entregar al visitante su primera cita
Esta persona ha entrado en el edificio como empleado, o no empleados. ¿Por qué es ¿este importante? Porque, como hemos visto en anteriores
historias, un atacante a menudo pasará él mismo un disfraz a la primera persona se encontró y como alguien a la siguiente. Es demasiado fácil para un atacante mostrar hasta en el vestíbulo, convencer al recepcionista que tiene una cita con, digamos, un ingeniero.., luego de ser escoltado a la Oficina del ingeniero donde afirma ser un rep de una empresa que quiere vender algún producto a la empresa.. y luego, después de la reunión con el ingeniero, él tiene libre acceso a moverse el edificio.

Antes de admitir a un empleado fuera del sitio a los locales, procedimientos adecuados debe seguirse para comprobar que la persona es verdaderamente un empleado; recepcionistas y guardias deben ser conscientes de los métodos utilizados por los atacantes a pretexto la identidad de un empleado para obtener acceso a los edificios de la empresa.

¿Por qué proteger contra el atacante contras su camino dentro del edificio ¿y logra conectar su portátil en un puerto de red detrás del firewall corporativo? Dada la tecnología actual, esto es un reto: salas de conferencias, salas de formación, y áreas similares no deben abandonar la red puertos no seguras, pero deben proteger ellos con firewalls o routers. Pero mejor protección vendría desde el uso de un método seguro para autenticar a los usuarios que se conectan a la red.

Asegurarla!
Una palabra a los sabios: en su propia empresa, probablemente sabe cada trabajador o puede averiguar en momentos cuánto están ganando, cuánto tarda el CEO casa, y quién los está usando el jet corporativo para ir de vacaciones de esquí.

Es posible incluso en algunas empresas de TI personas o contable a aumentar sus propios salarios, hacer pagos a un proveedor falso, quitar negativa clasificación de los registros de HR y así sucesivamente. A veces es sólo el miedo a obtener atrapados que les mantiene honesto.., y luego un día a lo largo viene alguien cuya avaricia Deshonestidad nativo hace él (ella) ignorar el riesgo y tomar cualquiera que sea su piensa que puede salirse con.

Las soluciones son, por supuesto. Archivos confidenciales pueden protegerse mediante la instalación de controles de acceso adecuado para que sólo las personas autorizadas pueden abrirlos. Algunos los sistemas operativos tienen controles de auditoría que pueden ser configurados para mantener un regist determinados eventos, como cada persona que intenta acceder a un archivo protegido, independientemente de si es o no el intento tiene éxito.

Si su empresa ha entendido esta cuestión y ha implementado un acceso adecuado controles y auditorías que protege archivos confidenciales--está tomando medidas eficaces la dirección correcta.

Capítulo 11
La combinación de tecnología y la ingeniería Social

Un ingeniero social vive por su habilidad para manipular a la gente a hacer cosas
le ayudara a lograr su objetivo, pero el éxito a menudo también requiere un elevado grado de
conocimientos y habilidades con sistemas informáticos y sistemas telefónicos.

Aquí es una muestra de estafas típicas de ingeniería social donde jugó tecnología
un papel importante.

BARRAS DETRÁS DE HACKING
¿Cuáles son algunas de las instalaciones más seguras, puede pensar, protegidos contra
¿robo, si física, telecomunicaciones, o por medios electrónicos en la naturaleza? Fuerte
¿Knox? Seguro. ¿La Casa Blanca? Absolutamente. NORAD, el aire de América del Norte
¿Instalación de defensa enterrado profundo bajo una montaña? Definitivamente.

¿Por qué las cárceles federales y centros de detención? Deben ser aproximadamente tan seguras
¿como cualquier lugar en el país, correcto? Gente rara vez escapar, y cuando lo hacen, ellos
normalmente se encuentran atrapados en poco tiempo. Se podría pensar que sería una instalación federal
ser invulnerable a ataques de ingeniería social. Pero sería erróneo--hay
no hay tal cosa como la seguridad infalible, en cualquier lugar.

Hace unos pocos años, un par de timadores (estafadores profesionales) se topó con un problema. Se
resultó que habían levantado un paquete grande de dinero en efectivo de un juez local. La pareja había
Estado en problemas con la ley y desactivar a través de los años, pero esta vez la federal
las autoridades tomaron un interés. Ellos nabbed uno de los timadores, Charles Gondorff,
y lo arrojó en un centro penitenciario cerca de San Diego. El magistrado federal
le ordenó detenidos como riesgo de vuelo y un peligro para la comunidad.

Su pal Johnny Hooker sabía que Charlie iba a necesitar a un abogado de la defensa.
¿Pero donde iba el dinero provienen? la mayoría de timadores, su dinero había
ido siempre buena ropa, apetece cam y las damas tan rápido como llegó.
Johnny larely tenido suficiente para vivir.

El dinero para un buen abogado tendría que provienen de otra estafa en ejecución.
Johnny no estaba hasta hacerlo en este propio. Siempre había sido Charlie Gondorff
los cerebros detrás de sus contras. Pero Johnny no se atreven visitar el centro de detención
pregunta a Charlie qué hacer, no cuando los federales sabían había dos hombres implicados
en la estafa y estaban tan ansiosos por poner sus manos sobre la otra. Especialmente
ya puede visitar la única familia. lo que significaba que tendría que mostrar identificación falsa
y la pretensión de ser un miembro de la familia. Intentando usar ID falso en una prisión federal no
suenan como una idea inteligente.

No, tendría que ponerse en contacto con Gondorff alguna otra manera.
No sería fácil. No se permite que ningún recluso en cualquier instalación federal, estatal o local recibir llamadas telefónicas. Un signo publicado por cada teléfono recluso en un federal Centro de detención dice algo como, \"este anuncio es asesorar al usuario que todos las conversaciones de este teléfono están sujetos a vigilancia. y el uso de la teléfono constituye el consentimiento a la supervisión. Con funcionarios del Gobierno escuchar sus llamadas telefónicas mientras comete un crimen tiene una forma de ampliar sus planes de vacaciones financiadas por el Gobierno Federal. Johnny sabía, sin embargo, que ciertas llamadas telefónicas no fueron supervisados: llamadas entre un prisionero y su abogado, protegidos por la Constitución como cliente-comunicaciones de la Procuraduría, por ejemplo. De hecho, las instalaciones donde Gondorff fue retenido tenía teléfonos conectados directamente al público federal Defensoría. Recoger uno de esos teléfonos y una conexión directa se realiza el teléfono correspondiente en la DOP. Las llamadas de empresa Este servicio Direct Connect. Las autoridades a asuman que el servicio es seguro y invulnerable a manipulaciones porque saliente llamadas sólo pueden ir a la DOP, y las llamadas entrantes están bloqueadas. Incluso si alguien de alguna manera pudieron averiguar el número de teléfono, los teléfonosestán programados en el conmutador de compañía de teléfono como negar a terminaque es un torpe término de compañía de teléfono de servicio donde no se permiten las llamadas entrantes.

Desde cualquier grifter decente hasta la mitad es versado en el arte del engaño, Johnny figuró tenía que ser una forma de resolver este problema. Desde la interior, Gondorff ya había intentado recoger uno de los teléfonos de DOP y diciendo: \"este es Tom, en el centro de reparación de compañía de teléfono.

JERGA
DIRECT CONNECT término de compañía de teléfono de una línea de teléfono que va directamente a un número específico cuando recogió

DENEGAR RESCINDIR un servicio de compañía de teléfono opción cuando de conmutación equipos se establece que no se puede recibir llamadas entrantes a un número de teléfono

Nos quedamos una prueba de esta línea y necesita intentar marcar nueve y luego cero-cero.\" Los nueve habría accede a una línea exterior, el cero a cero sería entonces han llegado a un operador de larga distancia. No funcionó la persona respondiendo a la teléfono en el PDO ya fue cadera a ese truco.

Johnny estaba teniendo éxito mejor. Rápidamente descubrió que hubo diez unidades de vivienda en el centro de detención, cada uno con una línea de teléfono de conexión directa a la Defensoría Pública. Johnny encontró algunos obstáculos, pero como un ingeniero social, fue capaz de pensar su manera alrededor de estos molestos tropezar

bloques. ¿Qué unidad fue Gondorff en? ¿Cuál fue el número de teléfono para el ¿servicios en dicha unidad de vivienda de conexión directa? Y cómo él inicialmente obtendría un ¿mensaje a Gondorff sin él ser interceptados por funcionarios de prisiones?

Lo que puede parecer imposible para la gente promedio, como obtener el secreto teléfono números localizadas en instituciones federales, es muy a menudo no más de una pocos teléfono llamadas fuera de un estafador. Después de un par de noches lanzando y torneado un plan de intercambio de ideas, Johnny despertó una mormng con todo lo establecido en su mente, en cinco pasos.

En primer lugar, encontraría fuera de los números de teléfono para esos diez conexión directa teléfonos pa la DOP.

Tendría los diez cambió de manera que los teléfonos permitiría las llamadas entrantes.

Encontraría fuera Gondorff fue en qué unidad de vivienda.

Entonces él sería averiguar qué número de teléfono fue a esa unidad.

Finalmente, él tuviera con Gondorff cuando a esperar su llamada, sin la Gobierno sospechando algo.

Pieza una \"tarta, pensó.

Llamando a Ma Bell...
Johnny comenzó llamando a la Oficina de negocios de compañía de teléfono bajo el pretexto de de la administración de servicios generales, la agenc responsable compra de bienes y servicios para el Gobierno federal.
Dijo que estaba trabajando en un pedido de adquisición de servicios adicionales y necesita saber la información de facturación para los servicios de conexión directa actualmente en uso, incluyendo el costo de números y mensual de teléfono de trabajo en el San Diego Centro de detención. Estaba feliz de la señora Ayuda.

Sólo para asegurarse, intentó marcar en una de esas líneas y fue contestada por el audichron típico de grabación, \"esta línea ha sido desconectada o ya no está en servicio \"— que sabía que carecía de tipo pero en su lugar, significa que la línea fue programado para bloquear las llamadas entrantes, tal como se esperaba.

Sabía de su extenso conocimiento de operaciones de la compañía de teléfono y procedimientos que necesitaba para llegar a un departamento llamado la reciente Cambio Centro de autorización de memoria o RCMAC (que siempre me pregunto quien conforman estos nombres!). Comenzó llamando a la compañía telefónica Negocio Oficina, dijo que estaba en reparación y necesita saber el número de la RCMAC

maneja el área de servicio para el código de área y prefijo dio, que fue
sirvió fuera de la misma oficina central para todos los de líneas telefónicas en la detención
Centro. Era una solicitud de rutina, el tipo previsto a los técnicos en el campo
necesitados de asistencia, y el empleado no dudó en darle el
número.

Llamado RCMAC, dio un nombre falso y nuevamente dijo que estaba en reparación
Tenía la señora que respondió uno de los números de teléfono que tenía acceso a
estafó a fuera de la Oficina de negocios algunas llamadas anteriormente; Cuando ella tenía hasta Johnny
¿preguntó, \"es el número establecido para negar la terminación?

There was an error deserializing the object of type System.String. Encountered unexpected char

There was an error deserializing the object of type System.String. Encountered unexpected character 'J'.
There was an error deserializing the object of type System.String. Unexpected end of file. Following
quitar el denegar terminar característica, ¿vale?\" Hubo una pausa como ella comprobada
otro sistema para comprobar que se había colocado un pedido de servicio a
autorizar el cambio. Ella dijo, \"que número se supone que es restringido para
saliente llamadassólo. Hay ninguna orden de servicio para un cambio\".

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
representante de cuentas regulares que maneja a este cliente fue casa enfermos y olvidó que
alguien cuidar de la orden por ella. Por supuesto es ahora el cliente hasta
armas sobre él\".

Después de una pausa momentánea, mientras que la dama reflexionaba sobre esta petición, que sería
fuera de lo común y en contra de procedimientos operativos estándar, dijo, \"Okay\".
Podía oír su escritura, entrando en el cambio. Y unos segundos más tarde, fue
hecho.
El hielo había sido roto, una especie de colusión entre ellos. Lectura
actitud y disposición para ayudar a la mujer, Johnny no dude en hacerlo
todos. Dijo, \"tienes unos minutos más para ayudarme?\"

There was an error deserializing the object of type System.String. Encountered unexpected characte

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
mismo problema. Leeré a los números, por lo que puede asegurarse de que no está listo
para denegar terminar--está bien?\" Ella dijo que estaba bien.

Unos minutos más tarde, todas las líneas de teléfono diez habían sido \"fijo\" para aceptar entrante
llamadas.

Buscar Gondorff
A continuación, averiguar qué unidad de vivienda fue Gondorff. Esta es la información que el personas que dirigen centros de detención y cárceles definitivamente no desean que los forasteros a saber. Una vez más Johnny tuvieron que confiar en sus habilidades de ingeniería social.

Colocó una llamada a una prisión federal en otra ciudad--llamó a Miami, pero cualquiera hubiera trabajado--y afirmó que estaba llamando desde la detención Centro de Nueva York. Pidió hablar con alguien que trabajó en la Oficina Equipo de Centinela, el sistema informático que contiene información sobre cada prisionero recluido en un centro de mesa de prisiones en todo el país.

Cuando esa persona en el teléfono, Johnny pone en su acento de Brooklyn. \"Hola\" dijo. \"Esto es Thomas en el FDC en Nueva York. Mantiene nuestra conexión a Centinela bajando, puede encontrar la ubicación de un prisionero para mí, creo que esta preso puede ser en la institución\"y le dio el nombre de Gondorff y su registro número.

There was an error deserializing the object of type System.String. The token 'true' was expected but foun
Centro Penitenciario de San Diego\".

Johnny fingió ser sorprendidos. \"San Diego! Se suponía que transferirse a Miami en puente aéreo del Mariscal la semana pasada! Estamos hablando el mismo tio-- ¿Qué es DOB del tío?\"

03\/12\/60,\"el hombre lee desde su pantalla.

Sí, es el mismo chico. ¿Qué unidad de vivienda está en?

There was an error deserializing the object of type System.String. The token 'true' was expected but fou
Aunque no hay ninguna razón concebible por qué un empleado de la cárcel en Nueva York necesitaría saber esto.

Johnny ahora tenía los teléfonos activados para llamadas entrantes y sabía que unidad de vivienda fue Gondorff. A continuación, averiguar qué número de teléfono conectado a unidad del Norte diez.

Este fue un poco difícil. Johnny había llamado uno de los números. Sabía que la ¿desactivar el timbre del teléfono; nadie sabría que estaba sonando. Por lo tanto él sentado leyendo Europa de Fodor} Guía de viajes de grandes ciudades. mientras escucha la constante sonar el altavoz hasta que finalmente alguien recogió. El recluso en el otro extremo sería, por supuesto, tratar de llegar a su abogado de oficio. Johnny se preparó con la respuesta esperada. \"Defensoría Pública,\" él anunciado.

Cuando el hombre le preguntó a su abogado, Johnny dijo, \"voy a ver si está disponible, lo que unidad de vivienda estás llamando desde?\" Él apuntó hacia abajo de la respuesta del hombre, hace clic en en suspenso, volvió después de un minuto y dijo: \"él está en corte, vas a tener que volver a llamar más tarde\"y colgó.

Había pasado la mayor parte de una mañana, pero podría haber sido peor; su cuarto intento resultado para ser de diez Norte. Así ahora, Johnny sabía el número de teléfono al teléfono PDO de unidad de vivienda de Gondorff.

Sincronizar sus relojes

Ahora llegar un mensaje a través de Gondorff en cuando a recoger la línea telefónica los reclusos que conecta directamente a la Defensoría Pública.]' era más fácil de lo que podría sonar.

Johnny llamado el centro de detención utilizando su voz suena oficial, identificado a sí mismo como un empleado y pidió ser transferido al norte de diez. La llamada fue corregir a través de. Cuando el oficial correccional se recogió, estafó a Johnny él mediante la abreviatura del insider para recepción y aprobación de la gestión, la unidad que procesos nuevos reclusos y los salientes fuera: \"este es Tyson en r dijo. \"Necesito hablar con el recluso Gondorff. Tenemos alguna propiedad de su que tenemos para enviar y necesitamos una dirección donde quiere recibirlo. Se le podría llamar la teléfono para mí?\"

Johnny podía oír la Guardia gritando en la sala de día. Después de una impaciente varios minutos, una voz familiar llegó a la línea.
Johnny le dijo, \"no decir nada hasta que explique lo que se trata\". Explicó el pretexto para Johnny podría sonar como él estaba discutiendo dónde su propiedad debe enviarse. Johnny entonces dijo, \"si se puede llegar a defensor público teléfono en uno esta tarde, no responden. Si no, entonces dices una vez que usted puede estar allí.\" Gondorff no responder. Johnny salió, \"bien. Estar allí en uno o ' Clock. Llamo luego. Recoger el teléfono.

Si empieza a sonar a la Oficina de defensores públicos, flash el gancho conmutador cada veinte segundos. Seguiremos intentando hasta que me escuchas en el otro extremo.\"

En 1, Gondorff recogió el teléfono y Johnny estaba allí esperando él. Tuvieron una conversación chatty, agradable, calmada, conduciendo a una serie de llamadas similares a plan de la estafa que plantearía el dinero para pagar legal del Gondorff honorarios--todos libres de la vigilancia del Gobierno.

Analizando el timo

Este episodio ofrece un buen ejemplo de cómo puede hacer un ingeniero social el aparentemente imposible pasar por la muerte de varias personas, cada uno haciendo

algo que, por sí mismo, parece intrascendente. En realidad, cada acción proporciona una pequeña pieza del rompecabezas hasta que se complete la con.

El primer empleado de compañía de teléfono pensaba que ella estaba dando información a alguien de la Oficina de Contabilidad General del Gobierno federal.

El próximo empleado de compañía de teléfono sabía que ella no pretende para cambiar la clase de servicio telefónico sin una orden de servicio, pero ayudó el hombre amable de todos modos. Esto hizo posible realizar llamadas a través de diez todos del público líneas de teléfono del Defensor 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 del equipo parece perfectamente razonable. Y aunque no me parecía ningún motivo gustaría saber la unidad de vivienda, ¿por qué no responder a la pregunta?

Y la Guardia Norte diez que creían que el llamador era realmente desde dentro ¿las mismas instalaciones, llamando en misión oficial? Era un perfectamente razonable solicitud, por lo que llamó al recluso Gondorff al teléfono. No hay gran cosa.

Una serie de historias bien planificadas que suman para completar el aguijón.

LA DESCARGA RÁPIDA

Diez años después de que habían terminado la escuela de derecho, Ned Racine vio a sus compañeros de c viven en casas Niza con césped frontal, pertenecientes a clubes de campo, jugar al golf una o dos veces por semana, mientras él todavía era tratando casos de penny previa para el tipo de personas que nunca tuvieron suficiente dinero para pagar su factura. Celos pueden ser una nasty compañero. Finalmente un día, Ned estaba harto.

El un buen cliente que tuvo alguna vez fue una pequeña pero muy exitosa firma de contabilidad especializado en fusiones y adquisiciones. No utilizaron a Ned por mucho tiempo, sólo tiempo suficiente para él para darse cuenta de que estaban involucrados en ofertas que, una vez que llegue periódicos, afectaría el precio de las acciones de uno o dos cotizan empresas. Penny previa, las existencias de tablón de anuncios, pero de alguna manera que fue incluso mejor--un pequeño salto en el precio podría representar una gran porcentaje de ganancia en un inversión. Si sólo podía acceder a sus archivos y averiguar cuáles eran trabajando en...

Sabía que un hombre que conocía a un hombre que era prudente sobre cosas no exactamente en el incorporar. El hombre escuchó el plan, se dispararon hasta y accedió a ayudar a. Para un suele cobra una tarifa menor que él, contra un porcentaje del mercado de valores de Ned

matar, el hombre dio a Ned instrucciones sobre qué hacer. Él también le dio una mano pequeño dispositivo a usar, algo nuevo en el mercado.

Durante unos días en una fila Ned mantiene vigilancia en el estacionamiento de la pequeña empresa Parque donde la contabilidad de la empresa tenía sus oficinas sin pretensiones, como escaparate. Mayoría de la gente deja entre 5:30 y 6. 7, El lote estaba vacío. La tripulación de limpieza se presentó alrededor de 7:30. Perfecto.

La noche siguiente en pocos minutos antes de 8, Ned aparcado en la calle desde el estacionamiento. Como se esperaba, el lote estaba vacío salvo por el camión de la empresa de servicios de conserjería. Ned pone su oreja a la puerta y escuchó el vacío ejecutar limpiador. Él golpeó a la puerta muy fuerte y se mantuvo allí esperando en su traje y corbata, sosteniendo su maletín bien. No hay respuesta, pero él fue paciente. Una vez más lo noqueó. Finalmente apareció un hombre de la tripulación de limpieza. \"Hola,\" Ned gritó a través de la puerta de vidrio, mostrando la tarjeta de presentación de uno de los socios que había recogido algún tiempo antes. \"Bloquean las llaves de mi en mi coche y necesito para llegar a mi escritorio\".

El hombre desbloquea la puerta, bloqueó nuevamente detrás de Ned y luego bajó la corredor encender luces para que Ned podía ver donde iba. Y por qué no--le estaba siendo amable con una de las personas que ayudaron a poner comida en su mesa. O lo tenían toda la razón a pensar.

MENSAJE DE MITNICK

Espías industriales e intrusos de equipo a veces hará una entrada física en los negocios específicas. En lugar de utilizar una palanca para romper, ingeniero social utiliza el arte del engaño para influir en la persona al otro lado de la puerta abierto para él.

Ned se sentó en el equipo de uno de los socios y había convertido. Mientras se estaba empezando, instaló el dispositivo pequeño le había dado en el puerto USB del equipo, un gadget lo suficientemente pequeño para llevar en un llavero, aún capaz de mantener más de 120 megabytes de datos. Conectado a la red con el nombre de usuario y la contraseña del Secretario del socio, que fueron escritos cómodamente abajo en una nota Post-it pegados a la pantalla. En menos de cinco minutos, había Ned Descargar cada archivo de hoja de cálculo y documentos almacenado en la estación de trabajo y desde el socio de directorio de red y fue en su camino a casa.

DINERO FÁCIL

Cuando me introdujo a los equipos en la escuela secundaria, tuvimos que conectar a través de un módem a una minicomputadora de DEC PDP 11 central en el centro de Los Ángeles

que comparten todas las escuelas secundarias en los Ángeles. El sistema operativo en el equipo se llamaba RSTS\/E, y era el sistema operativo que aprendí a trabajar con.

En ese momento, en 1981, DEC patrocinó una conferencia anual para los usuarios del producto, y un año leí que la Conferencia iba a celebrarse en L.A. Un popular revista para usuarios de este sistema operativo a un anuncio sobre un nuevo producto de seguridad, bloqueo-11. Se promueve el producto con un anuncio inteligente campaña que dijo algo como, \"es 3:30.M. y Johnny por la calle encuentra tu número telefónico, intente 555-0336, sobre su 336th. Es y estás fuera. Obtener bloqueo-11\". El producto, el anuncio sugerido, era a prueba de piratas informáticos. Y fue va a ser expuesto en la Conferencia.

Estaba ansioso por ver el producto por mí mismo. Un compañero de escuela secundaria y amigo, Vinny, mi pareja hacking durante varios años, quien más tarde se convirtió en un informante federal contra mí, compartir mi interés en el nuevo producto de DEC y me animó a ir a la Conferencia con él.

Efectivo en la línea

Llegamos a encontrar un gran zumbido ya va alrededor de la multitud en la Feria acerca de bloqueo-11. Parece que los desarrolladores apuesta dinero en efectivo en la línea en un apuesto que nadie podría irrumpir en sus productos. Sonaba como un reto que pudiera no resistir.

Nos dirigió directamente a la cabina de bloqueo-11 y encontró que tripulada por tres chicos ¿Quiénes eran los desarrolladores del producto; Les reconocí y reconocieron me--incluso como un adolescente, que ya tenía una reputación como hacker y phreaker porque de una gran historia el LA Times había quedado sobre mi primer pincel juvenil con el autoridades. El artículo informó que había hablado mi camino en un teléfono de Pacífico edificio en medio de la noche y andaba fuera con manuales de equipo, derecha bajo la nariz de su guardia de seguridad. (Parece que los tiempos querían ejecutar un historia sensacionalista y sirvieron a sus propósitos a publicar mi nombre; porque me todavía era un juvenil, el artículo violaba la costumbre, si no el derecho de retención los nombres de los menores acusaron de irregularidades.)

Cuando Vinny y caminó, ir creado cierto interés en ambos lados. Hubo un interés de su lado porque me reconocieron como el hacker habían leído sobre y estaban un poco sorprendidos al verme. Se creó un interés por nuestra parte porque cada uno de los tres promotores estaba de pie allí con una factura de $100 pegado de su insignia de la feria. El dinero del premio para alguien que podía derrotar a sus sistema sería el conjunto $300--que sonaba como un montón de dinero a un par de adolescentes. Dificilmente podríamos esperar para empezar a trabajar.

LOCK-11 fue diseñado en un principio establecido que se basó en dos niveles de seguridad. Un usuario tiene que tener un ID y una contraseña válidos como de costumbre, pero además que ID y contraseña sólo funcionaría cuando entró desde terminales autorizados, un enfoque llamado seguridad basada en el terminal. Para derrotar el sistema, sería un hacker no sólo necesitan tener conocimiento de un ID de cuenta y contraseña, pero también hay que introducir esa información desde la terminal correcta. El método fue bien establecido, y los inventores de bloqueo-11 estaban convencidos de mantendría el mal chicos de fuera. Decidimos que íbamos a enseñarles una lección y ganar tres cien bucks para arrancar.

Un chico sabía quien era considerado un gurú RSTS\/E ya nos había golpeado el stand. Años antes de que había sido uno de los chicos que tenían me desafió a romper en el equipo de desarrollo interno de DEC, tras lo cual sus colaboradores habían me convirtió. Desde esos días se había convertido en un respetado programador. Nos descubrí que había intentado derrotar el programa de seguridad de bloqueo-11 no mucho antes de que nos llegaron, pero no pudo. El incidente dio a los desarrolladores mayor confianza que su producto es realmente seguro.

JERGA
Seguridad basada en la TERMINAL basado en parte en la identificación de la terminal de computadora en particular se utiliza; Este método de seguridad era especialmente popular con mainframes de IBM.

El concurso fue un reto sencillo: usted entrar, ganar los bucks. A truco de buena publicidad..., a menos que alguien fue capaz de avergonzarles y tomar la dinero. Estaban tan seguros de su producto que eran aún lo suficientemente audaces tener un listado publicado en el stand de los números de cuenta y contraseñas correspondientes a algunas cuentas en el sistema. Y no sólo regular cuentas de usuario, pero todas las cuentas con privilegios.

Que fue realmente menos atrevida de lo que suena: en este tipo de configuración, yo sabía, cada uno terminal se conecta a un puerto en el propio equipo. No es ciencia espacial para figura que había fijado hasta las cinco terminales en la sala por lo que un visitante podría registrar sólo como un usuario sin privilegios--es decir, fueron posibles sólo a inicios de sesión cuentas sin privilegios de administrador del sistema. Parecía como si sólo hubiera dos vías: o bien omitir el software de seguridad en total--exactamente lo que el LOCK-11 fue diseñado para prevenir; o de alguna manera obtener todo el software de una forma que los desarrolladores no habían imaginado.

Tomando el reto
Vinny y me alejé y habló sobre el reto, y surgió con un Plan de. Vagó alrededor inocentemente, mantener un ojo en el stand de una distancia. Al mediodía, cuando la multitud se estrecharon a, toman los tres desarrolladores

ventaja de la ruptura y despegó juntos para conseguir algo de comer, dejando detrás de una mujer que podría haber sido la esposa o novia de uno de ellos. Nos sauntered espalda más y me distrajo la mujer, charlando arriba acerca de esto y que, \"cuánto tiempo ha estado con la empresa?\"¿Qué otros productos su empresa tiene en el mercado?\"y así sucesivamente.

Mientras tanto Vinny, fuera de su vista, había ido a trabajar, haciendo uso de una habilidad él y yo habíamos desarrollado. Además de la fascinación de dividir en equipos, y mi propio interés en la magia, nos habíamos ambos ha intrigado por aprender cómo abrir cerraduras. Como un chico joven, había rastreado los estantes de un metro librería en el Valle de San Fernando que tenían volúmenes sobre recolección de bloqueos, obtener de las esposas, crear identidades falsas--todo tipo de cosas que no era un niño se supone que para conocer.

Vinny, como yo, había practicado lock picking hasta que estuvimos bastante bien con cualquiera bloqueo de ferretería mediocres. Hubo un tiempo cuando recibí una patada fuera de bromas con bloqueos, como alguien que estaba utilizando dos bloqueos para manchas protección adicional, recogiendo los bloqueos y poner-anillo atrás en los lugares opuestos, que sería baffle y frustrar el propietario cuando trató de abrir cada uno de ellos con el tecla incorrecta.

En la sala de exposiciones, siguiera mantener la joven distraído mientras Vinny, cuclillas hacia abajo en la parte trasera de la cabina por lo que no podía beseen, escogió el bloqueo el gabinete que albergaba su minicomputadora PDP-11 y las terminaciones de cable. Llamar al gabinete bloqueado era casi una broma. Se fue asegurado con qué cerrajeros Consulte como un bloqueo de oblea, notoriamente fácil de elegir, incluso para aficionados, bastante torpe selectores de bloqueo como nosotros.

Tomó Vinny todos de aproximadamente un minuto para abrir la cerradura. Dentro del gabinete encontró justo lo que habíamos previsto: la franja de puertos para conectar los terminales de usuario, y un puerto para lo que ha llamado la consola terminal. Este fue el terminal utilizado por el operador de equipo o administrador del sistema para controlar todos los equipos. Vinny conectado el cable que conduce desde el puerto de consola en uno de los terminales el Mostrar piso.

Eso significaba que este uno terminal ahora fue reconocido como una consola de terminal. Me senté abajo en la máquina recabled y conectado mediante una contraseña los desarrolladores habían siempre tan audaz. Porque el software de bloqueo-11 ahora que he identificado se registro en desde un terminal autorizado, me dio acceso, y estaba conectado con privilegios de administrador del sistema. He aplicado el sistema operativo cambiando por lo que desde cualquiera de los terminales en el piso, podría ser capaz de Inicie sesión como un usuario con privilegios.

Una vez que se instaló mi parche secreta, Vinny volvió a trabajar a desconectar el Terminal cable conectarlo en donde había sido originalmente. A continuación, tomó el bloqueo una vez más, esta vez para sujetar la puerta gabinete cerrado.

Hice una lista para saber cuáles son los archivos en el equipo, de directorios buscando el programa de bloqueo-11 y los archivos asociados y tropezó en algo he encontrado impactante: un directorio que no debería haber estado en esta máquina. Los desarrolladores había sido tan confiado, para algunos su software era invencible, no había molestado en quitar el código fuente de su nuevo producto. Mover a la terminal adyacente de copia impresa, empecé a impresión a partes del código fuente en las continuas hojas del papel de rayas verde equipo utilizado en los días.

Vinny sólo apenas había terminado la recolección el candado cerrado y reincorporó me cuando los chicos regresaron de almuerzo. Ellos me encontraron sentado en el golpeteo de equipo las claves mientras la impresora continuada Batan lejos. \"What'cha haciendo, Kevin?\" uno de ellos preguntó.

There was an error deserializing the object of type System.String. End element 'root' from namespace '' curso. Hasta que miró la impresora y vio que realmente u, como las celosamente código protegido para su producto.

No creen que es posible que estaba registrado como un usuario con privilegios. There was an error deserializing the object of type System.String. Encountered unexpected character 'o'. apareció en la pantalla confirma mi reclamo. El tio huele a su frente, como Vinny dijo, \"trescientos dólares, por favor.\"

MENSAJE DE MITNICK
Aquí hay otro ejemplo de gente inteligente que subestimar al enemigo. ¿Qué --está usted tan seguro sobre garantías de seguridad de la compañía que lo haría ¿apuesta $300 contra un atacante rompiendo? A veces la forma alrededor de un dispositivo de seguridad tecnológica no es el que espera.

Pagaron. Vinny y caminó alrededor de la planta de feria para el resto de la día con los billetes de cien dólares pegados en nuestras insignias de Conferencia. Todo el mundo quien vio los billetes sabía lo representaban.

Por supuesto, Vinny y yo no habíamos derrotado su software y si el equipo de desarrolladores había pensado establecer mejores normas para el concurso, o había utilizado un bloqueo realmente seguro, había visto a su equipo más cuidadosamente, no habría sufrido el humillación de ese día--humillación a manos de un par de adolescentes.

Me enteré más tarde que el equipo de desarrolladores tuvo que parar por un banco para obtener dinero: los billetes de cien dólares representan todo el dinero de gasto que habían traído con ellos.

EL DICCIONARIO COMO UNA HERRAMIENTA DE ATAQUE

Cuando alguien obtiene su contraseña, es capaz de invadir el sistema. En la mayoría circunstancias, ni siquiera saben que nada malo ha sucedido.
Un joven atacante llamaré Ivan Peters tenía un objetivo de recuperar el código fuente de un nuevo juego electrónico. No tenía ningún problema en entrar en zona amplia de la empresa la red, porque un amigo hacker de su ya había comprometido uno de los servidores de Web de la empresa. Después de encontrar una vulnerabilidad de un-patched en la Web software de servidor, su compañero sólo había caído de su silla cuando se dio cuenta de se ha establecido el sistema como un host con base dual, lo que significaba que tenía una entrada punto de la red interna. .

Pero una vez que Ivan estaba conectado, luego se enfrentó a un reto que era como estar dentro de el Museo del Louvre y con la esperanza de encontrar a la Mona Lisa. Sin un plano de planta, usted podría vagar durante semanas. La empresa fue global, con cientos de oficinas y miles de servidores, y exactamente no proporcionan un índice de sistemas de desarrollo o de los servicios de un guía turístico le dirigir a la derecha.

En lugar de utilizar un enfoque técnico a buscar qué servidor necesitaba destino, Ivan utiliza un enfoque de ingeniería social. Colocó llamadas basadas en métodos similares a los descritos en otras partes de este libro. En primer lugar, llamándola soporte técnico, afirmó que un empleado de la empresa disponer de una interfaz problema de un producto que se estaba diseñando su grupo. y frecuentes para el número de teléfono el líder del proyecto para el equipo de desarrollo de juegos.

Entonces llamó el nombre que le había dado, haciéndose pasar por un chico de la misma. \"Más tarde esta noche,\"dijo,\"está intercambiando un enrutador y asegúrese de que la gente el equipo no pierda conectividad al servidor. Así que tenemos que saber que servidores tu equipo utiliza.\" La red se está actualizando todo el tiempo. Y ¿dando el nombre del servidor no duele nada de todas formas, ahora lo haría? Puesto que era protegido por contraseña, sólo tener el nombre no podía ayudar alguien romper. Por lo que el hombre dio el atacante el nombre del servidor. Incluso no se molestan en llamar el hombre vuelve a verificar su historia o escribir su nombre y número de teléfono. Él sólo le dio el nombre de los servidores, ATM5 y ATM6.

El ataque de contraseña

En este punto, Ivan cambió a un enfoque técnico para obtener la autenticación información. El primer paso con ataques más técnicos en los sistemas que proporcionan

capacidad de acceso remoto es identificar una cuenta con una contraseña débil, que proporciona un punto de entrada inicial del sistema.

Cuando un atacante intenta utilizar herramientas de hacking para identificar de forma remota las contraseñas, el esfuerzo puede exigirle a permanecer conectado a la empresa red durante horas en un momento. Claramente lo hace por su cuenta y riesgo: cuanto más tiempo permane conectado, mayor es el riesgo de detección y obtener atrapados.

Como un paso preliminar, Ivan haría una enumeración, que revela detalles sobre un sistema de destino. Una vez más la Internet convenientemente proporciona software para el objetivo (en http:\/\/ntsleuth.0catch.com; el personaje antes de \"captura\" es un cero). Ivan encontró varios públicamente disponibles herramientas de hacking en la Web que automatizada el proceso de enumeración, evitando la necesidad de hacerlo a mano, que llevaría ya y por lo tanto corren un riesgo mayor. Sabiendo que la organización principalmente implementado Servidores basados en Windows, descargado una copia de NBTEnum, un NetBIOS (básico utilidad de enumeración de Input\/output system). Ingresó a la dirección IP (Protocolo Internet) dirección del servidor ATM5 y comenzó ejecutando el programa. La enumeración herramienta fue capaz de identificar varias cuentas que existían en el servidor.

JERGA
Un proceso de enumeración que revela el servicio habilitado en el destino una lista de nombres de cuentas de los usuarios, la plataforma de sistema operativo y sistema que tengan acceso al sistema.

Una vez que las cuentas existentes habían sido identificadas, tenía la misma herramienta de enumeración la capacidad de lanzar un ataque de diccionario contra el sistema informático. Un diccionario ataque es algo que muchos amigos de seguridad del equipo y los intrusos son íntimamente familiarizado con, pero que la mayoría de la gente probablemente estará sorprendida al aprender es posible. Este ataque está dirigido a descubrir la contraseña de cada usuario en el sistema mediante el uso de las palabras utilizadas.
Somos todos vagos acerca de algunas cosas, pero nunca deja de sorprenderme que cuando personas eligen sus contraseñas, su creatividad e imaginación parecen desaparecen. La mayoría de nosotros desea una contraseña que nos da protección, pero que está en el mismo tiempo fácil de recordar, que generalmente significa algo estrechamente relacionado para nosotros. Nuestras iniciales, segundo nombre, apodo, nombre del cónyuge, canción favorita, película o brew, por ejemplo. El nombre de la calle vivimos o la ciudad que vivimos, el tipo de coche que conducimos, el pueblo frente a la playa nos gusta permanecer en Hawaii, o esa secuencia favorita con la mejor pesca de trucha alrededor. Reconocer el patrón ¿aquí? Estos son principalmente los nombres personales, nombres de lugar o palabras del diccionario. A ataque de diccionario corre a través de palabras de uso común en un muy rápido ritmo, intentando cada u una contraseña en una o más cuentas de usuario.

Iván corrió el ataque de diccionario en tres fases. Para el primero, usó una lista simple de unos 800 de las contraseñas más comunes; la lista incluye secreto, trabajo, y contraseña. También el programa permutated el diccionario de palabras para tratar de cada palabra con un dígito anexado o anexar el número del mes actual. El programa probado cada intento contra todas las cuentas de usuario que habían sido identificado. Sin suerte.

Para el siguiente intento, Iván pasó al motor de búsqueda de Google y escribe, \"introducir listas diccionarios\"y se encuentran miles de sitios con introducir listas extensas y diccionarios de inglés y varios idiomas extranjeros. Descargaron toda una Diccionario inglés electrónico. Luego mejorado esto descargando un número de palabra listas que encontró con Google. Ivan eligió el sitio en www.outpost9.com\/files\/WordLists.html.

Este sitio le permitió Descargar (todo esto para libre) una selección de archivos incluyendo los nombres de familia, dado namek, nombres del Congreso y palabras del actor. nombres, palabras y nombres de la Biblia.

Otro de los muchos sitios que ofrecen listas de palabras realmente se presta a través de Oxford Universidad, ftp:\/\/ftp.ox.ac.uk\/pub\/wordlists.

Otros sitios ofrecen listas con los nombres de personajes de dibujos animados, palabras usadas en Shakespeare, en la Odisea, Tolkien y la serie Star Trek, así como en Ciencia y religión y así. (Una empresa on-line vende una lista que contenga 4,4 millones de palabras y nombres por sólo $20.) Puede establecer el programa de ataque para probar los anagramas del diccionario de palabras, así como--otro método favorito que muchos usuarios de computadoras que aumenta su seguridad.

Más rápido de lo que usted piensa

Una vez Iván había decidido qué lista de palabras a utilizar y comenzó el ataque, el software corrió en piloto automático. Él fue capaz de dirigir su atención a otras cosas. Y aquí está el parte increíble: uno pensaría que dicho ataque permitiría el hacker tomar un Alarma de RIP van Winkle y el software todavía habría progresado poco cuando despertó. De hecho, dependiendo de la plataforma de ataque, la seguridad configuración del sistema y la conectividad de red, cada palabra en inglés Diccionario increíblemente, puede intentarse en menos de treinta minutos!

Mientras se ejecuta este ataque, Iván comenzó a otro equipo que ejecute un similar ataque en el otro servidor utilizado por el grupo de desarrollo, ATM6. Veinte minutos más tarde, el software de ataque había hecho lo que los usuarios más confiados como para Creo que es imposible: había roto una contraseña, revela que uno de los usuarios tenía elige la contraseña \"Frodo,\" uno de los Hobbits en el libro el señor de la Anillos.

Con esta contraseña en mano, Iván fue capaz de conectarse con el servidor de ATM6 mediante la cuenta del usuario.

Hubo buenas y malas noticias para nuestro atacante. La buena noticia fue que el cuenta él agrietado tenía privilegios de administrador, que serían fundamentales para la paso siguiente. La mala noticia fue que el código fuente para el juego en cualquier lugar a encontrarse. 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 era renunciar sólo todavía; todavía tenía algunos trucos más para probar.

En algunos sistemas operativos Windows y UNIX, hashes de contraseña (cifradas contraseñas) son abiertamente disponibles para cualquier persona que tenga acceso a la computadora son almacenados en. El razonamiento es que las contraseñas cifradas no pueden ser rotas y por lo tanto, no necesitan ser protegidos. La teoría está equivocada. Utiliza otra herramienta llamado pwdump3, también disponible en Internet, fue capaz de extraer la hashes de contraseña de la ATM6 de la máquina y descargarlos.

Un archivo típico de hashes de contraseña tiene este aspecto:

Administrador:
500:95E4321A38AD8D6AB75EOC8D76954A50:2E48927AO
BO4F3BFB341E26F6D6E9A97:::

akasper:
1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357
F157873D72D0490821:::

Digger: 1111:5D15COD58DD216C525AD3B83FA6627C7 :
17AD564144308B4 2B8403DOIAE256558:::

ellgan:
1112:2017D4A5D8D1383EFF17365FAFIFFE89:O7AEC950C22CBB9
C2C734EB89320DB13:::

tabeck: 1115:9F5890B3FECCAB7EAAD3B435B51404EE:
1FO115A72844721 2FCO5EID2D820B35B:::

vkantar :
1116:81A6A5DO35596E7DAAD3B435B51404EE:B933D36DD12258
946FCC7BD153F1CD6E:::

vwallwick: 1119: 25904EC665BA30F4449AF42E1054F192:15B2B7953FB6
32907455D2706A432469:::

mmcdonald: 1121:A4AEDO98D29A3217AAD3B435B51404EE:
E40670F936B7 9C2ED522F5ECA9398A27:::

kworkman: 1141:C5C598AF45768635AAD3B435B51404EE:
DEC8E827A1212 73EFO84CDBF5FD1925C:::

Con los algoritmos hash ahora descarga en su equipo, Ivan utiliza otra herramienta que realiza un sabor diferente de ataque contraseña conocida como fuerza bruta. Este tipo ataque trata de cada combinación de caracteres alfanuméricos y más especial símbolos.

Ivan utiliza una utilidad de software llamada L0phtcrack3 (pronunciado loft-crack; disponible en www.atstake.com; otra fuente para algunas herramientas de recuperación de contraseña excelente es www.elcomsoft.com). Los administradores de sistemas utilizan L0pht-crack3 auditoría débil contraseñas; los atacantes utilizan para descifrar contraseñas. La función de fuerza bruta en LC3 trata de contraseñas con combinaciones de letras, números y símbolos más incluyendo! @ #$ % ^
caracteres. (Nota, sin embargo, que si se utilizan los caracteres no imprimibles, será LC3 no se ha podido descubrir la contraseña)

El programa cuenta con una velocidad casi increíble, que puede llegar a tan alto como 2.8 millones intenta un segundo en una máquina con un procesador de 1 GHz. Incluso con este velocidad, y si el administrador del sistema haya configurado el funcionamiento de Windows sistema correctamente (deshabilitar el uso de hashes LANMAN), rompiendo una contraseña todavía se puede tomar una cantidad excesiva de tiempo.

JERGA
ATAQUE de fuerza bruta a contraseña detección estrategia trata cada combinaciones posibles de caracteres alfanuméricos y símbolos especiales.

Para motivo el atacante a menudo descargas los algoritmos hash y ejecuta el ataque a su o otra máquina, en lugar de permanecer en línea en la red de la empresa de destino y riesgo de detección.
Para Iván, la espera no fue tanto tiempo. Varias horas más tarde el programa presentado él con las contraseñas para cada uno de los miembros del equipo de desarrollo. Pero estos fueron las contraseñas de los usuarios en el equipo de ATM6, y él ya sabía la código de juego que fue después no era en este servidor.

¿Qué ocurre ahora? Él todavía no había sido capaz de obtener una contraseña de una cuenta el Máquina de ATM5. Utilizando su mentalidad hacker, comprender los hábitos de seguridad deficiente

de usuarios típicos, él ocupó uno de los miembros del equipo podría han elegido el mismo contraseña para ambos equipos.

De hecho, eso es exactamente lo que encontró. Uno de los miembros del equipo estaba utilizando el contraseña \"recibe\" en ATM5 y ATM6.

La puerta había oscilado abierta para Ivan a cazar alrededor hasta que encontró la fue después de los programas. Una vez que encuentra el árbol de código fuente y alegremente descargado, tomó un paso más típico de galletas de sistema: cambió la contraseña de una cuenta inactiva que tiene derechos de administrador, solo por si acaso él quería obtener una versión actualizada del software en algún momento en el futuro.

Analizando el timo
En este ataque que llama sobre vulnerabilidades técnicas y basada en las personas, la atacante comenzó con una llamada telefónica de pretexto para obtener los nombres de host y ubicación los servidores de desarrollo que se celebró la información propietaria.

Luego usó una utilidad de software para identificar los nombres de usuario de cuenta válido para todo el n que tenía una cuenta en el servidor de desarrollo. A continuación dirigió dos sucesivas ataques de contraseña, incluyendo un ataque de diccionario, que busca comúnmente utiliza contraseñas por tratar todas las palabras en un diccionario de inglés, a veces aumentada por varias listas de palabras que contengan nombres, lugares y elementos de especial interés.

Porque tanto comerciales como dominio público herramientas hacking pueden obtenerse por cualquier persona para cualquier propósito que tienen en mente, es más importante que estar vigilantes en la protección de su red y sistemas informáticos de empresa infraestructura.

La magnitud de esta amenaza no puede ser subestimada. Según el equipo
La revista World, un análisis basado en Nueva York Oppenheimer fondos llevó a una sorprendente descubrimiento. Vicepresidente de seguridad de la red y desastres de la empresa Recuperación tuvo un ataque de contraseña contra los empleados de su empresa mediante uno de los paquetes de software estándar. La revista informó en tres minutos logró descifrar las contraseñas de 800 empleados.

MENSAJE DE MITNICK
En la terminología del juego monopolio, si utiliza una palabra de diccionario para su contraseña: ir directamente a la cárcel. No pasan Go, no cobrar $200. Tienes que enseñar a sus empleados cómo elegir contraseñas que verdaderamente protegen sus activos.

PREVENIR LA CON

Ataques de ingeniería social pueden llegar a ser incluso más destructivo cuando el atacante agrega un elemento de tecnología. Prevenir este tipo de ataque normalmente implica adopción de medidas en los niveles técnicos y humanos.

Sólo decir que No

En la primera historia del capítulo, el empleado RCMAC de compañía de teléfono no debe han quitado el denegar terminar el estado de las líneas de diez teléfono cuando no hay servicio orden existía autorizando el cambio. No es suficiente para los empleados conocer el las políticas de seguridad y procedimientos; los empleados deben comprender cuán importante estas políticas son para la empresa en la prevención de daños.

Las políticas de seguridad deben desalentar la desviación del procedimiento a través de un sistema de recompensas y consecuencias. Naturalmente, las políticas deben ser realistas, no a empleados para llevar a cabo pasos tan onerosos que suelen ser ignorados.
También, un programa de concienciación de seguridad necesita convencer a los empleados a que, mientra importante para completar las asignaciones de trabajo en forma oportuna, teniendo un acceso directo elude la seguridad adecuados procedimientos pueden ser perjudiciales para la empresa y co trabajadores.

La misma cautela debe estar presente al proporcionar información a un extraño en el teléfono. No importa cómo persuasiva la persona presenta a sí mismo, independientemente del Estado o la antigüedad en la empresa, la persona absolutamente no debe disponerse de información siempre que no se designa como públicamente hasta se ha verificado positivamente la identidad del llamador. Si esta política ha sido estrictamente observado, el esquema de ingeniería social en esta historia hubiera fracasado y nunca habría sido capaz de planificar un nuevo susto con detenido Federal Gondorff su pal Johnny.

Este uno punto es tan importante que le reitero a lo largo de este libro: verificar, verificar, comprobar. Cualquier solicitud no se hizo en persona nunca debe aceptarse sin verificar la identidad del solicitante--período.

