5. Ingeniería Social

4. Phishing

4.1 Introducción

El phishing es el nombre de una estafa donde, a través de medios telemáticos, un atacante se hace pasar por una empresa u organismo para robar los datos de sus usuarios.

El proceso de un ataque de phishing es el siguiente: el estafador envía un mensaje, generalmente a millones de usuarios, a través de algún método de comunicación (SMS, correo electrónico, fax, teléfono,..) haciéndose pasar por alguna conocida empresa u organización y pidiendo datos personales o contraseñas a los usuarios. Un porcentaje de estos usuarios cree que el mensaje es auténtico y responde con la información que en él se solicita.

En otras ocasiones los atacantes falsifican páginas web donde copian el aspecto de páginas originales con el fin de que el usuario se crea que son auténticas e introduzca sus datos personales, contraseñas, datos bancarios, etc.

En ambos casos, las consecuencias de facilitar estos datos pueden ser el robo de dinero de la cuenta bancaria, el uso indebido de la tarjeta de crédito, el uso de los datos para realizar una suplantación de identidad, o incluso la venta de los datos personales.

4.2 Phishing vs Spam

Confundir el phishing y el spam es algo bastante habitual, por lo que vamos a intentar aclarar la diferencia entre ambos términos.

El spam, o correo basura, son correos electrónicos no deseados, generalmente con fines publicitarios. Los spammers envían sus mensajes a miles, incluso millones de direcciones de correo electrónico a la vez esperando que el mensaje llegue a cuantas más personas mejor para difundir una marca, una información, o cualquier tipo de publicidad. El correo electrónico no es el único medio por el cual se pueden recibir mensajes de spam, pero sí la forma más extendida.

El phishing, como ya se ha comentado, es un intento de engaño a usuarios para robar información personal, contraseñas o datos bancarios. Por tanto no hay que confundir el spam, que es publicidad no deseada, pero solo publicidad al fin y al cabo, con el phishing, cuyo objetivo es el robo de datos.

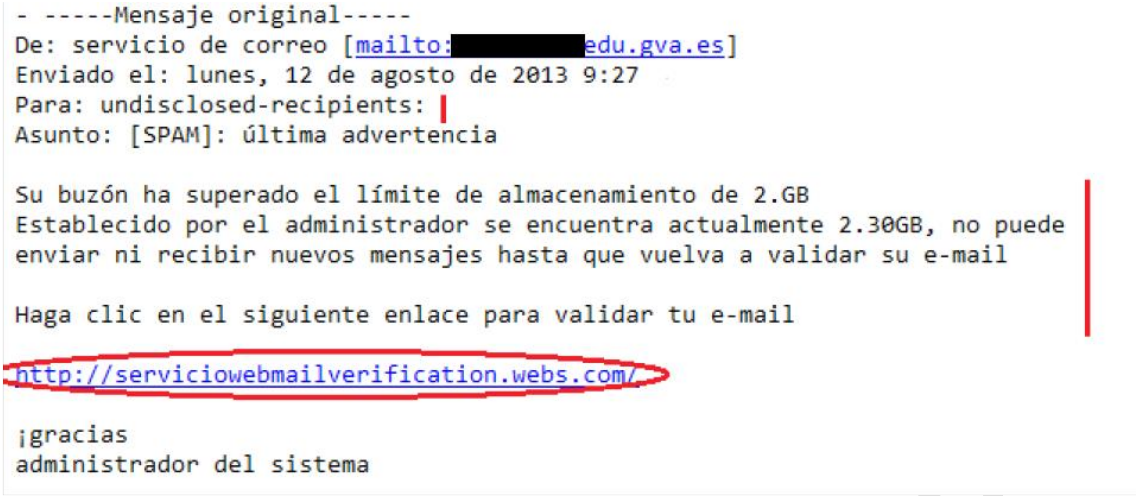
4.3 ¿Cómo Identificar el Phishing?