Limpieza

Para cualquier empresa que no tiene guardias de seguridad alrededor del reloj, el esquema un desafío en el que un atacante obtiene acceso a una oficina después de horas. Limpieza de personas generalmente tratará con respeto quien aparece con la empresa y parece legítima. Después de todo, se trata de alguien que pudo obtener ellos en problemas o despedidos. Por esa razón, limpieza de tripulaciones, ya sea interno o contrató a una agencia externa, debe ser capacitado en materia de seguridad física.

Trabajo de conserjería exactamente no requiere una educación universitaria, o incluso la capacidad de habla a inglés, y la formación habitual, si los hubiere, implica cuestiones conexas no son de seguridad

tales como qué tipo de limpieza producto para diferentes tareas. Generalmente estos personas no reciben una instrucción como, \"si alguien te pide que dejarlos después de horas, necesita ver su compañía de tarjeta de identificación, y, a continuación, llame a la limpieza Oficina de la empresa, explicar la situación y esperar autorización.\"

Una organización necesita para planificar una situación como la de este capítulo antes de pasa y capacitar personas en consecuencia. En mi experiencia personal, he encontrado que más, si no todos, las empresas del sector privado son muy laxas en esta área de la física seguridad. Podría intentar abordar el problema desde el otro extremo, poniendo el carga a sus empleados de la empresa. Una empresa sin guardia de 24 horas servicio debe decirle a sus empleados que para obtener horario, son llevar sus propias claves o tarjetas de acceso electrónico y debe ponen nunca la gente de limpieza la posición de decidir quién está bien admitir. Decirle a la empresa conserjería que su pueblo debe ser entrenado siempre que nadie es ser admitido en su locales por ellos en cualquier momento. Esta es una regla simple: no abrir la puerta para cualquiera. En su caso, esto podría poner a escribir como una condición del contrato con la empresa de limpieza.

También, cuadrillas de limpieza deben estar capacitados sobre Piggybacking técnicas (personas no autorizadas tras una persona autorizada en una entrada segura). También debe estar capacitados no para permitir que otra persona que siga en el edificio sólo porque la persona parece podrían ser un empleado.

Seguimiento cada ahora y después--digamos, tres o cuatro veces al año--por la puesta en escena un evaluación de vulnerabilidad o de prueba de penetración. Que alguien apareciera en la puerta Cuando la tripulación limpieza es en el trabajo y trata de hablar su camino hacia el edificio. En lugar de utilizar a sus propios empleados, se puede contratar una empresa que se especializa en este tipo de pruebas de penetración.

Pasarlo: Proteger sus contraseñas

Más organizaciones se están volviendo cada vez más atentos a cumplir políticas de seguridad a través de medios técnicos--por ejemplo, configurar el funcionamiento sistema para aplicar directivas de contraseña y limitar el número de inicio de sesión no válido intentos que pueden realizarse antes de bloquear la cuenta. De hecho, Microsoft Plataformas de negocio de Windows generalmente tienen esta función integrada. Aún así, Reconociendo los clientes cómo fácilmente molesto son las funciones que requieren extra esfuerzo, los productos se entregan normalmente con características de seguridad desactivadas. Tiene realmente sobre el tiempo que dejen de fabricantes de software ofrece productos con características de seguridad deshabilitadas de forma predeterminada, cuando debería ser al revés. (I sospechoso que voy averiguar esto pronto.)

Por supuesto, la política de seguridad corporativa debe mandato los administradores de sistemas aplicar directivas de seguridad a través de medios técnicos, siempre que sea posible, con el objetivo

de no confiar en los seres humanos falibles más que necesario. No es un-brainer que cuando es limitar el número de intentos de inicio de sesión no válidas sucesivas a un determinado cuenta, por ejemplo, hacer la vida de un atacante considerablemente más difícil.

Cada organización enfrenta a ese difícil equilibrio entre seguridad fuerte y productividad de los empleados, lo que lleva a algunos empleados que ignore las políticas de seguridad, no aceptar lo esencial son estas salvaguardas para proteger la integridad de información corporativa confidencial.

Si las políticas de la empresa dejan algunos temas un-addressed, los empleados pueden utilizar la camino de menor resistencia y no cualquier acción es más conveniente y hace su trabajo más fácil. Algunos empleados pueden se resisten al cambio y abiertamente desconocer bueno hábitos de seguridad. Puede que haya encontrado a un empleado así, que sigue las reglas sobre la longitud de la contraseña y complejidad, pero, a continuación, escribe la contraseña en una nota Post-it y desafiante pega a su monitor.

Una parte vital de la protección de su organización es el uso del disco duro para descubrir contraseñas, combinado con la configuración de seguridad fuerte en su tecnología.

Para una explicación detallada de las directivas de contraseña recomendadas, consulte el capítulo 16.

Capítulo 12
Ataques contra el empleado de nivel de entrada

Como muchas de las historias aquí demuestran, a menudo dirige el ingeniero social especializado personal de nivel inferior en la jerarquía organizativa. Puede ser fácil manipular estas personas para que revelen información aparentemente inocua que la atacante utiliza para avanzar un paso más para obtener más confidenciales de la empresa información.

Un atacante objetivos a básicos empleados porque normalmente ignoran el valor de información específica de la compañía o de los posibles resultados de determinados acciones. También, tienden a ser fácilmente influenciados por algunas de las más comunes enfoques de ingeniería social--un llamador que invoca la autoridad; una persona que parece amable y simpático; una persona que parece conocer gente en el empresa que se sabe que la víctima; es una petición que reclama el atacante urgente; o la inferencia de que la víctima obtenga algún tipo de favor o reconocimiento.

Aquí hay algunas ilustraciones del ataque a los empleados de nivel inferior en acción.

EL GUARDIA DE SEGURIDAD ÚTIL
Estafadores esperan encontrar una persona que es voraz porque son ellos los más probabilidades de caer en un juego con. Los ingenieros sociales, cuando a alguien como un miembros de una tripulación de saneamiento o un guardia de seguridad, la esperanza de encontrar a algu cordial, amable y confianza de los demás. Ellos son los más susceptibles de ser dispuestos a ayudar. Eso es justo lo que el atacante tenía en mente en el siguiente relato.

Vista de Elliot
Fecha y hora: 3:26 el martes por la mañana en febrero de 1998.
Ubicación: Facilidad Marchand Microsystems, Nashua, Nueva Hampshire

Elliot Staley sabía que él no supone abandonar su estación cuando él no estaba en su rondas programadas. Pero fue la mitad de la noche, para llorar en voz alta y él no había visto a una sola persona ya había venido de turno. Y era casi la hora hacer sus rondas de todos modos. El pobrecito el teléfono sonaba como él realmente necesitaba ayuda. Y hace que una persona sienta bien cuando se puede hacer algo bueno alguien.

Historia de Bill
Bill Goodrock tenían un objetivo simple, uno se había celebrado a, inalterada desde los años doce: a jubilarse por edad veinticuatro, nunca tocar un centavo de su Fondo Fiduciario.

Para mostrar a su padre, el banquero todopoderoso e implacable, que podría ser un éxito en solitario.

Sólo dos años izquierda y se la por ahora perfectamente claro no hará su fortuna en los próximos 24 meses por ser un empresario brillante y no hacerlo por ser un fuerte inversor. Una vez se preguntó acerca de robar bancos con una pistola pero eso es sólo el material de ficción--el riesgo-beneficio equilibrio es tan pésima. En su lugar imagina haciendo un Rifkin--robar un banco electrónicamente. La última Ley de tiempo en Europa con la familia, abrió un banco cuenta en Mónaco con 100 francos. Todavía tiene sólo 100 francos, pero él tiene un plan que podría ayudarle a llegar a siete dígitos a toda prisa. Incluso ocho si es suerte.

Novia de Bill Anne-marie trabajó en m mientras espera en sus oficinas hasta que ella salió de una reunión de la tarde, dio a curiosidad y conectado a su portátil en un puerto Ethernet en la sala de conferencias estaba usando. Sí!--se encontraba en su red interna, conectado dentro del Banco red.., detrás del firewall corporativo. Le dio una idea.

Combinaron su talento con un compañero que conocía a una joven llamada Julia, una candidato de doctorado ciencia brillante equipo haciendo una pasantía en Marchand Microsystems. Julia parecía una gran fuente de información privilegiada esencial. Le dijeron que estaban escribiendo un guión para una película y realmente creía ellos. Ella pensó que era divertido que conforman una historia con ellos y darles todo el detalles acerca de cómo realmente podría traer a la alcaparra habían descrito. Ella pensaba la idea era brillante, realmente y mantuvo les persuadida acerca de darle una pantalla de crédito, demasiado.

Advirtieron ella acerca de cómo a menudo ideas de guión consigue robados y hizo su juro ella nunca diría cualquiera.

Adecuadamente entrenado por Julia, Bill hizo la parte riesgosa a sí mismo y nunca dudaron de él podría ponerlo.

Llamé por la tarde y logró averiguar que el supervisor de la noche de la fuerza de seguridad era un hombre llamado a Isaías Adams. A las 9:30 de esa noche llamé a la construcción y hablé con la guardia en el mostrador de seguridad lobby. Mi historia fue todo basado en la urgencia y yo mismo hice sonar un poco de pánico. \"Tengo coche problemas y yo no podemos llegar a las instalaciones,\"dije. \"Tengo esta emergencia y yo realmente necesito su ayuda. He intentado llamar al supervisor de guardia, Isaías, pero de él no en casa. Puede simplemente me haces este favor una, realmente podría apreciarla? \"

Las habitaciones en ese gran centro fueron cada uno etiquetadas con un código de parada de correo por l
él la parada de correo del laboratorio de computación y le preguntó si sabía dónde era.
Dijo que sí y decidieron ir allí para mí. Dijo que le tomaría unos pocos
minutos para llegar a la habitación, y dijo que podría llamarlo en el laboratorio, dando la excusa
que yo estaba usando la única línea de teléfono disponible para mí y yo estaba usando para marcar en
la red para intentar solucionar el problema.

Ya estaba allí esperando por el momento llama y yo le dije dónde
encontrar la consola que me interesaba, buscando uno con una bandera de papel de lectura
There was an error deserializing the object of type System.String. End element 'root' from namespace '' e
sistema operativo que la empresa comercializa. Cuando dijo que había encontrado, me
sabía con certeza que Julia había estado alimentando nos buena información y mi corazón
omitió una paliza. Le tuve que pulsa la tecla Intro un par de veces, y lo dijo
imprime un signo. Que me dijo que el equipo ha iniciado la sesión como root, el
cuenta de superusuario con todos los privilegios de sistema. Fue un mecanógrafo hunt-and-peck y
tiene todo en un sudor cuando trató de hablar le mi comando siguiente,
que era más que un poco complicado:

Eco ' fix: x: 0:0:: \/: \/ bin\/sh' >> \/ etc\/passwd

Finalmente obtuvo derecho, y ahora nos habíamos previsto una cuenta con una corrección de nombre. Y
a continuación, le tuve que escribir

Eco ' arreglar:: 10300:0:0' 55\/etc\/shadow

Esto establece la contraseña cifrada, que va entre los dos puntos dobles.
Poner nada entre esos dos puntos significaba que la cuenta tendría un valor null
contraseña. Tan sólo esos dos comandos fue todos tardamos para anexar la revisión de la cuenta
para el archivo de contraseñas, con una contraseña nula. Lo mejor de todo, tendría la cuenta de la
mismos privilegios que un superusuario.

Lo siguiente le tuve que hacer fue introducir un comando de directorio recursiva que
imprime una larga lista de nombres de archivo. Luego lo hizo alimentar el papel hacia adelante, lo desgarr
apagado y llevarlo con él vuelve a su escritorio de guardia porque \"puedo te necesito leer
me algo de ella más adelante.\"

La belleza de esto es que él no tenía idea que había creado una nueva cuenta. Y yo
lo hizo imprimir el directorio listado de nombres de archivo porque necesitaba para asegurarse
los comandos que escribió anteriormente dejaría a la sala de informática con él. Que
manera el administrador del sistema o el operador no mancha nada el siguiente
mañana que estaría alerta que se había producido una violación de seguridad.

Ahora estaba configurado con una cuenta y una contraseña con privilegios completos. Un poco antes medianoche he marcado en y seguido las instrucciones que cuidadosamente, Julia había escrito hasta There was an error deserializing the object of type System.String. End element 'root' from namespace '' que contiene la copia maestra del código fuente para la nueva versión de la software de sistema operativo de la empresa.

He subido un parche que Julia había escrito, que dijo por última vez una rutina en uno de las bibliotecas del sistema operativo. En efecto, dicha revisión crearía una encubierta puerta trasera podría permitir el acceso remoto en el sistema con una contraseña secreta.

NOTA
El tipo de puerta trasera utilizado aquí no cambia el inicio de sesión del sistema operativo programa propio, más bien, una función específica dentro de la biblioteca dinámica utilizado por el inicio de sesión es reemplazado programa para crear el punto de entrada secreta. En típica ataques, equipo intrusos a menudo reemplazar o revisión del programa de inicio de sesión, pero los administradores del sistema fuerte pueden detectar el cambio por comparación con la versión enviado en medios como el cd, o por otros métodos de distribución.

He seguido atentamente las instrucciones que ella había escrito para mí, primero instalar el parche, luego tomar medidas que eliminan la cuenta de corrección y actualizan todos auditoría registra por lo que no habría ningún rastro de mis actividades, efectivamente borrado de registros.

Pronto la empresa comenzaría la nueva actualización del sistema operativo para de envío sus clientes: instituciones financieras de todo el mundo. Y cada copia se enviado fuera incluiría la puerta trasera había colocado en la distribución principal antes de se ha enviado, permitirme tener acceso a cualquier sistema informático de cada banco y la casa de corretaje que instala la actualización.

JERGA
PARCHE tradicionalmente un pedazo de código que, cuando se coloca en un archivo ejecutable programa, corrige un problema.

Por supuesto, yo no estaba muy doméstica libre--aún habría que hacer. Todavía tendría para acceder a la red interna de cada institución financiera que quería
There was an error deserializing the object of type System.String. Encountered unexpected character 'T'. transferencias y instalar el software de vigilancia para conocer los detalles de sus operaciones y exactamente cómo transferir fondos.

Todo eso lo pude hacer largas distancias. Desde un equipo situado en cualquier lugar. Decir, con vistas a una playa de arena. Tahití, aquí vengo.

La Guardia de la llamada, le agradeció su ayuda y le dijo que podía seguir adelante y tira la copia impresa.

Analizando el timo

El guardia de seguridad tenía instrucciones sobre sus funciones, pero incluso profundo, bien-instrucciones pensadas no pueden anticipar cada situación posible. Nadie había dicho el daño que puede hacerse escribiendo unas cuantas pulsaciones de teclas en un equipo para él un persona que pensó que era un empleado de la empresa.

Con la colaboración de la Guardia, fue relativamente fácil acceder a un críticos del sistema que almacena al patrón de distribución, a pesar de que era detrás de la puerta bloqueada de un laboratorio seguro. La Guardia, por supuesto, tenía llaves para puertas todo bloqueadas.

Incluso un empleado básicamente honesto (o, en este caso, el candidato de doctorado y Becario de la empresa, Julia) a veces puede ser sobornado o engañado para que revelen información de vital importancia para un ataque de ingeniería social, tales como dónde el equipo de destino se encuentra--y la clave para el éxito de este ataque--- cuando iban a construir la nueva versión del software para su distribución. Esto es importante, ya que un cambio de este tipo que se hizo demasiado pronto tiene una mayor probabi de ser detectado o ser anulado si el sistema operativo es reconstruido a partir de un limpio fuente.

Capturar el detalle de tener la Guardia retomar la impresión al lobby ¿escritorio y después destruirlo? Este fue un paso importante. Cuando el equipo operadores llegaron a trabajar la próxima jornada, el atacante no quería encontrar Este abrumadoras pruebas en el terminal de copia impresa o notarlo en la basura. Dando la Guardia una excusa plausible para tomar la impresión con él evita ese riesgo.

MENSAJE DE MITNICK

Cuando el intruso de equipo no puede obtener acceso físico a un sistema informático o red a sí mismo, él intentará manipular a otra persona a hacer por él. En casos donde es necesario para el plan, con la víctima como un proxy de acceso físico es incluso mejor que hacerlo él mismo, porque el atacante supone mucho menos riesgo de detección y aprensión.

EL PARCHE DE EMERGENCIA

Uno pensaría que un chico de soporte técnico podría comprender los peligros de dar el acceso a la red de equipo a un forastero. Pero cuando ese forastero es una inteligente ingeniero social haciéndose pasar como un proveedor de software útil, los resultados podrían no ser lo que esperas.

Una llamada de ayuda
¿El llamador quería saber quién está a cargo de equipos hay? y el
operador telefónico lo puso a través para el tipo de soporte técnico, Paul Ahearn.

El llamador identificó como \"Edward, con SeerWare, el proveedor de la base de datos.
Aparentemente un montón de nuestros clientes no recibe el correo electrónico sobre nuestra emergencia
actualización, por lo que nosotros estamos llamando a unos pocos para una verificación de control de ca
un problema al instalar el parche. Ha instalado la actualización todavía?\"

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

Edward said, \"bueno, podría provocar intermitente pérdida catastrófica de datos, por lo que nos
recomendamos que obtenga instalado tan pronto como sea posible\". Sí, eso era algo
Sin duda quería hacer, dijo Paul. \"Está bien\", respondió el llamador. \"Podemos enviar
es una cinta o CD con el parche, y quiero decirles, es realmente crítico--dos
las empresas ya perdieron varios días de datos. Lo que realmente debería obtener esto
instalado en cuanto llegue, antes de que suceda a su empresa\".

There was an error deserializing the object of type System.String. Encountered unexpected character 'P'.

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
lo desea, podemos tener nuestro centro de soporte al cliente instalar, de manera remota.
Podemos telefónico o utilizar Telnet para conectar al sistema, si usted puede apoyar
\"que.

There was an error deserializing the object of type System.String. Encountered unexpected character 'P'.
respondió. \"Si se puede utilizar SSH, que estaría bien,\" dijo, nombrar un producto
Proporciona transferencias de archivos de forma segura.
Sí. Contamos con SSH. ¿Cuál es la dirección IP?

Paul le dio la dirección IP, y cuando se le preguntó Andrew, \"y qué nombre de usuario y
contraseña puedo utilizar, \"Paul le dio, así.
Analizando el timo
Por supuesto, esa llamada telefónica realmente podría haber llegado desde la base de datos
fabricante. Pero, a continuación, la historia no pertenece a este libro.

El ingeniero social aquí influyó a la víctima creando una sensación de temor que
datos críticos podrían perderse y ofrecieron una solución inmediata que podría resolver
el problema.

También, cuando un ingeniero social dirige alguien que conoce el valor de la
información, tiene que venir con argumentos muy convincentes y persuasivas
para dar acceso remoto. A veces tiene que agregar el elemento de urgencia tan

la víctima es distraída por la necesidad de apresurarse y cumple antes de que él ha tenido una oportunidad de reflexionar mucho sobre la solicitud.

LA NUEVA CHICA
¿Qué tipo de información en archivos de la empresa un atacante podría obtener
¿acceso a? A veces puede ser algo que no creo que sea necesario para proteger
En absoluto.

Llamada de Sarah
Recursos humanos, se trata de Sarah.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
¿utilizar para entrar en el estacionamiento y elevadores? Bueno, tuvimos un problema y
es necesario reprogramar las tarjetas para las nuevas contrataciones en los últimos quince días\".

¿Por lo tanto necesita sus nombres?

Y sus números de teléfono.

Puedo comprobar nuestra nueva lista de alquiler y le devuelva la llamada. ¿Cuál es tu número de teléfon

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
hora?\"

AH. Esta bien.
Cuando llamó, dijo:

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
ese nuevo VP, el Sr. Underwood.\"
¿Y los números de teléfono?
There was an error deserializing the object of type System.String. Unexpected end of file. Follo
Bien, el Sr. Underwood es de 973. Anna hablando.\"
There was an error deserializing the object of type System.String. The token 'true' was expected bu

Llamada de Anna
Finanzas, Anna hablando.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
Editor de la División de negocios. No creo que hemos introducido. Bienvenido
a la empresa\".

Oh, gracias.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
de su tiempo\".

Claro. ¿Qué necesita?

There was an error deserializing the object of type System.String. Unexpected end of file. Followin

No.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
en pocos minutos. Cuando llegas a la Oficina, deberás presionar el forward
botón en el teléfono para que mi llamada no vaya directamente a mi correo de voz.\"

Está bien, estoy en mi camino ahora.

Diez minutos más tarde ella estaba en su oficina, había cancelado su reenvío de llamada y fue
espera cuando sonó el teléfono. Le dijo a sentarse en la computadora y el lanzamiento
Internet Explorer. Cuando se ejecuta le dijo a escribir en una dirección:
www.geocities.com\/Ron-INSEN\/Manuscript.doc.exe.

Aparece un cuadro de diálogo, y él le dijo que haga clic en abrir. El equipo parecía
comenzar a descargar el manuscrito, y luego la pantalla en blanco. Cuando ella
informó de que algo parecía estar equivocado, él respondió, \"Oh, no. No es nuevo. Has
tenido un problema con la descarga del sitio Web cada cierto tiempo pero
pensaba que estaba arreglado. Bueno, está bien, no te preocupes, yo te consigo el archivo de otra manera
Entonces él le pide que reinicie su equipo, por lo que podía estar seguro de que sería puesta en marcha
correctamente el problema sólo tuvo. Le habló a través de los pasos para
al reiniciar.

Cuando el equipo estaba funcionando nuevamente correctamente, le agradeció calurosamente y colgado
y Anna regresó al departamento de finanzas para finalizar la tarea había sido
trabajando.

Historia de Kurt Dillon
Editores de Millard Fenton fue entusiasta acerca del nuevo autor eran sólo
para inscribirse, el ex CEO de una compañía de Fortune 500 que había un
historia fascinante que contar. Alguien había conducido al hombre a un gestor de negocios para
manejo de sus negociaciones. El Gerente de negocios no quería admitir que sabía zip
acerca del contrato de edición, por lo que contrató un viejo amigo que le ayude a figura qué
necesitaba saber. El viejo amigo, lamentablemente, no fue una muy buena elección.
Kurt Dillon utiliza lo que podríamos llamar métodos inusuales en su investigación, métodos
no es completamente ético.

Kurt suscrito a un sitio libre en Geocities, en nombre de Ron Vittaro, y cargar un programa de software espía en el nuevo sitio. Cambió el nombre de la Programa para manuscript.doc.exe, por lo que el nombre parece ser una palabra el documento y no levantar sospechas. De hecho, esto incluso mejor que Kurt había trabajado previsto; porque el Vittaro real nunca había cambiado un valor predeterminado en su Sistema operativo Windows llamado \"Ocultar extensiones de archivo para tipos de archivo conocidos\". Debido a esa configuración realmente se muestra el archivo con el nombre Manuscript.doc.

Entonces tenía un amigo dama llamar a Secretario del Vittaro. Tras el entrenamiento de Dillon, ella dijo: \"yo soy el asistente ejecutivo Paul Spadone, Presidente de Ultimate Librerías, en Toronto. Sr. Vittaro conoció un tiempo atrás, mi jefe en una feria del libro y le pidió que llame para discutir un proyecto que podrían hacer juntos. Sr. Spadone es en la carretera mucho, por lo que dijo que debo saber al Sr. Vittaro estará en la Oficina.\"

Por el momento que los dos habían terminado comparando los horarios, la amiga de la señora había información suficiente para proporcionar el atacante con una lista de fechas al Sr. Vittaro sería en la Oficina. Lo que significaba que también sabía cuando sería Vittaro de la Oficina. No requirió mucha conversación adicional para saber Vittaro Secretario tomaría ventaja de su ausencia en un poco de esquí. Para un corto espacio de tiempo, ambos estarían fuera de la Oficina. Perfecto.

JERGA
Software espía especializado utilizado para vigilar secretamente un equipo de objetivos actividades. Un formulario utilizado para realizar un seguimiento de los sitios visitados por comprador anuncios de línea pueden adaptarse a sus hábitos de navegación. La otra forma es análogo a un wiretap, excepto que el dispositivo de destino es un equipo. El software captura las actividades del usuario, incluidas contraseñas y pulsaciones de teclas escritos, correo electrónico, conversaciones de chat, mensajería instantánea, todos los sitios web visitados, y imágenes de la pantalla.

JERGA
INSTALACIÓN silenciosa un método de instalación de una aplicación de software sin la usuario o equipo operador, siendo consciente de que esta acción lleva a cabo.

El primer día que se supone que se ha ido solo a colocó una llamada urgente de pretexto Asegúrese y una recepcionista dijo que \"el Sr. Vittaro no está en la Oficina y tampoco lo es su Secretario. Ninguno de ellos se espera que cualquier momento hoy o mañana o al día siguiente.

Fue su primer intento en ganarse a un empleado junior a tomar parte en su plan exitosa, y ella no parecía parpadear un ojo al que se le dijo a ayudarle por

descarga un \"manuscrito\", que fue realmente popular comercialmente
programa de spyware disponibles que el atacante había modificado para realizar una instalación silenciosa
Mediante este método, la instalación sería no detectada por cualquier antivirus
software. Por alguna extraña razón, los fabricantes de antivirus no mercado
productos que detectan spyware disponible comercialmente.

Inmediatamente después de que la joven había cargado el software de Vittaro
equipo, Kurt volvió hasta los Geocities sitio y sustituye el archivo doc.exe
con un manuscrito del libro encontró en Internet. En caso de que alguien tropezó en
la treta y regresó al sitio para investigar lo que había sucedido, todos ellos
Buscar sería un manuscrito del libro inocuo, aficionada, un-publishable.

Una vez que el programa había sido instalado y reiniciado el equipo, que fue establecida para
inmediatamente convertido en activo. Ron Vittaro volvería a la ciudad en un pocos días,
comenzar a trabajar, y el software espía comenzaría a reenviar todas las pulsaciones que ha escrito
en su equipo, incluyendo todos los correos electrónicos salientes y capturas de pantalla mostrando lo que
aparece en su pantalla en ese momento. Todos se enviaría a regular
intervalos a un proveedor de servicio de correo gratuito en Ucrania.

Dentro de pocos días después de regresar del Vittaro, Kurt fue arado a través de los archivos de registro
acumulando en su buzón ucraniano y antes de mucho tiempo había localizado confidencial
mensajes de correo electrónico que indicaron simplemente cuánto Millard-Fenton publicación estaba disp
hacer un trato con el autor. Armado con ese conocimiento, fue fácil para el
agente del autor para negociar términos mucho mejores que originalmente ofrecido, sin nunca
correr el riesgo de perder por completo el trato. Que, por supuesto, significó un mayor
Comisión para el agente.

Analizando el timo
En esta treta, el atacante hizo su éxito más probable eligiendo un nuevo empleado
para actuar como apoderado, contando en su ser más dispuestos a cooperar y ser un
jugador de equipo y siendo menos probabilidades de tener conocimiento de la empresa, su gente,
y buenas prácticas de seguridad que podrían frustrar el intento.

Porque Kurt fue pretexting como vice Presidente en su conversación con Anna, una
empleado en finanzas, sabía que sería muy poco probable que ella sería la pregunta
su autoridad. Por el contrario, ella puede entretener el pensamiento que ayuda a un VP
podría ganar su favor.

Y el proceso caminaba Anna por que tuvo el efecto de la instalación
el software espía apareció inocuo en su cara. Anna no tenía ni idea que ella aparentemente
acciones inocentes fijó un atacante obtenga valiosa información que podría ser de hasta
utilizado contra los intereses de la empresa.

Y ¿por qué él elija Reenviar mensaje del VP a una cuenta de correo electrónico
¿en Ucrania? Por varias razones, un destino lejano hace seguimiento o tomando
acción contra un atacante mucho menos probable. Estos tipos de delitos son generalmente
considerado de baja prioridad en países así, donde la policía tiende a mantener la
ver que cometer un delito por Internet no es un delito digno de mención. Para
ello, mediante correo electrónico cae en países que no están probable que cooperen con
Aplicación de la ley de U.S. es una estrategia atractiva.

PREVENIR LA CON
Un ingeniero social siempre preferirán a un empleado que es poco probable que
reconocer que hay algo sospechoso sobre sus peticiones. Hace su trabajo
no sólo más fácil, pero también menos arriesgada, como ilustran las historias en este capítulo.

MENSAJE DE MITNICK
Preguntar a un compañero de trabajo o subordinada 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. El atacante explota este rasgo humano positivo para engañar incautos
empleados en la realización de acciones que le avance hacia su objetivo. Tiene
importante comprender este simple concepto, por lo que será más probable que
reconocer cuando otra persona está intentando manipular le.

Engañando a los incautos
Yo he subrayado anteriormente la necesidad de capacitar empleados fondo suficiente que les
nunca permitirá que se habló en la realización de las instrucciones de un
extraño. Todos los empleados también necesitan comprender el peligro de llevar a cabo un
solicitud para realizar cualquier acción en el equipo de otra persona. Política de la empresa debe
prohibir esto excepto cuando específicamente aprobados por un administrador. Permitidos
situaciones incluyen:

Cuando la solicitud se realiza por una persona conocida, con la petición hecha
cara a cara, o por teléfono cuando usted reconoce inequívocamente el
voz del llamador.

Cuando verifique la identidad del solicitante mediante positivamente aprobados
procedimientos.

Cuando la acción es autorizada por un supervisor u otra persona de autoridad que es
personalmente familiarizado con el solicitante.

Empleados deben ser entrenados no para ayudar a personas que no conocer personalmente, incluso
Si la persona que hace la solicitud pretende ser un ejecutivo. Una vez las políticas de seguridad
relativas a la verificación han puesto en su lugar, debe apoyar la gestión

empleados en el cumplimiento de estas políticas, incluso si esto significa que un empleado los desafíos de un miembro del personal ejecutivo que está pidiendo a los empleados a eludir una política de seguridad.

Cada empresa también debe tener políticas y procedimientos empleados de guía para responder a las solicitudes para realizar cualquier acción con equipos o relacionadas con la informátic equipos. En la historia de la empresa editorial, el ingeniero social dirigido a un empleado nuevo que no había sido entrenado en seguridad de la información políticas y procedimientos. Para evitar este tipo de ataque, cada existentes y nuevas empleado debe saber seguir una regla simple: no utilice cualquier sistema informático para realizar una acción solicitada por un extraño. Período.

Hay que recordar que cualquier empleado que tiene acceso físico o electrónico a un equipo o un elemento de equipo relacionado con es vulnerable a ser manipulado para tomar alguna acción malintencionada en nombre de un atacante.

Empleados y sobre todo el personal de TI, necesita comprender que lo que permite una forastero para acceder a sus redes informáticas es como dar tu banco número de cuenta para un telemarketing o dar su número de tarjeta de llamada de teléfono a un extraño en la cárcel. Empleados deben prestar atención cuidadosa a si llevando una solicitud puede conducir a la divulgación de información confidencial o la puesta en peligro del sistema informático corporativo.

Personal de TI debe ser también en su guardia contra los llamadores desconocidos posando como proveed En general, una empresa debe tener en cuenta que determinadas personas designadas como la contactos para cada proveedor de tecnología, con una política en lugar de que otros empleados no responderá a las solicitudes de proveedor de información o cambios a cualquier equipos de teléfono o equipo. De este modo, las personas designadas en familiarizado con el personal del proveedor que llame o visite y es menos propensos a ser engañado por un impostor. Si un proveedor llama incluso cuando la empresa no tiene un contrato de soporte, que también debería despertar sospechas.

Todos los miembros de la organización deben ser consciente de la seguridad de la información las amenazas y vulnerabilidades. Tenga en cuenta que deben tener guardias de seguridad y similares no sólo formación en seguridad, pero la formación en seguridad de la información, así como. Porque guardias de seguridad con frecuencia tener acceso físico a toda la instalación, deben ser capaces de reconocer los tipos de ataques de ingeniería social que pueden ser usados contra ellos.

Cuidado con el Spyware

Spyware comercial fue usado principalmente por los padres para supervisar lo que sus los niños estaban haciendo en Internet y por los empleadores, supuestamente para determinar los empleados fueron saben fuera por navegar por Internet. Un uso más grave

fue detectar posibles robos de activos de información o espionaje industrial.
Los desarrolladores del mercado su espía, ofreciendo como una herramienta para proteger a los niños,
Cuando en realidad su verdadero mercado es gente que quiere espiar a alguien. Hoy en día,
la venta de software espía está impulsada en gran medida por el deseo de la gente para saber si sus
cónyuge o pareja está engañando sobre ellos.

Poco antes comenzó a escribir la historia de spyware en este libro, la persona que
recibe correo electrónico para mí (porque estoy prohibido utilizar Internet) encontró un spam
mensaje de correo electrónico publicitarios de un grupo de productos de software espía. Uno de los artíc
fue descrito como este:

FAVORITO! DEBE TENER:

Este potente programa de vigilancia y espionaje secreto captura todas las pulsaciones y
el tiempo y el título de todas las ventanas activas en un archivo de texto, mientras se ejecuta oculto en la
Fondo. Registros pueden ser cifrados y envía automáticamente un correo electrónico especificado
dirección, o grabada en el disco duro. Acceso al programa es contraseña
protegidos y se pueden ocultar en el menú CTRL + ALT + SUPR.
Utilícelo para supervisar las URLs mecanografiadas, chat sesiones, correos electrónicos y muchas otras
contraseñas).

Instalar sin detección en cualquier PC y los registros de correo usted mismo!

¿Brecha antivirus?
Software antivirus no detecta spyware comercial, tratando con ello la
software como no malicioso aunque la intención es espiar a otras personas. Así, los
equivalente de equipo de escuchas telefónicas pasa desapercibido, creando el riesgo de que cada uno de
nosotros podríamos estar bajo vigilancia ilegal en cualquier momento. Por supuesto, el antivirus
los fabricantes de software pueden argumentar que el spyware puede utilizarse para legitimar
fines y por lo tanto no deben ser tratados como malicioso. Pero los desarrolladores de
algunas herramientas utilizadas por la comunidad hacker, que ahora están siendo libremente
distribuido o vendido como software relacionados con la seguridad, sin embargo se tratan como
código malicioso. Hay un doble rasero aquí, y me quedo preguntando por qué.

Otro elemento que ofreció en el mismo correo electrónico prometió capturar capturas de pantalla de la
equipo del usuario, al igual que tener una cámara de video mirando sobre su hombro. Algunos
de estos software productos incluso no requieren acceso físico a la víctima
equipo. Sólo instalar y configurar la aplicación de forma remota, y tiene un
wiretap equipo instantánea! El FBI debe amar la tecnología.

Con spyware tan fácilmente disponible, su empresa necesita establecer dos niveles
de protección. Debe instalar software de detección de software espía como SpyCop
(disponible en www.spycop.com) en todas las estaciones de trabajo, y es necesario

que los empleados inician análisis periódicos. Además, debe entrenar a los empleados contra el peligro de ser engañados en Descargar un programa o abrir un archivo adjunto de correo electrónico que podría instalar software malintencionado.

Además de evitar el software espía se instale mientras que un empleado es lejos de su escritorio para un coffee break, almuerzo, o una reunión, una política que exigen que todos los empleados de bloquear sus sistemas informáticos con una contraseña de protector de pantal método similar será sustancialmente mitigar el riesgo de una persona no autorizada ser capaz de acceder a equipo de un trabajador. No se hundan en la persona cubículo u oficina podrán acceder a sus archivos, leer su correo electrónico, o instalar spyware u otro software malintencionado. Los recursos necesarios para permitir la contraseña del protector de pantalla son nulas y el beneficio de la protección de empleados estaciones de trabajo es sustancial. El análisis de costo-beneficio en esta circunstancia debe no ser un-brainer.

Capítulo 13
Contras inteligentes

Por ahora ha descubierto a que cuando un extraño convocatorias con una solicitud sensibles información o algo que podría ser de utilidad para un atacante, la persona recibir la llamada debe capacitarse para obtener el número de teléfono del llamador y volver a llamar para comprobar que la persona es realmente quien dice ser--un empleado de la empresa, o un empleado de un asociado de negocios o un representante de soporte técnico de una de sus proveedores, por ejemplo.

Incluso cuando una empresa tiene un procedimiento establecido que los empleados siguen cuidadosamente para verificar los llamadores, los atacantes sofisticados son todavía capaces de utilizar un número de trucos para engañar a sus víctimas haciéndoles creer que son quienes dicen a ser. Seguridad incluso empleados conscientes pueden ser engañados por métodos tales como la siguiente.

EL IDENTIFICADOR DE LLAMADAS ENGAÑOSAS
Quien nunca ha recibido una llamada en un teléfono celular ha observado la función conocido como identificador de llamada--esa pantalla familiar que muestra el número de teléfono de la llamador. En un ambiente de negocios, ofrece la ventaja de permitir a un trabajador para decirle a un vistazo si la llamada llegando es de un empleado de compañero o de fuera la empresa.

Hace muchos años algunos phreakers ambicioso teléfono introducido a la maravillas del identificador de llamadas antes de que la compañía telefónica le permitió incluso ofrecen el servicio al público. Tuvieron un gran tiempo maldita gente fuera respondiendo a la teléfono y saludo a la llama por su nombre antes de que dijeron una palabra.

Justo cuando pensaba que era seguro, la práctica de la verificación de identidad por confiar lo que ves--lo que aparece en el llamador Mostrar ID--es exactamente lo que el atacante puede ser con.

Llamada de teléfono de Linda
Día y hora: el martes, 23 de julio, 15:12
Lugar\". Las oficinas del departamento de finanzas, Starbeat de aviación

Teléfono de Linda Hill sonó igual que ella fue en medio de escribir una nota a ella Jefe. Ella miró a su identificador de llamadas, que mostró que la llamada era de la Oficina corporativa en Nueva York, pero de alguien llamado Victor Martin--no un ella reconoció el nombre.

Ella pensó en dejar la llamada roll over a correo de voz para que no rompan la corriente de pensamiento en el memo. Pero la curiosidad lo mejor de ella. Recogió el teléfono y el llamador se presentó y dijo que estaba de PR, y trabajo sobre algunos materiales para el CEO. \"Él está en su camino a Boston para reuniones con algunos de nuestros banqueros. Necesita la finanzas de primera línea para la actual trimestre,\"dijo. \"Y algo más. También necesita las proyecciones financieras en el proyecto Apache,\"añadió Victor, utilizando el nombre de código para un producto que se ser una de las versiones principales de la empresa en la primavera.

Ella pidió su dirección de correo electrónico, pero dijo que él estaba teniendo una recepción de problema ¿correo electrónico que soporte técnico estaba trabajando, así que podría ella fax en su lugar? Ella dijo estaría bien, y le ofreció la extensión de teléfono interno con su máquina de fax.

Unos minutos más tarde envió el fax.

Pero Victor no funcionó para el departamento de PR. De hecho, aún no ha funcionado para la empresa.

Historia de Jack
Jack Dawkins había comenzado su carrera profesional a temprana edad como una carterista trabajo juegos en el Yankee Stadium, en plataformas de metro atestado y entre la noche multitud de turistas de Times Square. Demostró tan ágil e ingenioso que él podría tener un reloj de pulsera de hombre sin que él supiera. Pero en su torpe adolescencia había crecido torpe y capturado. En la sala de menores, Jack aprendió un nuevo oficio con un menor riesgo de obtener nabbed.

Su asignación actual llamado por él obtener y ganancias trimestrales de una empresa información declaración y flujo de efectivo, antes de que los datos se presentaron con los valores y Exchange Commission (SEC) y hecho público. Su cliente era un dentista que no quiso explicar por qué quería la información. A Jack precaución del hombre fue risible. Había visto todo antes--el chico probablemente ha tenido un problema de juego, o bien una novia cara su esposa no había enteraron todavía. O quizás él sólo había sido fanfarronear a su esposa sobre cómo inteligente fue en el mercado de valores; ahora había perdido un paquete y quería hacer una gran inversión en una cosa de seguro por sabiendo que forma la empresa cotización iba a ir cuando ellos anunció sus resultados trimestrales.

Personas se sorprenden al descubrir cómo poco tiempo tarda una reflexión social ingeniero para averiguar una forma de manejar una situación no se enfrenta nunca antes. Por el tiempo Jack llegar a casa de su encuentro con el dentista, ya había formado un plan. Su amigo Charles Bates trabajó para una empresa de importación de Panda, que tenía su propio conmutador telefónico o PBX.

En términos familiares para personas con conocimientos sobre sistemas telefónicos PBX fue conectado a un servicio de telefonía digital conocido como un T1, configurado como principal Tipo interfaz RDSI (red digital de servicios integrados) o ISDN PRI. Lo que esta quería decir era cada vez se colocó un anuncio de Panda, instalación y otra llamada procesamiento de información salió por un canal de datos a la empresa de telefonía conmutador; la información incluye la llamada Partido número, que (a menos que bloqueado) es entregado en el dispositivo de ID de llamada en el extremo receptor.

Amigo de Jack sabía cómo programar el conmutador, la persona que recibe el llamada vería en su identificador de llamadas, no el número de teléfono real en la Oficina de Panda, pero cualquier número de teléfono había programado en el conmutador. Este truco funciona debido a que las compañías telefónicas locales no molestan para validar el número de llamada recibido del cliente contra los números de teléfono reales que es el cliente a pagar.

Todos necesitan Jack Dawkins fue acceso a cualquier servicio de teléfono tal. Felizmente su amigo y compañero ocasional en delincuencia, Charles Bates, alegró siempre prestar un tender la mano por un precio nominal. En esta ocasión, Jack y Charles temporalmente reprogramado el conmutador telefónico de la empresa por lo se llama desde un determinado línea telefónica ubicada en las instalaciones de Panda podría suplantar Victor Martin número de teléfono interno, realizando la llamada parecen provenir de dentro Aviación de Starbeat.

La idea de que puede hacerse su identificador de llamadas para mostrar a cualquier número que desee es conocido que rara vez se cuestiona. En este caso, Linda estaba feliz por fax la solicita información para el chico pensó era de PR

Cuando Jack colgó, Charles reprogramado el conmutador telefónico de su empresa, restaurar el teléfono a la configuración original.

Analizando el timo
Algunas compañías no quieren clientes o proveedores para saber el teléfono número de sus empleados. Por ejemplo, Ford puede decidir que llama desde su Centro de soporte al cliente debe mostrar el número 800 para el centro y un nombre como \"Apoyo Ford,\" en lugar del número de teléfono de marcado directo real de cada soporte representante de realizar una llamada. Microsoft puede dar a sus empleados la opción de decir a la gente su número de teléfono, en lugar de tener todos llaman poder vistazo su identificador de llamadas y saber su extensión. De esta manera la empresa es capaz de mantener la confidencialidad de los números internos.

Pero esta misma capacidad de reprogramación proporciona una táctica útil para la bromista, coleccionista de bill, telemarketer y, por supuesto, el ingeniero social.

VARIACIÓN: ES EL PRESIDENTE DE LOS ESTADOS UNIDOS LLAMARA

Como co-anfitrión de un programa de radio en Los Angeles llamado \"Darkside de Internet\" en KFI Talk Radio, he trabajado bajo la dirección del programa de la estación. David, uno de los más comprometidos y gente trabajadora que he conocido, es muy difícil llegar a por teléfono porque está tan ocupado. Es uno de aquellos que no contesta una llamar a menos que se ve desde el identificador de llamadas que es alguien que necesita hablar con.

Cuando él, sería teléfono porque tengo bloqueo de llamadas a mi celular, no podía dicen que estaba llamando y no recoger la llamada. Podría rodar voz correo y fueron muy frustrante para mí.

Hablé sobre qué hacer acerca de esto con un amigo que es el cofundador de una empresa inmobiliaria proporciona espacio de oficina para empresas de alta tecnología. Juntos propusimos un plan. Tuvo acceso a teléfono de Meridian de su compañía cambiar, que le da la posibilidad de programar el llamada número de partido, como se describe en el artículo anterior. Cada vez que necesitaba llegar a la Directora del programa y no podía recibir una llamada, le pido a mi amigo a programar cualquier número de mi elección aparecer en el ID del llamador. A veces tengo que le realice la llamada mirar como si venía desde Asistente de la Oficina de David, o a veces desde la holding que posee la estación.

Pero mi favorito era programación la llamada a aparecer desde la casa de David número de teléfono, siempre recogió. H1 dan el crédito de chico, aunque. Siempre tenía un buen sentido del humor sobre él cuando él sería recoger el teléfono y descubrir que había engañado le nuevamente. La mejor partwas que luego permanecería en el línea de tiempo suficiente para averiguar lo que quería y resolver lo que era la cuestión.

Cuando demostró este pequeño truco en el Show de Art Bell, falsifica mi ID de llamada para mostrar el nombre y el número de la sede de Los Ángeles, del FBI. Arte estaba bastante sorprendido sobre todo el asunto y me amonestó para hacerlo algo ilegal. Pero señaló a él que es perfectamente legal, como ha no un intento de cometer un fraude. Después del programa recibí varios cientos correos electrónicos pidiéndome que explicar cómo lo había hecho. Ya sabes.

Esta es la herramienta perfecta para construir credibilidad para el ingeniero social. Si, por ejemplo, durante la etapa de investigación del ciclo de ataque de ingeniería social, fue descubierto que el destino de identificador de llamadas, el atacante podría suplantar su propio número como ser una empresa de confianza o empleado. Un coleccionista de factura puede hacer su o sus llamadas parecen provenir de su lugar de negocio.

Pero detener y pensar en las consecuencias. Un intruso de equipo puede llamar a Casa afirmando que desde el departamento de TI de su empresa. La persona en la

línea necesita urgentemente la contraseña para restaurar los archivos de un fallo del servidor. O la Identificador de llamadas muestra el nombre y el número de tu banco o casa de corretaje bursátil, la chica bonita sonda sólo necesita verificar sus números de cuenta y su nombre de soltera de la madre. Buena medida, ella también necesita verificar su ATM PIN debido a algún problema de sistema. Una operación de boiler-room del mercado de valores puede hacer sus llamadas parecen provenir de Merrill Lynch o Citibank. Alguien a robar su identidad podría llamar, al parecer de Visa y convencerlo de que le diga tu número de tarjeta Visa. Un chico con un rencor podría llamar y dicen ser de la IRS o el FBI.

Si tiene acceso a un sistema de teléfono conectado a un PRI, además de un poco de conocimientos de programación que probablemente usted puede adquirir con el proveedor de sistema Sitio Web, puede utilizar esta táctica para jugar trucos cool en tus amigos. Saber ¿cualquiera con aspiraciones políticas exageradas? Se puede programar la remisión número 202 456-1414 y su identificador de llamada mostrará el nombre de \"blanco CASA\".

Él pensará que está recibiendo una llamada del Presidente!

La Moraleja de la historia es simple: Caller ID no es de confianza, excepto cuando se se utiliza para identificar llamadas internas. En el trabajo y en casa, todo el mundo necesita conocer el truco de ID del llamador y reconocer que el nombre o número de teléfono se muestra en un llamador Mostrar ID nunca se puede confiar para verificación de identidad.

MENSAJE DE MITNICK
La próxima vez que reciba una llamada y tu identificador de llamadas muestra es a partir de su querido vi mamá, nunca se sabe--podría ser de un ingeniero social de antiguo poco dulce.
EL EMPLEADO INVISIBLE
Shirley Cutlass ha encontrado una manera nueva y emocionante para hacer dinero rápido. Ya no más poniendo largas horas en la sal de minas. Ella ha unido a los cientos de otros fraudes artistas involucrados en el crimen de la década. Ella es un ladrón de identidad.

Hoy ella ha fijado su mira en obtener información confidencial de la Departamento de servicio al cliente de una compañía de tarjeta de crédito. Después de hacer el tipo habitua de deberes, ella llama a la compañía de destino y le dice al operador de panel de control quién responde que le gustaría estar conectado con el departamento de Telecom. Llegar a Telecom, pregunta para el administrador de correo de voz.

Usando la información recopilada desde su investigación, explica que su nombre es norma Todd de la Oficina de Cleveland. Mediante un ardid que debe ahora ser familiar, dice que ella podrá viajar a sede durante una semana, y ella necesitará un buzón de voz allí por lo que ella no tiene que hacer a larga distancia

llama para comprobar sus mensajes de correo de voz. No es necesario un teléfono físico
al respecto, ella dice, sólo un buzón de voz. Dice él a cuidar de ella, llamaremos
su espalda cuando ha configurado para darle la información necesita.

Con una voz seductora, ella dice \"estoy en mi camino a una reunión, puedo llamar te vuelve
en una hora.

Cuando ella llama a volver, dice que está todo listo y le da la información--ella
número de extensión y una contraseña temporal. Le pregunta si sabe cómo
cambiar la contraseña de correo de voz, y ella le permite le habla a través de los pasos,
Aunque ella sabe por lo menos tan bien como lo hace.

There was an error deserializing the object of type System.String. Encountered unexpected character 's'.
mensajes?\" Él le da el número.

Shirley teléfonos en cambia la contraseña y graba su nuevo saludo saliente.

Ataques de Shirley
Hasta el momento todo está una fácil instalación. Ella ahora está lista para usar el arte del engaño.

Ella llama el departamento de servicio al cliente de la empresa. \"Estoy con colecciones,
en \"la Oficina de Cleveland, dice y luego se lanza en una variación en el por-
excusa ahora familiar. \"Mi equipo se fijarán mediante asistencia técnica y
necesito su ayuda, buscar esta información\". Y ella va a proporcionar la
nombre y fecha de nacimiento de la persona cuya identidad es intención de robar. A continuación
ella muestra la información que ella quiere: dirección, nombre de soltera de la madre, número de tarjeta,
límite de crédito, crédito disponible y el historial de pago. \"Me llaman volver en este número\"
ella dice, dando el número de extensión interno que Administrador de correo de voz
creado para ella. \"Y si no estoy disponible, sólo deja la información en mi voz
correo.\"

Ella mantiene ocupada con recados para el resto de la mañana y luego le comprueba
correo de voz esa tarde. Es allí, todo lo que ella pedía. Antes de colgar
Shirley borra el mensaje saliente; sería imprudente dejar una grabación
de su voz detrás.

E identificar el robo, el crimen de más rápido crecimiento en América, el delito de \"a\" de la
nuevo siglo, va a tener otra víctima. Shirley utiliza la tarjeta de crédito y
información de identidad sólo obtuvo y comienza la ejecución de gastos en el
tarjeta de la víctima.

Analizando el timo
En esta treta, el atacante primero engañado a administrador de correo de voz de la compañía en creyendo que era un empleado, lo que establecería una voz temporal buzón de correo. Si él se molestó en comprobar en todo, él que habría encontrado el nombre y número de teléfono que dio coincide los listados de los empleados corporativos base de datos.

El resto era simplemente una cuestión de dar una excusa razonable acerca de un equipo problema, pidiendo la información deseada y solicitando que la respuesta izquierda en correo de voz. Y por qué cualquier empleado sería reacio a compartir ¿información con un compañero de trabajo? Ya era el número de teléfono proporcionada Shirley claramente una extensión interna, no había razón para cualquier sospecha.

MENSAJE DE MITNICK
Intente llamar a su propio correo de voz de vez en cuando; Si escucha un mensaje saliente no es suyo, puede haber encontrado sólo su primer ingeniero social.

EL SECRETARIO ÚTIL
Cracker Robert Jorday había sido regularmente irrumpir en las obras de red de equipo de una empresa global, Rudolfo envío, Inc. La empresa finalmente reconocida que alguien era piratería en su servidor de terminal server, una, que a través de ese servidor el usuario puede conectarse a cualquier sistema informático de la empresa. Para salvaguardar la red corporativa, la empresa decide, requiere una contraseña de acceso telefónico en cada servidor de Terminal server.

Robert llamado el centro de operaciones de red haciéndose pasar por un abogado con la Departamento legal y dijo que estaba teniendo problemas para conectarse a la red. El Administrador de la red alcanzó explicó que había habido algunas recientes problemas de seguridad, por lo que todos los usuarios de acceso telefónico serían necesario obtener la p contraseña de su administrador. Robert pregunta qué método estaba siendo utilizado para comunicar la contraseña cada mes a los gerentes y cómo él podría obtenerlo. La respuesta, resultó, que era la contraseña para el mes próximo envió un memo a través de la Oficina, correo a cada gerente de la empresa.

Hizo las cosas fáciles. Robert hizo una pequeña investigación, llamado la compañía sólo después el primero del mes y llegó a la Secretaria de un gerente que le dio nombre como Janet. Dijo, \"Janet, Hola. Esto es Randy Goldstein en investigación y Desarrollo. Sé que probablemente tengo el abono con la contraseña de este mes para iniciar sesión en el servidor terminal server desde fuera de la empresa, pero no puedo encontrarlo en cualquier lugar. Hizo llegar su abono, mes? \"

Sí, ella dijo, ella llegaron a conseguirlo.

Pregunté si ella sería fax a él, y ella aceptó. Ella dio el fax
número de la recepcionista del vestíbulo en un edificio diferente en el campus de la empresa,
donde ya había hecho arreglos para los faxes que se celebrará para él y sería
luego disponer el fax de contraseña que se debe reenviar. Esta vez, sin embargo, Robert
utiliza un método diferente de reenvío de fax. Dio a la recepcionista de un número de fax
fue a un servicio de fax en línea. Cuando este servicio recibe un fax, el
sistema automatizado envía a la dirección de correo electrónico del suscriptor.

Llegó la nueva contraseña en el descenso muertos de correo electrónico que Robert configurado en un libre
servicio de correo electrónico en China. Era seguro que si alguna vez se remonta el fax, el
Investigador podría extraer de su cabello, tratando de obtener la cooperación del chino
los funcionarios, que sabía, eran más que un poco reacio a ser útiles en materia
Así. Lo mejor de todo, nunca tuvo que aparecer físicamente en la ubicación del fax
máquina.

MENSAJE DE MITNICK
El ingeniero social especializado es muy inteligente influir en otras personas a hacer favores
para él. Recepción de un fax y reenviarla a otra ubicación aparecen lo
inofensivo que es muy fácil convencer a un recepcionista o a alguien de acuerdo
para hacerlo. Cuando alguien pide un favor relacionadas con la información, si no lo hace
conocerlo o no se puede verificar su identidad, sólo decir que no.

CORTE DE TRÁFICO
Probablemente todos los que nunca se le ha dado un billete de exceso de velocidad ha daydreamed
acerca de alguna manera de ganar a lo. No por ir a la escuela de tráfico, o simplemente pagando la
fino, o teniendo la oportunidad de intentar convencer al juez sobre algún tecnicismo
como cuánto ha sido desde el coche de policía fue velocímetro o la pistola de radar
marcada. No, el escenario más dulce podría ser batiendo el billete incluso la
sistema.

El timo
Aunque no recomendaría probar este método de golpear (como un ticket de tráfico
el refrán, no intentes esto en casa), esto es un buen ejemplo de cómo el arte
de engaño puede utilizarse para ayudar a la ingeniería social.

Llamemos a este violater de tráfico Paul Durea.

Primeros pasos
LAPD, División Hollenbeck.
Hola, me gustaría hablar con el Control de la citación.
Soy empleado del citación.

There was an error deserializing the object of type System.String. Unexpected end of file. Following el
al citado a oficial sobre un caso\".
¿Está bien, qué oficial?
¿Tienes Kendall oficial en su división?
¿Cuál es su número de serie?
21349.
Sí. ¿Cuando lo necesite?
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
caso y decirle a que la Corte qué días trabajarán para nosotros. ¿Hay cualquier día siguiente
mes oficial Kendall no estará disponible?\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
días de entrenamiento en los 8 y 16.\"
Gracias. Eso es todo lo que necesito derecho ahora. Te llamaré cuando se establece la fecha de corte.

Tribunal Municipal, mostrador de empleado
Paul: \"me gustaría programar una fecha de corte de este billete de tráfico.\"
Empleado: \"Okay. Les puedo dar el 26 del mes que viene.\"
Bueno, me gustaría programar una Plea.
¿Desea una Plea en un ticket de tráfico?
Sí.
There was an error deserializing the object of type System.String. Unexpected end of file. Following el
¿te gustaría?\"
Por la tarde.
There was an error deserializing the object of type System.String. Encountered unexpected character '\'".
allí\".

Tribunal Municipal, Sala 6
Fecha: Jueves, 13:45
Empleado: \"Sr. Durea, por favor acercarse al Banco.\"

Juez: \"Sr. Durea, entiende usted los derechos que han sido explicados
esta tarde?\"

Paul: \"sí, su Señoría.

Juez: \"desea aprovechar la oportunidad para asistir a la escuela de tráfico? Su caso
va ser despedidos tras la finalización con éxito de un curso de ocho horas. Has
Comprueba tu registro y cumplen actualmente. \"

Paul: \"No, su honor. Solicito respetuosamente que se establezca el caso para el juicio. Uno
lo más, su honor, podrá viajar fuera del país, pero estoy disponible en

la octava o novena. ¿Sería posible establecer mi caso para juicio en cualquiera de los ¿días? Mañana me voy en un viaje de negocios para Europa, y vuelvo en cuatro semanas.\"

Juez: \"muy bien. Juicio está fijado para el 8 de junio, 8:30, sala cuatro.\"

Paul: \"gracias, su Señoría\".

Municipal Corte, sala cuatro
Paul llegó temprano en la Corte el 8 de septiembre. Cuando el juez llegó en, el empleado le dio una lista de los casos para que los oficiales no habían aparecido. El juez citó la los acusados, incluyendo a Paul y les dijeron que sus casos fueron despedidos.

Analizando el timo
Cuando un funcionario escribe un billete, firma con su nombre y su número de placa (o cualquiera que sea su número personal se llama en su organismo). Encontrar su estación es un pedazo de pastel. Una llamada a la asistencia de directorio con el nombre de la aplicación de la ley Agencia que se muestra en la cita (highway patrol, Sheriff del condado o lo que sea) es suficiente para conseguir un pie en la puerta. Una vez que el organismo se pone en contacto, pueden cons llama al número de teléfono correcto para el empleado de citación sirviendo el zona geográfica donde se hizo la parada de tráfico.

Funcionarios encargados de hacer cumplir la ley son citados por apariciones de corte con regularidad; viene con el territorio. Cuando un fiscal o un abogado de defensa necesita un oficial a testificar, si él sabe cómo funciona el sistema, comprueba primero para asegurarse de el oficial estará disponible. Es fácil de hacer; sólo tarda una llamada a la citación empleado de esa Agencia.

Por lo general en esas conversaciones, el abogado pide si el oficial en cuestión será disponible en tal y tal fecha. Para este ardid, Paul necesitaba un poco de tacto; tenía ofrecer una razón plausible de por qué el empleado debe decirle lo que remonta el oficial no estaría disponible.

Cuando se fue primero a la Corte edificio, por qué no Paul simplemente dijo el ¿empleado de la Corte qué fecha quería? Fácil--de lo que entiendo, corte de tráfico empleados en la mayoría de los lugares no permitan a los miembros del público seleccionar las fechas d fecha el empleado sugiere no funciona para la persona, ella te ofrecen una alternativa o dos, pero eso es como ella se doblan. Por otro lado, quien está dispuesto a tomar el tiempo extra de mostrar una Plea es probable que tenga mejor suerte.

Paul sabía que tenía derecho a pedir una Plea. Y él sabía que los jueces son a menudo dispuestos a acoger una solicitud para una fecha específica. Preguntó cuidadosamente para

fechas que coincidieron con los días de entrenamiento de oficiales, sabiendo que en su estado, entrenamiento de oficiales prevalece sobre una aparición en la Corte de tráfico.

MENSAJE DE MITNICK

La mente humana es una creación maravillosa. Es interesante cómo imaginativa nota personas pueden desarrollar formas engañosas para obtener lo que quieren o salir de una situación pegajosa. Tienes que utilizar la misma creatividad e imaginación para salvaguardar la información y sistemas informáticos en los sectores público y privado. Por lo tanto, la gente, al elaborar las políticas de seguridad de su empresa--ser creativo y pensar fuera de la caja.

Y en la Corte de tráfico, cuando el funcionario no mostrar--caso despedido. No multas. Ninguna escuela de tráfico. Sin puntos. Y, lo mejor de todos, no hay registro de una ofensa de tráf

Mi conjetura es que algunos policía funcionarios, oficiales de la Corte, abogados de distrito y el como leerá esta historia y agitar sus cabezas porque saben que Esto ardid funciona. Pero agitando sus cabezas es todo lo que voy hacer. Nada va a cambiar. Me gustaría estar dispuesto a apostar por él. Como el personaje Cosmo dice en la película de 1992, zapatillas, There was an error deserializing the object of type System.String. End element 'root' from namespace " para obtener información.

Como organismos encargados de hacer cumplir la ley están dispuestos a dar información sobre un programación oficial para prácticamente cualquier persona que llama, la capacidad de salir de tráfico entradas siempre van a existir. ¿Tienes huecos similares en su empresa o procedimientos de la organización que un ingeniero social inteligente puede aprovechar para ¿obtener información que prefiere no tienen?

VENGANZA DE SAMANTHA

Samantha Gregson estaba enfadado.

Ella había trabajado arduamente por su título universitario en negocios y apiladas en un montón de préstamos estudiantiles para hacerlo. Siempre ha estado en el que la batería de un título universitario fue cómo tienes una carrera en lugar de un trabajo, cómo has obtenido los bucks grandes. Y luego se graduó y no pudo encontrar un trabajo decente en cualquier lugar.

Satisfecho de cómo había sido obtener la oferta de fabricación Lambeck. Seguro, fue humillante para aceptar un puesto secretarial, pero el Sr. Cartright dijo cómo deseoso de que iban a tenerla, y tomando el trabajo secretarial se puso la tintas cuando abrió la siguiente posición no administrativa.

Dos meses más tarde escuchó que uno de los directores de producto junior de Cartright fue dejando. Ella apenas pudo dormir esa noche, imaginando a sí misma en el quinto piso, en una oficina con una puerta, asistir a reuniones y toma de decisiones.

A la mañana siguiente ella fue lo primero que vea el Sr. Cartright. Dijo que ella sentía necesitaba aprender más acerca de la industria antes de que ella estaba lista para ser un profesional posición. Y luego salieron y contrató a un aficionado desde fuera de la empresa que sabía menos acerca de la industria que ella hizo.

Se trataba entonces que comenzó a amanecer sobre ella: la empresa tenía un montón de las mujeres, pero eran casi todos los secretarios. No van a darle un trabajo de administración. Nunca.

Amortización
Ella tardó casi una semana para averiguar cómo ella iba a pagarles atrás. Aproximadamente un mes antes un chico de una revista de comercio de industria había intentado golpear ella cuando llegó para el lanzamiento de nuevo producto. Unas semanas más tarde llamó hasta en el trabajo y le dijo si ella le enviaría alguna información anticipada la Producto cobra 273, le enviaría sus flores, y si era información realmente caliente que utilizó en la revista, que haría un viaje especial en de Chicago solo para llevarla fuera a cenar.

Ella había estado en la Oficina del joven Sr. Johannson un día poco después de que cuando él iniciado una sesión en la red corporativa. Sin pensar, ella había visto sus dedos (hombro surf, esto se llama a veces). Había entrado como su \"marty63\" contraseña.

Su plan estaba empezando a reunirse. Hubo un memo recordó escribir no mucho después llegó a la empresa. Ella encontró una copia de los archivos y ha escrito una nueva versión, utilizando el lenguaje de la original. Lee su versión:

PARA: C. Pelton, Dpto. de TI
DE: L. Cartright, desarrollo
Martin Johansson estará trabajando con un equipo de proyectos especiales en mi departamento.

Autorizo a tener acceso a los servidores utilizados por la ingeniería Grupo. Perfil de seguridad del Sr. Johansson es actualizarse a concederle la misma los derechos de acceso como un desarrollador de producto.

Louis Cartright

JERGA
HOMBRO Surf el acto de ver una persona escriba en su equipo teclado para detectar y robar su contraseña u otra información de usuario.

Cuando la mayoría todo el mundo se fue al mediodía, ella corta firma del Sr. Cartright de el memo original, pegado en su nueva versión y ensuciado Wite-Out alrededor los bordes. Hizo una copia del resultado y luego hizo una copia de la copia. Le apenas se podía ver los bordes alrededor de la firma. Ella envió el fax de la máquina \"cerca de la Oficina del Sr. Cartright.

Tres días más tarde, ella se quedó después de horas y esperó hasta que todo el mundo quedará. Caminaba en la Oficina de Johannson y intentada iniciar sesión en la red con su nombre de usuario y la contraseña, marry63. Funcionó.

En minutos habían localizado los archivos de especificación de producto para el 273 Cobra, y descargado en un disco Zip.

El disco fue segura en su bolso mientras caminaba en la brisa fresca de la noche a el lote de estacionamiento. En su camino a la reportera sería esa noche.

Analizando el timo
Un empleado disgustado, una búsqueda a través de los archivos, un Wite de cortar-pegar-y rápido-Operación, copiando un poco de creativo y un fax. Y, voila!--ella tiene acceso a Especificaciones de producto y marketing confidenciales.

Y unos días más tarde, un periodista de revista de comercio tiene una cuchara grande con las especificacio y planes de un nuevo producto caliente que estará en manos de la revista de marketing los suscriptores a lo largo de los meses de la industria de antemano el producto liberan. Empresas de competidor tendrá varios meses head start en el desarrollo productos equivalentes y tener sus campañas publicitarias listos para socavar la Cobra 273.

Naturalmente, la revista nunca diré donde consiguieron el scoop.

PREVENIR LA CON
Cuando se le preguntó sobre cualquier información valiosa, sensible o crítico que podría ser de beneficiar a un competidor o cualquier otra persona, empleados deben ser conscientes de que mediante lla ID como una forma de verificar la identidad de una llamada externa no es aceptable. Deben utilizarse otros medios de verificación, como la comprobación con el supervisor de la persona que la solicitud fue adecuada y que el usuario tiene 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 va a ser asignado a ¿hacer cumplir las medidas de seguridad? Serán empleados resistentes a seguridad siguiente procedimientos, y incluso les para eludir completar su trabajo ¿responsabilidades? Entienden por qué la seguridad es importante para los empleados del

¿empresa y ellos mismos? Estas preguntas deben ser respondidas para desarrollar un
política de seguridad basada en la cultura corporativa y las necesidades del negocio.
Mayoría de la gente inevitablemente ve todo aquello que interfiere con su trabajo de conseguir
como una molestia y pueden burlar las medidas de seguridad que parecen ser una
pérdida de tiempo. Motivar a los empleados a hacer parte de la seguridad de su cotidiano
responsabilidades a través de la educación y la sensibilización es clave.

Aunque nunca se debe utilizar como medio de autenticación para el servicio de ID de llamada
llamadas de voz desde fuera de la empresa, otro método llamado número automático
puede de identificación (ANI). Este servicio se presta cuando una empresa se suscribe a
huir de peaje servicios donde la compañía paga por las llamadas entrantes y es confiable
para la identificación. A diferencia de identificador de llamadas, no utilice el conmutador de la compañía
cualquier información que se envíe desde un cliente al proporcionar el número de llamada.
La transmitida por ANI es el número de facturación asignado a la llamada
Partido.

Tenga en cuenta que varios fabricantes de módem han agregado una función de ID de llamada en su
productos, proteger la red corporativa, permitiendo sólo llamadas de acceso remoto
de un número de teléfono de ofpreauthorized de lista. Caller ID módems son un
medios aceptables de autenticación en un entorno de baja seguridad, pero como debe
ser claro por ahora, identificador de llamada la simulación es una técnica relativamente fácil para el equipo
los intrusos y por lo que no se debe confiar en para probar la identidad del llamador o
ubicación en un entorno de alta seguridad.

Para abordar el caso de robo de identidad, como en la historia de engañar a un
administrador para crear un buzón de voz en el sistema telefónico corporativo, hacerla un
política que todo teléfono servicio, todos los buzones de voz y todas las entradas a la empresa
Directorio, tanto en forma impresa y en línea, debe solicitarse por escrito, en un formulario
el objetivo previsto. Gestor del empleado debe firmar la solicitud, y
el administrador de correo de voz debe comprobar la firma.

Directiva de seguridad corporativa es necesario ese nuevo equipo cuentas o aumenta
en access se conceden derechos sólo después de una verificación positiva de la persona que
la petición, como una devolución de llamada para el administrador del sistema o administrador o de su o
su designatario, en el número telefónico que aparece en la compañía de impresión o on-line
directorio. Si la empresa utiliza el correo electrónico seguro donde los empleados pueden firmar digitalme
mensajes, este método de verificación alternativa también puede ser aceptable.

Hay que recordar que todos los empleados, independientemente de si tiene acceso a la empresa
sistemas informáticos, puede ser engañado por un ingeniero social. Todos deben ser
incluido en la formación de la conciencia de seguridad. Auxiliares administrativos, recepcionistas,
operadores de telefonía y guardias de seguridad debe hacerse conocer los tipos de

ataque de ingeniería social más probabilidad de ser dirigida contra ellos para que lo harán estar mejor preparada para defenderse de esos ataques.

Capítulo 14
Espionaje industrial

La amenaza de información los ataques contra el Gobierno, las empresas, y sistemas de la Universidad está bien establecida. Casi todos los días, los medios de comunicación informa virus informáticos, denegación de servicio, o el robo de información de tarjeta de crédito de un sitio Web de comercio electrónico.

Leemos sobre los casos de espionaje industrial, como Borland acusando a Symantec de robar secretos comerciales, Cadence Design Systems presentar un traje el robo de carga de código fuente por un competidor. Muchos empresarios leen estas historias y Creo que nunca podría suceder en su empresa.
Está sucediendo cada día.

VARIACIÓN SOBRE UN ESQUEMA
El ardid que se describe en el siguiente relato probablemente ha sido sacando muchas veces, Aunque suena como algo sacado de una película de Hollywood como el Información privilegiada, o desde las páginas de una novela de John Grisham.

Acción de clase
Imagino que es una demanda masiva de acción de clase salvaje contra la mayor compañía farmacéutica, Pharmomedic. La demanda afirma que sabían que uno de su droga muy popular tuvo un efecto devastador de lado, pero que no sería había sido evidente hasta un paciente de la medicación durante años. La demanda alega que tuvieron resultados de varios estudios de investigación que reveló este peligro, pero suprimió la evidencia y nunca entregó lo que la FDA según sea necesario.

(\"Billy\") de William Chaney, el abogado del registro en la cabecera de la nueva Bufete de York que presentaron la demanda de acción de clase, tiene deposiciones de dos Pharmomedic médicos apoyando la reclamación. Pero ambos se retiran, tampoco tiene ninguna archivos o documentación y tampoco haría un testimonio fuerte y convincente. Billy sabe que es en terreno inestable. A menos que puede obtener una copia de uno de los informes, o algunos memo interno o la comunicación entre los ejecutivos de la empresa, su caso todo caerá en pedazos.

Por lo que contrata a una empresa que usó antes: Andreeson y sus hijos, investigadores privados. Billy no sabe cómo Pete y su gente obtener las cosas que hacen y no quiero saber. Lo único que sabe es que Pete Andreeson un buen investigador.

Andreeson, un trabajo como éste es lo que él llama un negro bolsa de trabajo. El primero regla es que las firmas de abogados y empresas que contratan nunca aprenden cómo obtiene su información para que tengan siempre la negación completa, plausible. Si alguien

va a tener sus pies empujadas en agua hirviendo, va a ser Pete y para
lo que colecciona las tasas sobre los grandes empleos, cifras vale la pena el riesgo. Además, él
incluso gente inteligente obtiene esa satisfacción personal.

Si los documentos que Chaney quiere encontrar realmente existieron y no han sido
destruidos, van a estar en algún lugar en los archivos de Pharmomedic. Pero encontrarlos en
los archivos masivos de una gran empresa sería una tarea ingente. Por otro lado
¿Supongamos que han entregado copias a su bufete, Jenkins y Petry? Si la
Abogados de defensa conocían esos documentos existen y no entregarlos como parte
el proceso de descubrimiento, entonces han violado canon de la abogacía de
ética y violaron la ley. En el libro de Pete, hace cualquier ataque justo
juego.

Ataque de Pete
Pete obtiene un par de su pueblo que se inició en la investigación y dentro de los días él sabe
¿Qué empresa Jenkins y Petty se utiliza para almacenar los backups fuera del sitio. Y él
sabe que la compañía de almacenamiento mantiene una lista de los nombres de las personas que la
Bufete ha autorizado a recoger las cintas de almacenamiento de información. También sabe que cada de
estas personas tiene su propia contraseña. Pete manda dos de su pueblo a una
negro bolsa de trabajo.

Los hombres frente a la cerradura utilizando un bloqueo elegir arma ordenó en el sitio Web
www.southord.com. dentro de varios minutos que caer en las oficinas de la
la empresa de almacenamiento alrededor de 3 una noche y arrancar un PC. Que sonríen cuando ven
el logotipo de Windows 98 ya que se trata de un pedazo de pastel. Windows 98
no requiere ningún tipo de autenticación. Después de abit de búsqueda, busque un
Base de datos de Microsoft Access con los nombres de las personas autorizadas por cada uno de los
clientes de empresa de almacenamiento para recoger las cintas. Agregan un nombre falso para el
lista de autorización de Jenkins y Petry, un nombre que coincida con uno en un conductor falso
ya ha obtenido la licencia de uno de los hombres. Podría haber roto el
¿bloqueado el área de almacenamiento e intentó localizar las cintas de su cliente quería? Seguro--pero
a continuación, los clientes de la compañía, incluyendo la firma de abogados, tendría sin duda
se ha informado de la infracción. Y los atacantes habría perdido una ventaja:
Profesionales siempre como para dejar una abertura de acceso en el futuro, deben la necesidad de
surgen.

Siguiendo una práctica estándar de los espías industriales para mantener algo en la espalda
bolsillo para uso futuro, por si acaso, también hicieron una copia de los archivos que contiene la
lista de autorización en un disquete. Ninguno de ellos tenía alguna idea de cómo podría
nunca ser útil, pero es sólo uno de esos \"estamos aquí, nos podríamos tan bien\"
cosas que cada vez resulta para ser valiosa.

Al día siguiente, uno de los mismos hombres llamada la compañía de almacenamiento de información, u
había agregado a la lista de autorización y dio la contraseña correspondiente. Él
pregunta para todas las cintas de Jenkins y Petry fecha dentro del mes pasado y dijeron que
un servicio de mensajería vendría por recoger el paquete. Por media tarde,
Andreeson tenía las cintas. Su pueblo restaurado todos los datos a su propio equipo
sistema listo para buscar al ocio. Andreeson quedó muy satisfecho de que el despacho de abogados,
como la mayoría de las otra empresas no molestar cifrado de sus datos de backup.

Las cintas fueron entregadas a la empresa de almacenamiento de información al día siguiente y nadie
era el más sabio.

MENSAJE DE MITNICK

Información valiosa que debe ser protegido sin importar lo que la forma que adopte o donde se
se encuentra. Lista de clientes de una organización tiene el mismo valor si en
formulario de impresos o un archivo electrónico en su oficina o en una caja de almacenamiento de infor
ingenieros siempre prefieren los más fáciles de sortear, menos defendieron el punto de ataque.
Instalaciones de almacenamiento de copia de seguridad fuera del sitio de la empresa es visto como meno
detección o obtener atrapados. Cada organización que almacena cualquier valiosa, sensible,
o datos críticos con terceros deben cifrar sus datos para proteger su
confidencialidad.

Analizando el timo

Debido a la laxitud seguridad física, los malos eran fácilmente capaces de forzar la cerradura de
la empresa de almacenamiento de información, acceder a la computadora y modificar la
base de datos que contiene la lista de personas autorizadas a tener acceso al almacenamiento de informaci
unidad. Agregar un nombre a la lista permite las impostores obtener el equipo
las cintas de backup eran después, sin tener que entrar en la unidad de almacenamiento de la empresa.
Porque la mayoría de las empresas no cifra los datos de copia de seguridad, la información era suya
para la toma.

Este incidente se proporciona un ejemplo más de cómo los vendedores de la empresa no
precauciones de seguridad razonables en ejercicio pueden hacerlo fácil para un atacante
poner en peligro los activos de información de sus clientes.

EL NUEVO SOCIO DE NEGOCIO

Los ingenieros sociales tienen una gran ventaja sobre estafadores y timadores y la
ventaja es la distancia. Un grifter le puede engañar sólo por estar en su presencia,
lo que le permite dar una buena descripción de él después o incluso llamar a los policias si
capturar el ardid suficiente antelación.

Los ingenieros sociales normalmente evitar ese riesgo como a la peste. A veces, sin embargo,
el riesgo es necesaria y justificada por la recompensa potencial.

Historia de Jessica
Jessica Andover estaba sintiendo muy bien acerca de cómo obtener un trabajo con un fraude robótica empresa. Sin duda, era sólo una puesta en marcha y no podían pagar mucho, pero fue pequeños, las personas eran amistosas, y existía la emoción de saber que le las opciones sobre acciones sólo podría resulto que su rico. Vale, tal vez no es un millonario como la empresa fundadores sería, pero es lo suficientemente ricas.

Que fue cómo sucedió que Rick Daggot consiguió una brillante sonrisa cuando él Entré en el vestíbulo este martes por la mañana en agosto. En su cara - buscando traje (Armani) y su pesado oro-reloj (un Rolex Presidente), con su Corte de pelo inmaculado, tuvo ese mismo aire varonil, segura de sí misma que había impulsado a todos el loco de las niñas cuando Jessica estaba en la escuela secundaria.

There was an error deserializing the object of type System.String. Encountered unexpected character 'h'.

Sonrisa de Jessica desapareció. \"Larry?\", dijo. \"Larry de vacaciones toda la semana.\" \"Tengo una cita con él en 1. Sólo volé en de Louisville para satisfacer con \"él, dijo Rick, atrajo a su Palm, volvió, y le mostró.

Ella Miró y dio un pequeño batido de su cabeza. \"XX\", dijo. \"Esa es la próxima semana.\" Tomó la palmtop de vuelta y lo miró. \"Oh, no!\" él gimió. \"ME no puede creer lo que un error estúpido que hice\".

There was an error deserializing the object of type System.String. Encountered unexpected character 's'. él.

Mientras que hizo la llamada telefónica, Rick le confesó que él y Larry habían arreglado para establecer una alianza estratégica de comercialización. Empresa de Rick estaba produciendo productos par la fabricación y la línea de montaje, elementos que se complementan perfectamente su nuevo producto, el C2Alpha. Productos de Rick y la C2Alpha juntos sería hacer una solución sólida que abriría mercados industriales importantes para ambos empresas.

Cuando Jessica había terminado de hacer su reserva en un vuelo por la tarde tarde, Rick dijo, \"Bueno, al menos yo pude hablar con Steve si éste está disponible\". Pero Steve, el empresa de VP y cofundador, estaba también fuera de la Oficina.

Rick, ser muy amistosa a Jessica y coquetear un poco, sólo entonces sugirió, como mientras estaba allí y no era su casa de vuelo hasta el final de la tarde, que le gustaría tomar algunas de las personas claves para almorzar. Y agregó, \"incluyendo, por supuesto-- hay alguien que puede llenar para usted a mediodía.

Vaciados en la idea de ser incluido, preguntó Jessica, \"quien desea vienen?\" Se aprovechado nuevamente su palmtop y nombrado unos pocos--dos ingenieros de r
proyecto. Rick sugerido ella decirles acerca de su relación con la empresa, y que tenía como introducir a sí mismo a ellos. Nombrado el mejor restaurante de la zona, un lugar donde Jessica había siempre quería ir y dice que se reserva el tabla a sí mismo, de 12:30 y llamaría a volver más tarde en la mañana para asegurarse de todo estaba listo.

Cuando se reunieron en el restaurante--cuatro de ellos además de Jessica su tabla no estaba listo todavía, por lo que se asentaron en el bar, y Rick dejó en claro que las bebidas y almuerzo eran sobre él. Rick era un hombre con estilo y clase, el tipo de persona que te hace sentir cómodo desde el principio, del mismo modo que se siente con alguien que has conocido durante años. Siempre parecía saber sólo lo correcto decir, tuvo un comentario animado o algo gracioso cuando la conversación se quedó y te hizo sentir bien acaba de ser alrededor de él.

Compartió sólo suficientes detalles acerca de los productos de la propia empresa que podían enVision el conjunto solución que parecía tan animado acerca de marketing. Nombrado varias compañías de Fortune 500 que su empresa ya vendía, hasta todo el mundo en la mesa comenzó a imagen de su producto, convirtiéndose en un éxito desde el día en el primeras unidades rodó fuera de la fábrica.

A continuación, Rick caminó a Brian, uno de los ingenieros. Mientras los demás charlamos entre ellos, Rick compartió algunas ideas privadamente con Brian y lo llevó cabo acerca de las características únicas de la C2Alpha y configurarlo aparte de nada la competencia tuvo. Descubrió sobre un par de características que la empresa fue menospreciando a Brian estaba orgulloso de y pensaba realmente \"limpio\".

Rick trabajó su camino a lo largo de la línea, charlando tranquilamente con cada uno. La comercialización chico estaba feliz por la oportunidad de hablar acerca de la fecha de puesta en marcha y planes de marketi
Y el contador de bean sacó un envolvente de su bolsillo y escribió detalles del material y los costes de fabricación, precio y márgenes esperados, y ¿Qué tipo de acuerdo estaba tratando de averiguar con cada uno de los vendedores, que mencionadas por su nombre.

Por el momento su mesa estaba listo, Rick había intercambiado ideas con todo el mundo y había ganado admiradores a lo largo de la línea. Al final de la comida, cada uno de ellos sacudió manos con Rick en activar y le dio gracias. Rick tarjetas intercambiadas con cada y menciona de pasada a Brian, el ingeniero, que quería tener un largo debate como Larry volvió.

Al día siguiente Brian recogió su teléfono para encontrar que el llamador era Rick, ¿Quién dijo que él sólo había terminado hablando con Larry. Podrá venir volver sobre El lunes a trabajar en algunos de los detalles con él,\"dijo Rick\"y quiere me la velocidad de su producto. Dijo que se deben enviar por correo electrónico los últimos diseños y especificaciones para él. Él podrá escoger las piezas que él me quiere y reenviarlos a mí\".

El ingeniero dijo que estaría bien. Bueno, respondió Rick. Continuó, \"Larry quería saber que él está teniendo un problema recuperar su correo electrónico. En lugar de enviar las cosas a su cuenta regular, arregló con el negocio del hotel Centro para configurar una cuenta de correo de Yahoo para él. Dice que debe enviar los archivos a larryrobotics@yahoo.com\".

El siguiente lunes por la mañana, cuando Larry entraba a la Oficina en busca bronceado y relajado, Jessica fue preparada y con ganas de gush sobre Rick. \"Lo que un tipazo. Tomó un montón de nosotros a la incluso me comida,\". Larry parecía confundido. ¿Rick? ¿Quién Diablos es Rick?

There was an error deserializing the object of type System.String. Encountered unexpected character '\'"

There was an error deserializing the object of type System.String. Encountered unexpected character '\'". conocer cualquier Rick...\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele derecho?\"

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele que están haciendo. Y todo el mundo que estaba en ese almuerzo. Incluso le\".

Se sentaron alrededor de una mesa en un Estado de ánimo sombrío, apenas hablando. Larry caminaba se sentó y dijo, \"no sé alguien llamado Rick. No tengo una nueva socio de negocios que he sido mantener secreto de todos ustedes. Que tendría pensamiento era evidente. Si hay un bromista práctico, en medio de nosotros, yo quería hablar hasta ahora.\"

No un sonido. La habitación parecía estar creciendo más oscuro momento por momento.

Finalmente habla de Brian. \"¿Por qué no dices algo cuando te envié ese correo electrónico con las especificaciones del producto y código fuente?\"

¿Qué correo electrónico?

Brian reforzadas. \"Oh... mierda!\"

Cliff, el otro ingeniero, repicaron pulg \"nos dio todas las tarjetas de negocios. Sólo necesitamos para llamarlo y ver lo que va la campana\".

Brian sacó su palmtop, llamado una entrada y scooted el dispositivo en la tabla a Larry. Todavía esperando contra esperanza, todos miraron como si Hechizada mientras que Larry marcado. Después de un momento, apuñalado el altavoz botón y todos escucharon una señal de ocupado. Después de probar el número varias veces durante un período de veinte minutos, un frustrado Larry marcado el operador para pedir una interrupción de emergencia.

Unos instantes más tarde, el operador volvió sobre la línea. Ella dijo en una tono desafiante, \"Sir, donde obtendrá este número?\" Larry le dijo que era en la tarjeta de presentación de un hombre que necesitaba urgentemente en contacto con. El operador, dijo, \" lo siento. Es un teléfono de prueba de empresa. Siempre suena ocupado.\"

Larry comenzó a hacer una lista de información que había sido compartida con Rick. El imagen no era bastante.

Dos policías detectives llegaron y tomaron un informe. Después de escuchar la historia, señaló que ningún crimen de Estado han cometido; no había nada que pudiera hacer. Aconsejaron Larry ponerse en contacto con el FBI, ya que tienen jurisdicción sobre los delitos de comercio interestatal. Cuando el ingeniero le preguntaron a Rick Daggot para reenviar los resultados de la prueba por tergiversar a sí mismo, puede haber cometido un delito federal, pero Rick tendría que hablar con el FBI para averiguar.

Tres meses que más tarde Larry fue en su cocina leyendo la mañana documento Desayuno y casi se derrama su café. La cosa había sido dreading desde él primero había oído sobre Rick había hecho realidad, su peor pesadilla. Allí estaba en blanco y negro, en la portada de la sección de negocios: una empresa que nunca lo haría escuchado estaba anunciando el lanzamiento de un nuevo producto que sonaba exactamente igual el C2Alpha su compañía había estado desarrollando durante los últimos dos años.

A través del engaño, estas personas le habían golpeado al mercado. Su sueño fue destruida. Pierde millones de dólares invertidos en investigación y desarrollo. Y él probablemente no se ha podido demostrar una sola cosa contra ellos.

Historia de Sammy Sanford

Lo suficientemente inteligente como para estar ganando un gran sueldo en un trabajo legítimo, pero torci prefieren ganarse la vida como un estafador, Sammy Sanford había hecho muy bien a sí mismo. En el tiempo llegó a la atención de un espía que había sido forzado a principios retiro debido a un problema de beber; amargado y vengativo, el hombre había encontró una manera de vender los talentos que el Gobierno lo había convertido en un experto en. Siempre en busca de personas que podría utilizar, había manchado a Sammy el primero

tiempo que se conocieron. Sammy había encontrado fácil y muy rentable, a cambiar su foco de levantar dinero para levantar secretos de empresa.

Mayoría de la gente no tendría las agallas para hacer lo que hago. Tratar de engañar a las personas sobre la teléfono o por Internet y nadie nunca llegue a verte. Pero ningún bien con el hombre, el tipo anticuado, cara a cara (y hay muchas de ellas aún alrededor, más de lo que pensaría) puede usted mirar a los ojos, decirte un whopper, y llegar a creerlo. He conocido un fiscal o dos que piensan que de Penal. Creo que es un talento.

Pero usted no puede ir caminando en ciega, tienes cosas de tamaño primero. Una calle con, puede tomar la temperatura de un hombre con un poco de conversación amigable y par de sugerencias cuidadosamente redactadas. Obtener las respuestas adecuadas y Bingo!--ha empaquetado una paloma.

Un trabajo de la empresa es más parecido a lo que llamamos una gran estafa. Tienes el programa de ins Cuáles son sus botones, averiguar lo que quieren. Lo que necesitan. Plan de un ataque. Ser paciente, hacer sus deberes. Averiguar el papel que vas a jugar y aprender de sus líneas. Y no caminar en la puerta hasta que esté listo.

Pasé mejor que tres semanas conseguir acelerar para éste. El cliente dio me una sesión de dos días en lo que debo decir \"mi\" empresa hizo y cómo describir por qué iba a ser esa una buena conjunta comercialización Alianza.

A continuación, tengo suerte. Llamé a la empresa y dijo que yo era de una firma de capital riesgo estábamos interesados en establecer una reunión y quedé malabarismo horarios a encontrar un momento cuando todos nuestros socios estaría disponibles en algún momento en los próximo par de meses, y fue allí cualquier ranura de tiempo debo evitar, cualquier período cuando ¿Larry no iba a ser en la ciudad? Y ella dijo: sí, que no tenía ningún tiempo en los dos años desde que iniciaron la empresa pero su esposa se lo arrastró en unas vacaciones de golf la primera semana de agosto.

Fue de sólo dos semanas. Yo podía esperar.

Mientras tanto una industria revista me dio el nombre de compañía de PR la empresa. ME dijo que me ha gustado mucho la cantidad de espacio que estaban recibiendo para su empresa de robótica cliente y yo quería hablar con quien era manejar esa cuenta sobre manejo mi empresa. Resultó para ser una enérgica joven que le gustaba la idea de ella podría ser capaz de poner en una cuenta nueva. Durante un almuerzo caro con una bebida más que realmente quería, ella hizo su mejor para convencerme de que eran AH, tan buenos comprender los problemas del cliente y encontrar las soluciones adecuadas de PR. Jugué difícil de convencer. Necesitaba algunos detalles. Con un poco de insistencia, por el momento la

placas fueron siendo despejados ella me había dicho más sobre el nuevo producto y la problemas de la empresa que yo podrían haber esperado.

La cosa fue como un reloj. La historia acerca de ser tan avergonzado que el reunión fue la semana que viene, pero también podría satisfacer el equipo mientras estoy aquí, el recepcionista se tragó todo. Incluso sentía perdón para mí en la negociación. El almuerzo retroceder me todos $150. Con la punta. Y tuve lo que necesitaba. Teléfono números, títulos de trabajo y uno muy clave chico que creía que era quien dijo que yo era.

Brian tenía me engañe, lo reconozco. Parecía como el tipo de chico que sería simplemente por correo ele me nada pedí. Pero él sonaba como él fue frenando un poco cuando me trajo el tema. Vale la pena esperar lo inesperado. Esa cuenta de correo electrónico en Nombre de Larry, lo tenía en mi bolsillo por si acaso. La gente de seguridad de Yahoo probablemente todavía sentado allí esperando alguien utilizar la cuenta de nuevo tan le puede rastrear. Tendrán una larga espera. La señora gorda ha cantado. Estoy fuera de otro proyecto.

Analizando el timo
Cualquier persona que trabaja en un cara a cara con tiene que ocultar a sí mismo en un aspecto que será le hacen aceptable para la marca. Él mismo voy a poner juntos una forma de aparecer en la pista de carreras, otro que aparezca en un abrevadero local, todavía otro para un barra de lujo en un hotel de lujo.

Es la misma forma con el espionaje industrial. Un ataque puede pedir un traje y corbata y un maletín costoso si el espionaje es haciéndose pasar por un ejecutivo de una establecidos firma, un consultor o un representante de ventas. En otro trabajo, tratando de pasar como un software Ingeniero, una persona técnica o alguien de la sala de correo, la ropa, la uniforme--la mirada toda sería diferente.

Para infiltrarse en la empresa, él sabía que el hombre que se llama a sí mismo Rick Daggot había para proyectar una imagen de confianza y competencia, respaldados por un exhaustivo conocimiento del producto y la industria de la empresa.

No mucha dificultad poniendo sus manos sobre la información que necesitaba de antemano. Ideó un ardid fácil para averiguar cuándo el CEO sería lejos. Un pequeño desafío, pero todavía no muy dura, era averiguar detalles suficientes sobre la proyecto que él podría sonar \"en el interior\" sobre lo que estaban haciendo. A menudo Esta información se conoce a varios proveedores de la empresa, así como los inversores, los capitalistas de riesgo que han abordado acerca de recaudar dinero, su banquero, y su bufete. El atacante tiene que tener cuidado, aunque: encontrar a alguien que lo verá parte con conocimiento de información privilegiada puede ser complicadas, pero intentaba dos o tres fuer hasta alguien que puede ser exprimido para información corre el riesgo de que la gente va

capturar el juego. De este modo encuentra en peligro. El Rick Daggots la necesidad del mundo Escoja con cuidado y pisan cada ruta de información sólo una vez.

El almuerzo fue otra propuesta pegajosa. En primer lugar, existe el problema de organizar cosas así tendría sólo unos minutos con cada persona, de oído de los demás. Dijo Jessica 12:30, pero reservó la mesa a 13, en un lujo, tipo de cuenta de gastos del restaurante. Esperaba que significaría que sería tienen que tener bebidas en el bar, que es exactamente lo que sucedió. Un perfecto oportunidad de moverse y charlar con cada individuo.

Todavía, hay tantas maneras de que un error--una respuesta equivocada o un descuido observación podría revelar Rick ser un impostor. Sólo un supremamente confiado y astuto espionaje industrial se atreven tendría una oportunidad de exponer a sí mismo de este modo. Pero los año de trabajo las calles como una confianza hombre había construido habilidades de Rick y dado él la confianza de que, aunque hizo un lapsus, 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 sintió poner fuera un aguijón como este le hizo darse cuenta por qué él no tenía que conducir coches rápidos o paracaidismo o engañar a su esposa--obtuvo un montón de emoción simplemente haciendo su trabajo. Cuántas personas, él ¿se pregunta, podría decir tanto?

MENSAJE DE MITNICK

Mientras que la mayoría de los ataques de ingeniería social se produce sobre el teléfono o el correo electró Suponga que un atacante negrita nunca aparecerán en persona en su negocio. En la mayoría casos, el impostor utiliza algún tipo de ingeniería social para obtener acceso a un edificio después de falsificación de una insignia de empleado usando un comúnmente disponibles programa de software como Photoshop.

¿Qué pasa con las tarjetas de negocios con la compañía telefónica prueba línea? La televisión Mostrar The Rockford Files, que fue una serie acerca de un investigador privado, ilustra una técnica inteligente y un poco de humor. Rockford (interpretado por el actor James Garner) tenía una máquina de impresión de tarjetas portátil en su coche, que él utilizado para imprimir una tarjeta adecuada sea cual sea la ocasión pedía. Estos días, un ingeniero social puede obtener tarjetas impresas en una hora en cualquier copia almacenar o imprimir en una impresora láser.

NOTA

John Le Carre, autor de The Spy Who Came en el frío, un espía perfecto, y muchos otros libros notables, que creció como el hijo de un pulido, participación permanente puede hombre. Le Carre fue golpeado como una jovencita para descubrir, con éxito como su padre era en engañar a otros, también fue crédulo, una víctima más de una vez a otro con hombre o mujer. Que sólo viene a demostrar que todo el mundo corre el riesgo de adoptando un ingeniero social, incluso otro ingeniero social.

¿Qué lleva a un grupo de hombres inteligentes y las mujeres a aceptar a un impostor? Tenemos el tamaño
situación por instinto e intelecto. Si la historia añade arriba--es el intelecto
parte--y un estafador consigue proyectar una imagen creíble, estamos dispuestos generalmente
para bajar la guardia. Es la imagen creíble que separa una con éxito
hombre o ingeniero social de uno que rápidamente terrenos tras las rejas.

Pregúntese: ¿seguro que soy yo que no caería nunca para una historia como la de Rick? Si
Usted puede estar seguro que no, pregúntese si alguna vez alguien ha puesto nada
más sobre usted. Si la respuesta a esta segunda pregunta es afirmativa, es probablemente la correcta
respuesta a la primera pregunta, así.

LEAPFROG
Un desafío: el siguiente relato no implican espionaje industrial. Como usted
leer, ver si se puede entender por qué he decidido ponerlo en este capítulo!

Harry Tardy atrás vivía en su casa, y fue amargo. Los Marines habían
parecía un gran escape hasta él lavado de boot camp. Ahora tenía
regresó a la ciudad natal de odiaba, estaba tomando cursos de informática en el local
community college\"y buscando una forma de huelga en el mundo.
Finalmente consiguió un plan. Sobre cervezas con un chico en una de sus clases, había sido
quejándose de su instructor, un sarcástico sabemos todo y juntos se
cocinado un plan perverso para grabar el tio: agarra el código fuente de un
popular asistente personal digital (PDA) y envió al instructor
equipo y asegúrese de dejar un rastro, por lo que la empresa podría pensar la
instructor era el malo.

El nuevo amigo, Karl Alexander, dijo que \"sabía algunos trucos\" y diría
Harry cómo llevar esta. Obtener árido lejos con ella.

Haciendo sus deberes
Una pequeña investigación inicial mostró Harry que el producto ha sido diseñado en el
Centro de desarrollo ubicado en la sede del fabricante de PDA extranjero.
Pero también fue un r
señalado, porque el intento de trabajar tiene que haber alguna compañía
instalaciones en los Estados Unidos que también necesita acceso al código fuente.

En ese momento Harry estaba listo para llamar al centro de desarrollo de ultramar. Aquí es
Cuando llegó una petición de simpatía, el \"Oh, querida, estoy en problemas, necesito ayuda,
por favor, por favor, ayúdame.\" Naturalmente, el motivo fue un poco más sutil que eso. Karl
escribió en una secuencia de comandos, pero Harry sonaba completamente falso tratando de leerlo. En
final, practicó con Karl para decirnos lo que necesitaba en una conversación
tono.

Lo que Harry finalmente dijo, con Karl sentado a su lado, pasó algo parecido a esto:

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
todo departamento. Hemos tenido que instalar el sistema operativo nuevo y cuando
fuimos a restaurar de copia de seguridad, ninguna de las copias de seguridad fue bueno. Adivina quien
¿iba a estar revisando la integridad de las copias de seguridad? Tuyo realmente. Por eso estoy
obtener gritó a mi jefe, y gestión es en armas que hemos perdido el
datos. Mira, necesito tener la revisión más reciente del árbol de código fuente tan rápida como
Puedes. Necesito a gzip el código fuente y enviar a mí.\"

En este punto Karl él garabateó una nota, y Harry le dijo al hombre en el otro extremo
del teléfono que él sólo quería transferir el archivo internamente, a Minneapolis
R
estaba claro que sólo se había pedido para enviar el archivo a otra parte de la
¿empresa, su mente estaba a gusto--lo que podría ser malo?