No hay una condición que se tenga que cumplir sí o sí para saber que estamos ante un caso de phishing, sino que debemos tener algunos aspectos en consideración para poder determinar que se trata de este tipo de ataque.

- En muchas ocasiones los mensajes de phishing no están dirigidos de manera personal. Normalmente éstos hacen referencia a un usuario genérico como “cliente”, “usuario”, o términos similares. También en bastantes casos aparecen ocultos los destinatarios del mensaje.
- Muchos ataques de phishing suelen contener errores graves de ortografía y de redacción por ser traducidos con herramientas automáticas.
- El objetivo del phishing es obtener información por lo que en los mensajes o páginas suplantadas se solicita al usuario sus datos de acceso a cuentas, números de cuentas bancarias o tarjetas de crédito, entre otros datos.
- Algunos correos de phishing contienen enlaces a páginas web donde se piden los datos a los usuarios. Estas webs falsas son fáciles de identificar ya que la dirección no es la de la web auténtica.

Al encontrar alguna de estas evidencias debemos sospechar que se trate de un caso de phishing.

4.4 Algunos Casos Reales



- -----Mensaje original-----
De: servicio de correo [mailto:[redacted]edu.gva.es]
Enviado el: lunes, 12 de agosto de 2013 9:27
Para: undisclosed-recipients:
Asunto: [SPAM]: última advertencia

Su buzón ha superado el límite de almacenamiento de 2.GB
Establecido por el administrador se encuentra actualmente 2.30GB, no puede
enviar ni recibir nuevos mensajes hasta que vuelva a validar su e-mail

Haga clic en el siguiente enlace para validar tu e-mail

http://serviciowebmailverification.webs.com/

¡gracias
administrador del sistema

En este caso real vemos como se cumplen todas las circunstancias que hemos comentado anteriormente para saber que se trata de phishing:

- No se dirige al usuario por su nombre y desconocemos los destinatarios del mensaje.
- La redacción y el lenguaje utilizado en el mismo no son correctos.
- Al pinchar en el enlace aparece una web que nos pide datos personales.
- El enlace en el que nos debemos validar no pertenece al dominio GVA.

En casos como este donde las sospechas de que se trate de un caso de phishing son numerosas recomendamos no pinchar en el enlace.

Asunto: Aviso de securidad
De: Bankia<service@bankia.es>

Estimado(a) cliente:

En Bankia somos conscientes de la necesidad de garantizar el tránsito de información entre el Banco y sus clientes. Por este motivo,
Bankia cuenta con las máximas medidas de seguridad para garantizar la confidencialidad de las comunicaciones entre el Banco y el cliente.

Le notificamos que su Acceso cliente a la área privada de Bankia net se ha suspendido temporalmente debido a intentos fallidos de acceso a su cuenta on-line.

Esta medida es temporal y se procederá a la reactivación automática de los servicios Bankia net una vez haya completado el proceso de verificacion.

Aviso Importante : Este proceso es obligatorio y deberá ser realizado en un plazo máximo de 48 horas.
Tenga en cuenta que el incumplimiento del proceso de reactivación podría generar
el bloqueo cautelar de todos los servicios prestados por nuestra entidad, que
permanecerán en este estado hasta que se realice una auditoría completa por
parte de nuestros técnicos.
Puede evitar este tipo de restricción accediendo aqui.

Bankia S.A. - 2013

http://pqh6995uac7617.jaguh.net/bankiaonline/

Una vez más, vemos que se cumplen la mayoría de los aspectos que nos hacen saber que este correo se trata de un caso de phishing:

- Se dirigen al destinatario como “Estimado(a) cliente” sin incluir el nombre.
- La ortografía es incorrecta, ya que se utilizan palabras como “securidad”, y en general redacción no es correcta.

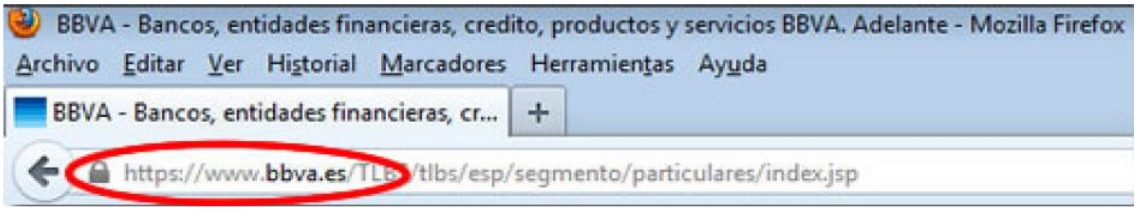
- Si hacemos clic en el enlace nos lleva a una web donde nos piden datos personales y la contraseña de acceso.
- Si nos ponemos sobre el texto del enlace vemos que nos lleva a la página http://pqh6995uac.jaguh.net/bankiaonline que nada tiene que ver con bankia.es.

Por tanto todo parece indicar que se trata de un mensaje de phishing.

En este caso vamos a ir un paso más allá y veremos cómo identificar una web falsa a la que generalmente llegaríamos desde un correo de phishing.

Tras acceder a la página vemos que la apariencia de la página aparentemente es legítima pero antes de introducir los datos nos fijamos en la dirección del portal.

En este caso vemos que la dirección es http://117.102.76.34/particulares, lo que nos hace sospechar de la autenticidad de la página. La URL real del banco en cuestión es https://www.bbva.es/ tal y como vemos en la siguiente captura:



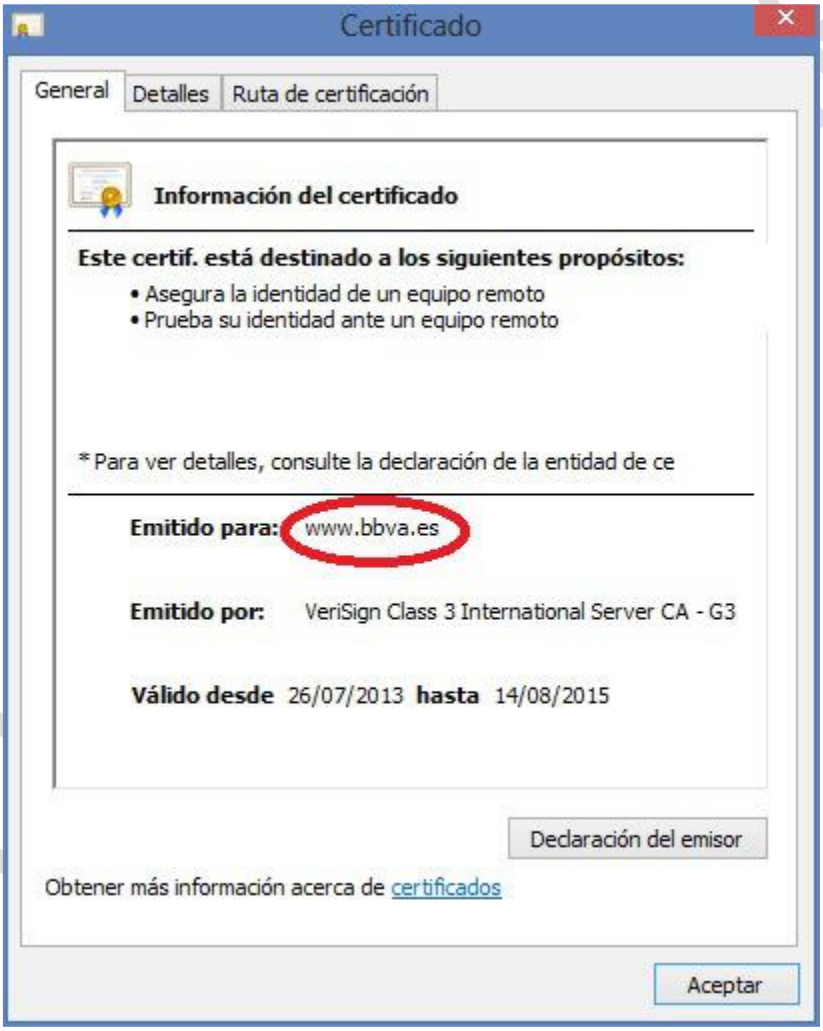
Como se ha podido comprobar la apariencia de la web puede llegar a ser muy similar pero hemos de estar atentos a la dirección de la web.