JERGA
GZIP a archivos en un único archivo comprimido mediante una utilidad de Linux GNU.
Acordó gzip y enviarlo. Paso a paso, con Karl en su codo, Harry habló
allí el hombre a través de introducción sobre el procedimiento para comprimir la enorme
código fuente en un archivo único, compacto. También le dio un nombre de archivo para utilizar en
el archivo comprimido, \"DatosNuevos\", explicando que este nombre evitaría cualquier
confusión con sus viejos archivos dañados.

Karl tuvo que explicar el siguiente paso dos veces antes de que Harry lo consiguió, pero fue fundamental p
el jueguito de leapfrog Karl había soñado. Harry fue a llamar a r
Minneapolis y alguien diga que \"quiero enviar un archivo a usted y luego me
desea enviar algún otro sitio para mí \", por supuesto todos vestidos con
razones que harían todo suenan plausibles. Lo que confunde Harry fue esto: él
iba a decir \"Me voy a enviarle un archivo,\" cuando no iba a ser
Harry enviar el archivo a todos. Tuvo que hacer el chico estaba hablando con en el
R
realmente va a recibir es el archivo de código fuente propietaria desde Europa. \"Por qué
¿le cuento viene de mí cuando realmente es procedentes de ultramar?\"
Harry quería saber.

There was an error deserializing the object of type System.String. Unexpected end of file. Following elem
él sólo está haciendo un favor a un compañero empleado aquí en los Estados Unidos, obteniendo un archi
usted y luego reenviarlo sólo para usted.

Harry finalmente entendido. Llamó a la r
recepcionista para conectarlo con el centro de cómputo, donde pidió hablar con un
operador de equipo. Un chico entró en la línea que sonaba tan joven como Harry

a sí mismo. Harry lo saludó, explicó que estaba llamando desde el Chicago
fabricación de división de la empresa y que tenía este archivo había estado tratando
enviar a uno de sus socios trabajando en un proyecto con ellos, pero, dijo, \"nos has
tengo este problema de enrutador y no llegue a su red. Me gustaría transferir el archivo a
usted, y después de recibirla, voy teléfono te lo puedo guiarte a través de
transferencia a equipo de compañero.

Hasta ahora, bien. Harry luego pidió al joven si su equipo centro
tenía una cuenta FTP anónima, una instalación que permite transferir archivos en
y de un directorio donde no es necesaria ninguna contraseña. Sí, un FTP anónimo
estaba disponible, y le dio a Harry la dirección de protocolo de Internet (IP) interna para
llegar a él.

JERGA
Programa FTP anónimo que proporciona acceso a un equipo remoto incluso
Aunque no tienes una cuenta utilizando el Protocolo de transferencia de archivos (FTP).
Aunque puede acceder sin contraseña, generalmente usuario - FTP anónimo
derechos de acceso a determinadas carpetas están restringidos.

Con esa información en mano, Harry llamado el centro de desarrollo
extranjero. Ya estaba listo el archivo comprimido, y Harry le dio las instrucciones
para transferir el archivo al sitio FTP anónimo. En menos de cinco minutos, el
archivo de código fuente comprimida fue enviado al kid en la r

Configuración de la víctima
A mitad de camino a la meta. Ahora Harry y Karl tuvieron que esperar para asegurarse de que el archivo h
llegaron antes de continuar. Durante la espera, caminaron a través de la sala a la
escritorio del instructor y cuidaba de dos otras medidas necesarias. En primer lugar establecieron un
servidor FTP anónimo en su máquina, que serviría como un destino para
el archivo en la última etapa de su plan.

El segundo paso proporciona una solución para un problema complicado lo contrario. Claramente que
no podía decirle a su hombre en la r
decir, warren@rms.ca.edu. El dominio \".edu\" sería un regalo muerto, desde
cualquier chico despierta medio equipo reconocería como la dirección de una escuela,
inmediatamente soplando toda la operación. Para evitar esto, se fueron en Windows
el equipo del instructor y buscó una dirección IP de la máquina,
daría como dirección de envío del archivo.

Por aquel entonces era tiempo para volver a llamar al operador del equipo en la r
lo consiguió en el teléfono y dijo, \"simplemente transferir el archivo que hablé con usted
acerca de. Puede comprobar que se recibió\"

Sí, había llegado. Harry luego le pedí que intente reenviarlo y le dio el Dirección IP. Permaneció en el teléfono, mientras que el joven hizo la conexión comenzó a transmitir el archivo y miraron con grandes muecas de en toda la el espacio como la luz del disco duro del equipo del instructor blinked y Blinked--ocupado recibiendo la descarga.

Harry intercambiaron un par de comentarios con el tio acerca de cómo tal vez un día equipos y periféricos serían más fiables, le agradecieron y dijo Adiós.

Los dos copió el archivo desde la máquina del instructor en un par de discos Zip, uno para cada uno de ellos, tan podrían mirarlo más tarde, como el robo de una pintura de un Museo que puede disfrutar pero no se atreven a mostrar a sus amigos. Excepto, en este caso, era más como habían tomado un duplicado original de la pintura, y el Museo todavía tenía su propia original.

Karl entonces habló Harry a través de los pasos de quitar el servidor FTP de la de instructor máquina y borrar la auditoría camino por lo que no habría ninguna evidencia de lo que habían hecho--el archivo robado, izquierdo donde se encuentra fácilmente.

Como paso final, que exponen una sección del código fuente en Usenet directamente desde equipo del instructor. Sólo una sección, por lo que no hacen ningún daño gran a la empresa, pero deja claras pistas directamente hacia el instructor. Él sería tienen algunos difícil explicar que hacer.

Analizando el timo

Aunque le costó la combinación de una serie de elementos para hacer esta escapada trabajo, no habría podido sin algunas habilidades ful playacting de apelación por simpatía y ayuda: estoy recibiendo gritó a mi jefe y administración está en armas y así sucesivamente. Que, combinado con una punta explicación de cómo el hombre en el otro extremo del teléfono podría ayudar a resolver el problema, resultado para ser un con poderosamente convincente. Trabajó aquí y ha trabajado en muchas otras ocasiones.

El segundo elemento fundamental: el hombre que entiende el valor del archivo fue pedido enviar a una dirección dentro de la empresa.

Y la tercera pieza del rompecabezas: el operador del equipo pudieron ver que el archivo había sido trasladado a él desde dentro de la empresa. Que sólo podría significar--o por lo que parecía--que el hombre que envió a él pudo él haber enviado a la destino final si sólo había trabajado su conexión de red externa. ¿Qué ¿posiblemente podría ser malo le ayuda mediante el envío de él?

Pero ¿por qué tener el archivo comprimido le asigna un nombre diferente? Aparentemente un elemento pequeño, pero importante. El atacante no podía permitirse tomar una oportunidad del archivo que llegan con un nombre que lo identifique como código fuente, o relacionadas con el producto. Una solicitud para enviar un archivo con un nombre que fuera de la empresa podría haber partió de alarma. Tener el archivo re-etiquetados con un nombre inocuo fue crucial. Como elaborado por los atacantes, el segundo joven no tenía reparo en enviar el archivo fuera de la empresa; un archivo con un nombre como nuevo datos, no dar ninguna pista sobre la verdadera naturaleza de la información, difícilmente haría lo sospechoso.

MITNICK MESSGAE
La regla subyacente que cada empleado debe haber plantado firmemente en su cerebro: excepto con la aprobación de la administración, no transferir archivos a personas que no conocer personalmente, incluso si el destino parece estar dentro de su empresa red interna.

Finalmente, usted averigua lo que está haciendo esta historia en un capítulo sobre industrial ¿espionaje? Si no, aquí está la respuesta: lo que hicieron estos dos estudiantes como un malintencionado broma podría fácilmente haber hecho por un espía industrial profesional, quizás en el pago de un competidor, o quizá en la paga 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 alcanzado el producto competitivo el mercado.

¿Con qué facilidad el mismo tipo de ataque se pudo realizar contra su empresa?

PREVENIR LA CON
Espionaje industrial, que ha sido durante mucho tiempo un desafío para las empresas, tiene ahora convertido en el pan y la mantequilla de espías tradicionales que han centrado sus esfuerzos en obtención de secretos de la compañía por un precio, ahora que ha terminado la guerra fría. Extranjeros los gobiernos y las empresas están usando ahora espías industriales autónomos para robar información. Las empresas nacionales también contratan agentes de información que cruzan el línea en sus esfuerzos para obtener inteligencia competitiva. En muchos casos son ex espías militares convirtieron corredores de información industrial que tienen los conocimientos previos y experiencia para explotar fácilmente las organizaciones, especialmente aquellos que no han podido implementar salvaguardas para proteger su información y educar a su pueblo.

Seguridad fuera del sitio
Lo que podría haber ayudado a la compañía que tuvo problemas con su ex situ ¿instalación de almacenamiento? El peligro aquí podría haberse evitado si la compañía había se han cifrado de sus datos. Sí, el cifrado requiere tiempo extra y los gastos, pero

vale el esfuerzo. Archivos cifrados deben ser spot-checked con regularidad para ser seguro que el cifrado y descifrado está funcionando sin problemas.

Siempre existe el peligro de que se perderán las claves de cifrado o que la única persona que sabe las claves se activará por un autobús. Pero el nivel de molestia puede ser minimizado y quien almacena información confidencial fuera del sitio con un empresa comercial y no es el no uso de cifrado, discúlpeme por ser contundente, una idiota. Es como caminar por la calle en un barrio malo con veinte dólares facturas pegado de su bolsillo, esencialmente pidiendo ser robados.

Dejando copia donde alguien podía caminar con él es un defecto común en seguridad. Hace varios años, estaba empleado en una empresa que podría haber hecho mejores esfuerzos para proteger la información del cliente. Personal de la operación dejado a la empresa cintas de backup fuera de la puerta de sala de equipo bloqueado por un mensajero recoger cada día. Nadie podría haber bajó con las cintas de backup, que contenía todos de la firma word-processed documentos en texto sin cifrar. Si los datos de copia de seguridad cifrado, pérdida del material es una molestia; Si no está cifrada--bueno, puede enVision el impacto sobre su empresa mejor que yo.

La necesidad de las empresas más grandes para almacenarlos confiable es prácticamente un determinado. Pero los procedimientos de seguridad de su empresa necesitan incluir una investigación de su empresa de almacenamiento de información para ver cómo conciencia son acerca de su propia seguridad las políticas y prácticas. Si no están tan dedicados como su propia empresa, todos sus los esfuerzos de seguridad pueden ser socavados.

Las pequeñas empresas tienen una buena opción alternativa para backup: enviar la nueva y cambiar archivos cada noche a una de las empresas que ofrecen almacenamiento en línea. Una vez más, es esencial que los datos se cifran. De lo contrario, la información está disponible no sólo a un empleado doblado en la empresa de almacenamiento de información, pero a cada intruso de que puede romper los sistemas informáticos de almacenamiento en línea companys o red.

Y por supuesto, cuando se configura un sistema de encriptación para proteger la seguridad de los archivos de copia de seguridad, también debe establecer un procedimiento altamente seguro para alm las claves de cifrado o las frases que se desbloquee. Claves secretas que se utiliza para cifrar datos deben almacenarse en una caja fuerte o caja fuerte. Necesita práctica empresa estándar prever la posibilidad de que el empleado en el manejo de estos datos podría repentinamente dejar, morir o tomar otro trabajo. Siempre debe haber al menos dos personas que conocer el lugar de almacenamiento de información y los procedimientos de cifrado y descifrado, así com políticas de cómo y cuándo son claves para cambiarse. Las políticas también deben exigir que las claves de cifrado cambiarse inmediatamente a la salida de cualquier empleados que tienen acceso a ellos.

¿Que es eso?
El ejemplo en este capítulo de un ingenioso estafador que utiliza el encanto para obtener empleados compartir información refuerza la importancia de la verificación de identidad. El solicitud de código de origen reenvía a un sitio FTP también apunta a la importancia de conocer a su solicitante.

En el capítulo 16 encontrará políticas específicas para verificar la identidad de cualquier desconocido que se hace una solicitud de información o una solicitud que alguna acción tomado. Hemos hablado de la necesidad de verificación en todo el libro; en Capítulo 16 obtendrá información específica de cómo debe hacerse.

Parte 4
Elevar el nivel

Capítulo 15
Formación y sensibilización de seguridad de información

Un ingeniero social ha recibido la asignación de obtención de los planes para su nuevo producto caliente fecha de estreno en dos meses.

¿Qué va a detenerlo?

¿El cortafuegos? Lol

¿Dispositivos de autenticación fuerte? Lol ¿Sistemas de detección de intrusiones? Lol ¿Cifrado? Lol

¿Acceso limitado a los números de teléfono para módems de acceso telefónico? No.

Código nombres de servidores que hacen difícil para un forastero a determinar que ¿servidor puede contener los planes de producto? Lol

La verdad es que no hay ninguna tecnología en el mundo que puede evitar una social Ingeniería de ataque.

SEGURIDAD A TRAVÉS DE TECNOLOGÍA, CAPACITACIÓN, Y PROCEDIMIENTOS

Las empresas que realizan pruebas de penetración de seguridad un informe que sus intentos de entrar en el equipo cliente de empresa son sistemas por métodos de ingeniería social casi 100 por ciento exitosa. Tecnologías de seguridad pueden hacer estos tipos de ataques más difíciles eliminando personas desde la toma de decisiones.

Sin embargo la forma sólo verdaderamente eficaz para mitigar la amenaza de la ingeniería social es mediante el uso de las tecnologías de seguridad combinadas con las políticas de seguridad que establecer reglas de comportamiento del empleado y adecuada educación y formación para los empleados.

Hay sólo una forma de mantener sus planes de producto seguro y que es por tener un capacitado y consciente y una fuerza de trabajo concienzudo. Esto implica la formación en el políticas y procedimientos, sino también--y probablemente aún más importante--un curso programa de sensibilización. Algunas autoridades recomiendan que 40 por ciento de la empresa presupuesto global de seguridad orientarse a la formación de la conciencia.

El primer paso es hacer que todos en la empresa sabe que sin escrúpulos personas existen que utilizará engaño para manipularlos psicológicamente. Empleados deben ser educados acerca de qué información necesita ser protegida, y

Cómo protegerla. Una vez las personas tienen una mejor comprensión de cómo se pueden manipulados, están en una posición mucho mejor para reconocer que es un ataque en marcha.

Conciencia de seguridad también significa educar a todos los miembros de la empresa en el las políticas de seguridad y procedimientos de la empresa. Como se explica en el capítulo 17, políticas son las normas necesarias para orientar el comportamiento de los empleados para proteger la informació sistemas e información confidencial.

En este capítulo y el siguiente proporcionan un plan de seguridad que podría ahorrar desde los ataques costosos. Si no tienes empleados capacitados y alertas tras bien procedimientos pensados, no es una cuestión de si, pero cuando pierdes valiosos información a un ingeniero social. No esperen que suceda antes de un ataque establecimiento de estas políticas: podría ser devastador para su negocio y su bienestar de los trabajadores.

COMPRENDER CÓMO LOS ATACANTES APROVECHAN DE NATURALEZA HUMANA

Para desarrollar un programa de capacitación exitoso, tienes que entender por qué las personas son vulnerables a ataques en primer lugar. Mediante la identificación de estas tendencias en su formación--por ejemplo, por llamar la atención sobre ellos en discusiones de rol-- Usted puede ayudar a sus empleados a entender por qué nos podemos todos ser manipulados por ingenieros sociales.

Manipulación ha sido estudiado por los científicos sociales durante al menos cincuenta años. Robert B. Cialdini, escrito en Scientific American (febrero de 2001), resumió esta investigación, presentando seis \"básicas tendencias de la naturaleza humana\" que participan en un intento de obtener el cumplimiento de una solicitud.

Estas seis tendencias son aquellas que dependen de los ingenieros sociales (conscientemente o, más a menudo, inconscientemente) en sus intentos de manipular.

Autoridad

Las personas tienen una tendencia a cumplir cuando se realiza una solicitud por una persona en autoridad. Como hemos comentado en otros lugares en estas páginas, una persona puede ser convencida cumplir con una petición si cree que el solicitante es una persona de autoridad o una persona que está autorizada para realizar dicha solicitud.

En su libro influencia, Dr. Cialdini escribe de un estudio en tres Midwestern hospitales en que veintidós separar estaciones de enfermeras fueron contactados por un llamador que pretenden ser un médico del hospital y dio instrucciones para administrar una medicamentos recetados a un paciente en la sala. Las enfermeras que recibieron estos instrucciones no sabía el llamador. Aún no sabían si era

realmente un médico (que no era). Recibieron las instrucciones para la prescripción por Telefónica, que era una violación de la política de hospital. La droga a que se les dijo administrar no estaba autorizado para su uso en los barrios y la dosis que les dijeron para administrar fue dos veces la dosis diaria máxima y así podría tener en peligro la vida del paciente. Sin embargo, en el 95 por ciento de los casos, Cialdini se informó, \"la enfermera procedió a obtener la dosis necesaria del ward Gabinete de medicina y estaba en su camino para administrar al paciente \"antes de ser interceptado por un observador y dijo del experimento.

Ejemplos de ataques: un ingeniero social intenta ocultar a sí mismo en el manto autoridad diciendo que él está con el departamento de TI, o que él es un Ejecutivo u obras para un ejecutivo en la empresa.

Gusto
La gente tiene la tendencia a cumplir cuando la persona hace una solicitud ha sido poder establecerse como agradable, o tener intereses similares, creencias, y actitudes como la víctima.

Ejemplos de ataques: a través de la conversación, el atacante logra aprender un pasatiempo o interés de la víctima y reclama un interés y entusiasmo por la misma afición o interés. O él puede aspirar a ser el mismo Estado o escolar, o tener objetivos similares. El ingeniero social intentará imitar el comportamientos de su destino para crear la apariencia de similitud.

Reciprocidad
Automáticamente podemos cumplir con una petición cuando hemos recibido o prometió algo de valor. El regalo puede ser un elemento material, o Consejo, o ayuda. Cuando alguien ha hecho algo para TI, sientes una inclinación a corresponder. Esta fuerte tendencia a corresponder existe incluso en situaciones donde la persona que recibe el regalo no ha pedido. Una de las formas más eficaces influenciar a la gente a hacer de nosotros un \"favor\" (cumplir con la petición) está dando algún regalo asistencia de r que constituye una obligación subyacente.

Miembros de la secta religiosa Hare Krishna fueron muy efectivos para influir en personas a donar a su causa, primero dándoles un libro o una flor como un regalo. Si el receptor trató de devolver el regalo, el dador negaría remarcando, \"es nuestro regalo para usted\". Este comportamiento principio de reciprocidad fue utilizado por los Krishnas aumentar sustancialmente las donaciones.
Ejemplos de ataques: un empleado recibe una llamada de una persona que identifica a sí mismo como desde el departamento de TI. El llamador explica que algunas empresa los equipos han sido infectados con un virus nuevo no reconocido por el antivirus software que puede destruir todos los archivos en un equipo y ofrece para hablar de la persona a través de algunas medidas para evitar problemas. Después de esto, el llamador solicita la

persona para probar una utilidad de software que sólo se ha actualizado recientemente para permitir usuarios cambien las contraseñas. El empleado es reacio a negarse, porque la persona que llama sólo se ha proporcionado la ayuda que supuestamente protegerá al usuario de un virus. Él reciproca por cumplir con la petición del llamador.

Consistencia
La gente tiene la tendencia a cumplir después de haber hecho un compromiso público o respaldo a una causa. Una vez que hemos prometido que haremos algo, no lo hacemos desea que aparezca poco fiables o indeseables y tienden a seguir a través de fin de ser coherentes con nuestra declaración o promesa.

Ejemplo de ataque: el atacante pone en contacto con un empleado relativamente nuevo y informa de acuerdo a acatar ciertas políticas de seguridad y procedimientos como una condición de ser permitido el uso de sistemas de información de la empresa. Después de discutir unas prácticas de seguridad, el llamador solicita al usuario su contraseña \"para verificar cumplimiento\"política sobre cómo elegir una contraseña difícil de adivinar. Una vez el usuario revela para que su contraseña, el llamador hace una recomendación construir futuro contraseñas de tal manera que el atacante será capaz de adivinar. La víctima cumple debido a su acuerdo previo a acatar las políticas de la empresa y su Suponiendo que el llamador simplemente es verificar su cumplimiento.

Validación social
La gente tiene la tendencia a cumplir cuando hacerlo así parece estar en consonancia con lo que otros están haciendo. La acción de los demás es aceptada como validación de que la comportamiento en cuestión es la acción correcta y adecuada.

Ejemplos de ataques: el llamador dice que está realizando una encuesta y otros nombres personas en el departamento que afirma ya han cooperado con él. El víctima, creyendo que la cooperación de otros valida la autenticidad de la solicitud, se compromete a participar. El llamador entonces pide una serie de preguntas, entre que son preguntas que atraer a la víctima a revelar su nombre de usuario del equipo y la contraseña.

Escasez
La gente tiene la tendencia a cumplir cuando se cree que es el objeto buscado en definitiva suministro y otros compiten por ella, o que está disponible sólo para un corto periodo de tiempo.

Ejemplo de ataque: el atacante envía mensajes de correo electrónico afirmando que las primeras 500 perso para inscribirse en el nuevo sitio Web de la empresa ganará entradas gratis para un nuevo película. Cuando un empleado desprevenido se registra en el sitio, se preguntó a

proporcionar a su empresa dirección de correo electrónico y una contraseña. Muchas personas, motivado por conveniencia, tienen la propensión a utilizar la misma o similar contraseña en cada sistema que utilizan. Aprovechando esto, la atacante intenta comprometer el objetivo de trabajo y equipo doméstico sistemas con el nombre de usuario y la contraseña que se han introducido en la Web proceso de registro del sitio.

CREAR PROGRAMAS DE CAPACITACIÓN Y SENSIBILIZACIÓN
Publicar un panfleto de la política de seguridad de información o dirigir a los empleados un página de intranet que detalla las políticas de seguridad será no, por sí mismo, mitigar el riesgo. Todos los negocios no sólo deben definir las reglas con políticas escritas, pero debe hacer el mayor esfuerzo para dirigir a todos los que trabajan con información corporativa o sistemas informáticos para aprender y seguir las reglas. Además, debe asegurarse de que todo el mundo entiende la razón detrás de cada política para que las personas no eludir la regla como una cuestión de conveniencia. De lo contrario, la ignorancia será siempre ser excusa del trabajador y la vulnerabilidad precisa que los ingenieros sociales explotar.

El objetivo central de cualquier programa de concienciación de seguridad es influenciar a la gente a para cambiar su comportamiento y actitudes, motivar a cada empleado que desee chip en y hacer su parte para proteger los activos de información de la organización. Un gran motivación en este caso es explicar cómo su participación beneficiará no sólo a la empresa, pero también los empleados individuales. Dado que la empresa retiene cierta información privada sobre cada trabajador, cuando empleados hagan su parte para proteger información o sistemas de información, son realmente proteger sus propios información, demasiado.

Un programa de formación de seguridad requiere un apoyo sustancial. Necesita el esfuerzo de capacitació para llegar a cada persona que tiene acceso a información confidencial o corporativo sistemas informáticos, debe ser constante y debe ser revisada continuamente para actualizar personal sobre las nuevas amenazas y vulnerabilidades. Los empleados deben ver ese senior Administración está plenamente comprometida con el programa. Ese compromiso debe ser real, no sólo un memo ratificada \"damos nuestras bendiciones\". Y el programa debe apoyarse con recursos suficientes para desarrollar, comunicar, probar y medir el éxito.

Objetivos
La orientación básica que debe tenerse en cuenta durante el desarrollo de un programa de formación y sensibilización de seguridad de información es que el programa necesita centrarse en la sensibilización de todos los empleados que su empresa podría ser bajo ataque en cualquier momento. Deben aprender que cada empleado desempeña un papel en defensa contra cualquier intento de obtener la entrada a los sistemas informáticos o a robar datos confidenciales.

Porque muchos aspectos de la seguridad de la información implican tecnología, resulta demasiado fácil para que los empleados a pensar que se trata el problema de firewalls y otros tecnologías de seguridad. Debe ser un objetivo primordial de la formación crear conciencia en cada empleado que son necesaria para proteger la seguridad general de la línea del frente la organización.

Formación en 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 obtener sus trabajos, para pasar por alto o ignorar sus responsabilidades de seguridad. Conocimientos acerca de las tácticas de ingeniería social y cómo defenderse de los ataques es importante, pero sólo será de valor si el entrenamiento está diseñado para centrarse fuertemente en motivar empleados para utilizar el conocimiento.

La empresa puede contar el programa como su objetivo final si todo el mundo completar la formación es completamente convencido y motivado por una básica concepto: la seguridad de la información es parte de su trabajo.

Los empleados deben llegar a apreciar y aceptar que la amenaza social ataques de ingeniería es real y que una grave pérdida de sensible corporativa información podría poner en peligro la empresa, así como su propio personal información y puestos de trabajo. En un sentido, siendo descuidada sobre seguridad de la información en trabajo es equivalente a ser descuidado con el número PIN de ATM o tarjeta de crédito. Esto puede ser una analogía convincente para generar entusiasmo para las prácticas de seguridad.

Establecer el programa de capacitación y sensibilización
La persona encargada de diseñar el programa de seguridad de la información que necesita para reconocer que no es un proyecto de \"talla única\". Por el contrario, las necesidades de capacitación para ser desarrollada para satisfacer las necesidades específicas de grupos distintos dentro la empresa. Mientras que muchas de las políticas de seguridad descritas en el capítulo 16 se aplican a todos los empleados a través de la Junta, muchos otros son únicos. En una mayoría mínima, las empresas necesitan programas de capacitación adaptados a estos grupos distintos: directores; Personal de TI; usuarios de computadoras; personal no técnico; administrativo asistentes; recepcionistas; y guardias de seguridad. (Véase el fracaso de las políticas asignación de trabajo en el capítulo 16.)

Desde obligar al personal de seguridad industrial de una empresa no son normalmente espera a ser equipo competente y, excepto quizás en forma muy limitada, lo no entrar en contacto con equipos de la empresa, no son generalmente considerados al diseñar la formación de este tipo. Sin embargo, los ingenieros sociales pueden engañar guardias de seguridad u otros en que les permita en un edificio o una oficina, o en realizando una acción que se traduce en una intrusión de equipo. Mientras que los miembros de la fuerza de guardia, sin duda, no es necesario la formación completa del personal que operan o utilizar

equipos, sin embargo, no deberán ser pasados por alto en la conciencia de seguridad programa.

Dentro del mundo empresarial hay probablemente pocos temas sobre los cuales todos los empleados necesitan ser educados que son simultáneamente como importante y inherentemente mitigar como seguridad. El mejor diseñado capacitación de seguridad de información programas deben informar tanto capturar la atención y el entusiasmo de la estudiantes.

El objetivo debería ser hacer conciencia de la información de seguridad y capacitación un experiencia interactiva y atractiva. Podrían incluir técnicas demostrando métodos de ingeniería social a través del rol; revisión de informes de los medios de recientes ataques a otros menos afortunados negocios y discutir las maneras de la las empresas podrían haber impedido la pérdida; o mostrando una seguridad video que entretenido y educativo al mismo tiempo. Hay varios de seguridad empresas de conciencia que mercado videos y materiales relacionados.

NOTA
Para aquellas empresas que no tienen los recursos para desarrollar un programa en-casa, existen varias empresas de capacitación que ofrecen formación de conciencia de seguridad servicios. Ferias como Secure World Expo (www.secureworldexpo.com) están reuniendo lugares para estas empresas

Las historias de este libro proporcionan abundante material para explicar los métodos y tácticas de ingeniería social, para crear conciencia de la amenaza y para demostrar las vulnerabilidades en el comportamiento humano. Considere el uso de sus escenarios como base para las actividades de rol. Las historias también ofrecen oportunidades coloridos de lively debate sobre cómo las víctimas podían han respondido diferente para evitar la ataques de ser exitoso.

Un desarrollador de curso hábil y hábiles instructores encontrarán un montón de desafíos, pero también muchas oportunidades, para mantener vivo el tiempo de aula y, en el proceso, motivar a la gente a formar parte de la solución.

Estructura de la formación
Debe elaborarse un programa de formación de conciencia de seguridad básica que todos los empleados deben asistir a la. Nuevos empleados deben asistir a la capacitación como parte de su adoctrinamiento inicial. No recomiendo que ningún empleado proporcionar acceso de equipo hasta que ha asistido a una toma de conciencia de seguridad básica período de sesiones.

Para esta toma de conciencia inicial y capacitación, sugiero que una sesión centra lo suficiente como para atención y short suficientemente que se recordarán los mensajes importantes. Mientras que la cantidad de material para ser cubiertos sin duda justifica más formación, la importancia de la sensibilización y motivación junto con una razonable número de mensajes esenciales en mi opinión supera cualquier noción de medio día o sesiones de día completo que dejan gente adormecida con demasiada información.

El énfasis de estas sesiones debe ser en transmitir un reconocimiento de la daño que se puede hacer a la sociedad y a los empleados individualmente, a menos que todos empleados seguir hábitos de trabajo de seguridad. Más importante que conocer prácticas de seguridad específico es la motivación que lleva a los empleados a aceptar responsabilidad personal de seguridad.

En situaciones donde algunos empleados fácilmente no pueden asistir a la sesiones de aula, el empresa debe considerar el desarrollo de sensibilización mediante otras formas de instrucción, como vídeos, formación por ordenador, cursos en línea, o escrito materiales.

Después de la sesión inicial de entrenamiento corto, sesiones más largas deben diseñarse para capacitar a los empleados acerca de las vulnerabilidades específicas y atacar técnicas relativas a su posición en la empresa. Entrenamiento debe al menos una vez un año. La naturaleza de la amenaza y los métodos utilizados para explotar las personas nunca son-cambiando, por lo que el contenido del programa debe mantenerse actualizado. Por otra parte, conciencia y lucidez mental de las personas disminuyan con el tiempo, por lo que debe repetirse la forma a intervalos razonables para reforzar los principios de seguridad. Aquí nuevamente el énfasis tiene que ser tan convencidos de la importancia de los empleados de mantener las políticas de seguridad y motivados a adherirse a ellos, como en exponer amenazas específicas y métodos de ingeniería social.

Los administradores deben permitir tiempo razonable para sus subordinados a familiarizarse con las políticas de seguridad y procedimientos y a participar en la toma de conciencia de seguridad programa. Empleados no deben esperarse para estudiar las políticas de seguridad o asistir a clases de seguridad en su propio tiempo. Nuevos empleados deben ser dado tiempo suficiente para revisar las políticas de seguridad y prácticas de seguridad publicadas antes al comienzo su responsabilidades de trabajo.

Empleados que cambian de posición dentro de la organización a un trabajo que implica acceso a sistemas de información o equipo sensibles, por supuesto, debe necesario para completar un programa de formación de seguridad adaptadas a su nuevo responsabilidades. Por ejemplo, cuando un operador de la computadora se vuelve un sistemas Administrador o una recepcionista se convierte en un auxiliar administrativo, nueva formación es necesario.

Contenido del curso de formación
Cuando se reduce a sus fundamentos, todos los ataques de ingeniería social tienen el mismo elemento común: engaño. La víctima es llevada a creer que el atacante es un compañero empleado o alguna otra persona que esté autorizado a acceder sensibles información, o está autorizado a dar la víctima instrucciones que implican tomar acciones en un equipo o equipos informáticos. Casi todos estos ataques podrían ser frustrados si el empleado destino simplemente sigue dos pasos:

Verificar la identidad de la persona que hace la solicitud: es la persona que realiza la ¿solicitar realmente quien dice ser?

Verificar si la persona está autorizada: la persona tiene la necesidad de saber, ¿o de lo contrario está autorizado para realizar esta solicitud?

NOTA
Porque la formación y sensibilización de seguridad nunca son perfectas, utilizar seguridad tecnologías siempre que sea posible crear un sistema de defensa en profundidad. Esto significa que la medida de seguridad es proporcionada por la tecnología en lugar de por empleados individuales, por ejemplo, cuando el sistema operativo está configurado para evitar que descarga el software desde Internet, o elegir un Resumen, fácilmente adivinar la contraseña.

Si las sesiones de formación de conciencia podrían cambiar el comportamiento de modo que cada emplea siempre sería coherente acerca de cómo probar cualquier petición contra estos criterios, la riesgo asociado con los ataques de ingeniería social se reducirá drásticamente.

Un programa de capacitación que aborda y conciencia de seguridad de información práctica aspectos humanos de comportamiento y la ingeniería social deben incluir lo siguiente:

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

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

Cómo reconocer un ataque posible de ingeniería social.

El procedimiento para tramitar una solicitud sospechosa.

Donde reportar intentos de ingeniería social o ataques con éxito.

La importancia de desafiar a quien realiza una solicitud sospechosa, independientemente de la posición de la persona reclamada o importancia.

El hecho de que debería no implícitamente confían otros sin verificación adecuada, a pesar de que su impulso es dar a otros el beneficio de la duda.

La importancia de verificar la identidad y la autoridad de cualquier persona que realiza un solicitud de información o acción. (Ver \"verificación y autorización Procedimientos,\"capítulo 16, formas de verificar identidad.)

Procedimientos para proteger la información confidencial, incluyendo familiaridad con cualquiera sistema de clasificación de datos.

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

Un resumen de las políticas de seguridad de claves y una explicación de su significado. Para ejemplo, cada empleado debe recibir instrucciones en cómo idear una difícil-a-contraseña de adivinar.

La obligación de todos los empleados para cumplir con las políticas y la consecuencias en caso de incumplimiento.

Ingeniería social por definición implica a algún tipo de interacción humana. Un atacante utilizará con mucha frecuencia una variedad de métodos de comunicación y tecnologías para intentar lograr su objetivo. Por esta razón, un bien-programa de sensibilización redondeado debe intentar cubrir algunos o todos los siguientes:

Políticas de seguridad relacionados con contraseñas de correo de voz y equipo.

El procedimiento para revelar información confidencial o materiales.

Política de uso de correo electrónico, incluidas las salvaguardias para evitar ataques malintencionados incluyendo virus, gusanos y caballos de Troya.

Requisitos de seguridad física, como llevar una insignia.

La responsabilidad a las personas de desafío en los locales que no llevaba un Insignia.

Mejores prácticas de seguridad de uso de correo de voz.

Cómo determinar la clasificación de la información y las salvaguardias adecuadas para protección de información confidencial.

Eliminación adecuada de documentos sensibles y soportes informáticos que contienen, o en cualquier momento en el pasado figuran, material confidencial.

También, si la empresa planea utilizar penetración pruebas para determinar la eficacia de las defensas contra ataques de ingeniería social, que debe ser una advertencia dado empleados puestos sobre aviso de esta práctica. Que los empleados sepan en algún tiempo pueden recibir una llamada telefónica o otra comunicación utilizando un técnicas del atacante como parte de una prueba. Utilizar los resultados de esas pruebas no castigar, bur para definir la necesidad de capacitación adicional en algunas zonas.

Encontrará detalles sobre todos los elementos mencionados en el capítulo 16.

PRUEBAS

Su empresa puede que desee probar a empleados en su dominio de la información presentado en la formación de conciencia de seguridad, antes de permitir que el sistema informático acceso. Si diseña pruebas para ser dados en línea, software de diseño de evaluación de muchos los programas permiten analizar fácilmente los resultados para determinar las áreas de la formación deben fortalecerse.

Su empresa también puede considerar proporcionar un certificado que acredite que el finalización de la formación en seguridad como un motivador de recompensa y empleado.

Como una parte rutinaria de completar el programa, se recomienda que cada empleado solicitará a firmar un acuerdo para acatar las políticas de seguridad y principios enseñan en el programa. La investigación sugiere que una persona que hace la compromiso de firmar un acuerdo de este tipo es más probable que hacer un esfuerzo para acatar los procedimientos.

SENSIBILIZACIÓN CONTINUA

Mayoría de las personas es consciente de que aprender, incluso sobre asuntos importantes, tiende a desap a menos que reforzado periódicamente. Debido a la importancia de mantener empleados marcha sobre el tema de la defensa contra ataques de ingeniería social, una programa de sensibilización continua es vital.

Es un método para mantener la seguridad en la vanguardia de empleado pensando hacer seguridad de la información específica de una trabajo responsable de cada persona en el empresa. Esto anima a los empleados a reconocer su papel crucial en la seguridad general de la empresa. De lo contrario, existe una fuerte tendencia a sentir que seguridad \"no es mi trabajo\".

Si bien la responsabilidad general de un programa de seguridad de la información es normalmente asignada a una persona en el departamento de seguridad o la tecnología de la información

Departamento de desarrollo de un programa de sensibilización de seguridad de información es probablemente mejor estructurado como un proyecto conjunto con el departamento de formación.

El programa de sensibilización continua debe ser creativo y utilizar cada disponible canal para comunicar mensajes de seguridad de manera que es memorable para que empleados se recuerda constantemente sobre los hábitos de buena seguridad. Métodos debe utilizar todos los tradicionales canales, además de tantos otros no tradicionales como la gente asignados desarrollar e implementar el programa puede imaginar. Como con la tradicional publicidad, humor y el ingenio ayudan. Variando la redacción de mensajes mantiene ellos se conviertan en tan familiar que se ignoran.

La lista de posibilidades para un programa de sensibilización continua puede incluir:

Proporcionar copias de este libro a todos los empleados.
Incluyendo elementos informativos en el boletín de la empresa: artículos, en caja avisos (preferiblemente cortos, recibiendo atención elementos), o dibujos animados, por ejemplo.

Publicar una foto de los empleados de seguridad del mes.

Colgando carteles en las áreas de empleado.

Publicar avisos de tablón de anuncios.

Proporcionar gabinetes impresos en sobres de nómina.

Envío de recordatorios por correo electrónico.

Uso de protectores de pantalla relacionados con la seguridad.

Transmitiendo anuncios de recordatorio de seguridad a través del sistema de correo de voz.

Impresión de pegatinas de teléfono con mensajes tales como \"es su llamador que dice que es?"!

Configuración de recordatorio de mensajes que aparecen en el equipo al iniciar la sesión, tal como \"si va a enviar información confidencial por correo electrónico, cifrarlo.\"

Incluye el conocimiento de la seguridad como un elemento estándar de informes de rendimiento del empl y exámenes anuales.

Proporcionar seguridad recordatorios de conciencia en la intranet, tal vez utilizando dibujos animados o humor, o de alguna otra manera atraer empleados para leerlos.

Utilizando un tablero de visualización de mensajes electrónicos en la cafetería, con una frecuencia cambiar el aviso de seguridad.

Distribución de volantes o folletos.

Y creo que los trucos, como galletas de la fortuna gratis en la cafetería, cada que contenga un aviso de seguridad en lugar de una fortuna.

La amenaza es constante; los avisos deben ser constantes así.

¿QUÉ ES EN ELLA PARA MÍ?\"
Además de conciencia de seguridad y programas de capacitación, recomiendo encarecidamente una programa de recompensas de Karadzic y activa. Debe reconocer los empleados que han detectado y evitado un ataque de intento de ingeniería social, o en alguna otra manera contribuido significativamente al éxito de la información programa de seguridad. La existencia del programa de recompensa debe hacerse conocer a deben ser empleados en todas las sesiones de toma de conciencia de seguridad y violaciones de seguridad amplia difusión en toda la organización.

Al otro lado de la moneda, las personas deben hacerse conscientes de las consecuencias de no acatar las políticas de seguridad de información, ya sea por descuido o resistencia. Aunque todos hacemos errores, repetidas violaciones de seguridad no deben tolerarse procedimientos.

Capítulo 16
Recomiendan las políticas corporativas de seguridad de información

Nueve de cada diez grandes corporaciones y agencias del Gobierno han sido atacado por los intrusos del equipo, a juzgar por los resultados de una encuesta realizada por el FBI y la Associated Press informó en abril de 2002. Curiosamente, el estudio halló que sólo una empresa en tres informó o públicamente reconoce cualquier ataque. Esa reticencia a revelar su victimización hace sentido. Para evitar la pérdida de confianza de los clientes y para prevenir nuevos ataques por intrusos que aprender que una empresa puede ser vulnerable, la mayoría de las empresas no informar públicamente de incidentes de seguridad del equipo.

Parece que no existen estadísticas sobre los ataques de ingeniería social y si hay fueron, que los números serían altamente confiables; en la mayoría de los casos una compañía nunca sabe cuando un ingeniero social tiene información \"robado\", por lo que muchos ataques ir desapercibido y no declarada.

Contramedidas eficaces se pueden poner en su lugar contra la mayoría de los tipos de social ataques de ingeniería. Pero vamos a afrontar la realidad aquí--a menos que todos los miembros de la empr entiende que la seguridad es importante y hace su negocio saber y adherirse a las políticas de seguridad de la empresa, ataques serán la ingeniería social siempre presentan un grave riesgo para la empresa.

De hecho, como se realizan mejoras si me las armas tecnológicas contra la seguridad infracciones, el enfoque de la ingeniería social al uso de personas para acceder a propietarios información de la empresa o penetrar casi ciertamente la voluntad de la red corporativa ser significativamente más frecuentes y atractivo para los ladrones de información. Un espionaje industrial, naturalmente, intentará lograr su objetivo utilizando el el método más fácil y el uno con el menor riesgo de detección. Como un asunto de hecho, una empresa que ha protegido a sus sistemas informáticos y red implementar el estado de las tecnologías de seguridad posteriormente puede estar más expuestos de los atacantes que utilizan la ingeniería social estrategias, métodos y tácticas para alcanzar sus objetivos.

Este capítulo presenta políticas específicas diseñadas para minimizar el riesgo de la empresa con respecto a los ataques de ingeniería social. Las políticas frente a los ataques que son basado no estrictamente en explotar las vulnerabilidades de la técnicas. Ellos involucran el uso de algunos tipo de pretexto o ardid para engañar a un empleado de confianza en el suministro de información o realizando una acción que da el acceso del autor al negocio sensible información o a los sistemas informáticos de empresas y redes.

¿QUÉ ES UNA POLÍTICA DE SEGURIDAD?
Políticas de seguridad son instrucciones claras que proporcionan las directrices para el empleado comportamiento para salvaguardar la información y son un edificio fundamental bloque desarrollo de controles efectivos para contrarrestar las amenazas de seguridad potenciales. Estas políticas son incluso más importantes a la hora de prevenir y detectar social ataques de ingeniería.

Controles de seguridad eficaces son ejecutados por la capacitación de los empleados con bien-procedimientos y políticas documentadas. Sin embargo, es importante tener en cuenta las políticas de seguridad, incluso si religiosamente seguido por todos los empleados, no son garantizado evitar que cada ataque de ingeniería social. Por el contrario, el objetivo razonable es siempre mitigar el riesgo a un nivel aceptable.

Las políticas que se presentan aquí incluyen medidas que, si bien no es estrictamente enfocado problemas de ingeniería social, no obstante pertenecer aquí porque tratan técnicas utilizadas en ataques de ingeniería social. Por ejemplo, las políticas acerca de cómo abrir los adjuntos de correo electrónico--que podrían instalar el troyano malicioso software que permite al atacante apoderarse de ordenador de la víctima--dirección un método utilizado frecuentemente por los intrusos del equipo.

Pasos para desarrollar un programa
Un programa de seguridad de información integral usualmente comienza con un riesgo evaluación encaminadas a determinar:

¿Qué activos de información de la empresa necesitan ser protegidos?

¿Qué amenazas específicas existen contra estos activos?

Qué daño podría deberse a la empresa si estas amenazas potenciales ¿materializar?

Es el principal objetivo de la evaluación del riesgo priorizar la información que están activos necesitan garantías inmediatos, y si de instituir salvaguardias voluntad ser costo-eficaz basada en un análisis de costo-beneficio. En pocas palabras, lo que van a ser activos ¿protegidos en primer lugar, y cuánto dinero debe gastar para proteger estos activos?

Es esencial que el directivo Inscríbete y apoyar firmemente la necesidad de desarrollo de las políticas de seguridad y un programa de seguridad de la información. Como con cualo otro programa corporativo, si es un programa de seguridad para tener éxito, debe de gestión hacer más que simplemente proporcionar un respaldo, debe demostrar un compromiso por ejemplo personal. Los empleados necesitan ser conscientes de que la administración fuertemente se adhiere a la creencia de que la seguridad de la información es vital para la empresa

operación, que la protección de información de negocios de la empresa es esencial para la permanecer en el negocio de la compañía, y que puede depender de trabajo de cada empleado la éxito del programa.

La persona asignada al proyecto de directivas de seguridad de información debe comprender que las políticas deben ser escritas en un estilo libre de jerga técnica y fácilmente se entiende por la técnica empleada. También es importante que el documento dejar claro por qué cada política es importante; de lo contrario pueden ignorar empleados algunas políticas como una pérdida de tiempo. El escritor de la política debe crear un documento presenta las políticas y un documento separado para los procedimientos, porque las políticas probablemente cambiará mucho menos frecuencia que los procedimientos específicos utilizados para aplicarlas.

Además, el escritor de la política debe ser consciente de las formas en que la seguridad tecnologías pueden utilizarse para aplicar prácticas de seguridad de buena información. Para ejemplo, la mayoría de los sistemas operativos hacen posible requieren que el usuario las contraseñas ajustarse a determinadas especificaciones tales como longitud. En algunas empresas, una política prohibir a los usuarios descargar programas puede ser controlado vía local o configuración de directiva global dentro del sistema operativo. Es necesario para las políticas uso de la tecnología de seguridad siempre rentable para quitar basados en humanos toma de decisiones.

Empleados deben ser advertidos de las consecuencias por no cumplir con las políticas de seguridad y procedimientos. Un conjunto de consecuencias apropiadas para violar las políticas deben desarrollarse y ampliamente publicitadas. También, un programa de recompensas debe crearse para empleados que demuestren buenas prácticas de seguridad o que reconocer y reportar un incidente de seguridad. Cuando un empleado es recompensado por frustrando una brecha de seguridad, debe ser difundido ampliamente en toda la empresa, por ejemplo, en un artículo publicado en el boletín de la empresa.

Uno de los objetivos de un programa de concienciación de seguridad es comunicar la importancia de las políticas de seguridad y los daños que pueden derivarse del incumplimiento de dichas normas. Dada la naturaleza humana, empleados que, a veces, ignorar o eludir las políticas que aparecen injustificada o demasiado lento. Es una responsabilidad de gestión asegurar que los empleados entiendan la importancia de las políticas y son motivados a cumplir, en lugar de tratarlos como obstáculos a eludirse.

Es importante señalar que las políticas de seguridad de la información no pueden ser escritas en piedra. Como empresa necesita cambiar, como nuevas tecnologías de seguridad llegan al mercado y como vulnerabilidades de seguridad evolucionan, las políticas deben modificarse o completarse. Un proceso de revisión periódica y actualización debe ponerse en el lugar. Hacer la políticas de seguridad corporativas y procedimientos disponibles a través de la intranet corporativa o mantener esas políticas en una carpeta pública. Esto incrementa la probabilidad

que esas políticas y procedimientos se revisará con mayor frecuencia y proporciona un método conveniente para los empleados a encontrar rápidamente la respuesta a cualquier seguridad de la información relacionada con la pregunta.

Por último, pruebas de penetración periódicas y evaluaciones de la vulnerabilidad mediante social Ingeniería de métodos y tácticas que deben realizarse para exponer cualquier debilidad en capacitación o falta de adherencia a las políticas de empresa y procedimientos. Antes de utilizar cualquier tácticas engañosas pruebas de penetración, los empleados se deben poner en aviso que dichas pruebas pueden ocurrir de vez en cuando.

Cómo utilizar estas políticas

Las políticas detalladas 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 segu En consecuencia, las políticas incluidas aquí no deben considerarse como una lista completa de las políticas de seguridad de la información. Por el contrario, son la base para creación de un cuerpo amplio de las políticas de seguridad adecuadas a la específica necesidades de su empresa.

Escritores de la política de una organización tendrá que elegir las políticas que son apropiado basado en entorno único de su empresa y objetivos de negocios. Cada organización, tener requisitos de seguridad distintos basados en negocios necesidades, requisitos legales, cultura organizacional y los sistemas de información utilizado por la empresa, tendrá lo que necesita de las políticas que se presentan, y omitir el resto.

También hay opciones sobre cómo estrictas políticas estará en cada uno categoría. Una empresa más pequeña ubicada en un centro único donde la mayoría de los empleados Sé uno con el otro no tiene que preocuparse mucho por un atacante llamar en el teléfono y pretendiendo ser un empleado (aunque por supuesto un impostor puede enmascararse como un proveedor). También, a pesar de los riesgos mayores, una empresa enmarcado alrededor de un casual, relajada cultura corporativa tal vez desee adoptar sólo una subconjunto limitado de políticas recomendadas para satisfacer sus objetivos de seguridad.

CLASIFICACIÓN DE DATOS

Una política de clasificación de datos es fundamental a la protección de una organización conjuntos de categorías para que regulen el sensible y activos de información información. Esta Directiva establece un marco para la protección corporativa información por concienciar a todos los empleados del nivel de sensibilidad de cada uno pieza de información.

Funcionamiento sin una política de clasificación de datos--el statu quo en casi todos las empresas hoy en día--deja la mayoría de estas decisiones en manos del individuo

trabajadores. Naturalmente, las decisiones empleado en gran medida se basan en factores subjetivos, en lugar de en el valor de la información, sensibilidad y criticidad. La información es también lanzado debido a que los empleados son ignorantes de la posibilidad de que en la respuesta a solicitud de la información, pueden ser puesta en manos de un atacante.

La política de clasificación de datos establece directrices para la clasificación de valiosos información en uno de varios niveles. Con cada artículo asignado una clasificación, empleados pueden seguir una serie de procedimientos de manipulación de datos que proteger a la empres desde la liberación inadvertida o descuidada de información confidencial. Estos procedimientos mitigar la posibilidad de que los empleados se serán engañados para que revelen sus sensibles información a personas no autorizadas.

Todos los empleados deben ser entrenados sobre la política de clasificación de datos corporativos, los que normalmente no usan equipos o comunicaciones corporativas incluidos sistemas. Porque todos los miembros de la fuerza de trabajo corporativo--incluyendo la limpieza de la tripulación, guardias del edificio y personal de la sala de la copia, así como consultores, contratistas y pasantes incluso--pueden tener acceso a información confidencial, nadie podría ser el blanco de un ataque.

Administración deberá asignar un propietario de la información que será responsable de cualquier información que está actualmente en uso en la empresa. Entre otras cosas, la Propietario de la información es responsable de la protección de los activos de información. Normalmente, el propietario decide qué nivel de clasificación para asignar basándose en la necesidad de proteger la información, evalúan periódicamente el nivel de clasificación asignado y decide si los cambios son necesarios. Propietario de la información puede también delegar la responsabilidad de proteger los datos a un custodio o designatario.

Categorías de clasificación. y definiciones
Información debe estar separado en distintos niveles de clasificación basada en su sensibilidad. Una vez que se configura un sistema de clasificación particular, es demasiado caro y proceso lento para reclasificar la información en categorías nuevas. En nuestro ejemplo de una directiva que escogí cuatro niveles de clasificación, que es apropiado para la mayoría empresas de tamaño mediana a grandes. Dependiendo del número y tipos de sensible información, negocio puede elegir agregar más categorías a mayor control tipos específicos de información. En las empresas más pequeñas, una clasificación de tres niveles esquema puede ser suficiente. Recuerde: cuanto más compleja la clasificación esquema, el gasto más a la organización en la capacitación de los empleados y aplicar el sistema.

Confidencial. Esta categoría de información es la más sensible. Confidencial información está destinada únicamente dentro de la organización. En la mayoría de los casos, se sólo debe ser compartida con un número muy limitado de personas con absoluta

necesidad de saber. La naturaleza de la información confidencial es tal que cualquier divulgación no autorizada podría afectar seriamente la empresa, sus accionistas, sus asociados de negocios y sus clientes. Elementos de información confidencial generalmente caen en una de estas categorías:

Información sobre secretos comerciales, código fuente propietaria, técnicas o especificaciones funcionales o información del producto que puede ser de ventaja a un competidor.

Información financiera y de marketing no está disponible al público.

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

Privada. Esta categoría abarca información de carácter personal que pretende para uso sólo dentro de la organización. Cualquier divulgación no autorizada de privado información podría afectar seriamente empleados, o la empresa si obtenida por cualquiera personas no autorizadas (especialmente los ingenieros sociales). Elementos de información privada sería incluir historial médico empleado, beneficios para la salud, cuenta bancaria información, historia de salario o cualquier otra información de identificación personal que es no de registro público.

NOTA
La categoría interna de información a menudo se denomina sensibles de seguridad personal. Tengo que usar interna porque el término en sí mismo explica la ideada audiencia. He utilizado el término sensible no como una clasificación de seguridad, sino como un método conveniente de referirse a la información interna, confidencial y privado; dicho de otra manera, sensible se refiere a cualquier información de la empresa que no es específicamente designado como público.

Interna. Esta categoría de información puede proporcionarse libremente a cualquier persona empleados de la organización. Normalmente, no autorizado, divulgación de interna información no pretende provocar graves perjuicios a la empresa, su accionistas, sus socios de negocios, sus clientes o sus empleados. Sin embargo, las personas adeptas en técnicas de ingeniería social pueden utilizar esta información para enmascararse como un empleado autorizado, contratista o proveedor para engañar incautos personal en proporcionar información más confidencial que daría como resultado acceso no autorizado a sistemas informáticos corporativos.

Debe firmarse un acuerdo de confidencialidad antes información interna puede ser cedidos a terceros, como los empleados de las empresas de proveedores, trabajo de contratista, las empresas asociadas y así sucesivamente. Información interna generalmente incluye nada utilizado el curso de la actividad diaria que no debe liberarse a los forasteros, tales

organigramas corporativos, números de red de marcado telefónico, sistema interno nombres, procedimientos de acceso remoto, códigos de centro de costos y así sucesivamente.

Público. Información específicamente designado para el lanzamiento al público. Esto tipo de información se puede distribuir libremente a nadie, como comunicados de prensa, información de contacto de soporte al cliente, o catálogos de productos. Tenga en cuenta que cualquier información no específicamente designada como público debe tratarse como sensibles información.

Terminología de datos clasificados
Basado en su clasificación, datos deberían distribuirse a determinadas categorías de personas. Una serie de políticas en este capítulo se refieren a la información que una persona sin verificar. A los efectos de estas políticas, es una persona sin verificar alguien a quien no conoce personalmente el empleado para ser un empleado activo o b un empleado con el rango adecuado para tener acceso a la información, o que no ha sido avalado por un tercero de confianza.

A los efectos de estas políticas, una persona de confianza es una persona que haya cumplido con cara a cara que le es conocido como un empleado de la empresa, cliente, o Consultor de la empresa con el rango adecuado para tener acceso a la información. A Persona también podría ser un empleado de una empresa tener un establecido de confianza relación con su empresa (por ejemplo, un cliente, proveedor, o estratégica socio de negocios que ha firmado un acuerdo de no divulgación).

En tercero dar fe, una persona de confianza proporciona verificación de una persona empleo o el Estado y la autoridad de la persona a solicitar información o una acción. Nota que en algunos casos, estas políticas requieren para comprobar que el Persona todavía es empleado por la empresa antes de responder a una solicitud de confianza para obtener información o acción por alguien a quien han avalado.

Una cuenta con privilegios es un equipo o en otra cuenta que requieren permiso de acceso más allá de la cuenta de usuario básica, como una cuenta de administrador de sistemas. Empleados con cuentas con privilegios suelen tengan la capacidad de modificar usuario privilegios o realizar funciones del sistema.

Un buzón departamental general es un buzón de voz respondido con un genérico mensaje para el departamento. Un buzón de correo se utiliza para proteger los nombres y extensiones de teléfono de los empleados que trabajan en un departamento en particular.

PROCEDIMIENTOS DE VERIFICACIÓN Y AUTORIZACIÓN
Ladrones de información suelen utilizan tácticas engañosas para acceder u obtener información comercial confidencial haciéndose pasar como empleados legítimos, por contratistas, proveedores o socios comerciales. Para mantener la información efectiva

seguridad, un empleado recibe una solicitud para realizar una acción o proporcionar información confidencial positivamente debe identificar el llamador y verificar su autoridad previo a la concesión de una solicitud.

Los procedimientos recomendados en este capítulo están diseñados para ayudar a una empleado que recibe una petición a través de cualquier método de comunicación tales como teléfono, correo electrónico o fax para determinar si la solicitud y la persona que realiza son legítimos.

Solicitudes de una persona de confianza
Puede requerir una petición de información o acción de una persona de confianza:

Verificación de que la empresa emplea activamente o que tiene una relación con el persona cuando esa relación es una condición de acceso a esta categoría de información. Esto es para evitar terminados empleados, proveedores, contratistas, y otros que ya no están asociados con la compañía de disfrazada de personal activo.

Comprobación de que la persona tiene una necesidad de saber, y está autorizado a tener acceso a la información o para solicitar la acción.

Solicitudes de una persona sin verificar
Cuando se realiza una solicitud por una persona sin verificar, una verificación razonable proceso debe implementarse para identificar positivamente a la persona que efectúa la solicitud autorizado para recibir la información solicitada, especialmente cuando la solicitud de ninguna manera involucra computadoras o equipos informáticos. Este proceso es la control fundamental para prevenir los ataques exitosos ingeniería social: si estos procedimientos de verificación, reducirá considerablemente exitosa ataques de ingeniería social.

Es importante que no hagas el proceso tan engorroso que es costo-prohibitivo, o que los empleados ignoran.

Como se detalla a continuación, el proceso de verificación consta de tres pasos:

Verificar que la persona es quien dice ser.

Determinar que el solicitante es empleado actualmente o comparte una necesidad de saber relación con la empresa.

Determinar que la persona está autorizada para recibir la información específica o a Convocatoria para la acción solicitada.

Paso 1: Verificación de identidad
Continuación se muestran los pasos recomendados para la verificación en orden de eficacia: cuanto mayor sea el número, más eficaz el método. También incluido con cada elemento es una statemen.t sobre la debilidad de ese particular método y la forma en que un ingeniero social puede vencer o burlar la método para engañar a un empleado.

1. Identificador de llamada (suponiendo que esta característica está incluida en el teléfono de la empresa sistema). Desde la pantalla de ID del llamador, determinar si la llamada es desde dentro o fuera de la empresa y muestra el nombre o número de teléfono coincide con la identidad proporcionada por el llamador.

Debilidad: Información de ID del llamador externo puede ser refutada por cualquiera con acceso a un conmutador PBX o teléfono conectado al servicio telefónico digital.

2. Devolución de llamada. Buscar en el directorio de la empresa solicitante y devolver la llamada a la extensión lista para comprobar therequester es un empleado.

Debilidad: Un atacante con conocimientos suficientes puede llamada reenvío una empresa extensión de modo que, cuando el empleado coloca la llamada de verificación a la lista número de teléfono, la llamada se transfiere al número de teléfono fuera del atacante.

3. Dar fe. Verifica una persona de confianza que da fe de la identidad del solicitante el solicitante.

Debilidad: Los atacantes con un pretexto son frecuentemente capaces de convencer a otro empleado de su identidad y conseguir ese empleado para atestiguar para ellos.

4. Secreto compartido. Un secreto compartido de toda la empresa, tales como apassword o código diario.

Debilidad.\" Si mucha gente conoce el secreto compartido, puede ser fácil para un atacante para aprenderlo.

5. Supervisor y administrador de empleado. Teléfono del employee'simmediate supervisor y solicitud de verificación.

Debilidad: Si el solicitante ha proporcionado el número de teléfono para llegar a su o su manager, llega a la persona del empleado cuando llamando el número no puede el Gerente real pero puede, de hecho, ser cómplice del atacante.

6. Proteger el correo electrónico. Solicitar un mensaje firmado digitalmente.

Debilidad: Si un atacante ya ha comprometido equipo del empleado y instalado un registrador de pulsaciones de teclas para obtener la primera frase del empleado, él puede env correo electrónico firmado digitalmente que parece ser del empleado.

7. Personal reconocimiento de voz. La persona que recibe la solicitud se ha ocupado de el solicitante (preferiblemente presencial), sabe de determinados la persona realmente es una persona de confianza y es lo suficientemente familiarizados con la persona a reconocer su voz en el teléfono.

Debilidad: Se trata de un método bastante seguro, no es fácil eludido por un atacante, pero es inútil si la persona que recibe la solicitud nunca ha conocido o hablado con el solicitante.

8. Solución dinámica de la contraseña. El solicitante autentica a sí mismo o a sí misma mediante el uso de una solución de contraseña dinámica como un identificador de seguridad.

Debilidad: Derrotar a este método, el atacante tendría que obtener uno de los dispositivos de contraseña dinámica, como también el acompañamiento PIN del empleado quien el dispositivo legítimamente pertenece, o tendría que engañar a un empleado en leer la información en la pantalla del dispositivo y proporcionando el PIN.

9. En persona con ID. El solicitante aparece en persona andpresents un empleado Insignia u otra identificación adecuada, preferiblemente un identificador de imagen.

Debilidad: Los atacantes a menudo son capaces de robar una insignia de empleado, o crear un falsos Insignia que parece auténtico; Sin embargo, los atacantes suelen rehuir este enfoque debido a que aparece en persona pone el atacante en riesgo significativo de identificado y detenido.

Paso 2: Verificación de estado de empleo

La mayor amenaza de seguridad de la información no es de lo social profesional Ingeniero, ni desde el intruso equipo calificados, sino de alguien mucho más cercano: el empleado despedido sólo venganza o con la esperanza de establecer a sí mismo en el negocio utilizando la información robada de la empresa. (Tenga en cuenta que una versión de este procedimiento También puede utilizarse para comprobar que alguien goza de otro tipo de negocio relación con su empresa, como un proveedor, consultor o contrato trabajador).

Antes de proporcionar información confidencial a otra persona o Aceptar instrucciones para las acciones que impliquen el equipo o equipos informáticos, Compruebe que el solicitante es todavía un empleado actual mediante uno de estos métodos:

Verificación de directorio de empleados. Si la empresa mantiene a un empleado en línea directorio que refleja con precisión los empleados activos, verificar que el solicitante es sigue apareciendo.

Verificación de Manager del solicitante. Gestor del solicitante mediante un teléfono de llamadas número que aparece en el directorio de la empresa, no un número proporcionado por el solicitante.

Departamento o grupo de trabajo verificación del solicitante. Llame al solicitante Departamento o grupo de trabajo y determinar de nadie en ese departamento o Grupo de trabajo que el solicitante todavía es empleado por la empresa.

Paso 3: Verificación de la necesidad de saber
Más allá de verificar que el solicitante es un empleado actual o tiene una relación con su empresa, todavía queda la cuestión de si el solicitante es autorizadas a tener acceso a la información que se solicita, o está autorizado para solicitud específica de que las acciones que afectan a ordenadores o equipos informáticos ser tomado.

Esta determinación puede realizarse mediante uno de estos métodos:

Consultar listas de grupos de trabajo\/título\/responsabilidades de trabajo. Una empresa puede proporcion acceso a la información de autorización mediante la publicación de las listas de los cuales son empleados derecho a la información. Estas listas pueden ser organizadas en términos de empleado trabajo de título, departamentos de empleados y grupos de trabajo, responsabilidades de los empleados, o una combinación de éstos. Dichas listas serían necesario para mantenerse en línea para ser mantener actualizados y proporcionan un acceso rápido a la información de autorización. Ordinariamente, Los propietarios de información sería responsables de supervisar la creación y mantenimiento de las listas de acceso a la información bajo control del propietario.

NOTA
Es importante señalar que mantener estas listas es una invitación a lo social ingeniero. Tenga en cuenta: Si el atacante dirige una empresa toma conciencia que el empresa mantiene dichas listas, hay una fuerte motivación para obtener uno. Vez en mano, dicha lista abre muchas puertas para el atacante y pone la empresa en riesgo grave.

Obtener la autoridad de un administrador. Un contactos empleado su propio Administrador, o del solicitante, para poder cumplir con la solicitud.

Obtener autoridad del propietario de la información o un designatario. La información Propietario es el último juez de si debe concederse una determinada persona acceso. El proceso de control de acceso basado en el equipo es para el empleado

Póngase en contacto con su administrador de inmediato para aprobar una solicitud de acceso a información basada en perfiles de trabajo existentes. Si no existe tal perfil, es el responsabilidad del administrador ponerse en contacto con los propietario de los datos pertinentes para e cadena de mando deben seguirse por lo que no son propietarios de la información barraged con solicitudes cuando hay una frecuente necesita saber.

Obtener autoridad por medio de un paquete de Software propietario. Para un gran empresa en una industria altamente competitiva, puede resultar práctico desarrollar un paquete de software propietario que proporciona la necesidad de obtener autorización. Tal un base de datos almacena los nombres de los empleados y los privilegios de acceso a la información clasifi Los usuarios no puedan buscar los derechos de acceso de cada individuo, sino entraría a nombre del solicitante y el identificador asociado con el información que se busca. El software proporciona una respuesta que indica Si o no el empleado está autorizado para acceder a dicha información. Esto alternativa evita el peligro de crear una lista de personal con acceso respectivo derechos a la información valiosa, crítico o sensible que podrían ser robados.

POLÍTICAS DE ADMINISTRACIÓN

Las siguientes políticas corresponden a empleados de nivel de gestión. Estos son
dividida en las áreas de clasificación de la información, divulgación de información, teléfono
Administración y políticas diversas. Tenga en cuenta que cada categoría de políticas
utiliza una estructura de numeración única para facilitar la identificación de las distintas políticas.

Políticas de clasificación de datos
Clasificación de datos se refiere a cómo clasifica a la sensibilidad de su empresa
información y quién debería tener acceso a esa información.

Clasificación de datos de asignar 1-1
Política: Toda la información valiosa, sensibles o críticos de negocios debe asignarse
a una categoría de clasificación por el propietario de la información o delegado designado.

Explicación\/notas: El propietario o el delegado designado asignará el adecuado
clasificación de los datos a cualquier información que se utiliza habitualmente para realizar negocios
objetivos. El propietario también controla quién puede tener acceso a dicha información y lo utilice
puede hacerse de ella. El propietario de la información puede reasignar la clasificación
y podrá designar un período de tiempo para la desclasificación automática.
Cualquier elemento no marcado debe clasificarse como sensibles.

Procedimientos de manipulación de publicar clasificado de 1-2
Política: La empresa debe establecer procedimientos que regulen el
información en cada categoría.

Explicación y notas\". Una vez que se establecen las clasificaciones, procedimientos para liberar
información a empleados y a los extranjeros debe establecerse, como se detalla en el
Verificación y autorización de procedimientos descritos anteriormente en este capítulo.

1-3 Etiquetar todos los elementos
Política\". Marque claramente los materiales impresos y almacenamiento de medios de comunicación que
Información confidencial, privada o interna para mostrar los datos adecuados
clasificación.

Explicación y notas\". Documentos impresos deben tener una portada, con una
etiqueta de clasificación destacado y una etiqueta de clasificación en cada
página que está visible cuando se abre el documento.

Todos los archivos electrónicos que fácilmente pueden etiquetarse con datos adecuados
clasificaciones (base de datos o archivos de datos raw) deben ser protegidas mediante controles de acceso
para asegurar que dicha información no es indebidamente divulgada, y que no puede ser
cambiado, destruidos o hicieron inaccesibles.

Todos los soportes informáticos como disquetes, cintas y CD-ROM deben etiquetarse con la clasificación más alta de cualquier información contenida en él.

Revelación de información
Revelación de información implica la divulgación de información a diversas partes basado en su identidad y la necesidad de saber.

Procedimiento de verificación de empleados de 2-1
Política: La empresa debe establecer procedimientos integrales que utilizado poremplеados para verificar la identidad, estado de empleo, y autorización de una persona antes de soltar confidenciales o sensibles información o realizar cualquier tarea que implica utilizar de cualquier hardware o software.

Notas de la explicación: cuando esté justificado por el tamaño de las necesidades de la empresa y la segur se deberían utilizar tecnologías de seguridad avanzada para autenticar la identidad. Lo mejor práctica de seguridad sería implementar tokens de autenticación en combinación con un secreto compartido para identificar positivamente a las personas hacen solicitudes. Si bien esta práctica sustancialmente minimizar el riesgo, el costo puede ser prohibitivo para algunos empresas. En esas circunstancias, la empresa debe utilizar un nivel de empresa secreto compartido, como un diario contraseña o código.

2-2 Divulgación de información a terceros
Política: Un conjunto de procedimientos de divulgación de información recomendada debe disposición y todos los empleados deben ser entrenados para seguirlos.

Explicación\/notas: Generalmente, los procedimientos de distribución deben establecerse para:

Información disponible dentro de la empresa.

Distribución de información a particulares y empleados de las organizaciones que tienen una relación establecida con la empresa, tales como consultores, temporales los trabajadores, pasantes, empleados de organizaciones que tienen una relación de proveedor o acuerdo de asociación estratégica con la empresa y así sucesivamente.
Información disponible fuera de la empresa.

Información en cada nivel de clasificación, cuando se entrega la información en persona, por teléfono, por correo electrónico, por fax, por correo de voz, por servicio postal, por servicio de entrega de firmas y por transferencia electrónica.

Información de distribución confidencial de 2-3
Política: Información confidencial, que es la información de la empresa que podría causar daño importante si obtenidos por personas no autorizadas, podrá entregarse solamente a un Confianza de quien está autorizado para recibirla.

Explicación\/notas: Información confidencial en una forma física (que es, impreso copia o en un medio de almacenamiento extraíble) se pueden suministrar:

En persona.

Por correo interno, sellado y marcado con la clasificación confidencial.

Fuera de la empresa por un servicio de entrega confianza (es decir, FedEx, UPS etc.) con la firma del destinatario requerido, o por un servicio postal mediante un certificado o clase registrada de correo.

Información confidencial en forma electrónica (archivos de computadora, archivos de base de datos, co se pueden suministrar:

En el cuerpo del correo electrónico codificado.

Por adjunto de correo electrónico, como un archivo cifrado.

Por transferencia electrónica a un servidor dentro de la red interna de la empresa.

Mediante un programa de fax desde un ordenador, siempre que sólo las utilizaciones destinatarios el destino de máquina, o que el destinatario está esperando en el destino máquina mientras se envía el fax. Como alternativa, se pueden enviar facsímiles sin destinatario presente si se envían a través de un vínculo telefónico codificado para una servidor de fax protegido con contraseña.

Información confidencial puede discutirse en persona; por teléfono en el empresa; por teléfono fuera de la empresa si cifrado; por satélite cifrada transmisión; por enlace de videoconferencia cifrados; y por cifra voz sobre Protocolo de Internet (VoIP).

Para la transmisión de la máquina de fax, se llama el método recomendado para el remitente transmitir una portada; el receptor, al recibir la página, transmite una página en respuesta, demostrando que está en la máquina de fax. El remitente, a continuación transmite el fax.

No son aceptables para la discusión de los siguientes medios de comunicación o distribuir información confidencial: sin cifrar correo electrónico, mensaje de correo de voz,

correo ordinario, o cualquier método de comunicación inalámbrica (celulares, mensajes cortos Servicio o inalámbricos).

Información de distribución de privada de 2-4
Política: Información privada, que es información personal acerca de un empleado o empleados que si revelado, podrían utilizarse para perjudicar a los empleados o la empresa, podrán entregarse sólo a una persona de confianza que esté autorizado a recibirla.

Explicación\/notas: Información privada en forma física (es decir, impresos o podrán entregarse los datos en un medio de almacenamiento extraíble):

En persona

Por correo interno, sellado y marcado con la clasificación privada

Por correo ordinario

Puede obtener información privada en forma electrónica (archivos de computadora, archivos de base de entregarse:

Por correo electrónico interno.

Por transferencia electrónica a un servidor dentro de la red interna de la empresa.

Por fax, siempre que el destinatario utiliza el destino
máquina, o que el destinatario está esperando en la máquina de destino mientras se envía el fax. Facsímiles también pueden enviarse por fax protegido con contraseña servidores. Como alternativa, se pueden enviar facsímiles sin el destinatario si presente enviados a través de un vínculo telefónico codificado a un servidor de fax protegido con contraseña.

Información privada puede ser discutido en persona; por teléfono; por satélite transmisión; por enlace de videoconferencia; y por cifra Vole

No son aceptables para la discusión de los siguientes medios de comunicación o distribuir información privada: sin cifrar correo electrónico, mensaje de correo de voz, regular correo y por cualquier medio de comunicación inalámbrica (celular, SMS, o inalámbricos).

Información de distribución interna de 2-5
Política: Información interna es información para ser compartida sólo dentro de la empresa o con otras personas de confianza que han firmado un acuerdo de no divulgación. Le debe establecer directrices para la distribución de información interna.

Explicación\/notas: Información interna puede distribuirse en cualquier forma,
incluido el correo electrónico interno, pero no podrá ser distribuida fuera de la empresa de correo electró
formar a menos que la cifra.

2-6 Discutir información confidencial por teléfono
Política: antes de publicar cualquier información que no está designado como público sobre el
Telefónica, la persona liberar dicha información personalmente debe reconocer la
voz del solicitante a través del contacto de negocios previa, o el sistema de teléfono de la empresa
debe identificar la llamada como de un número de teléfono interno que ha sido
asignado al solicitante.

Explicación\/notas: Si no se conoce la voz del solicitante, llame al solicitante
número de teléfono interno para verificar la voz del solicitante a través de un correo de voz grabada
el mensaje, o tiene el administrador del solicitante verificar la identidad del solicitante y que tiene
Saber.

Procedimientos de personal de lobby o recepción de 2-7
Política: Personal de Lobby debe obtener antes de lanzar cualquier identificación con foto
paquete a cualquier persona que no es conocido por ser un empleado activo. Un registro debe
mantenerse para registrar el nombre de la persona, el número de licencia de conducir, fecha de nacimiento
elemento recogido y la fecha y hora de dicha recogida.

Explicación\/notas: Esta política también se aplica a entregar paquetes salientes
cualquier servicio de messenger o de mensajería como FedEx, UPS o Airborne Express.
Estas empresas emiten tarjetas de identificación que puede utilizarse para verificar empleados
identidad.

2-8 Transferencia de software de terceros
Política: antes de realizar la transferencia o divulgación de cualquier software, programa o equipo
instrucciones, identidad del solicitante debe ser verificado positivamente, y debe ser
establecido si esa versión es compatible con la clasificación de datos
asignado a dicha información. Normalmente, el software desarrollado internamente en origen-
formato de código es considerado confidencial altamente propietaria y clasificada.

Explicación\/notas: Determinación de autorización generalmente se basa en si
el solicitante necesita acceso al software para hacer su trabajo.

Lleva 2-9 ventas y marketing de calificación del cliente
Política: Personal de venta y marketing debe calificar oportunidades de ventas antes de soltar
números de devolución de llamada interna, planes de producto, contactos de grupo de producto u otros
Información confidencial para cualquier cliente potencial.

Explicación\/notas: Es una táctica común para espías industriales contactar a ventas y representante de marketing y hacerle creer que puede ser una compra grande en el Vista. En un esfuerzo por aprovechar la oportunidad de venta, marketing y venta los representantes de liberar a menudo información que puede ser utilizada por el atacante como un chip obtener acceso a sensible información.

2-10 Transferencia de archivos o datos
Política: Otros datos electrónicos o archivos no se trasladara a cualquier extraíbles medios de comunicación a menos que el solicitante es una persona de confianza cuya identidad ha sido v y que tiene una necesidad de tener esos datos en ese formato.

Explicación\/notas: Un ingeniero social fácilmente puede hacer un empleado proporcionando un solicitud plausible para tener información confidencial copiado en una cinta, disco Zip, o otros medios extraíbles y envió a él o celebrada en el lobby para su recogida.

Administración de teléfono
Las políticas de administración de Telefónica garantizan que los empleados puedan verificar la identidad y proteger su propia información de contacto de los llamando a la compañía.

Reenvío de llamadas de 3-1 sobre el número telefónico o de fax
Política: Llame a servicios de reenvío que permitan el reenvío de llamadas al exterior números de teléfono no se colocará en cualquier módem telefónico o fax teléfono números dentro de la empresa.

Explicación\/notas: Los atacantes sofisticados pueden intentar engañando teléfono personal de la empresa o los trabajadores de telecom interna en números internos de reenvío a una línea de teléfono externo bajo control de un atacante. Este ataque permite el intruso para interceptar los faxes, solicitar información confidencial a enviarse por fax dentro de la empresa (personal de asume que el fax dentro de la organización debe ser seguro) o engañando a los usuarios de acceso telefónico en proporcionar sus contraseñas de cuenta mediante el r líneas de acceso telefónico a un equipo de señuelo que simula el proceso de inicio de sesión.

Dependiendo del servicio de teléfono utilizado dentro de la empresa, el reenvío de llamadas función puede estar bajo control del proveedor de comunicaciones, en lugar de Departamento de telecomunicaciones. En tales circunstancias, se hará una solicitud a el proveedor de comunicaciones para asegurar la llamada función de reenvío no está presente los números de teléfono asignados a las líneas de acceso telefónico y de fax.

3-2 Caller ID
Política: El sistema telefónico corporativo debe proporcionar la línea llamada identificación (caller ID) en todos los conjuntos de teléfono interno y, si es posible, permitir distintivo timbre para indicar cuando una llamada es de fuera de la empresa.

Explicación\/notas: Si empleados pueden verificar la identidad de las llamadas telefónicas de fuera de la empresa puede ayudarles a prevenir un ataque, o identificar al atacante al personal de seguridad apropiadas.

Teléfonos de cortesía de 3-3
Política: Para impedir que los visitantes haciéndose pasar como empresa trabajadores, cada cortesía teléfono indicará claramente la ubicación del llamador (por ejemplo, There was an error deserializing the object of type System.String. Encountered unexpected charact

Explicación y notas\". Si el identificador de llamada para llamadas internas muestra el número de extensión sólo apropiado debe prever llamadas colocadas desde teléfonos de la empresa en el área de recepción y otras áreas públicas. No debe ser posible para un atacante para realizar una llamada de uno de estos teléfonos y engañar a un empleado a creer que la llamada se ha colocado internamente de teléfono de un empleado.

Contraseñas predeterminadas de 3-4 fabricante suministradas con sistemas telefónicos
Política: El administrador de correo de voz debe cambiar todas las contraseñas por defecto que fueron enviados con el previo sistema de teléfono a utilizar por personal de la empresa.

Explicación\/notas: los ingenieros sociales pueden obtener listas de contraseñas predeterminadas de los fabricantes y utilizarlo para acceder a las cuentas de administrador.

Buzones de correo de voz de departamento de 3-5
Política\". Configurar un buzón de voz genérica para cada departamento que normalmente tiene contacto con el público.

Explicación\/notas: El primer paso de la ingeniería social consiste en reunir información sobre la empresa y su personal. Limitando la accesibilidad de los nombres y números de teléfono de los empleados, una empresa hace más difícil para el ingeniero social identificar los objetivos de la empresa, o nombres de empleados legítimos destinados a engañar a otros miembros del personal.

Verificación de 3-6 de los vendedores de sistemas de teléfono
Política: No técnicos de asistencia de proveedores se permitirá acceso de forma remota la sistema telefónico sin identificación positiva de los vendedores de la empresa y autorización para efectuar dicho trabajo.

Explicación\/notas: Intrusos de equipo que acceder al teléfono corporativo sistemas obtienen la capacidad de crear buzones de voz, interceptar mensajes destinados para otros usuarios, o hacer llamadas de teléfono gratis a expensas de la Corporación.

3-7 Configuración del sistema de teléfono
Política\". El administrador de correo de voz hará valer los requisitos de seguridad por configuración de los parámetros de seguridad apropiados en el sistema telefónico.

Explicación\/notas: Sistemas telefónicos pueden configurarse con mayor o menor grado de seguridad para mensajes de correo de voz. El administrador debe ser consciente de la empresa preocupaciones de seguridad y trabajar con personal de seguridad para configurar el teléfono sistema para proteger los datos confidenciales.

Función de seguimiento de llamada 3-8
Política: dependiendo de las limitaciones del proveedor de comunicaciones, el seguimiento de llamadas de función se activará a nivel mundial para permitir a los empleados activar la trampa-y-traza característica cuando el llamador es sospechoso de ser el atacante.

Explicación\/notas: Los empleados deberán recibir una formación sobre el uso de seguimiento de llamadas circunstancias apropiadas cuando debe utilizarse. Se debería iniciar un seguimiento de llamadas Cuando el llamador claramente está intentando obtener acceso no autorizado a la empresa sistemas informáticos o solicitando información confidencial. Cuando un empleado activa la función de seguimiento de llamada, debe enviarse una notificación inmediata al incidente Grupo de informe.

Sistemas de teléfono automatizado de 3-9
Política\". Si la empresa utiliza un sistema telefónico automatizado de respuesta, el sistema debe ser programado para que las extensiones de teléfono no se anunció cuándo transferir una llamada a un empleado o departamento.

Explicación\/notas: Los intrusos pueden utilizar el sistema de teléfono automatizado de la empresa para asignar nombres de los empleados a extensiones telefónicas. Los atacantes pueden utilizar conocimiento de esas extensiones para convencer a los destinatarios de la llamada que son empleados con derecho a información privilegiada.

3-10 Buzones de voz a desactivará después de sucesiva acceso no válido intentos de
Política: Programa el sistema telefónico corporativo para bloquear cualquier correo de voz cuenta cada vez que intente un número especificado de acceso válido sucesiva han se han realizado.

Explicación y notas\". El administrador de telecomunicaciones debe bloquear un buzón de voz después de cinco intentos sucesivos de válido para iniciar sesión. El administrador debe entonces restablecer cualquier bloqueos de correo de voz manualmente.

Extensiones de teléfono restringido de 3-11
Política\". Todo interno teléfono extensiones a departamentos o grupos de trabajo que

normalmente no reciben llamadas de llamadores externos (mesa de ayuda, sala de informática, soporte técnico empleado y así sucesivamente) deben ser programado para que estos teléfonos pueden alcanzarse sólo de extensiones internas. Alternativamente, se pueden protegido por contraseña así empleados y otras personas autorización llamando desde el exterior debe introducir la contraseña correcta.

Explicación\/notas: Mientras el uso de esta política se bloque más intentos por aficionados los ingenieros sociales para alcanzar sus objetivos probables, debe señalarse que un determinado atacante a veces será capaz de hablar de un empleado en llamar restringido extensión y pidiendo a la persona que contesta el teléfono para llamar al atacante, o simplemente la Conferencia en la extensión limitada. Durante el entrenamiento de seguridad, esto método de engañar empleados en ayudar al intruso debe discutirse a empleado de sensibilizar acerca de estas tácticas.

Varios
Diseño de placa de 4-1 empleado
Política: Insignias empleado deben estar diseñados para incluir una fotografía grande que puede ser reconocido desde la distancia.

Explicación\/notas: Es la fotografía corporativas acreditaciones de diseño estándar, por motivos de seguridad, sólo ligeramente mejores que nada. La distancia entre un persona entrando en el edificio y el guardia o recepcionista que tiene el responsabilidad de comprobar la identificación es generalmente tan grande que la imagen es demasiado pequeño para reconocer cuando la persona camina por. Para la foto de valor en Esta situación, un rediseño de la insignia es necesario.

Revisión de los derechos de acceso de 4-2 al cambiar de posición o responsabilidades
Política: Cada vez que un empleado de la compañía cambia posiciones o se le da mayor o disminución de trabajo responsabilidades, gestor del empleado notificará de la cambio de responsabilidades del empleado hasta que el perfil de seguridad adecuado pueden asignarse.

Explicación\/notas: Gestión de los derechos de acceso del personal es necesario para limitar la divulgación de información protegida. La regla de privilegio mínimo será aplicar: los derechos de acceso asignados a los usuarios será el mínimo necesario para realizar su trabajo. Las solicitudes de cambios que resultan de los derechos de acceso elevado debe estar en conformidad con una política de concesión de derechos de acceso elevado.

Administrador del trabajador o el departamento de recursos humanos tendrá la responsabilidad de notificar al departamento de tecnología de información correctamente ajustar los derechos de acceso del titular de la cuenta según sea necesario.

4-3 Especial de identificación para los empleados no
Política: Su empresa debe emitir una insignia de empresa foto especial de confianza
gente de entrega y no empleados que tienen un negocio necesitan introducir la empresa
locales sobre una base regular.

Explicación\/notas: No empleados que necesitan entrar en el edificio regularmente (para
ejemplo, para hacer las entregas de alimentos o bebidas a la cafetería, o para reparar
máquinas de copiar o hacer instalaciones telefónicas) puede representar una amenaza para su
empresa. Además de publicar identificación a estos visitantes, asegúrese de que su
los empleados están capacitados para detectar un visitante sin una insignia y saber cómo actuar en
esa situación.

4-4 Deshabilitar cuentas de equipo para contratistas
Política: Cuando un contratista que ha recibido una cuenta de equipo
ha completado su asignación, o cuando expire el contrato, el
administrador responsable notificará inmediatamente a la tecnología de la información
Departamento para deshabilitar cuentas de equipo del contratista, incluyendo las cuentas
utilizado para el acceso de la base de datos, dial-up o acceso a Internet desde ubicaciones remotas.

Notas de la explicación: W-gallina empleo del trabajador se termina, hay un
peligro que él o ella usará el conocimiento de los sistemas de su empresa y
procedimientos para obtener acceso a datos. Cuentas de equipo todos conocido o utilizado por el
trabajador debe desactivarse con prontitud. Esto incluye las cuentas que proporcionan acceso a
bases de datos de producción, cuentas de acceso telefónico remotas y las cuentas utilizadas para el acceso
dispositivos informáticos.

Incidente de 4-5 organización
Política: Un incidente informes debe establecerse la organización o, en menor
las empresas, un incidente informes individual y copia de seguridad designado, para
recibir y distribuir alertas sobre posibles incidentes en
progreso.

Explicación\/notas: mediante la centralización de los informes de presuntos incidentes de seguridad,
puede detectarse un ataque que lo contrario puede haber pasado desapercibido. En el evento
que ataques sistemáticos a través de la organización son detectados y denunciados, el
incidente de organización puede ser capaz de determinar cuál es el atacante
por lo que pueden hacer esfuerzos especiales para proteger los activos de destinatarios.

Empleados asignados a recibir informes de incidentes deben familiarizarse con social
Ingeniería de métodos y tácticas, permitiéndoles evaluar informes y
reconocer cuándo puede ser un ataque en curso.

Incidente de 4-6 informes línea directa
Política: Una línea directa al incidente de informes de la organización o persona, que puede consisten en una extensión de teléfono fácil de recordar, debe establecerse.

Explicación\/notas: Cuando los empleados sospechan que son el destino de un social ataque de ingeniería, debe ser capaces de notificar de inmediato a la denuncia de incidentes Organización. A fin de que la notificación oportuna, todos de la compañía telefónica operadores y recepcionistas debe el número publicado o de otro tipo inmediatamente a su disposición.

Un sistema de alerta temprana de toda la empresa puede ayudar sustancialmente a la organización en detectar y responder a un ataque constante. Los empleados deben ser suficientemente bien entrenados que uno que sospecha que él o ella ha sido el destino de una social Ingeniería ataque llamará inmediatamente el incidente de informes en línea directa. En el incidente personal informes de conformidad con procedimientos publicados, será notificar inmediatamente a los grupos específicos que una intrusión puede ser tan en progreso el personal estará en alerta. Para que la notificación oportuna, la presentación de informes número de teléfono debe distribuirse ampliamente en toda la empresa.

Deben protegerse las zonas sensibles de 4-7
Política: Un guardia de seguridad se proyectará el acceso a áreas sensibles o seguros y debe requieren dos formas de autenticación.

Explicación\/notas: Una forma aceptable de autenticación utiliza digital cerradura electrónica requiere un empleado a deslizar su insignia de empleado y escriba un código de acceso. Es el mejor método para proteger las zonas sensibles registrar una seguridad Guardia quien observa cualquier entrada de acceso controlado. En donde se trata de organizaciones no rentable, dos formas de autenticación deben utilizarse para validar la identidad. Según el riesgo y costo, se recomienda una tarjeta de acceso biométrico habilitado.

Armarios de red y teléfono 4-8
Política: Archivadores, armarios o locales que contengan cableado de red, cableado, teléfono o puntos de acceso de red deben estar asegurados en todo momento.

Explicación\/notas: Sólo el personal autorizado podrá acceso al teléfono y red armarios, habitaciones o armarios. Cualquiera fuera personal de personas o un proveedor de mantenimiento debe identificarse positivamente mediante la procedimientos publicados por el departamento responsable de la seguridad de la información. Acceso a líneas telefónicas, concentradores de red, conmutadores, puentes u otros relacionados con equipo podría utilizarse por un atacante poner en peligro el equipo y la red seguridad.

4-9 Bandejas de correo de Intracompany
Política: Intracompany bandejas de correo no se colocarán en las zonas accesibles al público.

Explicación\/notas: Espías industriales o intrusos de equipo que tienen
el acceso a cualquier recogida de correo intracompany puntos pueden enviar fácilmente falsificados
cartas de autorización o formas internas que autorizan personal para liberar
Información confidencial o para realizar acción .un que asiste al atacante.
Además, el atacante puede enviar un disquete o medios electrónicos con
instrucciones para instalar una actualización de software, o abrir un archivo que se ha incorporado la macr
comandos que sirven a los objetivos del intruso. Naturalmente, cualquier solicitud recibida por
correo intracompany se asume que es auténtico por la parte que lo recibe.

4-10 El tablón de anuncios de empresa

Política: no se debe publicado boletines para beneficio de los trabajadores de la empresa
en lugares donde el público tiene acceso.

Explicación\/notas: Muchas empresas tienen tableros donde privado empresa
o se envía información personal para que cualquiera pueda leer. Avisos de empleador,
listas de empleados, memorandos internos, números de contacto Inicio empleados enumerados en el
la Junta con frecuencia se publican anuncios y otra información similar.

Boletines pueden estar situados cerca de cafeterías de la compañía, o muy cerca
fumar o salto de áreas donde los visitantes tienen acceso libre. Este tipo de información
no se hagan a los visitantes o el público.

Entrada de centro de equipo de 4-11
Política: El equipo sala o centro de datos debe ser bloqueado en todo momento y
el personal debe autenticar su identidad antes de escribir.

Explicación\/notas: Seguridad de la empresa debería considerar la implementación de una electrónica
lector de tarjetas insignia o acceso para todas las entradas se pueden registrar electrónicamente y
auditados.

4-12 Cuentas de clientes con los proveedores de servicios
Política: Personal de la empresa que coloca pedidos de servicio con proveedores que ofrecen
servicios críticos para la empresa deben establecer una contraseña de la cuenta para evitar que
personas no autorizadas de pedidos en nombre de la empresa.

Explicación\/notas: Empresas de servicios públicos y muchos otros proveedores permiten a los clientes
configurar una contraseña en la solicitud; la empresa debe establecer contraseñas con todos
proveedores que ofrecen servicios de misión crítica. Esta política es especialmente crítica para
telecomunicaciones y servicios de Internet. Pueden ser cualquier servicios críticos de tiempo

afectados, un secreto compartido es necesario verificar que el llamador está autorizado a colocar tales órdenes. Nota, también, identificadores tales como número de la seguridad social, número de identificación corporativo del contribuyente, apellido materno o identificadores similares deben no deben utilizarse. Un ingeniero social podría, por ejemplo, llamar a la compañía telefónica y dar órdenes para agregar características como llamada reenvío a marcado en líneas de módem o hacer una solicitud al proveedor de servicios de Internet para cambiar la traducción información para proporcionar una dirección IP falsa cuando los usuarios realizan un nombre de host búsqueda.

Persona de contacto de 4-13 departamental
Política: Su empresa puede instituir un programa en virtud de que cada departamento o Grupo de trabajo asigna a un empleado la responsabilidad de actuar como un punto de contacto tan que cualquier personal fácilmente puede verificar la identidad de personas desconocidas que pretenden ser de ese departamento. Por ejemplo, puede comunicarse con la mesa de ayuda el persona punto departamentales para verificar la identidad de un empleado que está solicitando apoyo.

Explicación\/notas: Este método de verificación de identidad reduce el grupo de empleados que están autorizados para atestiguar empleados dentro de su departamento cuando dichos empleados solicitan apoyo tales como el restablecimiento de contraseñas u otros cuestiones relacionadas con la cuenta de equipo.

Ataques de ingeniería social son exitosos, en parte porque soporte técnico personal es presionado por el tiempo y no comprobar correctamente la identidad de solicitantes. Por lo general apoyo personal no puede reconocer personalmente todos autorizados personal debido a la cantidad de empleados en las organizaciones más grandes. El punto-método de la persona de dar fe limita el número de empleados soporte técnico personal que deba estar familiarizado personalmente con fines de verificación.

Contraseñas del cliente de 4-14
Política: Los representantes de servicio al cliente no tendrá la capacidad para recuperar contraseñas de cuentas de cliente.

Explicación\/notas: ingenieros sociales frecuentemente llaman a clientes departamentos de servicio y, con un pretexto, intentar obtener información de autenticación del cliente, como la contraseña o número de seguridad social. Con esta información, la social Ingeniero, a continuación, puede llamar a otro representante de servicio, pretensión que el cliente, y obtener información o realizar pedidos fraudulentos.
Para impedir que estos intentos sucesivos, software de servicio al cliente deberán estar diseñados para que los representantes sólo pueden escribir en la autenticación información proporcionada por el llamador y recibir una respuesta del sistema de indica si la contraseña es correcta o no.

Pruebas de vulnerabilidad de 4-15
Política: Notificación de la empresa utilice tácticas de ingeniería social para probar seguridad vulnerabilidades es necesario durante el empleado y la formación de conciencia de seguridad orientación.

Explicación\/notas: sin notificación de pruebas de penetración de la ingeniería social, personal de la empresa puede sufrir vergüenza, enojo u otros traumas emocionales el uso de tácticas engañosas utilizadas contra ellos por otros empleados o contratistas. Colocando nuevas contrataciones en aviso durante la orientación del proceso pueden ser sometidas a esta prueba, prevención de tales conflictos.

Pantalla de 4-16 de la empresa información confidencial
Política: Información de la empresa no designado para hacerlo público no será aparece en las zonas accesibles al público.

Explicación\/notas: Además de información de producto o procedimiento confidencial, información de contacto interno como teléfono interno o listas de empleados, o creación de listas que contienen una lista de personal de administración para cada departamento dentro de la empresa también debe mantenerse fuera de la vista.

Formación de conciencia de seguridad de 4-17
Política: Todas las personas empleadas por la empresa deben completar una seguridad curso de formación de conciencia durante la orientación del empleado. Además, cada empleado debe tomar un curso de repaso de conciencia de seguridad a intervalos periódicos, no debe exceder de doce meses, según lo requiera el Departamento asignado con responsabilidad de la formación en seguridad.

Explicación\/notas: Muchas organizaciones desatender la formación de conciencia del usuario final en total. Segun el 2001 información seguridad Encuesta Global, sólo 30 por ciento de las organizaciones encuestadas gastar dinero en la formación de la conciencia para su comunidad de usuarios. Formación de conciencia es un requisito esencial para mitigar infracciones de seguridad exitoso utilizando técnicas de ingeniería social.

4-18 Curso de formación de seguridad para el acceso de equipo
Política: El personal debe asistir y completar correctamente una información de seguridad curso antes de ser dado acceso a los sistemas informáticos corporativos.

Explicación\/notas: ingenieros sociales nuevos empleados, conocer destino que como grupo son generalmente las personas menos probables que sea consciente de la las directivas de seguridad de la empresa y los procedimientos apropiados para determinar la clasificación y manejo de información confidencial.

Su formación debe incluir una oportunidad a los empleados para hacer preguntas sobre políticas de seguridad. Después de un entrenamiento, titular de la cuenta deben firmar un documento reconociendo su comprensión de las políticas de seguridad y sus acuerdo para acatar las políticas.

Insignia de 4-19 empleados debe ser codificados por colores
Política: Insignias de identificación deben ser codificados por colores para indicar si la insignia titular es un empleado, contratista, temporal, proveedor, consultor, visitante, o pasante.
Explicación\/notas: El color de la insignia es una excelente manera de determinar el estado de una persona a distancia. Una alternativa sería utilizar grandes letras para indicar el titular de la tarjeta de identificación Estado, pero utilizando una combinación de colo inconfundible y fáciles de ver.

Es una táctica común de ingeniería social para obtener acceso a un edificio físico vestirse como un técnico de persona o reparación de entrega. Una vez dentro de las instalaciones, la atacante será hacerse pasar por otro empleado o mentir sobre su condición para obtener cooperación de empleados confiados. El propósito de esta política es impedir que la gente entrando en el edificio legítimamente y penetrar en zonas no deben tener acceso a. Por ejemplo, una persona entrando en el fondo como un técnico de reparaciones de teléfono no sería capaz de hacerse pasar por un empleado: el color de la insignia le daría lejos.

POLÍTICAS DE TECNOLOGÍAS DE LA INFORMACIÓN
El departamento de tecnología de información de cualquier empresa tiene una necesidad especial las políticas que ayudarle a protegen los activos de información de las organizaciones. Para reflejar la estructura típica de las operaciones de TI de una organización, he dividido la TI políticas en General, Help Desk, administración de equipo y equipo Operaciones.

General
Información contacto de empleado de departamento de TI de 5-1
Política: Direcciones de correo electrónico y números de teléfono de cada departamento de TI empleados no deben ser divulgados a cualquier persona sin necesidad de saber.