4.5 Seguridad en las Páginas Web

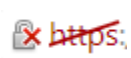
Ya hemos aprendido a identificar correos falsos y páginas web falsas, pero existen casos complicados en los que se podría llegar a falsificarse incluso la dirección de la web. Para evitar estas situaciones existen los certificados web, los cuales vamos a aprender cómo funcionan.

Las páginas que necesitan niveles importantes de seguridad (banca electrónica, inicio de sesión, cambios de contraseñas, etc.), tienen un certificado digital que confirma que esa web que se está viendo se corresponde con la dirección que se ve en el navegador. Generalmente un candado verde como este

junto a la dirección de la web querrá decir que la web es auténtica. Si hacemos clic sobre el certificado podremos ver sus detalles:



En cambio si la web tiene un certificado falso veremos que el candado cambia de color



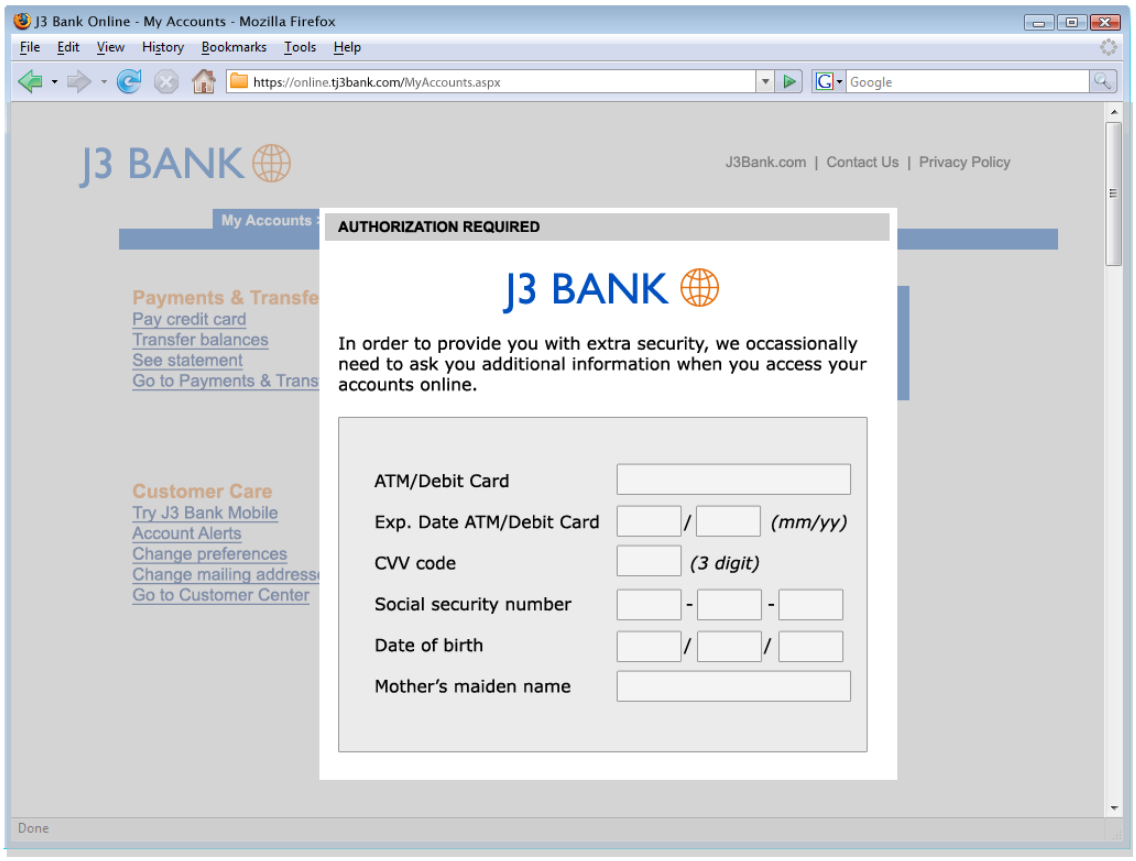
y en ocasiones se muestra una pantalla como la siguiente:

4.6 Spear Phishing

Últimamente hemos asistido a un cambio rápido y sustancial; hemos pasado de ataques de phishing amplios y dispersos a ataques selectivos avanzados con graves consecuencias para las empresas contra las que se dirigen. Algunos de los ataques selectivos avanzados más conocidos, como los llevados a cabo contra RSA y HBGary Federal, y la conocida como Operación Aurora, emplearon técnicas de phishing selectivo (o spear phishing). El aumento del uso de esta técnica se justifica sobradamente por el hecho de que funciona, ya que las defensas de seguridad tradicionales se revelan ineficaces contra este tipo de ataques.

El "phishing selectivo", como indica su nombre, es una versión más focalizada de los ataques de phishing, que combina tácticas como la selección de la víctima, la personalización de los mensajes de correo electrónico o la suplantación del remitente, con otras encaminadas a sortear los filtros de correo electrónico y conseguir que las víctimas hagan clic en un vínculo o abran un archivo adjunto. Mientras que un ataque de phishing puede afectar a toda una base de datos de direcciones de correo electrónico, en el caso del phishing selectivo, los objetivos son personas concretas de empresas específicas. Gracias a las redes sociales, por ejemplo, la personalización y la suplantación de identidad que se utiliza en los mensajes de correo electrónico de phishing selectivo pueden ser extremadamente precisas y totalmente convincentes. Una vez que se hace clic en un vínculo o se abre un archivo adjunto, se abre una vía de acceso a la red que permite a los autores de los ataques de phishing selectivo seguir con su ataque avanzado.

Los ataques de phishing selectivo deben examinarse en el contexto de los ataques selectivos avanzados, también denominados ataques mediante amenazas persistentes avanzadas (APT). En la actualidad, sofisticados ciberdelincuentes, así como naciones, llevan a cabo ataques mediante APT a través del uso de malware avanzado y de ataques prolongados, multivectoriales y multifase, con el fin de llegar a un objetivo concreto. En la mayoría de los casos, los ataques mediante APT tienen como objetivo el acceso a largo plazo a las redes, datos y recursos confidenciales de una empresa.



Los ataques avanzados que utilizan phishing selectivo no son una excepción; representan un giro evidente en los métodos que emplean los ciberdelincuentes. En lugar de llevar a cabo ataques de phishing masivos, los ciberdelincuentes se inclinan cada vez con más frecuencia por ataques de mucha menor envergadura y más selectivos, ya que está demostrado que son más eficaces. Un estudio reciente reveló lo siguiente:

- Entre 2010 y 2011, los ingresos anuales por ataques basados en el envío masivo de correo electrónico descendieron de 1100 millones a 500 millones de dólares. Durante el mismo período, el volumen de spam descendió de 300 000 millones a 40 000 millones de mensajes al día.
- En ese mismo período, los ataques de phishing selectivo se multiplicaron por tres.
- Los mensajes de phishing selectivo se abrieron en un 70 % de los casos, comparado con el 3 % en el caso de los mensajes de correo electrónico enviados mediante campañas de envío masivo. Además, el 50 % de los destinatarios que abrieron mensajes de phishing selectivo también hicieron clic en los vínculos que contenían, lo que multiplica por 10 los casos del envío masivo de mensajes.
- En comparación con los mensajes de correo electrónico enviados a gran escala, el phishing selectivo cuesta 20 veces más por individuo atacado. Sin embargo, el beneficio medio obtenido por víctima de phishing selectivo es 40 veces mayor que el del phishing general.
- Es probable que una campaña de phishing selectivo compuesta por 1000 mensajes genere 10 veces más ingresos que una de envío masivo de phishing dirigida a 1 millón de personas.

A continuación se enumeran algunas de las principales características de los ataques de phishing selectivo avanzados:

- Amenaza combinada/multivectorial. El phishing selectivo utiliza una combinación de técnicas basadas en la falsificación de mensajes de correo electrónico, el aprovechamiento de vulnerabilidades de aplicaciones desconocidas (zero-day), el empleo de URL dinámicas y las descargas desapercibidas, con el fin de sortear las defensas tradicionales.
- Aprovecha vulnerabilidades desconocidas (zero-day). Los ataques de phishing selectivo avanzados aprovechan vulnerabilidades desconocidas en navegadores, complementos y aplicaciones de escritorio para comprometer los sistemas.
- Ataque multifase. El exploit inicial de los sistemas es la primera fase de un ataque ATP que se compone de otras fases, como comunicaciones salientes del malware, descargas binarias y filtración de datos.
- No comparte las características del spam. Las amenazas de phishing selectivo a través del correo electrónico son focalizadas y se dirigen a menudo contra personas concretas, por lo que no se parecen al spam tradicional, que funciona con grandes volúmenes de mensajes y depende de la transmisión. Esto significa que es poco probable que los filtros de reputación detecten estos mensajes, lo que reduce las probabilidades de que sean neutralizados por los filtros de spam.

Los ataques dirigidos contra RSA, la división de seguridad de EMC Corp., en 2011 dejaron ver con claridad cómo prepara el terreno el phishing selectivo para un mayor asalto devastador y de increíbles consecuencias para una empresa — y sus clientes. El asalto se inició con una serie de ataques de phishing selectivo que enviaron a los usuarios elegidos un mensaje de correo electrónico con un archivo de Microsoft Excel adjunto que aprovechaba un fallo desconocido en Adobe Flash. Está claro que el ataque no solo iba dirigido contra RSA y, sin embargo, solo cuatro de sus empleados recibieron los mensajes maliciosos. Bastó que un usuario abriera el mensaje de correo electrónico y el adjunto para descargar un troyano en su computadora.

Este exitoso ataque de phishing selectivo formaba parte de un ataque avanzado mucho más complejo. Una vez que se instaló el malware en el PC de la víctima, los ciberdelincuentes pudieron rastrear la red, apoderarse de las credenciales de administrador y finalmente conseguir acceso a un servidor que albergaba información confidencial sobre la plataforma de autenticación de dos factores SecurID.

Pero el ataque no acabó ahí. De hecho, no era sino un paso previo para conseguir el objetivo final: el acceso a las redes de los clientes de RSA, especialmente de los relacionados con la industria de la defensa. Gracias a la información robada, los ciberdelincuentes atacaron a un buen número de clientes importantes de SecurID, como los contratistas de defensa Lockheed Martin, L-3 y Northrop Grumman.

El mensaje para las empresas es que este ejemplo deja claro que incluso ataques aparentemente rudimentarios pueden ser solo el comienzo de una serie de acciones delictivas avanzadas, coordinadas y devastadoras. Además, los ataques selectivos avanzados contra recursos o empleados en apariencia de bajo nivel, sin funciones de gran responsabilidad ni permisos especiales, pueden abrir la puerta a información vital y tener enormes consecuencias.