Explicación\/notas: El propósito de esta política es evitar que la información de contacto de ser maltratado por los ingenieros sociales. Por sólo revelar un contacto general número o correo electrónico, se bloquearán los forasteros de ponerse en contacto con lo personal de departamento directamente. La dirección de correo electrónico del sitio administrativo y contactos técnicos sólo debe consisten en genérico nombres como admin@CompanyName.com; publicado teléfono números deben conectarse a un buzón de voz departamental, no a los trabajadores individuales.

Cuando hay disponible información de contacto directa, es fácil para un equipo intruso para llegar a empleados de TI específicos y engañar que proporciona información que puede utilizarse en un ataque, o para hacerse pasar por empleados de TI mediante el uso de sus los nombres e información de contacto.

Solicitudes de soporte técnico de 5-2
Política: Todas las solicitudes de asistencia técnica deben remitirse al grupo que controla esas solicitudes.

Explicación\/notas: ingenieros sociales pueden intentar dirigir al personal de TI que hacen normalmente no manejar problemas de soporte técnico, y que no sea consciente de la procedimientos de seguridad adecuados cuando dichas solicitudes. En consecuencia, el personal de TI debe estar formado para negar estas solicitudes y el llamador se refieren al grupo que ha la responsabilidad de proporcionar apoyo.

Mesa de ayuda
Procedimientos de acceso remoto de 6-1
Política: Personal del servicio de ayuda no debe divulgar detalles o instrucciones con respecto a acceso remoto, incluyendo números de acceso telefónico, o puntos de acceso de red externa a menos que el solicitante ha sido:

Verificado como autorizado para recibir información interna; y,

Verificado como autorizado para conectarse a la red corporativa como un usuario externo.
A menos que se conoce sobre una base de persona a persona, el solicitante debe ser positiva identificados de conformidad con la verificación y procedimientos de autorización se indica al principio de este capítulo.

Explicación\/notas: La mesa de ayuda corporativa es a menudo un objetivo principal para la ingeniero social, porque la naturaleza de su trabajo es ayudar a los usuarios con cuestiones relacionadas con la informática, y debido a generalmente han elevado sistema privilegios. Todo el personal de recepción ayuda deberá recibir una formación para actuar como un serv prevenir la divulgación no autorizada de información que ayudará a cualquier no autorizado personas que obtengan acceso a recursos de la empresa. La regla simple es nunca divulgar los procedimientos de acceso remoto a nadie hasta la verificación positiva de la identidad se ha hecho.

Contraseñas de restablecimiento de 6-2
Política: La contraseña para una cuenta de usuario puede reiniciarse sólo a petición de la titular de la cuenta.

Explicación\/notas: La estratagema más comunes utilizada por los ingenieros sociales es tener contraseña de cuenta de otra persona restablecer o cambiado. El atacante se hace pasar por el

empleado con el pretexto de que su contraseña fue perdido u olvidado. En un esfuerzo para reducir el éxito de este tipo de ataque, un empleado de TI recibir una solicitud de debe llamar a restablecer una contraseña empleado antes a realizar ninguna acción; el llama de regreso no debe hacerse a un número de teléfono proporcionado por el solicitante, sino a una número obtenido el directorio telefónico de empleados. Consulte verificación y Procedimientos de autorización para obtener más información acerca de este procedimiento.

Privilegios de acceso de cambio de 6-3
Política: Todas las solicitudes para aumentar los privilegios del usuario o los derechos de acceso deben ser aprobado por escrito por el administrador del titular de la cuenta. Cuando el cambio se realiza un confirmación debe enviarse al administrador solicitante vía correo intracompany. Además, dichas solicitudes deben verificarse como auténticos de conformidad con el Verificación y procedimientos de autorización.

Explicación\/notas: Una vez que un intruso de equipo ha comprometido un usuario estándar cuenta, el siguiente paso es elevar sus privilegios por lo que el atacante tiene control total sobre el sistema comprometido. Un atacante que tiene conocimiento de la autorización de proceso puede simular una solicitud autorizada al correo electrónico, fax, o teléfono sirven para transmitirlo. Por ejemplo, el atacante puede teléfono técnica apoyo o la mesa de ayuda y intento de persuadir a un técnico para otorgar adicionales derechos de acceso a la cuenta del peligro.

Autorización de cuenta nueva de 6-4
Política: Una petición para crear una cuenta nueva para un empleado, contratista, o persona autorizada debe ser hecha ya sea por escrito y firmado por el Gestor del empleado, o enviado por correo electrónico firmado digitalmente. Estas solicitudes También debe verificarse mediante el envío de una confirmación de la solicitud a través de intracompany correo.

Explicación\/notas: Porque las contraseñas y otra información útil para romper en equipo, los sistemas son los más altos objetivos prioritarios de ladrones de información para para acceder, precauciones especiales son necesarias. La intención de esta política es para impedir que los intrusos equipo suplantando autorizado personal o forja solicitudes para nuevas cuentas. Por lo tanto, todas estas solicitudes deben ser positivamente verificado mediante la verificación y procedimientos de autorización.

6-5 Entrega de nuevas contraseñas
Política: Nuevas contraseñas deben manejarse como empresa de información confidencial, entregado por métodos seguros incluidos en persona; por una entrega de firmas necesarias servicio como correo certificado; o por UPS o FedEx. Ver las políticas relativas a distribución de la información confidencial.

Explicación\/notas: Correo Intracompany también puede utilizarse, pero se recomienda que las contraseñas se envían en sobres seguros que oscurecen el contenido. Una propuesta método consiste en establecer una persona punto de equipo en cada departamento que tiene el responsabilidad de controlar la distribución de nuevos detalles de la cuenta y dar fe la identidad del personal que pierde u olvida su contraseña. En estos circunstancias, personal de apoyo estaría siempre trabajando con un grupo menor de empleados que reconocería personalmente.

6-6 Deshabilitar una cuenta
Política: a la desactivación de una cuenta de usuario debe necesita verificación positiva que la solicitud fue hecha por personal autorizado.

Explicación\/notas: La intención de esta política es evitar que un atacante suplantación de una solicitud para deshabilitar una cuenta y, a continuación, llamar a solucionar la incapacidad del usuario para acceder al sistema de equipo. Cuando llama el ingeniero social haciéndose pasar por un técnico con conocimientos preexistentes de incapacidad del usuario para iniciar se en, la víctima a menudo cumple con una solicitud para revelar su contraseña durante el proceso de solución de problemas.

Deshabilitar puertos de red o dispositivos de 6-7
Política: Ningún empleado debe deshabilitar cualquier puerto o dispositivo de red para cualquier personal de soporte técnico sin verificar.

Explicación\/notas: La intención de esta política es evitar que un atacante simulación de una solicitud para deshabilitar un puerto de red y, a continuación, llamar al trabajador solucionar problemas de su propia incapacidad para acceder a la red.

Cuando el ingeniero social, haciéndose pasar por un técnico útil, llama con preexistentes 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 procedimientos para el acceso inalámbrico
Política: Ningún personal debe revelar los procedimientos para acceder a los sistemas de la empresa través de redes inalámbricas a partes no autorizadas para conectar con el wireless red.

Explicación\/notas: Siempre obtener verificación previa de un solicitante como una persona autorizados a conectarse a la red corporativa como un usuario externo antes de Liberación de información de acceso inalámbrico. Consulte verificación y autorización Procedimientos.

6-9 Tickets de problemas de usuario

Política: Los nombres de los empleados que han reportado relacionadas con la informática problemas no deben ser revelados fuera del departamento de tecnología de información.

Explicación\/notas: En un ataque típico, un ingeniero social llamará la Mesa de ayuda y pedir los nombres de cualquier personal que ha reportado recientes problemas del equipo. El llamador puede pretender ser un empleado, proveedor, o un empleado de la compañía telefónica. Una vez que obtiene los nombres de las personas informes de problemas, el ingeniero social, haciéndose pasar por una mesa de ayuda o soporte técnico persona, contacta con el empleado y dice que está llamando para solucionar el problema. Durante la llamada, el atacante engaña a la víctima en proporcionar la desea información o en realizar una acción que facilite el atacante objetivo.

6-10 Iniciación ejecutar comandos o programas en ejecución
Política: El personal empleado en el departamento de TI que han privilegiado las cuentas no debe ejecutar todos los comandos o ejecutar los programas de aplicación a petición de cualquier persona conocida no personalmente a ellos.

Explicación\/notas: Un uso común de los atacantes de método para instalar un troyano programa u otro software malintencionado es cambiar el nombre de una existente programa y entonces llamada quejándose de mesa de ayuda que es un mensaje de error aparece cuando se intenta ejecutar el programa. El atacante persuade al técnico de mesa de ayuda para ejecutar el programa en sí mismo. Cuando el técnico cumple, el software malintencionado hereda los permisos del usuario ejecutar el programa y realiza una tarea, que da el atacante igual privilegios de equipo como el empleado de mesa de ayuda. Esto puede permitir al atacante tomar el control del sistema del empresa.
Esta política establece una contramedida a esta táctica, que requieren que el apoyo personal verifica el estado de empleo antes de ejecutar cualquier programa a petición un llamador.

Administración de equipo
Cambio global de 7-1 los derechos de acceso
Política: Una solicitud para cambiar los derechos de acceso global asociados con una electrónica Perfil de trabajo debe ser aprobado por el grupo asignado la responsabilidad de gestión de los derechos de acceso de la red corporativa.

Notas de la explicación: el personal autorizado analizará cada solicitud que determinar si el cambio podría implicar una amenaza para la seguridad de la información. Si es así, el responsable ocupará de las cuestiones pertinentes con el solicitante y conjuntamente, llegar a una decisión sobre los cambios a realizarse.

Solicitudes de acceso remoto de 7-2
Política: Solamente se proporcionará acceso remoto computadora personal que tienen un demostrada la necesidad de acceder a sistemas informáticos corporativos desde lugares remotos. La solicitud debe ser hecha por el administrador del empleado y verificada como se describe en la sección de verificación y procedimientos de autorización.

Explicación\/notas: Reconociendo la necesidad de acceso externo en la empresa red por personal autorizado, limitar dicho acceso sólo a las personas con una necesidad puede reducir drásticamente riesgo y gestión de usuarios de acceso remoto. El menor el número de personas con acceso telefónico externo privilegios, cuanto menor sea la Piscina de posibles objetivos para un atacante. Nunca olvidar que el atacante también puede los usuarios remotos con la intención de secuestrar su conexión en el corporativo de destino la red, o haciéndose pasar como ellos durante un pretexto por llamar.

Contraseñas de cuentas de restableciendo el privilegio de 7-3
Política: Una solicitud para restablecer una contraseña para una cuenta con privilegios debe ser aprobada por el administrador del sistema o el administrador responsable de equipo en el que existe la cuenta. La nueva contraseña debe enviarse por correo intracompany o entrega en persona.

Explicación y notas\". Las cuentas con privilegios tienen acceso a todos los recursos de sistema y archivos almacenados en el sistema informático. Naturalmente, estas cuentas merecen la mayor protección posible.

7-4 Fuera de acceso remoto del personal de apoyo
Política: No fuera persona de apoyo (tales como proveedor de software o hardware personal) puede darse cualquier información de acceso remoto o estar permitido el acceso a cualquier sistema informático de empresa o dispositivos relacionados sin verificación positiva de identidad y autorización para realizar dichos servicios. Si el proveedor requiere acceso privilegiado para proporcionar servicios de apoyo, la contraseña para la cuenta utilizada el proveedor deberá cambiarse inmediatamente después de que el servicios de proveedor ha sido completado.

Explicación\/notas: Los atacantes del equipo pueden plantear como proveedores para obtener acceso a redes corporativas de equipo o de telecomunicaciones. Por lo tanto, es esencial que verificar la identidad del proveedor además de su autorización para realizar cualquier trabajo en el sistema. Además, deben ser de golpe las puertas en el sistema cerrar una vez que su trabajo es hecho por cambiar la contraseña de la cuenta utilizada por el proveedor.

Ningún proveedor debe poder elegir su propia contraseña de cualquier cuenta, incluso temporalmente. Algunos proveedores han sido conocidos por utilizar la misma o similar contraseñas en múltiples sistemas de cliente. Por ejemplo, seguridad de una red

empresa configura cuentas con privilegios en los sistemas de sus clientes con el mismo contraseña y para añadir insulto a la injuria, con acceso exterior de Telnet activado.

Autenticación segura de 7-5 para el acceso remoto a sistemas corporativos
Política: Los puntos de conexión en la red corporativa desde ubicaciones remotas debe protegerse mediante el uso de dispositivos de autenticación fuerte, tales como contraseñas dinámicas o biometría.

Explicación\/notas: Muchas empresas dependen de contraseñas estáticas como el único medio de autenticación para usuarios remotos. Esta práctica es peligrosa porque es inseguridad: intrusos equipo destino cualquier punto de acceso remoto que puede ser la eslabón débil en la red de la víctima. Recuerde que nunca se sabe cuándo alguien sabe la contraseña.

En consecuencia, se deben proteger los puntos de acceso remoto con fuerte autenticación como símbolos basados en el tiempo, las tarjetas inteligentes o dispositivos biométricos, po que las contraseñas interceptadas son de ningún valor para un atacante.

Cuando la autenticación basada en contraseñas dinámicas es impracticable, los usuarios de computadoras religiosamente debe adherirse a la política para elegir contraseñas difíciles de adivinar.

Configuración del sistema operativo 7-6
Política: Los administradores de sistemas velará por que, siempre que sea posible, de funcionamiento los sistemas están configurados para que sean coherentes con toda seguridad pertinente políticas y procedimientos.

Explicación\/notas: Elaboración y distribución de las políticas de seguridad son un fundamental paso hacia la reducción del riesgo, pero en la mayoría de los casos, cumplimiento necesariamente queda ha el empleado individual. Hay, sin embargo, cualquier número de informáticos políticas que se pueden hacer obligatorias a través de la configuración del sistema operativo, tales como la longitud requerida de contraseñas. Automatizar las políticas de seguridad de configuración de parámetros de sistema operativo efectivamente toma la decisión de los humanos manos del elemento, aumentar la seguridad general de la organización.

Caducidad obligatoria de 7-7
Política: Todas las cuentas de equipo deben establecerse a punto de caducar después de un año.

Explicación\/notas: La intención de esta política es eliminar la existencia de cuentas de equipo que ya no se utilizan, desde intrusos de equipo comúnmente latentes cuentas de destino. El proceso asegura a cualquier equipo cuentas pertenecientes a ex empleados o contratistas que han sin darse cuenta dejó en su lugar se desactivan automáticamente.

A discreción de la administración, podrá exigir que los empleados deben tener una seguridad cursos de repaso del curso en el momento de la renovación, o debe revisar la seguridad de la información políticas y firmar un acuse de recibo de su acuerdo a que se adhieran a ellos.

Direcciones de correo electrónico genérico de 7-8
Política: El departamento de tecnología de la información establecerá un correo genérico dirección para cada departamento dentro de la organización que ordinariamente se comunica con el. público.

Explicación\/notas: La dirección de correo electrónico genérico puede ser lanzada al público por la recepcionista de teléfono o publicado en el sitio de Web de la empresa. De lo contrario, cada empleado sólo deberá revelar su dirección de correo electrónico personal a personas que tiene verdadera necesidad de saber.

Durante la primera fase de un ataque de ingeniería social, el atacante a menudo intenta obtener números de teléfono, nombres y títulos de los empleados. En la mayoría de los casos, esto información está disponible públicamente en el sitio Web de empresa o simplemente por la pregunta. Creación de buzones de voz genérica o direcciones de correo electrónico hace que sea difícil asociar nombres de empleados con responsabilidades o departamentos particulares.

Información de contacto de 7-9 para registros de dominio
Política: Cuando se registra para la adquisición de espacio de direcciones de Internet o nombres de host, la información de contacto administrativo, técnico u otros personal no debería identificar a cualquier personal individual por su nombre. En su lugar, le debe poner una dirección de correo electrónico genérico y el número de teléfono principal corporativa.

Explicación\/notas: El propósito de esta política es evitar que la información de contacto de ser abusado por un intruso de equipo. Cuando los nombres y números de teléfono de los individuos son siempre, un intruso puede utilizar esta información para ponerse en contacto con el individuos e intentar engañarles para que revelen información del sistema, o a realizar un elemento de acción que facilita el objetivo del atacante. O lo social ingeniero puede suplantar a una persona enumerada en un esfuerzo por engañar a otra empresa personal.
En lugar de una dirección de correo electrónico a un empleado en particular, la información de contacto debe ser en forma de administrator@company.com. Telecomunicaciones personal del departamento puede establecer un buzón de voz genérica para administrativo o contactos técnicos para limitar la divulgación de información que sería útil en un ataque de ingeniería social.

7-10 Instalación de actualizaciones de seguridad y sistema operativo
Política: Todos los parches de seguridad para el sistema operativo y software de aplicación serán instalarse tan pronto como estén disponibles. Si esta política entra en conflicto con la

funcionamiento de los sistemas de misión crítica producciones, dichas actualizaciones deben ser lleva a cabo tan pronto como sea posible.

Explicación\/notas: Una vez que se ha detectado una vulnerabilidad, el software fabricante debe ser contactado inmediatamente para determinar si un parche o una solución temporal ha sido a disposición de cerrar la vulnerabilidad. Un sistema informático un-patched representa uno de los mayor seguridad amenazas para la empresa. Cuando los administradores del sistema pereza sobre aplicar las correcciones necesarias, está abierta la ventana de exposición tan amplia que ningún atacante puede subir a través de.

Docenas de vulnerabilidades de seguridad se identifican y publicados semanalmente en la Internet. Hasta personal de tecnología de información esté vigilante en sus esfuerzos por aplicar toda la seguridad y parches lo antes posible, a pesar de estos sistemas están detrás del firewall de la empresa, la red corporativa siempre estará en riesgo de sufre un incidente de seguridad. Es extremadamente importante mantener informada de vulnerabilidades de seguridad publicados identificadas en el sistema operativo o cualquier programas de aplicación utilizados durante el curso del negocio.

Información de contacto de 7-11 en sitios Web
Política: Sitio Web externo de la compañía no divulgarán ningún detalle de las empresas estructura o identificar a los empleados por su nombre.

Explicación\/notas: Información de estructura empresarial, como organigramas, gráficos de jerarquía, empleado o listas departamentales, informes de estructura, nombres, posiciones, números de contacto internos, número de empleados o información similar que se utiliza para procesos internos no se hagan en público sitios Web accesibles.

Los intrusos de equipo a menudo obtienen información muy útil sobre el sitio de Web de destino. El atacante utiliza esta información para que aparezca como un empleado conocedor de 206 Cuando se utiliza un pretexto o una treta. El ingeniero social es más probable que establecer credibilidad al tener esta información a su disposición.
Por otra parte, el atacante puede analizar esta información para averiguar los objetivos probables que tengan acceso a información valiosa, sensible o crítico.

7-12 Creación de cuentas con privilegios
Política\". No debe crearse ninguna cuenta privilegiada o sistema privilegios otorgados a cualquier cuenta salvo autorización por el administrador del sistema o el administrador del sistema.

Explicación y notas\". Los intrusos equipo plantean frecuentemente como hardware o software proveedores en un intento de dpdo personal de tecnología de información en la creación de cuentas no autorizadas. La intención de esta política es bloquear estos ataques por

establecer un mayor control sobre la creación de cuentas con privilegios. El sistema Administrador o administrador del sistema debe aprobar cualquier solicitud de crear una cuenta con privilegios elevados.

Cuentas de invitado de 7-13
Política: Las cuentas de invitado en los sistemas informáticos o relacionados conexos dispositivos de red será desactivado o eliminado, excepto para un servidor FTP (file transfer protocol) aprobados por la gerencia con habilitado el acceso anónimo.

Explicación\/notas: La intención de la cuenta de invitado es proporcionar temporal acceso para personas que no necesitan tener su propia cuenta. Varios operativos sistemas se instalan de forma predeterminada con una cuenta de invitado habilitada. Cuentas de invitado siempre debe estar deshabilitada porque su existencia viola el principio de usuario rendición de cuentas. Debe ser capaz de cualquier actividad relacionada con el equipo de auditoría y se re que a un usuario específico.

Los ingenieros sociales son fácilmente capaces de tomar ventaja de estas cuentas de invitado para obtener acceso no autorizado, ya sea directamente o por timar autorizado personal en uso de una cuenta de invitado.

7-14 El cifrado de datos de copia de seguridad fuera del sitio
Política: Los datos de la empresa que se almacenan fuera del sitio deben estar cifrados para evitar acceso no autorizado.

Explicación\/notas: Personal de operaciones debe asegurar que los datos son recuperables en el evento que cualquier información necesita ser restaurada. Esto requiere prueba regular descifrado de un muestreo aleatorio de archivos cifrados para asegurarse de que los datos puede ser recuperado. Además, las claves utilizadas para cifrar los datos deberán ser escrowed con un Administrador de confianza en el evento las claves de cifrado se pierde o no está disponible.

Acceso de visitantes de 7-15 para las conexiones de red
Política: Todos los puntos de acceso Ethernet públicamente accesibles deben estar en un segmentado red para impedir el acceso no autorizado a la red interna.

Explicación\/notas: La intención de esta política es evitar a cualquier foráneos de conexión a la red interna cuando en instalaciones de la empresa. Conectores de Ethernet instalado en salas de conferencias, la cafetería, centros de capacitación u otras áreas accesible a los visitantes será filtrados para impedir el acceso no autorizado por los visitantes los sistemas informáticos corporativos.

El administrador de red o de seguridad, puede configurar un virtual LAN en un switch, si está disponible, para controlar el acceso de estas ubicaciones.

Módems de acceso telefónico de 7-16
Política: Los módems para acceso telefónico llamadas se fijará para responder no antes que el cuarto anillo.

Explicación\/notas: Como se muestra en la película juegos de guerra, los piratas informáticos utilizan un técnica conocida como Guerra de marcado para localizar líneas telefónicas que tienen módems conectados a ellos. El proceso comienza con el atacante identificar el teléfono prefijos utilizados en el área donde se encuentra la compañía de destino. Un análisis programa se utiliza para tratar cada número de teléfono en los prefijos, para localizar aquellos que responden con un módem. Para acelerar el proceso, estos programas son configurado para esperar uno o dos anillos para una respuesta de módem antes de ir a Pruebe el siguiente número. Cuando una empresa establece la respuesta automática en las líneas de móde menos cuatro anillos, programas de análisis no reconocer la línea como un módem línea.

Software antivirus 7-17
Política: Cada equipo tendrá versiones actuales del software antivirus instalado y activado.

Explicación\/notas: para aquellas empresas que no empuje automáticamente hacia abajo archivos antivirus de patrón y software (programas que reconocen patrones comunes a software antivirus para reconocer nuevos virus) a los escritorios de los usuarios estaciones de trabajo, usuarios individuales deben asumir la responsabilidad de instalar y mantener el software en sus propios sistemas, incluidos cualquier equipo utilizado para acceso a la red corporativa remotamente.

Si es posible, debe establecerse este software de actualización automática de virus y troyanos firmas por la noche. Cuando moscas patrón o firma no son empujados hacia abajo al usuario computadoras de escritorio, los usuarios de computadoras tendrán la responsabilidad para actualizar arch menos semanalmente.

Estas disposiciones se aplican a todas las máquinas de escritorio y equipos portátiles que utilizan para acc sistemas informáticos de la empresa y se aplican si el equipo es empresa propiedad o propiedad personalmente.

Adjuntos de correo electrónico entrantes de 7-18 (requisitos de alta seguridad)
Política: en una organización con requisitos de alta seguridad, el firewall corporativo deberá configurarse para filtrar todos los adjuntos de correo electrónico.

Explicación\/notas: Esta política se aplica sólo a las empresas con alta seguridad requisitos, o a aquellos que no tienen ningún negocio que deba recibir adjuntos a través de correo electrónico.

7-19 Autenticación de software
Política: Todo nuevo software o soluciones de software o actualizaciones, si en física
medios de comunicación o obtenida a través de Internet, deben verificarse como auténticos antes
instalación. Esta política es especialmente relevante para la tecnología de la información
Departamento al instalar cualquier software que requiera privilegios de sistema.

Explicación y notas: Incluyen programas informáticos mencionados en esta política
componentes del sistema operativo, software de aplicación, correcciones, revisiones o cualquier
actualizaciones de software. Muchos fabricantes de software han implementado métodos
según la cual los clientes pueden comprobar la integridad de cualquier distribución, generalmente por un
firma digital. En cualquier caso donde la integridad no puede verificarse, el
fabricante debe ser consultado para verificar que el software es auténtico.

Los atacantes del equipo han llegado a enviar el software a una víctima, envasada para
parece como si el fabricante del software había producido y enviado a la
empresa. Es imprescindible que verifique cualquier software que recibe como auténticos,
especialmente si no solicitados, antes de instalar en los sistemas de la empresa.
Tenga en cuenta que un atacante sofisticado podría averiguar que su organización ha
software ordenado de un fabricante. Con esa información en mano, el atacante
puede cancelar el pedido al fabricante real y ordenar el software mismo.
El software entonces se modifica para realizar alguna función malintencionado y se envía
o entregados a su empresa, en su embalaje original, con si paletización
es necesario. Una vez instalado el producto, el atacante está en control.

Contraseñas predeterminadas de 7-20
Política: Todos operan los dispositivos de hardware y software de sistema que inicialmente
tienen un conjunto de contraseña en un valor predeterminado debe tener sus contraseñas restablecer en
conformidad con la Directiva de contraseñas de la empresa.

Explicación y notas: Son varios sistemas operativos y dispositivos informáticos
acompaña las contraseñas por defecto--es decir, con la misma contraseña activada
cada unidad vendida. Fracaso para cambiar la contraseña predeterminada es un grave error que coloca
la empresa en situación de riesgo.
Contraseñas predeterminadas son ampliamente conocidas y están disponibles en la Web de Internet
sitios. En un ataque, la primera contraseña que un intruso intenta es el valor por defecto de fabricante s
contraseña.

Bloqueo (bajo a nivel de seguridad medio) de intentos de acceso no válido de 7-21
Política: especialmente en una organización con bajos requerimientos de seguridad media,
siempre un número especificado de inicio de sesión no válido sucesivo intentos a un determinado
se han hecho la cuenta, la cuenta debe ser bloqueada por un período de tiempo.

Explicación\/notas: Todos los servidores y estaciones de trabajo de empresa deben establecer

para limitar el número de inválidos sucesivos intentos iniciar sesión en. Esta política es necesarias para impedir la contraseña adivinando por ensayo y error, los ataques de diccionario, o fuerza bruta intenta obtener acceso no autorizado.

El administrador del sistema debe establecer la configuración de seguridad para bloquear un cuenta siempre ha sido el umbral deseado de sucesivos intentos no válidos alcanzado. Se recomienda que se bloquee una cuenta de al menos treinta minutos después de siete intentos sucesivos de inicio de sesión.

Cuenta deshabilitada (alta seguridad) de intentos de acceso no válido de 7-22
Política: en una organización con requisitos de alta seguridad, siempre que un especificado número de intentos de inicio de sesión no válidas sucesivas en una cuenta determinada ha sido hecho, la cuenta debe deshabilitar hasta restablecer por el grupo responsable cuenta de apoyo.

Explicación\/notas: Todos los servidores y estaciones de trabajo de empresa deben establecerse para limit número de sucesivos intentos no válidos para iniciar sesión. Esta política es necesaria control para prevenir la contraseña adivinando por ensayo y error, los ataques de diccionario, o fuerza bruta intenta obtener acceso no autorizado.

El administrador del sistema debe establecer la configuración de seguridad para desactivar el cuenta después de cinco intentos de inicio de sesión no válido. Tras este ataque, la cuenta titular será necesario llamar al soporte técnico o el grupo responsable de cuenta soporte para habilitar la cuenta. Antes de restablecer la cuenta, el departamento responsable debe identificar positivamente la cuenta titular, siguiendo el Verificación y procedimientos de autorización.

7-23 Cambio periódico de privilegios
Política: Todos los titulares de la cuenta con privilegios deberán cambiar sus contraseñas por lo menos cada treinta días.

Explicación\/notas: dependiendo de las limitaciones del sistema operativo, los sistemas administrador debe imponer esta política por la configuración de parámetros de seguridad software del sistema.

7-24 Periódico cambio de contraseñas de usuario
Política: Todos los titulares de cuentas deben cambiar sus contraseñas al menos cada sesenta días.

Explicación\/notas: con sistemas operativos que ofrecen esta característica, los sistemas administrador debe imponer esta política por la configuración de parámetros de seguridad el software.

7-25 Nueva contraseña de la cuenta configurar
Política: Nuevas cuentas de equipo deben establecerse con una contraseña inicial que es pre-expired, que requieren de la titular de la cuenta seleccionar una nueva contraseña a inicial utilizar.

Explicación\/notas: Este requisito asegura que será sólo el titular de la cuenta tener conocimiento de su contraseña.

Contraseñas de inicio de 7-26
Política: Todos los sistemas informáticos deben configurarse para solicitar una contraseña de arranque.

Explicación\/notas: Los equipos deben configurarse para que cuando el equipo está activado, es necesaria una contraseña antes de que se iniciará el sistema operativo. Esto impide que a 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.

7-27 Requisitos de contraseña para cuentas con privilegios
Política: M1 el privilegio de cuentas deben tener una contraseña segura: la contraseña debe:
No se encuentra una palabra en un diccionario en cualquier idioma
Ser mixto mayúsculas y minúsculas con al menos una letra, un símbolo y una numeral
Tener al menos 12 caracteres de longitud
No estar relacionados a la empresa o individuo de ninguna manera.

Explicación\/notas: En la mayoría de los casos los intrusos equipo tendrá como objetivo cuentas específica tiene privilegios de sistema. Ocasionalmente otros aprovecharán el atacante vulnerabilidades para obtener el control total sobre el sistema.

Las contraseñas primeras que intruso tratará son las palabras simples, utilizadas se encuentra en un diccionario. Selección de contraseñas seguras mejora la seguridad por reducir la posibilidad de un atacante encontrará la contraseña por ensayo y error, ataque de diccionario, o ataque de fuerza bruta.

7-28 Puntos de acceso inalámbrico
Política: Todos los usuarios que acceden a una red inalámbrica deben utilizar VPN (Virtual Private Tecnología de red) para proteger la red corporativa.

Explicación\/notas: Redes inalámbricas están siendo atacadas por una nueva técnica llamado de conducción de la guerra. Esta técnica consiste en simplemente conduciendo o caminando con un portátil equipado con un 802. 11b tarjeta NIC hasta que una red inalámbrica detectado.

Muchas empresas han implementado redes inalámbricas sin incluso habilitar WEP (inalámbricas Protocolo de equivalencia), que se utiliza para asegurar la conexión inalámbrica mediante el uso de cifrado. Pero incluso cuando se activa, la versión actual de WEP (mediados de 2002) es ineficaz: ha sido craqueada abierto y varios sitios Web se dedican a proporcionar los medios para localizar sistemas inalámbricos abiertos y craqueo puntos de acceso inalámbrico WEP activado.

En consecuencia, es esencial para añadir una capa de protección alrededor de la 802. 11b protocolo mediante la implementación de la tecnología VPN.

7-29 Archivos de antivirus de patrón de actualización
Política: Cada equipo debe programarse para actualizar automáticamente archivos de patrones de antivirus y anti-Trojan.

Explicación y notas: Como mínimo, dichas actualizaciones se producen al menos semanalmente. En las empresas donde los empleados abandonar sus equipos activada, se 302 es altamente archivos de patrones se recomienda actualizar noches.

El software antivirus es ineficaz si no se actualiza para detectar todas las formas nuevas de código malicioso. Desde la amenaza de virus, gusano y troyano infecciones es aumentado considerablemente si no se actualizan los archivos de patrones, es esencial que antivirus o productos de código malicioso se mantenga actualizada.

Operaciones de equipo
8-1 Entrando comandos o programas en ejecución
Política.: Personal de operaciones del equipo no debe introducir comandos o ejecutar programas a petición de cualquier persona que no conocida a ellos. Si surge una situación Cuando una persona no parece tener razón para hacer tal solicitud, se no debe ser cumplido con sin primero obtener aprobación del administrador.

Explicación \/ notas.: empleados de operaciones del equipo son populares destinos de sociales ingenieros, desde sus posiciones normalmente requieren cuenta con privilegios de acceso y la atacante espera que van a ser menos experimentados y menos conocedor de procedimientos de la empresa que otros trabajadores de TI. La intención de esta política es agregar una verificación adecuada y equilibrio para evitar que los ingenieros sociales timar personal de operaciones del equipo.

8-2 Trabajadores con cuentas con privilegios
Política: Los empleados con cuentas con privilegios no deben proporcionar asistencia o información a cualquier persona sin verificar. En particular se refiere a no proporcionar ayuda de equipo (como la capacitación sobre el uso de la aplicación), acceder a cualquier empresa base de datos, descarga de software, o revelar nombres de personal que tienen capacidades de acceso remoto,

Explicación\/notas: ingenieros sociales dirigidas a menudo empleados con privilegios
cuentas. La intención de esta política es para dirigirla personal con cuentas con privilegios
manejar correctamente las llamadas que pueden representar los ataques de ingeniería sociales.

Información de sistemas internos de 8-3
Política: Personal de operaciones del equipo nunca debe revelar cualquier información relacionada con
sistemas informáticos de empresa o dispositivos relacionados sin comprobar positivamente la
identidad del solicitante.

Explicación\/notas: Intrusos equipo con con frecuencia operaciones de equipo
empleados para obtener información valiosa, como sistema de procedimientos de acceso,
acceso remoto y números de teléfono marcado de puntos externos
valor sustancial al atacante.

En las empresas que tienen personal de soporte técnico o un help desk, pide
para el personal de operaciones del equipo para obtener información acerca de sistemas informáticos o
dispositivos relacionados deben considerarse inusuales. Cualquier solicitud de información debe ser
examinada bajo la política de clasificación de datos de la empresa para determinar si
el solicitante está autorizado a disponer de dicha información. Cuando la clase de
no se puede determinar la información, la información debe considerarse
Interna.

En algunos casos, fuera proveedor de asistencia técnica tendrá que comunicarse con
personas que tienen acceso a sistemas de computación de la empresa. Los proveedores deben tener
específica de contactos en el departamento de TI para que pueden reconocer a aquellos individuos
entre sí para fines de verificación.

8-4 Divulgación de contraseñas
Política: Personal de operaciones del equipo nunca debe revelar su contraseña, o
cualquier otras contraseñas que se les encargados, sin aprobación previa de una información
Director de tecnología.

Explicación\/notas: en general, revelar ninguna contraseña a otro es estrictamente
prohibido. Esta política reconoce que el personal de operaciones deba revelar
una contraseña a un tercero cuando surgen situaciones exigentes. Esta excepción a la
la política general que prohíbe la divulgación de cualquier contraseña requiere aprobación específica
un administrador de tecnología de la información. Por medida de precaución adicional, esta responsabilida
divulgar información de autenticación debe limitarse a un pequeño grupo de
personas que han recibido capacitación especial sobre los procedimientos de verificación.

Medios electrónicos de 8-5
Política: Los medios electrónicos que contiene información no destinada al público
lanzamiento será bloqueado en una ubicación físicamente segura.

Explicación\/notas: La intención de esta política es evitar el robo físico de
Información confidencial almacenada en medios electrónicos.
Medios de copia de seguridad de 8-6
Política: El personal de operaciones debe almacenar medios de backup en una compañía de segura o
otra ubicación segura.

Explicación\/notas: Medios de copia de seguridad son otro objetivo principal de los intrusos del equipo.
Un atacante no va a gastar tiempo tratando de poner en peligro un equipo
sistema o red cuando el eslabón en la cadena podría ser físicamente
medios de backup sin protección. Una vez que los medios de backup es robado, el atacante puede
poner en peligro la confidencialidad de los datos almacenados en él, salvo que los datos
cifrado. Por lo tanto, asegurar físicamente los medios de backup es un proceso fundamental para
proteger la confidencialidad de la información corporativa.

POLÍTICAS PARA TODOS LOS EMPLEADOS
En ella o en recursos humanos, el departamento de contabilidad, o el
personal de mantenimiento, hay ciertas políticas de seguridad que cada empleado de su
empresa debe saber. Estas políticas dividen en las categorías de General, equipo
Uso, uso de correo electrónico, las políticas para teletrabajadores, uso, uso de Fax, correo de voz por telé
Uso y las contraseñas.

General
9-1 Informes llamadas sospechosas
Política: Empleados que sospechan que pueden ser objeto de una seguridad
violación, incluyendo las solicitudes sospechosas para divulgar la información o para realizar
elementos de acción en un equipo, debe informar inmediatamente el evento para la empresa
Grupo de informe de incidente.

Explicación \/ notas.: cuando falla un ingeniero social convencer a su destino a
cumplir con una demanda, el atacante siempre tratará de alguien. Por informes de un
llamada sospechosa o evento, un empleado toma el primer paso para alertar a la empresa
que un ataque podría estar en marcha. Por lo tanto, los empleados individuales son la primera línea de
defensa contra ataques de ingeniería social.

9-2 Documentación llamadas sospechosas

Política: en caso de una llamada sospechosa que parece ser una social
ataque de ingeniería, el empleado deberá, a la medida de lo práctico, extraer el llamador
para conocer detalles que podrían revelar lo que el atacante está intentando llevar a cabo,
y tomar nota de estos detalles para generar informes.

Explicación\/notas: Cuando informó al grupo informes de incidente, tales detalles puede ayudar a detectar el objeto o el patrón de ataque.

9-3 Divulgación de números de acceso telefónico
Política: Personal de la empresa no debe revelar teléfono módem de empresa los números, pero debe siempre referirse dichas solicitudes a la mesa de ayuda técnica personal de apoyo.

Explicación\/notas: Números de teléfono de Dial-up deben tratarse como interna información, que debe facilitarse a los empleados que necesiten conocer tal información para llevar a cabo sus responsabilidades de trabajo.
Los ingenieros sociales rutinariamente destino empleados o departamentos que puedan ser menos protección de la información solicitada. Por ejemplo, el atacante puede llamar el departamento de cuentas por pagar disfrazada de una compañía telefónica empleado que está tratando de resolver un problema de facturación. El atacante entonces pide cualquier fax conocido o números de acceso telefónico a fin de resolver el problema. El intruso a menudo está dirigida a un empleado que es poco probable que dan cuenta del peligro de liberar tales información, o que carece de capacitación con respecto a la política de divulgación de la empresa y procedimientos.

9-4 Corporate ID badges
Política: Salvo cuando en su zona de oficina, todo el personal de empresa, incluyendo la administración y el personal ejecutivo, deben llevar sus insignias de empleado en todos los tiempos.

Explicación\/notas: Todos los trabajadores, incluidos los ejecutivos corporativos, deben ser capacitado y motivado para entender llevaba un gafete es obligatorio en todas partes en compañía locales distintos de las áreas públicas y la persona área de oficina o grupo de trabajo.

9-5 Violaciones de insignia de Challenging ID
Política: Todos los empleados deben desafiar inmediatamente cualquier persona desconocida que es no llevaba una insignia de empleado o tarjeta de visitante.

Explicación\/notas: Mientras que ninguna empresa quiere crear una cultura donde eagle-Eyed empleados buscar una manera atrapar a sus compañeros para aventurarse en el pasillo sin sus insignias, no obstante, cualquier empresa preocupada con proteger su información necesita tomar en serio la amenaza de un ingeniero social vagando por sus instalaciones indiscutidas. Motivación para los empleados que demuestren diligente en ayudar a imponer las insignias siempre política puede reconocerse en formas familiares, como el reconocimiento en el periódico o boletín juntas; unas horas apagado con goce de sueldo; o una carta de felicitación en su personal registros.

9-6 Piggybacking (pasando por entradas seguras)
Política: Empleados entrando en un edificio no deben permitir que nadie no personalmente conocido para ellos seguir detrás de ellos cuando ha utilizado un medio seguro, tal como una clave de tarjeta, para poder entrar (piggybacking).

Explicación y notas\". Empleados deben entender que no es grosero requerir personas desconocidas para autenticarse antes de ayudarles a entrar en una instalación o acceder a una zona segura.
Los ingenieros sociales frecuentemente usan una técnica conocida como piggybacking, en el que acechan para otra persona que está entrando en una instalación o zona sensible, y a continuación, simplemente entrar con ellos. Mayoría de las personas se siente incómoda desafiando a otr Suponiendo que son empleados probablemente legítimos. Otro piggybacking técnica consiste en llevar varios cuadros para que un trabajador confiado abre o mantiene la puerta para ayudar.

9-7 Destrucción de documentos confidenciales
Política: Documentos sensibles a descartarse debe purgar Cruz; medios de comunicación incluyendo unidades de disco duro que hayan contenido nunca información confidencial o materiales deben ser destruidos de conformidad con los procedimientos establecidos por el grupo responsables de seguridad de la información.

Explicación\/notas: Trituradoras estándar no adecuadamente destruir documentos; Cruz-Trituradoras convierten documentos en pulpa. Es la mejor práctica de seguridad presumo que se van estriado competidores de jefe de la organización a través de descartan materiales buscando cualquier inteligencia que podría ser beneficioso para ellos.

Espías industriales y los atacantes del equipo regularmente obtienen información confidencial desde materiales arrojó a la basura. En algunos casos, han sido competidores del negocio conocido por intento de soborno de tripulaciones pasar basura de empresa de limpieza. En uno ejemplo reciente, un empleado de Goldman Sachs descubierto elementos que fueron utilizados en un régimen de comercio de información privilegiada de la basura.

9-8 Identificadores personales
Política: Identificadores personales como el número de empleados, número de seguridad social, número de licencia de conductor, fecha y lugar de nacimiento y nombre de soltera de la madre nunca debe utilizarse como un medio de verificación de identidad. Estos identificadores no son secreto y puede obtenerse 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 c tarjeta y acceso a Internet pueden obtener estas piezas de identificación personal.
Aún a pesar de la evidente peligro, bancos, empresas de servicios públicos y tarjetas de crédito

las empresas suelen utilizan estos identificadores. Esta es una razón que es el robo de identidad el delito de más rápido crecimiento de la década.

9-9 Organigramas
Política\". Detalles que se muestran en el organigrama de la empresa no deben ser reveladas a nadie más que los empleados de la empresa.

Explicación\/notas: Información de la estructura corporativa incluye organigramas, gráficos de jerarquía, listas de empleados departamentales, estructura jerárquica, empleado nombres, puestos de empleados, números de contacto internos, número de empleados, o información similar.
En la primera fase de un ataque de ingeniería social, el objetivo es reunir información sobre la estructura interna de la empresa. Esta información es entonces se utiliza para planear estrategias de un plan de ataque. El atacante también puede analizar esta informació determinar qué empleados puedan tener acceso a los datos que busca.
Durante el ataque, la información hace que el atacante aparezca como un experto empleado; lo más probable vas engañando a su víctima en cumplimiento de las normas.

9-10 Información privada acerca de los empleados
Política.: Cualquier solicitud de información de los empleados privados debe remitirse a los recursos humanos.

Explicación\/notas: Una excepción a esta política puede ser el número de teléfono un empleado que necesita ser contactado acerca de un problema relacionado con el trabajo o que es actuando en un papel de guardia. Sin embargo, siempre es preferible que el solicitante número de teléfono y que el empleado llame a él o a su espalda.

Uso de equipo
10-1 Introducir comandos en un equipo
Política: Personal de la empresa nunca debe introducir comandos en un equipo o equipos informáticos a petición de otra persona a menos que el solicitante se ha comprobado que un empleado del departamento de tecnología de información.

Explicación\/notas: Una táctica común de los ingenieros sociales es para solicitar que un empleado introduzca un comando que realiza un cambio en la configuración del sistema, permite que el atacante para tener acceso a equipo de la víctima sin proporcionar autenticación, o permite que el atacante recuperar información que puede utilizarse para facilitar un ataque técnico.

Convenciones de nomenclatura internas de 10-2
Política: Los empleados no deben revelar los nombres internos de los sistemas informáticos o bases de datos sin la previa comprobación de que el solicitante es empleado de la empresa.

Explicación\/notas: ingenieros sociales a veces intentará obtener los nombres de los sistemas informáticos de empresa; una vez que se conocen los nombres, el atacante coloca un llamada a la empresa y mascaradas como un legítimo empleado tiene problemas acceder o usar uno de los sistemas. Conociendo el nombre interno asignado a el sistema en particular, el ingeniero social gana credibilidad.

Solicitudes de 10-3 para ejecutar programas
Política: Personal de la empresa nunca debe ejecutar las aplicaciones de cualquier equipo o programas a petición de otra persona a menos que el solicitante ha sido verificado como un empleado del departamento de tecnología de información.

Explicación\/notas: Toda solicitud para ejecutar programas, aplicaciones, o realice debe denegarse la actividad en un equipo a menos que el solicitante es positivamente identificado como empleado en el departamento de tecnología de información. Si la solicitud implica revelar información confidencial de cualquier archivo o electrónicos mensaje, respondiendo a la solicitud debe ser de conformidad con los procedimientos para Liberación de información confidencial. Consulte la política de divulgación de información.

Los atacantes del equipo engañan personas en ejecución de programas que permiten la intruso para hacerse con el control del sistema. Cuando un desprevenido usuario ejecuta un programa plantado por un atacante, el resultado puede dar el acceso de intrusos a la víctima sistema informático. Otros programas grabación las actividades del usuario del equipo y devolver dicha información al atacante. Mientras que un ingeniero social puede engañar a una persona en equipo de ejecutar instrucciones que pueden hacer daño, una base técnica ataque trucos del sistema operativo en la ejecución de equipo instrucciones que pueden causar al mismo tipo de daño.

10-4 Descarga o instalar software
Política: Personal de la empresa debe nunca Descargar o instalar el software en el solicitud de otra persona, a menos que el solicitante ha sido verificado como empleado con el departamento de tecnología de la información.

Explicación\/notas: Empleados deben estar en alerta para cualquier solicitud de inusual que implica a cualquier tipo de transacción con equipos informáticos.
Es una táctica común utilizada por los ingenieros sociales engañar a incautos víctimas en Descargando e instalando un programa que ayuda al atacante realizar su o su objetivo de comprometer la seguridad del equipo o la red. En algunos casos, la programa secretamente puede espiar al usuario o permitir al atacante tomar el control de la sistema informático a través del uso de una aplicación encubierta de control remoto.

10-5 Contraseñas de texto y correo electrónico
Política: Las contraseñas serán no se enviarán a través de un correo electrónico a menos que cifrado.
Explicación\/notas: Si bien no se recomienda, esta política se autorizan

por e-commerce sitios en ciertas circunstancias limitadas, tales como:
Envío de contraseñas para los clientes que se han registrado en el sitio.

Envío de contraseñas para los clientes que han perdido u olvidado sus contraseñas.

Software relacionados con la seguridad de 10-6
Política: Personal de la empresa debe nunca quitar o desactivar antivirus \/ troyano
Caballo, firewall u otro software relacionados con la seguridad sin la aprobación previa de la
Departamento de tecnología de la información.

Explicación\/notas: Los usuarios de computadoras a veces desactivan software relacionados con la seguri
sin provocación, pensando que se incrementará la velocidad de su equipo.

Un ingeniero social puede intentar engañar a un empleado en deshabilitar o quitar
software que se necesita para proteger la empresa contra la seguridad relacionada con las amenazas.

Instalación de 10-7 de módems
Política... Ningún módem puede estar conectado a ningún equipo hasta que tenga aprobación previa
se han obtenido desde el departamento de TI.

Explicación \/ notas.: es importante reconocer que módems en ordenadores de sobremesa o
estaciones de trabajo en el lugar de trabajo representan una amenaza de seguridad importante, especialme
conectado a la red corporativa. En consecuencia, esta directiva controla el módem
procedimientos de conexión.

Piratas informáticos utilizan una técnica llamada guerra marcado para identificar las líneas de módem activ
dentro de un rango de números de teléfono. La misma técnica puede utilizarse para localizar
números de teléfono conexión a módems dentro de la empresa. Un atacante puede
fácilmente comprometer la red corporativa si él o ella identifica un equipo
sistema conectado a un módem con el software de acceso remoto vulnerables, que
está configurado con una contraseña fácilmente poco o ninguna en absoluto.

10-8 Módems y configuración de respuesta automática
Política: M1 ordenadores personales o estaciones de trabajo con módems aprobados por TI tendrá la
característica de respuesta automática de módem deshabilitada para evitar que alguien marcado en la
sistema informático.

Explicación \/ notas. - siempre que sea posible, el departamento de tecnología de la información
debe implementar un conjunto de módems de acceso telefónico de salida para aquellos empleados que ne
sistemas de ordenador externo a través de módem.

Herramientas de cracking de 10-9
Política: Los empleados no Descargar o utilizar cualquier herramienta de software diseñado para derrota a mecanismos de protección.

Explicación\/notas: Internet tiene docenas de sitios dedicados al software diseñado shareware de crack y productos de software comercial. El uso de estas herramientas no sólo viola derechos de autor del propietario del software, pero también es extremadamente peligroso. Porque estos programas provienen de fuentes desconocidas, que pueden contener oculta el código malicioso que puede dañar al equipo del usuario o una planta una Caballo de Troya que da al autor del programa de acceso a la computadora del usuario.

Información de empresa de registro de 10-10 en línea
Política: Los empleados no revelará ningún detalle en cuanto a hardware de empresa o software en cualquier grupo de noticias público, foro o tablón de anuncios y no revelará Póngase en contacto con información distinta de conformidad con la política.

Explicación\/notas: Cualquier mensaje enviado a la Usenet, foros en línea, tablones de anuncios o listas de correo pueden buscarse para reunir información de inteligencia sobre un o empresa o un destino individual. Durante la fase de investigación de una ingeniería social ataque, el atacante puede buscar en Internet cualquier puesto que contienen útiles información sobre la empresa, sus productos o su pueblo.

Algunos puestos contienen cositas muy útiles de información que el atacante puede utilizar para lograr un ataque. Por ejemplo, un administrador de red puede publicar un pregunta sobre la configuración firewall filtra en una determinada marca y modelo de cortafuegos. Un atacante que descubre este mensaje aprenderán información valiosa sobre el tipo y la configuración del firewall companys que le permite sortear para obtener acceso a la red de la empresa.

Este problema puede ser reducido o evitarse mediante la aplicación de una política que permite a los empleados registrar a grupos de noticias de cuentas anónimas que no identificar la empresa desde que se originó. Naturalmente, la política debe exigen los empleados no incluyen ninguna información de contacto que puede identificar el empresa.

10-11 Disquetes y otros medios electrónicos
Política: Si los medios usados para almacenar información del equipo, tales como disquete discos o CD-ROM ha quedado en un área de trabajo o en el escritorio del empleado, y son que los medios de una fuente desconocida, no debe insertarse en cualquier equipo sistema.

Explicación\/notas: Un método utilizado por los atacantes para instalar código malicioso es colocar programas en un disquete o CD-ROM y etiquetar con algo muy

seductor (por ejemplo, \"Personal datos nómina--confidenciales\"). Ellos, a continuación, soltar varios ejemplares en las áreas utilizadas por los empleados. Si una sola copia se inserta en un equipo y los archivos se abrió, el atacante del malintencionado se ejecuta código. Esto puede crear una puerta trasera, que se utiliza para poner en peligro el sistema, o causar otros daños a la red.

Medios extraíbles de descarte de 10-12
Política: antes de descartar cualquier medio electrónico que contenía alguna vez sensibles información de la empresa, incluso si se ha eliminado esa información, el tema será Fondo desmagnetizada o dañado más allá de la recuperación.

Explicación\/notas: Mientras la destrucción de documentos impresos es algo habitual estos días, trabajadores de la empresa pueden pasar por alto la amenaza de descarte de medios electrónicos contenía ar datos confidenciales de cualquier rima. Los atacantes del equipo intentan recuperar los datos almacenados en medios electrónicos desechados. Los trabajadores pueden presumir por sólo eliminar archivos, aseguran que no se pueden recuperar los archivos. Esta presunción es absolutamente incorrecto y puede causar la información comercial confidencial caer en las manos equivocadas. En consecuencia, los medios electrónicos que contiene o previamente información contenida no designado como público debe ser borrado limpio o destruidos utilizando los procedimientos aprobados por el grupo responsable.

Protectores de pantalla protegido por contraseña de 10-13
Política: Todos los usuarios de ordenador deben establecer una contraseña de protector de pantalla y la ina límite de tiempo de espera para 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 espera de inactividad de no más de diez minutos. El intención de esta política es evitar que a cualquier persona no autorizada mediante otro equipo de la persona. Además, esta política protege los sistemas informáticos de empresa desde accediendo fácilmente a los extranjeros que se han ganado el acceso al edificio.

10-14 Divulgación o uso compartido de la declaración de contraseñas
Política: antes de la creación de una nueva cuenta de equipo, el empleado o contratista debe firmar una declaración escrita reconociendo que él o ella entiende contraseñas nunca deben ser reveladas o compartidas con nadie y que él o ella se compromete a acatar esta política.

Explicación\/notas: El acuerdo también debe incluir un aviso de esa violación de tal acuerdo puede conducir a medidas disciplinarias hasta e incluyendo la terminación.

Uso de correo electrónico
Archivos adjuntos de correo electrónico de 11-1

Política: Archivos adjuntos de correo electrónico deben no abrirse a menos que el archivo adjunto espera que en el ejercicio de la profesión o fue enviado por una persona de confianza.

Explicación\/notas: Todos los adjuntos de correo electrónico deben controlarse estrechamente. Usted puede requieren que se da aviso previo por una persona de confianza que es un archivo adjunto de correo electr se envía antes de que el destinatario abre los datos adjuntos. Esto reducirá el riesgo de atacantes usando tácticas de ingeniería social para engañar a personas apertura archivos adjuntos.

Un método de poner en peligro un sistema informático es truco un empleado en la ejecución de un programa malintencionado crea una vulnerabilidad, proporcionando el atacante con acceso al sistema. Enviando un archivo adjunto de correo electrónico que ha código ejecutable o macros, el atacante puede ser capaz de hacerse con el control de los usuarios equipo.

Un ingeniero social puede enviar un archivo adjunto de correo electrónico malintencionados, entonces l intentan persuadir al destinatario a abrir el archivo adjunto.

Reenvío automático de 11-2 a direcciones externas
Política: Reenvío automático de correo electrónico entrante a una dirección de correo electrónico externa prohibido.

Explicación\/notas: La intención de esta política es evitar a un outsider de recepción de correo electrónico enviados a una dirección de correo electrónico interno.

Empleados ocasionalmente configuración el reenvío de correo electrónico de su correo entrante a una dirección de correo electrónico fuera de la empresa cuando estén fuera de la Oficina. O una intruso puede ser capaz de engañar a un empleado en la creación de un correo electrónico interno dirección que envía a una dirección fuera de la empresa. El atacante puede entonces plantean como un legítimo insider por tener una dirección de correo electrónico interno de la empresa y personas a enviar información confidencial a la dirección de correo electrónico interno.

11-3 Reenvío de mensajes de correo electrónico
Política: Toda solicitud de una persona sin verificar para transmitir un mensaje de correo electrónico mensaje a otra persona sin verificar requiere la verificación del solicitante identidad.

Correo electrónico de verificación de 11-4
Política: Un mensaje de correo electrónico que parece proceder de una persona de confianza que contiene una solicitud de información no designados como público, o para realizar una acción con cualquieræquipos informáticos, requiere una forma adicional de autenticación. Consulte los procedimientos de autorización y verificación.

Explicación\/notas: Un atacante fácilmente puede forjar un mensaje de correo electrónico y su encabezad
haciendo que parezca como si el mensaje se originó en otra dirección de correo electrónico. Un
atacante puede enviar también un mensaje de correo electrónico desde un equipo comprometido,
proporcionar falsa autorización para divulgar información o realizar una acción. Incluso
al examinar el encabezado de un mensaje de correo electrónico no puede detectar mensajes de correo ele
enviado desde un sistema informático interno comprometido.

Uso del teléfono
12-1, Participando en encuestas telefónicas
Política: Empleados no podrán participar en encuestas por responder a cualquier pregunta
de cualquiera fuera la organización o persona. Dichas solicitudes deben remitirse a la
Departamento de relaciones públicas o cualquier otra persona designada.

Explicación\/notas: Un método utilizado por los ingenieros sociales para obtener valiosos
información que puede ser utilizada contra la empresa es llamar a un empleado y
pretenden hacer una encuesta. Es sorprendente cómo muchas personas están encantadas de proporcionar
información sobre la empresa y ellos mismos a los extraños cuando creen
está participando en la investigación legítima. Entre las preguntas inocuas, la
llamador insertará unas preguntas que el atacante quiere saber. Finalmente,
dicha información puede ser utilizada para comprometer la red corporativa.

12-2 Divulgación de números de teléfono interno
Política: Si una persona no verificadas le pide a un empleado por su número de teléfono del
empleado puede hacer una determinación razonable de divulgación sea
es necesario llevar a cabo la empresa.
Explicación\/notas: La intención de esta política es exigir a los empleados hacer un
considerada decisión sobre si la divulgación de su extensión telefónica
es necesario. Cuando se necesita tratar con personas que no han demostrado un verdadero
para conocer la extensión, el curso más seguro es que les exigen para llamar a los principales
número de teléfono de la compañía y ser transferido.

12-3 Contraseñas en mensajes de correo de voz
Política.: Dejando mensajes que contienen información de contraseña en la voz de nadie
buzón está prohibido.

Explicación\/notas: Un ingeniero social a menudo puede obtener acceso a un empleado
buzón de voz ya está adecuadamente protegido con un acceso fácil de adivinar
código. En un tipo de ataque, un intruso sofisticado equipo es capaz de crear su
propietario de buzón de voz falsa y persuadir a otro empleado para dejar un mensaje
transmisión de información de la contraseña. Esta política vence a esa treta.

Uso de fax
13-1 Transmitir faxes

Política: No fax puede ser recibido y reenviado a otra parte sin verificación de la identidad del solicitante.

Explicación\/notas: Ladrones de información pueden engañar a empleados de confianza en el envío de fax información confidencial a una máquina de fax ubicada en las instalaciones de la empresa. Prior para el atacante dando el número de fax a la víctima, el impostor teléfonos un empleado desprevenido, como una secretaria o auxiliar administrativo y le pregunta si un documento puede enviarse por fax a ellos para su posterior recogida. Posteriormente, después de la empleado desprevenido recibe el fax, el atacante teléfonos del empleado y pide que el fax se envía a otro lugar, quizás afirmando que es necesarios para una reunión urgente. Puesto que la persona preguntó a retransmitir el fax normalmente tien no hay comprensión del valor de la información, él o ella cumple con la solicitud.

13-2 Verificación de autorizaciones por fax
Política: Antes de llevar a cabo las instrucciones recibieron por fax, el remitente deben verificarse como un empleado u otra persona de confianza. Realizar una llamada de teléfono al remitente para verificar la solicitud es generalmente suficiente.

Explicación\/notas: Empleados deben tener cuidado cuando las solicitudes inusuales Enviado por fax, como una solicitud para introducir comandos en un equipo o revelar información. Los datos en el encabezado de un documento por fax pueden ser refutados por cambiar la configuración de la máquina de fax de envío. Por lo tanto, la cabecera de un fax no debe aceptarse como medio de establecer la identidad o la autorización.

13-3 Enviar información confidencial por fax
Política: antes de enviar información confidencial por fax a una máquina que se encuentra en una zona accesible a otros funcionarios, el remitente transmitirá una portada. El receptor, al recibir la página, transmite una página de respuesta, demostrando que él\/él es físicamente presente en la máquina de fax. El emisor transmite entonces la fax.

Explicación\/notas: Este proceso mutuo asegura el remitente que el destinatario está físicamente presente en el extremo receptor. Además, este proceso verifica que el número de teléfono de fax de recepción no se ha remitido a otra ubicación.

13-4 Faxing contraseñas prohibidas
Política: Las contraseñas no deben enviar mediante fax bajo ninguna circunstancia.

Explicación\/notas: Información de autenticación enviando por fax no es segura. La mayoría de máquinas de fax son accesibles a un número de empleados. Además, se dependen de la red telefónica pública conmutada, que puede ser manipulada por llamada

el número de teléfono de la máquina de fax receptora de reenvío para que sea el fax enviado al atacante a otro número.

Uso de correo de voz
Contraseñas de correo de voz de 14-1
Política: Contraseñas de correo de voz no deben nunca ser reveladas a nadie para ningún propósito. Además, las contraseñas de correo de voz deben cambiarse cada noventa días o antes.
Explicación\/notas: Información confidencial de la compañía puede dejarse en el correo de voz mensajes. Para proteger esta información, los empleados deben cambiar su correo de voz las contraseñas con frecuencia y nunca revelar. Además, los usuarios de correo de voz no debe utilizar las contraseñas de correo de voz de la misma o similar dentro de un mes de doce período.

Contraseñas de 14-2 en varios sistemas
Política... Los usuarios de correo de voz no deben utilizar la misma contraseña en cualquier otro teléfono sistema informático, ya sea interno o externo a la empresa.
Explicación y notas\". Uso de una contraseña idéntico o similar para varios dispositivos, como correo de voz y equipo, facilita a los ingenieros sociales adivinar todos las contraseñas de usuario tras identificar sólo uno.

Contraseñas de correo de voz de 14-3 Configuración
Política: Los administradores y los usuarios de correo de voz deben crear voz contraseñas de correo son difíciles de adivinar. No deben estar relacionados en modo alguno a la persona con ella, o la empresa y no debe contener un patrón predecible que es probablemente se adivinar.

Explicación\/notas: Contraseñas no pueden contener dígitos secuenciales o repetidas (es decir 1111 1234, 1010), no debe ser igual o basándose en la extensión de teléfono número y no debe estar relacionado con la dirección, código postal, fecha de nacimiento, matrícula, número de teléfono, peso, I.Q. u otra información personal predecible.

14-4 Mensajes marcados como \"el viejo\"
Política: Cuando los mensajes de correo de voz previamente desconocida no están marcados como nuevo mensajes, el administrador de correo de voz deberán ser notificados de una seguridad posible inmediatamente deben cambiarse la violación y la contraseña de correo de voz.

Explicación\/notas: los ingenieros sociales pueden acceder a un buzón de voz en un variedad de formas. Un empleado que tenga conocimiento de que los mensajes no tienen nunca escuchado no se están anunciando como deben asumir nuevos mensajes que otro persona ha obtenido acceso no autorizado al buzón de voz y escuchar la mensajes propios.

14-5 Saludos de correo de voz externo
Política: Los trabajadores de la empresa limitará su divulgación de información sobre sus saludo saliente externo en su correo de voz. Normalmente la información relacionada con un horario de rutina o viaje diario del trabajador no debe revelarse.

Explicación\/notas: Un saludo externo (jugado para los llamadores externos) no debe incluir el último nombre, extensión o motivo de ausencia (tales como viajes, vacaciones horario o itinerario diario). Un atacante puede utilizar esta información para desarrollar un historia plausible en su intento de hacer otro tipo de personal.

Patrones de contraseña de correo de voz de 14-6
Política: Los usuarios de correo de voz no seleccionará una contraseña cuando una parte de la contraseña permanece fijo, mientras que otra parte cambios en un patrón predecible.

Explicación\/notas: por ejemplo, no utilice una contraseña como 743501, 743502, 743503 y así sucesivamente, donde los dos últimos dígitos corresponden al mes actual.

Información confidencial o privada de 14-7
Política: No se revelará información confidencial o privada en un correo de voz Mensaje.

Explicación\/notas: El sistema telefónico corporativo es normalmente más vulnerable de sistemas corporativos. Las contraseñas son normalmente una cadena de dígitos, que limita sustancialmente el número de posibilidades para un atacante de adivinar. Además, en algunas organizaciones, las contraseñas de correo de voz pueden ser compartidas con Secretarios o otro personal administrativo que tienen la responsabilidad de tomar mensajes para sus directivos. En vista de lo anterior, ninguna información sensible nunca debe dejarse en el correo de voz de cualquier persona.

Contraseñas
Seguridad de teléfono 15-1
Política: Las contraseñas no se mencionará por teléfono en cualquier momento.

Explicación\/notas: Los atacantes pueden encontrar formas para escuchar conversaciones telefónicas, ya sea en persona o a través de un dispositivo tecnológico.

Contraseñas de equipo Revealing de 15-2
Política: Bajo ninguna circunstancia cualquier usuario del equipo divulgarán su contraseña a cualquier persona para cualquier propósito sin el previo consentimiento por escrito de la Director de tecnología de información responsable.

Explicación\/notas: El objetivo de muchos ataques de ingeniería social implica engañando a las personas desprevenidas en revelando su cuenta nombres y

contraseñas. Esta política es un paso crucial para reducir el riesgo de éxito social Ingeniería ataques contra la empresa. En consecuencia, esta política debe ser seguido religiosamente en toda la empresa.

Contraseñas de Internet de 15-3
Política: Personal nunca debe utilizar una contraseña que sea igual o similar a una utilizan en cualquier sistema corporativo en un sitio de Internet.

Explicación\/notas: Operadores de sitio Web malintencionado pueden configurar un sitio que pretende ofrecer algo de valor o la posibilidad de ganar un premio. Para registrarse, un visitante del sitio debe introducir una dirección de correo electrónico, nombre de usuario y contraseña. De muchas personas utilizan la misma o similar sesión información repetidamente, la sitio Web malintencionado operador intentará utilizar la contraseña elegida y variaciones de la misma para atacar el sistema de equipo de trabajo o casa del destino. El equipo de trabajo del visitante a veces puede ser identificado por la dirección de correo electrónico introd durante el proceso de registro.

15-4 Contraseñas en varios sistemas
Política: Personal de la empresa nunca debe utilizar el mismo o una contraseña similar en más de un sistema. Esta política se refiere a diversos tipos de dispositivos (equipo o correo de voz); varias localidades de dispositivos (hogar o trabajos); y diversos tipos de sistemas, dispositivos (router o firewall) o programas (base de datos o aplicación).

Explicación\/notas: Los atacantes dependen de la naturaleza humana para entrar en el equipo sistemas y redes. Ellos saben que, para evitar la molestia de hacer el seguimiento de varias contraseñas, muchas personas utilizan la misma o una contraseña similar en cada sistema que tienen acceso. Como tal, el intruso intentará conocer la contraseña de un sistema donde el destino tiene una cuenta. Una vez obtenido, es muy probable que Esta contraseña o una variación del mismo dará acceso a otros sistemas y dispositivos utilizado por el empleado.

Contraseñas de reutilización de 15-5
Política: Ningún usuario de equipo utilizarán el mismo o una contraseña similar dentro de la mismo período de dieciocho meses.

Explicación\/Nota: Si un atacante descubrir la contraseña del usuario, frecuentes cambio de la contraseña minimiza el daño que se puede hacer. Haciendo la nueva contraseña única de contraseñas anteriores hace más difícil para el atacante adivinar.

15-6 Patrones de contraseña
Política\". Empleados no deben seleccionar una contraseña donde una parte permanece fija, y otro cambio de elemento en un patrón predecible.

Explicación\/notas: por ejemplo, no utilice una contraseña como Kevin01, Kevin02, Kevin03 etc., donde los dos últimos dígitos corresponden a la corriente mes.

15-7 Elegir contraseñas
Política: Los usuarios de computadoras deben crear o elegir una contraseña que se adhiere los siguientes requisitos. La contraseña debe:

Tener al menos ocho caracteres tiempo para cuentas de usuario estándar y al menos doce caracteres de longitud para las cuentas con privilegios.

Contienen al menos un número, por lo menos un símbolo (como $,-, que, letra minúscula y al menos una mayúscula (en la medida en que tales las 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 relacionado con la familia de un empleado, ocio, vehículos, trabajo, matrícula, número de seguridad social, dirección, teléfono, nombre de mascota, cumpleaños o frases con esas palabras.

No ser una variación de una contraseña utilizada anteriormente, con uno de los elementos restantes del mismo y otro elemento cambia, como kevin, kevin 1, kevin2; o kevinjan, kevinfeb.

Explicación\/notas: Los parámetros indicados producirá una contraseña que es difícil para el ingeniero social de adivinar. Otra opción es la consonante-vocal método, que proporciona una contraseña fácil de recordar y pronunciable. Para construir este tipo de consonantes de sustituto de contraseña para cada letra c y las vocales para la letra V, utilizando la máscara de \"CVCVCVCV\". Ejemplos serían MIXOCASO; CUSOJENA.

Contraseñas de escritura de 15-8 hacia abajo
Política: Los empleados deben escribir contraseñas abajo sólo cuando almacenan en un lugar seguro lejos de la computadora u otro dispositivo protegido con contraseña.

Explicación\/notas: Empleados son desalentados de jamás escrito abajo contraseñas. Bajo ciertas condiciones, sin embargo, puede ser necesario; para por ejemplo, en un empleado que tiene varias cuentas en otro equipo sistemas. Las contraseñas escritas deberán fijarse en un lugar seguro lejos el equipo. Bajo ninguna circunstancia puede una contraseña se almacena en virtud del teclado o conectada a la pantalla del ordenador.

Contraseñas de texto simple de 15-9 en ficheros informáticos

Política: Contraseñas de texto simple no se guardan en el archivo de cualquier equipo o almacenadas com
texto llamado pulsando una tecla de función. Cuando es necesario, pueden guardarse las contraseñas
utilizando una utilidad de encriptación aprobada por el departamento de TI para evitar cualquier
accesos no autorizados.

Explicación\/notas: Las contraseñas pueden fácilmente recuperarse por un atacante si almacena en
cifrar en los archivos de datos de computadora, archivos por lotes, teclas de función terminal, inicio de ses
archivos, macros o secuencias de comandos de programas o cualquier dato que contienen las contraseña
Sitios FTP.

POLÍTICAS PARA TELETRABAJADORES
Teletrabajadores son fuera del firewall corporativo y por lo tanto más vulnerables
para atacar. Estas políticas le ayudará a impedir que los ingenieros sociales mediante su
empleados de teletrabajador \/ como una puerta de enlace a los datos.

Clientes ligeros de 16-1
Política: Todo personal de la empresa que ha sido autorizado a conectarse vía remota
acceso deberá utilizar a un cliente ligero para conectarse a la red corporativa.

Explicación\/notas: Cuando un atacante analiza una estrategia de ataque, él o ella será
tratar de identificar a los usuarios que acceden a la red corporativa desde ubicaciones externas. Como
tal, teletrabajadores son los principales objetivos. Sus equipos son menos propensos a tener
controles de seguridad muy estrictas, y puede ser un eslabón débil que puede poner en peligro la
red corporativa.

Cualquier equipo que se conecta a una red de confianza puede ser trampas explosivas con
registradores de pulsaciones, o su conexión autenticada puede ser secuestrado. Un cliente liviano
estrategia puede utilizarse para evitar problemas. Un cliente liviano es similar a un disco
estación de trabajo o una terminal tonta; el equipo remoto no tiene almacenamiento
capacidades, pero en cambio el sistema operativo, aplicaciones y datos
residen en la red corporativa. Acceso a la red a través de un cliente liviano
reduce sustancialmente el riesgo que plantean los sistemas un-patched, desfasados de funcionamiento
sistemas y programas malintencionados. En consecuencia, gestión de la seguridad de
teletrabajadores es eficaces y facilitado mediante la centralización de los controles de seguridad.
En lugar de depender de los inexperto teletrabajador \/ gestionar adecuadamente
cuestiones relacionadas con la seguridad, estas responsabilidades quedan mejor con el sistema de formació
red, o los administradores de seguridad.
Software de seguridad de 16-2 para sistemas informáticos de teletrabajador \/
Política: Cualquier ordenador externo sistema que se utiliza para conectar a la empresa
red debe tener un personal, software antivirus y software Anti-Trojan
Firewall (hardware o software). Archivos antivirus y Antitroyanos patrón deben ser
actualizado al menos semanalmente.

Explicación\/notas: Normalmente, teletrabajadores no están capacitados en seguridad-relacionadas problemas y pueden inadvertidamente\"o por negligencia dejar su sistema informático y el red corporativa abierta al ataque. Teletrabajadores, por tanto, suponen un grave riesgo de seguridad si no están adecuadamente capacitados. Además de instalar antivirus y Trojan software de caballo para proteger contra programas malintencionados, un firewall es necesario para bloquear cualquier hostiles usuarios obtengan acceso a los servicios activado en sistema del teletrabajador \/.

El riesgo de no implementar las tecnologías de seguridad mínima para evitar malintencionado código de propagación no debe ser subestimada, como un ataque contra Microsoft demuestra. Un sistema informático perteneciente al teletrabajador \/ Microsoft, usado para conectarse a la red corporativa de Microsoft, fue infectado con un troyano programa. El intruso o intrusos fueron capaces de utilizar el teletrabajador \/ de confianza conexión a la red de desarrollo de Microsoft para robar el origen del desarrollo código.

POLÍTICAS DE RECURSOS HUMANOS

Los departamentos de recursos humanos tienen una carga especial para proteger a los trabajadores de aquellos que intentan descubrir información personal a través de su lugar de trabajo. HR los profesionales también tienen la responsabilidad de proteger su empresa contra las acciones de ex empleados descontentos.

17-1 Saliendo empleados

Política: Cada vez que una persona empleada por la compañía deja o se termina, Recursos humanos debe hacer inmediatamente lo siguiente:

Quitar de la lista de la persona desde el directorio en línea empleado\/teléfono y deshabilitar o reenviar su correo de voz;

Notificación a personal a la construcción de entradas o vestíbulos de empresa; y

Agregar el nombre del empleado a la lista de salida del empleado, que deberá ser enviada a todo el personal no menos a menudo que una vez por semana.

Explicación\/notas: Deben ser empleados que están estacionados en creación de entradas notificación para evitar que a un ex empleado de reingresar a los locales. Además, notificación al demás personal puede impedir que al ex empleado de correctamente disfrazada de un empleado activo y embaucando personal a tomar algunas acción perjudicial para la empresa.

En algunas circunstancias, puede ser necesario exigir a cada usuario dentro de la Departamento del ex empleado para cambiar sus contraseñas. (Cuando era

terminación de GTE únicamente debido a mi reputación como un hacker, la empresa requiere a todos los empleados en toda la empresa para cambiar su contraseña).

Notificación de departamento de TI de 17-2
Política: Cada vez que una persona empleada por la compañía deja o se termina, Recursos humanos debe notificar inmediatamente a la tecnología de la información Departamento para desactivar las cuentas de equipo del ex empleado, incluyendo cualquier cuentas utilizadas para el acceso de la base de datos, dial-up o acceso a Internet desde el remoto ubicaciones.

Notas de la explicación: es esencial para deshabilitar el acceso de cualquier ex trabajador a todos sistemas informáticos, dispositivos de red, bases de datos o cualquier otro equipo-relacionadas dispositivos inmediatamente después de la terminación. De lo contrario, la empresa puede dejar la puertas abiertas para un empleado disgustado a los sistemas informáticos de acceso empresa y causar daños significativos.

17-3 Información confidencial utilizada en el proceso de contratación
Política: Anuncios y otras formas de solicitación pública de los candidatos para llenar ofertas de empleo, a la medida de lo posible, eviten identificación de hardware informático y el software utilizado por la empresa.

Explicación\/notas: Personal de recursos humanos y directivos sólo debe divulgar información relacionada con la empresa equipo hardware y software que es razonablemente necesario para obtener los currículos de candidatos calificados.

Equipo intrusos leen periódicos y comunicados de prensa de la empresa y visitar Sitios de Internet, para encontrar anuncios de trabajo. A menudo, las compañías revelar demasiado información sobre los tipos de hardware y software que se utiliza para atraer a posibles empleados. Una vez que el intruso tiene conocimiento de los sistemas de información del destino, él está armado para la siguiente fase del ataque. Por ejemplo, al saber que un empresa particular utiliza el sistema operativo VMS, el atacante puede colocar pretexto de llamadas para determinar la versión y, a continuación, enviar una emergencia falsa parche de seguridad para aparecer como si provinieran de los desarrolladores de software. Una vez el se instala el parche, el atacante.

Información personal del empleado 17-4

Política: El departamento de recursos humanos nunca debe divulgar información personal acerca de cualquier actual o ex empleado, contratista, asesor, trabajador temporal, o pasante, excepto con previo expresar consentimiento por escrito de los empleados o humanos Administrador de recursos.

Explicación\/notas: Head-hunters, investigadores privados y ladrones de identidad información de empleado privado de destino como el número de empleados, seguridad social números, fechas de nacimiento, historial de sueldo, datos financieros, incluyendo el depósito directo información e información de beneficios relacionados con la salud. El ingeniero social puede obtener esta información para hacerse pasar por el individuo. Además revelar los nombres de los nuevos empleados puede ser extremadamente valiosa información ladrones. Nuevas contrataciones puedan cumplir con cualquier solicitud de las personas con antigüedad o en una posición de autoridad, o alguien afirmando ser de corporativa seguridad.

Antecedentes de 17-5
Política: Un cheque de fondo debe ser necesario para los nuevos empleados, contratistas, consultores, los trabajadores temporales o pasantes antes a una oferta de empleo o establecimiento de una relación contractual.

Explicación y notas: Debido a consideraciones de costo, el requisito para antecedentes podrán limitarse a determinados cargos de confianza. Sin embargo, que cualquier persona que se da acceso físico a oficinas corporativas puede ser un amenaza potencial. Por ejemplo, las cuadrillas de limpieza tienen acceso a las oficinas de personal, que les da acceso a los sistemas informáticos ubicados allí. Un atacante con acceso físico a un equipo puede instalar un registrador de pulsaciones de teclas de hardware en menos de un minuto para capturar contraseñas.

Los intrusos equipo irá a veces al esfuerzo de obtener un trabajo como un medio de acceso a redes y sistemas informáticos de una compañía de destino. Un atacante puede obtener fácilmente el nombre del contratista de limpieza de la compañía llamando al el funcionario responsable de la empresa de destino, afirmando ser de una conserjería la empresa busca para su negocio y, a continuación, obtener el nombre de la empresa actualmente proporciona tales servicios.

POLÍTICAS DE SEGURIDAD FÍSICA

Aunque los ingenieros sociales intentan evitar aparecer en persona en un lugar de trabajo deseado, hay veces que cuando van a vulnerar su espacio. Estas políticas le ayudará a proteger sus instalaciones físicas de amenaza.

Identificación de 18-1 para empleados no
Política: Gente de entrega y otros empleados no necesitan introducir la empresa locales sobre una base regular deben tener un distintivo especial u otra forma de identificación de conformidad con la política establecida por la seguridad de la empresa.

Explicación\/notas: No empleados que necesitan entrar en el edificio regularmente (para ejemplo, para hacer las entregas de alimentos o bebidas a la cafetería, o para reparar

máquinas de copiar o instalar teléfonos) debe expedirse una forma especial de placa de identificación de empresa previsto para este fin. Otros que necesitan entrar sólo ocasionalmente o sobre una base temporal deben ser tratados como visitantes y debe ser acompañado en todo momento.

Identificación de visitante de 18-2
Política: Todos los visitantes deben presentar licencia de conducir válida o otra imagen identificación para ser admitido a los locales.

Explicación\/notas: El personal de seguridad o recepcionista debe hacer una fotocopia del el documento de identificación a la expedición de la tarjeta de visitante. La copia debe ser mantuvo con registro de visitantes. Alternativamente, puede ser la información de identificación registrado en el registro del visitante por la recepcionista o Guardia; los visitantes no deben permite anotar su propia información de ID.
Los ingenieros sociales tratando de entrar a un edificio siempre escribirá información falsa en el registro. Aunque no es difícil obtener ID falsa y conocer el nombre de un empleado que él o ella puede presumir de ser visitante, que requieren el responsable debe iniciar la entrada agrega un nivel de seguridad para la proceso.

18-3 Escorting visitantes
Política: Los visitantes deben ser escoltados o en compañía de un empleado en todo momento.

Explicación \/ notas.: es un ardid popular de ingenieros sociales organizar para visitar a un empleado de la empresa (por ejemplo, visitando con un ingeniero de producto en el pretexto de ser el empleado de un socio estratégico). Después de haber sido acompañado a la reunión inicial, el ingeniero social asegura su anfitrión que puede encontrar su propia camino de regreso al lobby. Por este medio gana la libertad de moverse el edificio y posiblemente acceder a sensible información.

18-4 Placas temporales
Política: La compañía desde otra ubicación de empleados que no tienen sus insignias de empleado con ellos deben presentar licencia de conducir válida o otra imagen ID y expedirá la tarjeta de un visitante temporal.

Explicación\/notas: Los atacantes a menudo plantean como empleados de una Oficina diferente o sucursal de una empresa para poder entrar a una empresa.

Evacuación de emergencia de 18-5
Política: En cualquier situación de emergencia o simulacro, personal de seguridad debe garantizar todo el mundo ha evacuado las instalaciones.

Explicación\/notas: Personal de seguridad debe comprobar cualquier rezagados que pueden ser abandonados en baños o zonas de oficinas. Autorizado por el departamento de bomberos o otra autoridad a cargo de la escena, la fuerza de seguridad tiene que ser en la alerta para cualquiera que salgan del edificio durante mucho tiempo después de la evacuación.

Espías industriales o equipo sofisticado intrusos pueden causar una desviación ganar el acceso a un área seguro o edificio. Es una desviación utilizada para liberar un inofensivo producto químico conocido como mercaptano de butilo en el aire. El efecto es crear la impresión de que hay una fuga de gas natural. Una vez empiece a personal de evacuación procedimientos, el atacante negrita utiliza esta desviación, ya sea robar información o a acceder a sistemas de computación de la empresa. Otra táctica utilizada por información ladrones implica permanecer detrás, a veces en un baño o un armario, en el momento de un simulacro de evacuación programada, o tras la configuración de una bengala humo u otro dispositiv provocar una evacuación de emergencia.

18-6 Visitantes en la sala de correo
Política: no debe permitirse que ningún visitante en la sala de correo sin la supervisión de un trabajador de la empresa.

Explicación\/notas: La intención de esta política es evitar a un outsider de intercambio, enviar o robando correo intracompany.

18-7 Números de matrícula de vehículos
Política: Si la empresa tiene un área de estacionamiento vigilado, personal de seguridad deberá registrar v números de matrícula de cualquier vehículo que penetren en la zona.
Contenedores de basura de 18-8
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 del equipo y espías industriales pueden obtener valiosos información de contenedores de basura de la empresa. Los tribunales han sostenido que la basura es considerado propiedad legalmente abandonada, por lo que el acto de recolección urbana es perfectamente legal, como los recipientes de basura son de propiedad pública. Por este motivo, es importante que los recipientes de basura situada en

propiedad de la empresa, donde la empresa tiene un derecho legal para proteger los contenedores y su contenido.

POLÍTICAS PARA RECEPCIONISTAS
Recepcionistas son a menudo en las líneas del frente a la hora de tratar de sociales ingenieros, pero rara vez se dan bastante seguridad capacitación para reconocer y detener un invasor. Instituto estas políticas para ayudar a su recepcionista a proteger mejor tu empresa y sus datos.

Directorio interno de 19-1
Política: Divulgación de la información en el directorio interno de la empresa debe ser limitado a las personas empleadas por la empresa.

Explicación\/notas: Todos los cargos de los empleados, nombres, números de teléfono y direcciones dentro de la empresa directorio debe considerarse interna información y sólo debe revelarse en cumplimiento de la política relacionada con clasificación de datos e información interna.

Además, cualquier parte de la llamada debe tener el nombre o la extensión de la parte están intentando contactar. Aunque la recepcionista puede poner una llamada a través una individuales cuando llama no sabe la extensión, contando el llamador el número de extensión debe prohibirse. (Para las curiosa gente que siga por ejemplo, puede experimentar este procedimiento por llamar a cualquier Gobierno de Estados Unidos Agencia y pidiendo el operador para proporcionar una extensión.)

19-2 Números de teléfono para grupos de departamentos específicos
Política: Empleados no deberán proporcionar números de teléfono directo para la empresa Mesa de ayuda, departamento de telecomunicaciones, las operaciones del equipo o sistema personal de 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 llamador.
Explicación\/notas: Aunque algunas organizaciones pueden encontrar esta política excesivamente restrictiva, esta regla hace más difícil para un ingeniero social a hacerse pasar por un empleado por engañar a otros empleados en transferir la llamada de su extensión (que en algunos sistemas telefónicos provoca la llamada a parecen originarse desde dentro de la empresa), o demostrar conocimiento de estas extensiones a la víctima a fin de crear un sentido de autenticidad.

19-3 Transmitir información
Política: Los operadores de teléfono y recepcionistas no deberían tomar mensajes o relé información en nombre de cualquiera de las partes no personalmente conocido por ser un activo empleado.

Explicación\/notas: ingenieros sociales son adeptas a engañar a los empleados en sin querer dar fe de su identidad. Es un truco de ingeniería social obtener el número de teléfono de la recepcionista y, con un pretexto, pedir la recepcionista a tomar cualquier mensaje que pueda surgir para él. Entonces, durante una llamada a la víctima, el atacante pretende ser un empleado, pide alguna información confidencial o a realizar una tarea y da el número de centralita principal como un número de llamada de vuelta. El atacante más tarde vuelve a llamar a la recepcionista y recibe cualquier mensaje dejado para él la víctima confiados.

19-4 Elementos izquierda para su recogida
Política: antes de lanzar cualquier elemento a un mensajero o a otra persona sin verificar, la Recepcionista o guardia de seguridad debe obtener la identificación de la imagen y escriba el identificación información en el registro de recogida como requerido por aprobado procedimientos.

Explicación y notas\". Es una táctica de ingeniería social engañar a un empleado en Liberación de materiales sensibles a otro supuestamente autorizado a empleado por caer tales materiales al recepcionista o al escritorio de lobby para su recogida. Naturalmente, la recepcionista o guardia de seguridad asume que el paquete está autorizado para el lanzamiento. El ingeniero social se muestra a sí mismo o tiene un mensajero servicio de recoger el paquete.

POLÍTICAS PARA EL GRUPO DE INFORMES DE INCIDENTES
Cada empresa debe establecer un grupo centralizado que debe ser notificado cuando se identifica cualquier forma de ataque a la seguridad de la empresa. Lo que sigue son algunos directrices para configurar y estructurar las actividades de este grupo.

Grupo de informes de incidente de 20-1
Política: Un individuo o grupo debe ser designado y empleados deben ser instrucciones de incidentes de seguridad informe a ellos. Todos los empleados deben proporcionarse con la información de contacto para el grupo.

Explicación\/notas: Empleados deben entender cómo identificar una amenaza a su seguridad, y estar capacitado para informar de cualquier amenaza a un grupo de informes incidente específico. Tam importante que una organización establezca procedimientos específicos y autoridad para un grupo para actuar cuando se informó de una amenaza.

20-2 Ataques en curso
Política: Cuando el grupo informe incidente ha recibido informes de un curso ataque de ingeniería social inmediatamente iniciará procedimientos de alerta todos los empleados asignados a los grupos afectados.
Explicación\/notas: El incidente informes de grupo o Gerente responsable debe también tomar una decisión sobre si enviar una empresa amplia alerta. Una vez el persona responsable o el grupo tiene una creencia de buena fe que puede ser un ataque en progreso, mitigación de los daños debe hacerse una prioridad mediante notificación a la empresa personal que en su guardia.

Seguridad de un vistazo

La versión de referencia listas y listas de siguientes proporcionan social rápida métodos de ingeniería discutieron en los capítulos 2 a 14 y verificación de procedimientos detallada en el capítulo 16. Modificar esta información para su organización y hacer disponible a los empleados para referirse a una pregunta de seguridad de la información surge.

IDENTIFICACIÓN DE UN ATAQUE DE SEGURIDAD
Estas tablas y listas de verificación le ayudará a detectar un ataque de ingeniería social.

El ciclo de la ingeniería Social

ACCIÓN \/ DESCRIPCIÓN

Investigación
Puede incluir información de código abierto como presentaciones a la SEC y los informes anuales, folletos de marketing, aplicaciones de patentes, prensa, revistas del sector, Contenido del sitio Web. También la recolección urbana.

Desarrollo de rapport y confianza
Uso de información privilegiada, tergiversar la identidad, los conocidos a citando víctima, necesidad de ayuda, o autoridad.

Aprovechamiento de la confianza
Pidiendo información o una acción por parte de la víctima. En inversa aguijón, manipular víctima al atacante para pedir ayuda.

Utilizar la información
Si la información obtenida es sólo un paso hacia la meta final, el atacante regresa a anterior los pasos en el ciclo hasta que se alcanza el objetivo.

Métodos de ingeniería Social común

Haciéndose pasar por un empleado de compañero

Haciéndose pasar por un empleado de un proveedor, empresa asociada o aplicación de la ley

Haciéndose pasar por alguien en autoridad

Haciéndose pasar por un empleado nuevo solicitando ayuda

Haciéndose pasar por un proveedor o llamada de fabricante de sistemas para ofrecer una revisión del siste
actualización

Oferta de ayuda si surge algún problema, entonces que el problema se producen, con lo cual
manipulación de la víctima para pedir la ayuda

Envío de software libre o parche de víctima instalar

Enviar un virus o un troyano como datos adjuntos de correo electrónico

Mediante una ventana emergente falsa pidiendo usuario vuelva a iniciar sesión o iniciar sesión con
contraseña

Captura las pulsaciones de la víctima con el programa o sistema informático fungible

Dejando a un disquete o CD todo el lugar de trabajo con software malintencionado en ella

Utilizando jerga privilegiada y terminología para ganar confianza

Ofreciendo un premio para registrarse en un sitio Web con el nombre de usuario y contraseña

Colocar un archivo o documento en la sala de correo de empresa para la entrega de intraoffice

Modificación de la partida de máquina de fax que parecen provenir de una ubicación interna

Solicita recepcionista para recibir luego reenviar un fax

Pidiendo un archivo para ser transferido a una ubicación aparentemente interna

Obtener un buzón de correo de voz configurado así llamada espalda percibe atacante como interna

Pretende ser de oficinas remotas y pidiendo acceso a correo electrónico localmente

Señales de advertencia de un ataque

Negativa a dar vuelta número de llamada

Petición de salida de corriente

Reclamación de la autoridad

Destaca urgencia

Amenaza de consecuencias negativas del incumplimiento

Muestra incomodidad cuando se le preguntó

Colocar el nombre

Piropos o halagos

Ligar

Objetivos comunes de ataques
TIPO DE DESTINO \/ EJEMPLOS

Conscientes del valor de la información
Recepcionistas, telefonistas, auxiliares administrativos, guardias de seguridad.

Privilegios especiales
Ayuda de escritorio o soporte técnico, los administradores de sistemas, operadores de equipo, administradores del sistema telefónico.

Fabricante \/ proveedor
Hardware del equipo, los fabricantes de software, proveedores de sistemas de correo de voz.

Departamentos específicos
Contabilidad, recursos humanos.

Factores que hacen más Vulnerable a los ataques de las empresas

Gran número de empleados

Múltiples instalaciones

Información sobre empleados paradero dejado en mensajes de correo de voz

Información de la extensión de teléfono disponible

Falta de formación en seguridad

Falta de sistema de clasificación de datos

Ningún plan de información y respuesta a incidentes

VERIFICACIÓN UNA D DE CLASIFICACIÓN DE DATOS
Estas tablas y gráficos le ayudarán a responder a las solicitudes de información o acción que puede ser ataques de ingeniería social.

Verificación de identidad de procedimiento
ACCIÓN \/ DESCRIPCIÓN
Identificador de llamadas
Verificar la llamada es interno, y número de nombre o la extensión coincide con la identidad de la llamador.

Devolución de llamada
Buscar solicitante en el directorio de la empresa y la extensión de la lista de devolución de llamada.

Dar fe
Pedir a un empleado de confianza para garantizar la identidad del solicitante.

Clave común compartida
Solicitud de secreto compartido de toda la empresa, como una contraseña o código diaria.

Supervisor o administrador
Contacto del empleado inmediato supervisor y solicitud de verificación de identidad y Estado de empleo.

Correo electrónico seguro
Solicitar un mensaje firmado digitalmente.

Reconocimiento de voz personal
Para que un llamador sabe que empleado, validar por voz del llamador.

Contraseñas dinámicas
Verificar contra una solución dinámica contraseña como Secure ID o otros fuertes dispositivo de autenticación.

En persona
Exigir del solicitante que aparezca en persona con una insignia de empleado o identificación.

Verificación del procedimiento de estado de empleo
ACCIÓN \/ DESCRIPCIÓN
Verificación de directorio de empleados
Compruebe que el solicitante aparece en el directorio en línea.

Verificación de administrador del solicitante
Llamar a administrador del solicitante mediante el número telefónico que aparece en el directorio de la e

Verificación de departamento o grupo de trabajo del solicitante
Llame el departamento o grupo de trabajo del solicitante y determinar que el solicitante es todavía empleados de la empresa.

Procedimiento para determinar la necesidad de saber
ACCIÓN \/ DESCRIPCIÓN
Consultar marea de trabajo \/ grupos de trabajo \/ lista de responsabilidades
Comprobar listas publicadas de que los trabajadores tienen derecho a específicos clasificados información.

Obtener la autoridad del administrador
Póngase en contacto con su administrador, o del solicitante, para poder cumplir con la solicitud.

Obtener la autoridad de la información propietaria o designatario
Pregunte al propietario de la información si el solicitante tiene una necesidad de saber.

Obtener autoridad con una herramienta automatizada
Buscar base de datos de software propietario personal autorizado.

Criterios de verificación de empleados no
CRITERIO \/ ACCIÓN
Relación
Verificar firma de el solicitante tiene un proveedor, socio estratégico u otros adecuados relación.

Identidad
Compruebe el estado de empleo y la identidad del solicitante en la firma del proveedor\/socio.

No divulgación
Compruebe que el solicitante tiene un acuerdo de confidencialidad firmado en archivo.

Acceso
Remitir la solicitud a la administración cuando la información es clasificada por encima Interna.

Clasificación de datos
CLASIFICACIÓN Y DESCRIPCIÓN \/ PROCEDIMIENTO

Público
Puede publicarse libremente al público

No es necesario verificar.
Interna
Para uso dentro de la empresa

Verifica la identidad del solicitante como empleado activo o acuerdo de no divulgación sobre aprobación de archivo y gestión de los empleados no.

Clasificación de datos (continuada)
CLASIFICACIÓN Y DESCRIPCIÓN \/ PROCEDIMIENTO
Privada
Información de carácter personal destinado sólo dentro de la organización

Verificar la identidad del solicitante como empleado activo o sólo dentro de empleado no con la organización, autorización. Consulte con el departamento de recursos humanos divulgar información privada a los empleados autorizados o solicitantes externos.

Confidencial
Compartido sólo con personas con una necesidad absoluta de saber dentro de la organización

Verificar la identidad del solicitante y necesita saber de información designado
Propietario. Suelte sólo con el consentimiento escrito previo del administrador, o información
Propietario o designatario. Si hay acuerdo de no divulgación en archivo. Sólo
personal de administración podrá revelar a las personas no empleadas por la empresa.

FUENTES

CAPÍTULO 1

BloomBecker, Buck. 1990. Espectacular delitos informáticos: Lo que son y ¿Cómo cuestan estadounidenses Business media mil millones de dólares un Dar. Irwin Publicación profesional.

Littman, Jonathan. 1997. Juego fugitivo: En línea con Kevin Mitnick. Little Brown

Penenberg, Adam L. April 19, 1999. \"La demonización de un pirata informático.\" Forbes.

CAPÍTULO 2

La historia de Stanley Rifldn se basa en las siguientes cuentas:

Instituto de seguridad del equipo. Sin fecha. \"Pérdidas financieras debido a las intrusiones de Internet, robo de secretos comerciales y otros delitos cibernéticos soar.\" Comunicado de prensa. Epstein, Edward Jay. Inédito. \"La invención de diamante\". Holwick, el Reverendo David. Inédito cuenta.

El Sr. Rifkin, él mismo fue amable en el reconocimiento de que las cuentas de su explotación difieren porque él ha protegido su anonimato por el descenso a ser entrevistados.

CAPÍTULO 16

Cialdini, Robert B. 2000. Influencia: Ciencia y práctica, 4ª edición. Allyn y Bacon.

Cialdini, Robert B. febrero de 2001. \"La ciencia de la persuasión\". Científicos Estadounidense. 284:2.

CAPÍTULO 17

Algunas políticas en este capítulo se basan en ideas contenidas en: madera, Charles Cresson. 1999. \"Información directivas de seguridad fácil.\" Software de base.

Agradecimientos

DE KEVIN MITNICK
Verdadera amistad ha sido definido como una sola mente en dos cuerpos; no mucha gente en la vida de nadie puede ser llamada a un verdadero amigo. Jack Biello fue un amante y cuidado persona que habló en contra del maltrato extraordinario soportó en el manos de periodistas inmorales y fiscales del Gobierno entusiasta. Fue un voz clave en el movimiento de Kevin libre y un escritor que tuvo una extraordinaria talento para escribir artículos convincentes exponiendo la información que el Gobierno no quiere que se sepa. Jack siempre estaba allí para hablar sin temor que en mi nombre y a trabajar junto conmigo preparando discursos y artículos, y, en un momento dado, me representan como un enlace de medios de comunicación.

Este libro está dedicado, por tanto, con amor a mi querido amigo Jack Biello, cuya muerte reciente de cáncer igual terminamos el manuscrito me ha dejado sintiendo una gran sensación de pérdida y tristeza.

Este libro no hubiera sido posible sin el amor y el apoyo de mi familia. Mi madre, Shelly Jaffe y mi abuela, Reba Vartanian, tienen me da amor incondicional y el apoyo a lo largo de mi vida. Me siento tan afortunada de se han planteado por tal una amorosa y dedicada madre, que también considero mi Mejor amigo. Mi abuela ha sido como un segundo morn para mí, me que con el mismo cuidado y amor que sólo una madre puede dar. Como cuidar y gente compasiva, has me enseñaron los principios de preocuparse por otros y echar una mano de ayuda a los menos afortunados. Y o, imitando el patrón de cuidar y dar, en un sentido seguir los caminos de sus vidas. Espero que te Perdóname por ponerlos en segundo lugar durante el proceso de escribir esto libro, pasando chances a verlos con la excusa de trabajo y plazos para satisfacer. Este libro no hubiera sido posible sin su continuo amor y apoyo que siempre te tengo cerca a mi corazón.

¿Cómo quiero mi papá, Alan Mitnick y mi hermano, Adam Mitnick, tendría vivió lo suficiente para salto de abrir una botella de champagne conmigo el día esto libro aparece por primera vez en una librería. Como propietario vendedor y negocios, mi padre me enseñó muchas de las cosas buenas que nunca olvidaré. Durante los últimos meses de la vida de mi papá estaba suficientemente afortunado como poder estar a su lado para reconfortarlo lo mejor que pude, pero fue una experiencia muy dolorosa que todavía no la tengo recuperado.

Mi tía pollito Leventhal siempre tendrá un lugar especial en mi corazón;
Aunque ella estaba decepcionada con algunos de los errores estúpidos que he hecho,
Sin embargo ella estaba siempre allí para mí, ofreciendo su amor y apoyo. Durante mi intensa devoción a escribir este libro, sacrificado muchas oportunidades para unirse a

ella, mi primo, Mitch Leventhal y su novio, el Dr. Robert Berkowitz, para nuestra celebración de shabat semanal.

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

Hermano de mi papá claramente merece muchos elogios; se podría decir que heredé de mi oficio de ingeniería social de tío Mitchell, quien supo manipular el mundo y su gente de maneras que nunca espero entender, mucho menos maestro. Suerte para él, nunca tuvo mi pasión por la tecnología de informática durante los años usó su personalidad encantadora para influir en cualquier persona que desee. Él siempre celebrará el título del ingeniero social de gran Maestre.

Y por eso escribo estos agradecimientos, me doy cuenta que tengo tanta gente a dar las gracias y para expresar agradecimiento a para ofrecer su apoyo, amor y amistad. ME no se puede comenzar a recordar los nombres de todos los tipo y gente generosa que has se reunió en los últimos años, pero baste decir que necesitaría un equipo para almacenarlos todos. Ha habido tantas personas de todo el mundo que han escrito a yo con palabras de aliento, elogio y apoyo. Estas palabras han significado un mucho para mí, especialmente durante los tiempos que más lo necesitaba.

Estoy especialmente agradecido a todos mis seguidores que ascendía por mí y pasó sus valioso tiempo y energía salir la palabra a quien escucharía, Expresando su preocupación y objeción sobre mi trato injusto y la hipérbole creado por quienes tratan de sacar provecho de la \"El mito de Kevin Mitnick\".

He tenido la fortuna extraordinaria de se asoció con el autor más vendido Bill Simon y hemos trabajado diligentemente juntos a pesar de nuestras diferentes patrones de trabajo. Bill es altamente organizado, se levanta temprano y trabaja en una deliberada y estilo bien planificada. Estoy agradecido de que Bill fue amable suficiente para acomodar mi horario de trabajo de la noche. Mi dedicación a este proyecto y largas horas de trabajo me mantuvieron bien entrada la madrugada que entraban en conflicto con el horario habitual de trabajo del proyecto de ley.
No sólo fui afortunado al ser asociado con alguien que podía transformar mis ideas en frases (principalmente) es digno de un lector sofisticado, pero también Bill un muy hombre paciente que aguantar con el estilo de mi programador de centrarse en los detalles. De hecho hemos dejado pasar. Aún así, quiero pedir disculpas proyecto de ley en estos agradecimientos que va siempre lamento ser el, porque mi orientación a precisión y detalle, que le llevó a ser tarde para un plazo para la primera y única vez en su larga escribiendo carrera. Un escritor tiene el orgullo que me Finalmente han llegado a comprender y compartir; Esperamos poder hacer otros libros juntos.

El deleite de estar en el casa en Rancho Santa Fe a trabajar y a ser Simon
mimado por la esposa de Bill, Arynne, podría ser considerada un punto culminante de este escrito
proyecto. De Arynne conversación y cocina dará batalla en mi memoria para primero
lugar. Ella es una dama de calidad y sabiduría, llena de alegría, que ha creado una casa de
calidez y belleza. Y nunca voy beber un refresco de dieta nuevamente sin audiencia
Voz de Arynne en el fondo de mi mente me advertía sobre los peligros de
Aspartamo, Stacey Kirkland significa mucho para mí. Ella ha dedicado muchos
horas de su tiempo ayudando a me en Macintosh para diseñar las tablas y gráficos
ayudó a dar autoridad visual a mis ideas. Admiro sus cualidades maravillosas;
Ella es realmente una persona amorosa y compasiva que merece sólo lo bueno
en la vida. Ella me dio aliento como un amigo de cuidado y es alguien que me importa
profundamente sobre. Deseo darle las gracias por todo su apoyo amoroso y por estar ahí
para mí siempre lo necesitaba.
Alex Kasper, Nexspace, es no sólo mi mejor amigo, sino también un socio de negocios
y colega. Juntos organizamos un popular Internet talk radio show conocido como
There was an error deserializing the object of type System.String. Encountered unexpected character 'o'.
orientación del programa Director David g. Hall. Alex gentilmente proporcionado su
una valiosa asistencia y asesoramiento a este proyecto de libro. Su influencia ha siempre
sido positiva y útil con una bondad y generosidad que frecuentemente se extiende mucho
más allá de la medianoche. Alex y he terminado recientemente una película o vídeo para ayudar a las em
capacitar a su gente en la prevención de ataques de ingeniería social.

Paul Dryman, decisión informada, es un amigo de la familia y más allá. Esto altamente
respeto y confianza de investigador privado me ayudó a entender las tendencias y
procesos de investigaciones de fondo. Conocimiento de Paul y
experiencia me ayudó a enfrentar al personal descrita en la parte 4 de problemas de seguridad
este libro.

Uno de mis mejores amigos, Candi laico, siempre me ha ofrecido apoyo y
amor. Realmente es una persona maravillosa que merece lo mejor de la vida. Durante la
trágicos días de mi vida, Candi siempre ofreció aliento y amistad. Soy
afortunados que han cumplido con esa maravilloso y cuidado compasivo ser humano,
y quiero darle las gracias por estar ahí para mí.

Sin duda mi primer cheque de regalías se destinará a mi compañía de teléfono celular para todos los
tiempo que pasé hablando con Erin Finn. Sin duda, Erin es como mi alma gemela.
Somos iguales en tantos formas es aterrador. Ambos tenemos un amor
para la tecnología, los mismos gustos en comida, música y películas. AT
definitivamente perder dinero para darme todas las llamadas de \"huir de noches y fines de semana\" a
su casa en Chicago. Por lo menos no estoy utilizando el plan de Kevin Mitnick ya.
Su entusiasmo y su creencia en este libro habían potenciado mis espíritus. Que suerte estoy a
tenerla como un amigo.

Estoy ansioso por dar las gracias a aquellas personas que representan mi carrera profesional y dedicado de manera extraordinaria. Mis charlas son administradas por Amy Gray (una honesta y cuidar persona que admiro y adoro) David Fugate, de Producciones imponente, es un agente de libro que fue a batear para mí en muchos ocasiones antes y después de que se firmó el contrato de libro; y Los Angeles abogado Gregory Vinson, que estuvo en mi equipo de defensa durante mi años de duración batalla con el Gobierno. Estoy seguro de que él puede relacionar con la comprensión del proyecto de ley y paciencia para mi estrecha atención a los detalles; ha tenido el mismo trabajo de experiencia conmigo en documentos jurídicos ha escrito en mi nombre.

He tenido muchas 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, intensificado y se ofreció a ayudarme cuando estaba en necesidad desesperada. De las palabras amables a implicación profunda con mi caso, conocí a muchos que no encajan en absoluto el estereotipo de la Procuraduría egocéntrico. ME han llegado a respetar, admirar y apreciar la bondad y la generosidad de espíritu que me han dado tan libremente por tantos. Cada uno de ellos merece ser reconocidos con una párrafo palabras favorables; Por lo menos mencionaré les todo por su nombre, para cada uno de ellos vive en mi corazón rodeado de reconocimiento: Greg Aclin, Bob Carmen, John Dusenbury, Sherman Ellison, Omar Figueroa, Carolyn Hagin, robar Hale, Alvin Michaelson, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Richard Sherman, omitir Pizarras, Karen Smith, Richard Steingard, el Honorable Robert Talcott, Barry Tarlow, John Yzurdiaga y Gregory Vinson.

Aprecio mucho la oportunidad de John Wiley al autor de este libro y su confianza en un autor de primera vez. Quiero dar las gracias las siguientes personas Wiley que hicieron 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, asociados de negocios que han dado me asesoramiento y apoyo y han llegado a de muchas maneras, son importantes para reconocer y reconocer. Son: j. j. Abrams, David Agger, Bob Arkow, Stephen Barnes, Dr. Robert Berkowitz, Dale Coddington, Eric Corley, Delin Cormeny, Ed Cummings, Art Davis, Michelle Delio, Sam Downing, John Draper, Paul Dryman, Nick Duva, Roy Eskapa, Alex Fielding, Lisa Flores, Brock Franco, Steve Gibson, Jerry Greenblatt, Greg Grunberg, Bill manejar, David G. Detener, Dave Harrison, Leslie Herman, Jim Hill, Dan Howard, Steve Hunt, Rez Johar, Steve Knittle, Gary Kremen, Barry Krugel, Earl Krugel, Adrian Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, CJ poco, Jonathan Littman, marcar Maifrett, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Munoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Kevin Poulsen, prensa Scott, Linda y Art Pryor,

Jennifer Reade, Israel y Rachel Rosencrantz, Mark Ross, William Royer, Irv Rubin, Ryan Russell, Neil Saavedra, Schwartu Wynn, Pete Shipley, Joh tamizar, Dan Sokol, Trudy Spector, Matt Spergel, Eliza Amadea Sultan, Douglas Thomas, Roy There was an error deserializing the object of type System.String. Unexpected end of file. Following el Wortman, Steve Wozniak y todos mis amigos en el W6NUT (147.435 MHz) repetidor en Los Angeles.

Y mi agente de libertad vigilada, Larry Hawley, merece especial agradecimiento por haberme dado autorización para actuar como asesor y consultor en asuntos relacionados con la seguridad edición de este libro.
Y por último debo reconocer los hombres y mujeres de la aplicación de la ley. ME simplemente no tienen ninguna malicia hacia estas personas que sólo están haciendo su trabajo. Creo firmemente que poner el interés del público por delante de uno propio y dedicar su vida al servicio público es algo que merece respeto, y
Si bien he sido arrogante a veces, quiero que todos ustedes saben que me gusta mucho este país y hará cuanto esté en mi poder para ayudar a hacer el lugar más seguro el mundo, que es precisamente una de las razones de por qué he escrito este libro.

DE BILL SIMON
Tengo esta idea de que hay una persona correcta que hay para todos; es justo algunas personas no suerte nunca a encontrar sus Sr. o la Sra. derecho. Otros suerte. Tengo suerte lo suficientemente temprano en la vida para pasar un buen hace ya muchos años (y contar con muchos más el gasto) con uno de los tesoros de Dios, mi esposa, Arynne... Si Nunca olvido que suerte estoy, basta con prestar atención a cuántas personas Buscamos y apreciamos su compañía. Arynne--gracias por caminar por la vida con Me.

Durante la escritura de este libro, conté con la ayuda de un fiel grupo de amigos que proporciona la garantía de que Kevin y yo estábamos logrando nuestro objetivo de hecho de combinar y fascinación en este insólito libro. Cada una de estas personas representa el valor verdadero y leal y sabe que él o ella puede denominarse como llego en mi próximo proyecto de escritura. En orden alfabético: Jean-Claude Beneventi, Linda Brown, Brown de Walt,. General Don Johnson, Dorothy Ryan, Guri Stark, Chris Empinada, Michael Steep y John Votaw.
Reconocimiento especial va a John Lucich, Presidente de la seguridad de red Grupo, que estaba dispuesto a dedicar tiempo para un amigo-de petición de un amigo y a Vestimenta de Gordon, quien amablemente envió numerosas llamadas telefónicas sobre las operaciones d

A veces en la vida, un amigo gana un lugar exaltado por la presentación de alguien otro que se convierte en un buen amigo. En agencia literaria Waterside producciones, en Cardiff, California, agente David Fugate fue responsable de concebir la idea para este libro y para ponerme junto con co-author-convertido-amigo Kevin. Gracias, David. Y a la cabeza de Waterside, el incomparable Bill Gladstone,

¿Quién administra para mantenerme ocupado con el proyecto de un libro tras otro: me alegra tenerte en mi en la esquina.

En nuestro hogar y mi Oficina en casa, Arynne es ayudado por un capaz de personal que incluye asistente administrativo Jessica Dudgeon y ama de llaves Josie Rodriguez.

Agradezco a Mis padres Marjorie y i. B. Simon, que ojalá estuviera aquí en la tierra disfrutar de mi éxito como escritor. También quiero agradecer a mi hija, Victoria. Cuando estoy con ella me doy cuenta de lo mucho que admiro, respeto y orgullo en quien ella es.

Analizado por kineticstomp

Suplemento

SWIFT

[Capítulo 1 - prohibido Edition]

Historia de Kevin

Por Kevin Mitnick

Yo era reacio a escribir esta sección porque estaba seguro de que sonaría self-sirviendo. Bueno, está bien, es egoísta. Pero he sido contactado por literalmente cientos de personas que quieren saber \"quién es Kevin Mitnick?\". Para aquellos que no dan un carajo, por favor dirigirse a capítulo 2. Para todo el mundo, aquí, por lo que Vale, es mi historia.

Kevin habla algunos piratas informáticos destruyen archivos del pueblo o las unidades de Bardo todo; son llamado galletas o vándalos. Algunos piratas informáticos novato no te molestes en aprendizaje el la tecnología, pero simplemente Descargar herramientas de hackers de irrumpir en los sistemas informáti llamamos a script kiddies. Hackers más experimentados con conocimientos de programación desarrollar programas de hacker y publicarlos en la Web y Boletín sistemas. Y luego hay personas que no tienen ningún interés en la tecnología, pero el equipo simplemente como una herramienta para ayudarlos en robar dinero, bienes, o servicios. A pesar del mito creado por medio de Kevin Mitnick, no soy un malintencionado hacker. Lo que hice no fue incluso en contra de la ley cuando comenzó, sino se convirtió en un delito después fue aprobada la nueva legislación. Siguen de todos modos y fue capturado. Mi tratamiento por el Gobierno federal estaba basado no en los crímenes, sino en hacer un ejemplo de mí. No merezco ser tratada como un terrorista o violento penales: tener mi residencia buscado con una orden de búsqueda en blanco; ser inicia en solitario durante meses; niegan los derechos constitucionales fundamentales garantiza a toda persona acusada de un delito; se les niega no sólo libertad bajo fianza pero una fianza audiencia; y se vieran obligados a pasar años luchando por obtener el Gobierno pruebas para que mi Tribunal designado abogado podría preparar mi defensa.

¿Mi derecho a un juicio rápido? Durante años me concedieron una elección cada seis meses: firmar un documento de renuncia a su derecho constitucional a un juicio rápido o ir a juicio con un abogado que está desprevenido; Elegí a firmar. Pero me estoy poniendo por delante de mi historia. Empezando por mi camino probablemente se estableció temprano en la vida. Fui un feliz-ir

suerte chaval, pero aburrido. Después mi padre cuando yo tenía tres años, mi madre trabajaba como camarera para apoyarnos. A ver me luego un hijo único, siendo criado por un madre que ponen en días largos, hostigados en una programación a veces errática tendría sido al ver a un joven en sus propio casi todas sus horas vigilia. Era mi propia niñera. Creció en una comunidad del Valle de San Fernando me dio todo de Los Angeles para explorar y a los doce años había descubrí una forma de viajar gratis en toda la zona de L.A. todo mayor. Me di cuenta un día, mientras el caballo el autobús que la seguridad de los traslados en autobús que había comprado dependía de la inusual patrón de la perforadora de papel que los controladores utilizados para marcar el día, hora y ruta en los resguardos de transferencia. Un conductor amable, responder a mi pregunta cuidadosamente plantados me dónde comprar ese tipo especial de punch. Las transferencias están diseñadas para permitirle cambiar autobuses y continuar un viaje a su destino, pero he trabajado cómo utilizar para viajar a cualquier lugar que quería ir por libre. Obtener a transferencias en blanco fue un paseo por el Parque: siempre estaban llenos de las papeleras en las terminales de autobuses sólo en parte utilizado libros de transferencias que los controladores arrojó lejos al final de su turnos. Con un pad de espacios en blanco y el puñetazo, pude Marcar mis propias transferencias y viajar a cualquier lugar que iba de autobuses L.A.. En poco tiempo, pero todo había memorizado el horarios de autobuses de todo el sistema. Esto fue un ejemplo temprano de mi sorprendente memoria para ciertos tipos de información; aún así, hoy puedo recordar teléfono números, contraseñas y otros elementos como en mi infancia. Otro interés personal que surgieron en una edad temprana fue mi fascinación con la realización de magia. Una vez que aprendí cómo funcionaba un truco nuevo, sería práctica, práctica, y práctica hasta que lo domina. En cierta medida, era a través de la magia que descubrí el disfrute de la gente. Desde teléfono Phreak, a mi primer Hacker encuentro con lo que sería eventualmente aprendo llamar ingeniería social llegó sobre durante mi alta escuela de años, cuando conocí a otro estudiante que fue pillada hasta en un hobby llamado teléfono phreaking. Teléfono phreaking es un tipo de piratería le permite explorar la red telefónica mediante la explotación de los sistemas telefónicos y empleados de la compañía de teléfono. Me mostró aseados trucos que podía hacer con una teléfono, como obtener cualquier información de la compañía telefónica en cualquier cliente y utilizando un secreto prueba número para hacer llamadas de larga distancia gratis realmente libre sólo a nosotros--descubrí mucho más tarde que no era un número secreto de prueba a todos: las llamadas fueron en realidad se facturan a algunos pobres empresa MCI). Fue mi introducción a la ingeniería social-mi jardín de infantes, por así decirlo. Él y otra phreaker de teléfono que conocí poco después me deja escuchar como cada uno de ellos hizo llamadas de pretexto a la compañía telefónica. He escuchado las cosas dijeron les suenan creíbles, aprendí sobre las oficinas de la empresa de teléfono diferente, lingo y procedimientos. Pero que la \"formación\" no duró mucho; no tuve que. Pronto estaba hacer que todos en mi propia, aprendiendo como fui, haciendo incluso mejor que los primeros profesores. Se ha creado el curso de que mi vida seguiría durante los próximos quince años.

Uno de mis bromas favoritas de todos los tiempos fue obtener acceso no autorizado a la conmutador telefónico y cambiar la clase de servicio de un compañero por teléfono phreak.

Cuando él intentó hacer una llamada desde su casa, obtendría un mensaje diciéndole que depositar un centavo, porque la Telefónica empresa recibida de entrada indicó que estaba llamando desde un teléfono público.

Me convertí en absorbida en todo lo relacionado con teléfonos, no sólo de la electrónica, conmutadores y equipos; pero también la organización empresarial, los procedimientos, y la terminología. Después de un tiempo, probablemente sabía más sobre el sistema de teléfono que cualquier empleado solo.

Y, había desarrollado mis habilidades de ingeniería social hasta el punto que, a los diecisiete años años edad, fui capaz de hablar la mayoría empleados de telecomunicaciones en casi nada, si Yo estaba hablando con ellos en persona o por teléfono. Mi carrera pirateo comenzado cuando estaba en secundaria. Entonces usamos el hacker de plazo a una persona que pasó mucho tiempo retoques con hardware y software, ya sea para desarrollar programas más eficientes o a omitir los pasos innecesarios y conseguir el trabajo hacer más rápidamente. El término se ha convertido en un peyorativo, llevando el significado de \"delincuente malicioso\". En estas páginas utilizo el término de la manera que siempre he usado que en su sentido más benigno, anterior. A finales de 1979, un grupo de compañeros hacker tipos quienes trabajaron para el distrito escolar unificado de Los Ángeles atrevió me intentar hackear en el arca, el sistema informático en Digital Equipment Corporation utiliza para desarrollo de su software de sistema operativo RSTS\/E. Quería ser aceptado por los chicos de este grupo de hackers por lo que pude recoger sus cerebros para obtener más información a sistemas operativos. Estos nuevos \"amigos\" han logrado tener en sus manos la número telefónico para el sistema informático de DEC. Pero ellos sabían el número telefónico no me hacen ningún bien: sin un nombre de cuenta y contraseña, nunca podría ser capaz de conseguir. Estaban a punto de descubrir que cuando usted subestima a otros, puede volver a morder le en el trasero. Resultó, para mí, incluso en ese joven, piratería en el sistema de DEC fue un pushover. Afirmando ser Anton Chernoff, uno de los proyecto llevar los desarrolladores, puse una simple llamada telefónica a la Administrador del sistema. Dijo no se ha podido iniciar sesión en uno de \"Mis\" cuentas y fue convencer lo suficiente como para hablar del chico para que me den acceso y permitirme Seleccione una contraseña de mi elección.Como un nivel adicional de protección, siempre que nadie ha marcado en el sistema de desarrollo, el usuario tenía también proporcionar un acceso telefónico contraseña. El administrador del sistema me dijo la contraseña. Fue \"bufón\", que supongo que describe lo que debe haber sintió como posteriormente cuando mentira descubrió lo que había sucedido. En menos de cinco minutos, que había obtenido acceso a Digital Sistema de desarrollo de RSTE\/E. Y no estaba registrado tan sólo como un usuario normal, pero como alguien con todos los privilegios de un programador de sistemas. Al principio mi nuevo amigos llamados se negaron a creer que había obtenido acceso a The Ark. Uno de ellos marcado por el sistema y empujada del teclado delante de mí con un desafiante mirar en su rostro. Su boca bajó a abrir como sarcasmo iniciado sesión en una cuenta con privilegios. Me enteré después que marchó a otro lugar y, el mismo día, comenzó a descargar componentes de código fuente del DEC

Sistema operativo. Y entonces fue mi turno de ser pisos. Después tuvieron
Descargar todo el software que querían, que llamaron la seguridad corporativa
Departamento en DEC y les dijo que alguien había hackeado en la empresa
red corporativa. Y dieron mi nombre. Mis amigos llamados utilizadas por primera vez mi
acceso para copiar el código fuente muy sensible y luego se me convirtió.

Hubo aquí una lección, pero no uno pude aprender fácilmente. A través de los años
por venir, repetidamente obtendría en problemas porque yo confié en las personas que me
pensamiento eran mis amigos. Después de la escuela secundaria estudié equipos en el equipo
Centro de aprendizaje en Los Angeles.

Dentro de unos meses, manager del equipo de la escuela se dio cuenta de que había encontrado un
vulnerabilidad en el sistema operativo y obtuvo privilegios administrativos completos en
su minicomputadora de IBM. Los mejores expertos del equipo de su personal docente
no se ha podido averiguar cómo lo había hecho. En lo que pudo haber sido uno de los primeros
ejemplos de \"alquiler del hacker\", me dio una oferta no podía rechazar: hacer un
proyecto para mejorar la seguridad del equipo de la escuela, o enfrentar la suspensión de honores
el sistema de hacking. Por supuesto decidió hacer el proyecto de honores y terminó
se graduó Cum Laude con honores. Convirtiéndose en un Social ingeniero algunas personas
levantarse de la cama cada mañana horrorizado su rutina de trabajo diaria en la proverbial
minas de sal. He tenido la suerte de disfrutar de mi trabajo. En particular no se puede
Imagine el desafío, recompensa y placer que tenía en el tiempo que pasé como un privado
investigador. Yo estuve afilando mis talentos en el arte de performance llamado social
Ingeniería recibiendo gente a hacer cosas que normalmente no hacen por un extraño-
y ser pagado por ello. Para mí no fue difícil convertirse en experto en social
Ingeniería. Había sido parte de mi padre de la familia en el campo de ventas para
generaciones, por lo que el arte de la influencia y la persuasión podría haber sido un heredado
rasgo. Cuando combinas una inclinación para engañar a las personas con los talentos de
influencia y persuasión que llegas en el perfil de un ingeniero social. Usted podría
decir que hay dos especialidades dentro de la clasificación de puestos del estafador. Alguien
que estafas y trampas de gente de su dinero pertenece a un sub-specialty,
grifter. Alguien que utiliza el engaño, la influencia y la persuasión contra
las empresas, generalmente dirigidas a su información, pertenece a los otro sub-specialty,
el ingeniero social. Desde el momento de mi truco de transferencia de bus, cuando yo era demasiado joven
saber que no había nada malo con lo que estaba haciendo, había comenzado a
reconocer un talento para descubrir los secretos que no se supone que tienen. Construí
ese talento mediante engaño, conocer la jerga y desarrollando un un
habilidad de manipulación.

Una forma que solía trabajar en el desarrollo de las habilidades en mi oficio (si puedo llamarlo un
artesanía) fue destacar algún dato realmente no importa y ver
Si pude hablar alguien en el otro extremo del teléfono en proporcionar, sólo
mejorar mi talento. De la misma manera que solía practicar mis trucos de magia, me

practica pretexting. A través de estos ensayos, encontré pronto que pude adquirir prácticamente cualquier información que dirigido. En su testimonio del Congreso ante senadores Lieberman y Thompson años más tarde, les dije, he ganado no autorizado\" acceso a sistemas informáticos en algunas de las corporaciones más grandes del planeta, y han penetrado con éxito algunos de los sistemas informáticos más resistentes jamás desarrollado. He utilizado medios técnicos y no técnicos para obtener el código fuente para diversos sistemas operativos y dispositivos de telecomunicaciones estudio de sus vulnerabilidades y su funcionamiento interno\". Todo esto fue realmente satisfacer mi curiosidad, ver lo que podía hacer y encontrar información secreta acerca de sistemas operativos, teléfonos celulares y cualquier otra cosa despertó mi curiosidad. El tren de eventos que cambiaría mi vida comenzado cuando me convertí en el tema un 04 de julio de 1994 primera plana, por encima de pliegue historia en el New York Times. Durante la noche, que una historia convertido mi imagen desde una molestia poco conocida de una hacker en público enemigo número uno del ciberespacio. John Markoff, el Grifter de los medios de comunicación

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
Mitnick es un programador de computadoras ejecutar amok\". (El New York Times, 04\/07\/94.) La combinación del edad de edad deseo alcanzar inmerecida fortuna con el poder publican historias falsas y difamatorias sobre sus súbditos en la portada de la New York Times, John Markoff fue verdaderamente un reportero de tecnología ejecutar amok. Markoff fue ganar él mismo más 1 millón de dólares mediante la creación de lo que él solo etiqueta \"El mito de Kevin Mitnick\". Llegó a ser muy rico a través de la muy misma técnica que usé para comprometer sistemas informáticos y redes de todo el Mundial: engaño. En este caso, sin embargo, no era la víctima del engaño un único usuario o administrador del sistema, es cada persona que confía en el Noticias publicaron en las páginas de la mayoría de los Times.Cyberspace Nueva York Quería el artículo del Times de Markoff fue claramente diseñado para aterrizar un contrato para una libro sobre la historia de mi vida. Nunca he conocido a Markoff, y sin embargo se ha convertido literalm un millonario a través de su difamatorias y calumniosas \"informes\" acerca de mí en el Veces y en su libro de 1991, Cyberpunk. En su artículo, incluyó algunas decenas denuncias sobre mí que declaró como hecho sin citar sus fuentes y incluso un proceso mínimo de hecho comprobar (que pensé todo navío periódicos requieren sus reporteros hacer) habría revelado como falso o no probada. En el único artículo falso y difamatorio, Markoff etiquetados como yo
There was an error deserializing the object of type System.String. Encountered unexpected character 'a'.
criminales,\"sin justificación, razón o evidencias, con no más discreción que un escritor de un tabloide de supermercado. En su artículo calumnioso, Markoff falsamente que había wiretapped el FBI (no); que tenía dividido en los equipos a NORAD (que aún no estén conectados a cualquier red en el exterior); y que yo era un equipo \"vándalos\", a pesar de que Había dañado nunca intencionalmente cualquier equipo que nunca visitada. Estos, entre otras denuncias escandalosas, eran completamente falsas y diseñado para crear un

sensación de temor acerca de mis capacidades. En otra violación de la ética periodística, Markoff no pudo revelar en dicho artículo y en todos sus posteriores a artículos preexistente relación conmigo, una animosidad personal basada en mi haber se negó a participar en el libro, además de Cyberpunk, había le costó un paquete de los ingresos potenciales por negarse a renovar una opción para una película basada en la libro. Artículo de Markoff fue también claramente diseñado para mofarse de la ley de los Estados Unidos organismos de represión.

There was an error deserializing the object of type System.String. Encountered unexpected character 'M'. artículo fue engañó deliberadamente ponerme como número de enemigo público del ciberespacio Uno para influir en el departamento de justicia para elevar la prioridad de mi caso. Unos meses más tarde, serían de Markoff y su cohorte de Tsutomu Shimomura Ambos participan a agentes del Gobierno como de facto en mi detención, en violación de ambos la Ley Federal y la ética periodística. Ambos serían cercanos al blanco tres órdenes fueron utilizados en una búsqueda ilegal de mi residencia y estar presente en mi arresto. Y, durante su investigación de mis actividades, los dos también violaría Ley Federal por interceptar una llamada telefónica personal mío. Al tiempo que me ser un villano, Markoff, en un artículo posterior, configurar Shimomura como la héroe número uno del ciberespacio. Nuevamente estaba violando la ética periodística por no revelar una relación preexistente: este héroe en realidad había sido amigo personal de Markoff durante años. Mi primer encuentro con Markoff había llegado a finales los años ochenta, cuando él y su esposa Katie Hafner contactaron conmigo mientras estaban en el proceso de la escritura Cyberpunk, que iba a ser la historia de tres hackers: un Niño alemán conocido como Pengo, Robert Morris y yo mismo.

¿Cuál sería mi indemnización por participar? Nada. No pude ver la punto de darles mi historia si beneficiaría de ella y yo no, lo se negó a ayudar. Markoff me dio un ultimátum: o bien entrevista con nosotros o todo lo que oímos de cualquier origen sea aceptado como la verdad. Fue claramente frustrado y molesto que no cooperaría y fue dejarme saber él tenían los medios para hacerme arrepentir. Eligieron a mi tierra y no cooperar a pesar de sus tácticas de presión. Cuando se publicó, el libro retrata como yo There was an error deserializing the object of type System.String. End element 'root' from namespace " e no admitidas, falsas declaraciones a fin de volver a mí por no cooperar con ellos. Haciendo mi personaje aparecen más siniestro y me casting en un falso luz, probablemente aumentaron las ventas del libro. Telefoneó a un productor de la película con una gran noticia: Hollywood estaba interesado en hacer una película acerca de la Darkside Hacker representado en Cyberpunk. Señalé que la historia estaba llena de imprecisiones y falsedades sobre mí, pero todavía estaba muy emocionado por la proyecto. Acepté $5.000 para una opción de dos años, contra un adicional de $45.000 si eran capaces de obtener un contrato de producción y avanzar. Cuando la opción caducado, la productora pidió una prórroga de seis meses. En este momento me fue remunerado y tuvo poca motivación para ver una película producida

me mostró en una luz desfavorable y falsa. Me negué a ir junto con
la extensión. Que mató el negocio de película para todos, incluyendo Markoff, quien
probablemente esperaba hacer una gran cantidad de dinero del proyecto. Aquí fue
una razón más para John Markoff ser vengativos hacia mí. En la época
Cyberpunk fue publicado, Markoff mantuvo correspondencia de correo electrónico permanente con su
amigo Shimomura. Curiosamente ambos estaban interesados en mi paradero
y lo que estaba haciendo. Sorprendentemente, un mensaje de correo electrónico contiene inteligencia
que ellos habían aprendido asistía a la Universidad de Nevada, Las Vegas, y
tenía el uso del laboratorio de computación de estudiante. Podría ser que Markoff y Shimomura
¿estaban interesados en hacer otro libro acerca de mí? De lo contrario, ¿por qué se les importa
¿lo que fui hasta? Markoff en persecución tomar un paso hacia finales de 1992. Fui acercando
al final de mi liberación supervisada para comprometer el equipo Digital
Red corporativa de la Corporación. Mientras tanto me di cuenta que el Gobierno
estaba tratando de armar otro caso contra mí, ésto para llevar a cabo
contrainteligencia para averiguar por qué se habían colocados pinchazos en las líneas de teléfono
de una empresa de Los Angeles P.II. En mi excavación, he confirmado mi sospecha: el Pacífico
Gente de seguridad Bell de hecho estaban investigando la firma. Así que fue un delito informático
Adjunto del Departamento del Sheriff del Condado de Los Angeles. (Que adjunto activa
fuera a ser co-casualmente, el hermano gemelo de mi coautor de este libro. Pequeño
mundo.) Acerca de este tiempo, los Feds configurar un informante criminal y lo envió a
atrapan me. Sabían que siempre intentaba mantener fichas en cualquier agencia de investigación
Me. Así que tuvieron este informante me amistad y sugerencia que me que estaba siendo
supervisados. También compartió conmigo los detalles de un sistema informático utilizado en
Pacific Bell que me dejaría hacer Contravigilancia de su vigilancia. Cuando
He descubierto su complot, rápidamente las tablas le traicionara y le expuso para
fraude con tarjetas de crédito estaba llevando a cabo mientras trabajaba para el Gobierno en un
capacidad del Informador. Estoy seguro de que la Feds aprecia! Mi vida cambió en
Día de la independencia, cuando mi localizador me despertó en la madrugada de 1994. El
llamador dijo que inmediatamente debo recoger una copia del New York Times. ME
no podía creerlo cuando vi que Markoff no sólo había escrito un artículo sobre
Me, pero los tiempos habíamos colocado en la portada. El primer pensamiento que llegó a
mente era para mi seguridad personal-ahora el Gobierno sería sustancialmente
aumentar sus esfuerzos para encontrarme. Estaba aliviado que en un esfuerzo para demonizar
Me, el Times había utilizado una imagen muy impropia. Yo no estaba temeroso de ser
reconoció que habían escogido una imagen tan obsoleto que no mira nada
como yo! Como comencé a leer el artículo, me di cuenta que era establecer Markoff
el propio hasta para escribir el libro de Kevin Mitnick, igual que siempre había querido. ME
simplemente no podía creer el New York Times correría el riesgo de imprimir el
claramente falsas declaraciones que él había escrito acerca de mí. Me sentí impotente. Incluso si
Había estado en condiciones de responder, sin duda no tendría una audiencia igual
en el New York Times s para rebatir las mentiras escandalosas de Markoff. Si bien estoy de acuerdo
ha sido un dolor en el culo, yo nunca había destruido información ni utilizados o
divulgada a terceros cualquier información que había obtenido. Pérdidas reales de las empresas

desde mis actividades piratas ascendieron al costo de llamadas telefónicas que había hecho en gastos de la compañía telefónica, el dinero invertido por las empresas para tapar la seguridad vulnerabilidades que mis ataques había revelado y en algunos casos posiblemente empresas causa a instalar sus sistemas operativos y aplicaciones de miedo I podría han modificado el software en una forma que me permitiera acceso en el futuro. Aquellos las empresas habrían quedado vulnerables a daños mucho peor si mis actividades no había hecho consciente de los puntos débiles en su cadena de seguridad. Aunque tuve causó algunas pérdidas, mis acciones y las intenciones no eran malintencionadas... y, a continuación, John Markoff cambió la percepción del mundo del peligro que representaba. El poder de un reportero poco ética de tal un influyente periódico escribir un falso y historia difamatorio sobre alguien debería rondar todos y cada uno de nosotros. El siguiente destino podría ser usted.

Después de mi detención fui transportado a la cárcel de condado en Smithfield, norte Carolina, donde el servicio de Marshals de los Estados Unidos ordenó a carceleros para colocarme en ' el Hole'-incomunicación. Dentro de una semana, los fiscales federales y mi abogado llegaron a un acuerdo que yo no podía negarse. Podría ser trasladado fuera del régimen la condición de que renunciar a mis derechos fundamentales y que acordaron: un) sin fianza audiencia; b) ninguna audiencia preliminar; y c) no hay llamadas telefónicas, excepto con mi abogado y dos miembros de la familia. Signo y podríamos sacar de solitario. Firmé.El fiscales federales en el caso jugaron cada trastada en el libro hasta fue lanzado casi cinco años más tarde. Varias veces me he visto obligado a renunciar a mis derechos en orden a ser tratada como cualquier otro acusado. Pero este fue el caso de Kevin Mitnick: No existían reglas. Sin necesidad de respetar los derechos constitucionales de los acusado. Mi caso no era sobre la justicia, pero sobre el del Gobierno determinación de ganar a toda costa. Los fiscales habían hecho enormemente exagerados reclamos a la Corte sobre el daño había causado y la amenaza representaba, y los medios de comunicación habían ido a la ciudad citando al sensacionalista declaraciones; ahora era demasiado tarde para los fiscales a echarse atrás. El Gobierno no podía permitirse perder el caso de Mitnick. Estaba viendo el mundo.

Creo que los tribunales compraban el temor generado por los medios de comunicación, desde muchos de los periodistas más éticos han recogido los \"hechos\" de los estimados New York Times y les repite. El mito generado por medios aparentemente incluso miedo funcionarios policiales. Un documento confidencial obtenido por mi fiscal mostró que el servicio de Marshals de los Estados Unidos emitió una advertencia a toda ley agentes encargados de hacer cumplir nunca a revelar cualquier información personal para mí; de lo contra pueden encontrar sus vidas destruidas por vía electrónica. Nuestra Constitución requiere que el acusado se presuma su inocencia antes del juicio, así, conceder a todos los ciudadanos la derecho a una audiencia de fianza, donde el acusado tiene la oportunidad de estar representado por el abogado, presentar pruebas y contrainterrogar a testigos. Increíblemente, el Gobierno había podido eludir estas protecciones basadas en la falsa histeria generada por los reporteros irresponsables como John Markoff. Sin

precedente, me mantuve como preventiva detenido una persona en prisión preventiva o condena-cuatro y medio años. Negativa del juez para que me conceda una fianza audiencia fue litigado todo el camino a la Corte Suprema. Al final, mi equipo de defensa me aconsejó que me había marcado otro precedente: era la federal sólo detenido en la historia de Estados Unidos negó una audiencia de fianza. Esto significaba el Gobierno nun tenían que cumplir con la carga de probar que no hubo ninguna condición de liberación que razonablemente aseguraría mi comparecencia en corte. Al menos en este caso, federal fiscales no se atrevan a alegan que podría iniciar una guerra nuclear por silbar en en un caso anterior había hecho un teléfono público, como otros fiscales federales. La mayoría graves cargos contra mí fueron que yo había copiado código fuente propietaria de varios teléfonos celulares y sistemas operativos más populares. Sin embargo la fiscales denunció públicamente y ante el Tribunal que había causado pérdidas colectivas superior a 300 millones de dólares a varias empresas. Los detalles de las cantidades de pérdida todavía bajo el sello con la Corte, supuestamente proteger a las empresas involucradas; mi equipo de defensa, sin embargo, cree que la petición de la Fiscalía para sellar la información se inició para encubrir sus malversaciones bruto en mi caso. También vale Tomando nota de que ninguna de las víctimas en mi caso informó que las pérdidas para la Securities and Exchange Commission como requiere la ley. O bien varios empresas multinacionales violan en Ley Federal el proceso engañando a la SEC, accionistas y analistas--o las pérdidas atribuibles a mi piratería fueron, de hecho, demasiado trivial para informarse. En su libro él juego fugitivo, Jonathan Li wan informes que dentro de una semana de la historia de primera plana del New York Times, agente de Markoff había There was an error deserializing the object of type System.String. Encountered unexpected character 'w'. acerca de la campaña me rastrear. El avance fue ser un estimado $750.000. Según Littman, había que ser una película de Hollywood, así, con Miramax entrega $200.000 para la opción y \"una total $650.000 para ser pagado al comienzo de la filmación\". Una fuente confidencial ha recientemente me informó que trato de Markoff fue en realidad mucho más de lo que había de Littman originalmente se pensó. Así John Markoff consiguió un millón de dólares, más o menos, y me subí durante cinco años. Un libro que examina los aspectos jurídicos de mi caso fue escrito por un hombre que había sido él mismo un fiscal en el fiscal de distrito de Los Ángeles Oficina, un colega de los abogados que me procesados. En su libro espectacular Los delitos informáticos, Buck Bloombecker escribió, apena me tiene que escribir\" acerca de mis antiguos colegas en términos menos halagador.... Me Admisión de ayudante de Estados Unidos abogado James Asperger que mucha de la argumento utilizado para mantener entre rejas a Mitnick se basaba en rumores que no pan \". Él va a decir, \"era malo suficiente que los fiscales de cargos en la Corte se extendió a millones de lectores por periódicos de todo el país. Pero es mucho peor que esas falsas acusaciones fueron una gran parte de la base para mantener Mitnick tras las rejas sin posibilidad de libertad bajo fianza de contabilización?\" Él sigue con cierto detenimiento, escribiendo sobre las normas éticas que fiscales debe vivir por y, a continuación, escribe, \"caso de Mitnick sugiere que las falsas acusaciones utilizado para mantenerlo custodia perjudicado también la consideración de la Corte de una feria

frase.\" En su artículo de Forbes 1999, describió elocuentemente Adam Penenberg de L.
mi situación de esta manera: \"los crímenes de Mitnick fueron curiosamente inocuos. Rompió
equipos corporativos, pero la evidencia indica que destruyó datos. O vendidos
cualquier cosa que copió. Sí, él hurtadas software pero al hacerlo dejó \". El
artículo dijo que mi crimen fue \"pulgar su nariz en la seguridad del equipo costoso
sistemas empleados por las grandes corporaciones\". Y en el libro The Game fugitivo,
autor Jonathan Littman señaló, \"el Gobierno podría comprender la codicia. Pero un
hacker que ejercían el poder para su propio bien... era algo que no podían
alcance.\" En otros lugares en el mismo libro, Littman escribió: Estados Unidos abogado James
Sanders admitieron a juez Pfaelzer que daños de Mitnick a DEC no estaba la 4 $
millones que habían hecho los titulares pero $160.000. Incluso esa cantidad no era
daños causados por Mitnick, pero el coste bruto de seguimiento de las deficiencias de seguridad que
sus incursiones habían traído a la atención de DEC. El gobierno reconocido
no tenía ninguna evidencia de las reclamaciones silvestres que habían ayudado a celebrar Mitnick sin fianz
en régimen de incomunicación. Ninguna prueba Mitnick nunca había comprometido la seguridad de
la NSA. Ninguna prueba que Mitnick nunca había emitido un falso comunicado de prensa para la segurida
Banco del Pacífico. Ninguna prueba que Mitnick cambiado nunca la TRW de crédito informe de un
juez. Pero el juez, tal vez influenciado por la aterradora de medios de comunicación,
rechazó el acuerdo y condenado Mitnick a continuación a un largo plazo, incluso la
el Gobierno quería. A lo largo de los años que pasó como un aficionado de hacker, has
ganó notoriedad no deseado, se ha redactado en numerosos informes de noticias y
artículos de revistas, y han escrito cuatro libros sobre mí. Markoff y
Libro calumnioso de Shimomura fue convertida en una película llamada Takedown. Cuando
la secuencia de comandos que encontró su camino en Internet, muchos de mis partidarios señaladas
Miramax Films para llamar la atención pública a la caracterización inexacta y falsa
de mí. Sin la ayuda de muchos tipo y gente generosa, the motion picture
seguramente habría falsamente interpretado me como el Lector de Aníbal del ciberespacio.
Presionado por mis partidarios, la productora decidieron resolver el caso en
términos confidenciales para evitar que me presentar una acción de difamación contra ellos.

Reflexiones finales

A pesar de John Markoff indignantes y calumniosas descripciones de mí, mi
crímenes fueron simples delitos de traspaso del equipo y hacer llamadas telefónicas gratuitas.
He reconocido desde mi detención que las acciones que tomó fueron ilegales ya
compromiso de invasiones de privacidad. Pero sugerir, sin justificación, razón, o
prueba, al igual que los artículos Markoff, había privó a otros de su dinero o
propiedad por fraude de equipo o alambre, es simplemente falsa y no admitida por el
pruebas. Mis fechorías estaban motivados por curiosidad: yo quería saber tanto
como pude sobre el funcionamiento de redes de telefonía y los entresijos del equipo
seguridad. Pasé de ser un niño que le encantaba realizar trucos de magia para convertirse en
hacker más famoso del mundo, temido por las corporaciones y el Gobierno.
Como pienso volver en mi vida durante los últimos treinta años, admito que he hecho algunos

decisiones extremadamente pobres, impulsadas por mi curiosidad, el deseo de aprender acerca de la tecnología y un buen reto intelectual. Ahora soy una persona cambiada. Soy volviendo a mi talento y los conocimientos que he reunido acerca de la información tácticas de ingeniería social y la seguridad para ayudar a gobierno, empresas y individuos prevención, detectan y responden a las amenazas de seguridad de la información. Esto libro es una forma más que puedo utilizar mi experiencia para ayudar a otros a evitar la esfuerzos de los ladrones de información malintencionada del mundo. Creo que encontrará el reveladora agradable, historias y educativos.

Kevin Mitnick

Capítulo que se encuentra perdida de Mitnick

Por Michelle Delio
Wired.com, 05 de noviembre de 2002

Se ha publicado un capítulo falta de libro reciente del hacker Kevin Mitnick en la 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 uno apareció sólo en unos 300 galera independiente copia esa publicación empresa Wiley distribuido a los medios de comunicación varios meses antes de lanzar la libro, de acuerdo con un portavoz de Wiley.

La editorial decidió eliminar el capítulo poco antes de soltar el libro. Wiley representantes no pudieron comentar inmediatamente por qué el capítulo fue retirado.

El capítulo contiene la primera relata por Mitnick de su vida como un hacker y un fugitivo, así como su detención, juicio y prisión perpetua.

El capítulo incluye también denuncias por Mitnick John Markoff, tecnología reportero de The New York Times, imprime historias malintencionadas sobre Mitnick durante años de hacker como un fugitivo.

El capítulo faltante fue el primer hecho sábado finales disponibles al público en un Yahoo Grupo de discusión llamado \"Historia de Kevin\". Desde entonces ha aparecido en otros sitios Web.

Mitnick dijo que no sabía que había publicado en línea el capítulo. Envía un correo electrónico a la dirección de Yahoo.com enumerado con el post original fue sin respuesta.

There was an error deserializing the object of type System.String. Encountered unexpected character 'M'. tiempo fui retratado como el Osama bin Laden de Internet y que quería para poder decirle a mi lado de la historia. Quería ser capaz de explicar exactamente lo que Lo hice y lo que no hice a gente que pensaba que me conocían\".

Gran parte del material en el capítulo\"faltan\" detalles ante de Mitnick Markoff.

Es motivo de preocupación principal a Mitnick que Markoff \"no se pudo reconocer una pre-relación existente\"con Mitnick en una historia de 04 de julio de 1994, que apareció en el portada de The New York Times.

Historia de Markoff calificó de Mitnick un hacker altamente peligroso capaz de dividir en equipos críticos del Gobierno y destacó que Mitnick había hasta ahora fácilmente evadido funcionarios policiales.

Mitnick cargos que Markoff estaba enojado con él debido a una cantidad de errores de película basada en el libro de 1991 de Markoff, Cyberpunk: bandidos y Hackers en el Frontera de equipo.

En el momento de la publicación, Mitnick disputaron la veracidad del libro pero más tarde aceptó $5.000 de una oferta total de $50.000 para actuar como consultor para la película basada en la libro porque necesitaba el dinero.

Dos años más tarde, cuando el estudio quiso renovar el contrato, Mitnick, entonces empleado, se negó a renovar. Esa negativa, segun Mitnick y dos fuentes familiarizado con el incidente, que causó la muerte.

Mitnick dijo que Markoff debería mencionado el negocio fallido en su artículos siguientes de Mitnick. También afirma que muchos de los hacks que se le atribuyen Markoff nunca sucedió.

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
\"Creo que eres suficientemente cualificados para eludir la detección, dijo Mitnick.

Markoff se negó rotundamente a comentar ninguno de los alegatos de Mitnick en capítulo Uno.

Mitnick dice el capítulo se han publicado con el libro, pero la decisión que respete su editor.

There was an error deserializing the object of type System.String. Unexpected end of file. Following ele
información al mundo,\"agregó Mitnick. \"Estoy contando los días hasta que pueda
Conecte de nuevo.\"

Mitnick ha sido prohibido de utilizar la Internet como condición de su supervisión
lanzamiento. Él es libre de ir en línea nuevamente el 21 de enero de 2003, tras cerca de ocho
años sin conexión.

El primer sitio que visita es blog de su novia.

There was an error deserializing the object of type System.String. Encountered unexpected character 'M'.
dijo. \"Me encantaría saber lo que ella ha estado diciendo acerca de mí.\"
