Phishing: Fraude informático y como evitarlo

Mamani Castillo Carla María
Universidad Mayor De San Andrés
Carrera De Informática
Simulación de Sistemas
krlis_t@hotmail.com

RESUMEN

"Phishing", uno de los principales némesis en la Red, este tipo fraude informático esta cada vez más presente.

Los ataques de phishing son más sofisticados actualmente, pero la mayoría tienen una forma de actuar muy típica.

Este artículo tratará hasta cierto detalle este concepto delictivo, para lograr que el cibernavegante esté alerta ante una situación de estas características y las medidas a tomar para evitar ser una víctima más.

Palabras clave

Phishing, e-mail, entidades financieras, URL.

1. INTRODUCCIÓN

Si creía que su buzón estaba seguro, recuerde que hay una nueva forma de correo no deseado al acecho. Este tipo de correo basura no sólo es inesperado y molesto, sino que también facilita el robo de sus números de tarjetas de crédito, contraseñas, información de cuentas y otra información personal. Este presente artículo se profundiza acerca de esta técnica que se denomina phishing.

El phishing es ya un problema importante tanto para los consumidores y lo organismos, y el alcance del problema sigue creciendo. El número de ataques de phishing crece un 50 por ciento cada mes, de acuerdo con el Anti-Phishing Working Group.

Así las entidades bancarias como los organismos no saben como parar esta "nueva estafa", aunque estén cansados de advertir a sus clientes que hagan caso omiso a este tipo de comunicaciones electrónicas. Todos debemos ser precavidos con nuestros datos, ya que es mejor prevenir que lamentar.

2. MARCO TEÓRICO

El phishing es un mal al que se agarran los escépticos del medio online para echar en cara su uso y las posibilidades del comercio electrónico, al punto extremo de llegar a declarar como muchos temerosos que "la computadora buena es aquella que se encuentra apagada". La cuestión es tener claro como reconocer cuándo un e-mail es spam, que a su vez es phishing y detrás hay un ladrón que quiere robarnos nuestros datos bancarios. Sabiendo reconocerlos se pueden evitar, y por tanto perder el miedo a su presencia. El problema principal del phishing afecta a la seguridad de nuestros datos personales.

2.1. Phishing

El phishing es una modalidad de estafa diseñada para engañar al usuario que simulan provenir de organismos, empresas privadas o entidades financieras (entidades públicas o privadas que pudieran tener algún acceso a datos financieros) con el fin de conseguir datos confidenciales, como claves de acceso, datos de tarjeta de crédito, correo electrónico, entre otros. Generalmente se basa en enlaces fraudulentos que invitan al usuario a introducir sus datos en un sitio falso y los cuales son enviados al atacante (figura 1).

Si nos consiguen engañar, en 10 minutos pueden haber utilizado la información que hayamos introducido: nos pueden vaciar nuestra cuenta bancaria, usar nuestra tarjeta de crédito, usar nuestra información persona, etc. Por eso es importante saberlo detectar a tiempo.

En términos más coloquiales, podemos entender el phishing como "pescando datos" o "pesca de datos", al asimilar la fonética de la palabra "phishing" con el gerundio "fishing" (**ll**'98 pescando).

2.2. Cómo funciona el phishing

La técnica del phishing consiste en enviar millones de mensajes falsos que parecen provenir de sitios Web reconocidos o de su confianza, como por ejemplo su banco o la empresa de su tarjeta de crédito. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. En la práctica, es relativamente fácil falsificar el remitente de un e-mail o mensaje (tal y como ocurre con los mensajes generados por gusanos, que suelen utilizar la misma técnica de forma automática). Así también es sencillo falsificar su contenido, ya que los elementos gráficos de las empresas suelen estar disponibles -de forma pública- en los sitios Web. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, confiado introduce información personal sin saber

Figura 1. Modus operandi en Phishing

que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

Recientemente se conoció una nueva técnica de phishing que consiste en cambiar una pieza poco conocida de software en la mayoría de los equipos dispuestos en Web llamado "archivo de host". Todos los sitios de Internet tienen una dirección numérica, denominadas direcciones IP, que contienen una serie de cuatro números, como por ejemplo 207.46.150.20. También han de usar, fácil de recordar nombres como MSNBC.com. Los nombres y los números están unidos por medio de un catálogo que se mantiene en varios equipos conectados a Internet llamados servidores de nombres de dominio. Pero las computadoras siempre comprueban el archivo de host local para el catálogo y reemplaza el archivo de host local de la información contenida en los servidores de Internet de nombres de dominio.

En esencia, la táctica redirecciona el ordenador de la víctima a un sitio Web controlado por un tiempo, y el criminal. Incluso si la víctima sigue un acceso directo o link navegador de Internet (Figura 2) favorito, el equipo está perfectamente dirigido al sitio del criminal en su lugar. Una vez allí, es fácil engañar a un consumidor confundido a escribir los números de cuenta bancaria y de inicios de sesión, porque él o ella son fácilmente convencidos de que el destino es el sitio de un banco correcto.

3. ASPECTOS QUE SE DEBEN TOMAR EN CUENTA PARA EVITAR EL PHISHING

En general, sospeche de cualquier e-mail que nos pida información personal o información financiera. (Mensaje que solicite datos confidenciales como nombres de usuario, contraseñas, números de tarjeta de crédito, etc.) Si es el caso, puede telefonear a la entidad que supuestamente le ha enviado el e-mail para que se lo confirmen.

Dado que el phishing es una técnica de envío masivo de correos electrónicos a múltiples usuarios, es posible que reciba correos electrónicos de entidades o empresas de las que usted no es cliente, y en los que se solicita igualmente dichos datos. En estos casos, directamente, descártelos.

Si la dirección web es un poco extraña podemos sospechar que se trata de un ataque de phishing.

A continuación se describen los aspectos a tomar en cuenta:

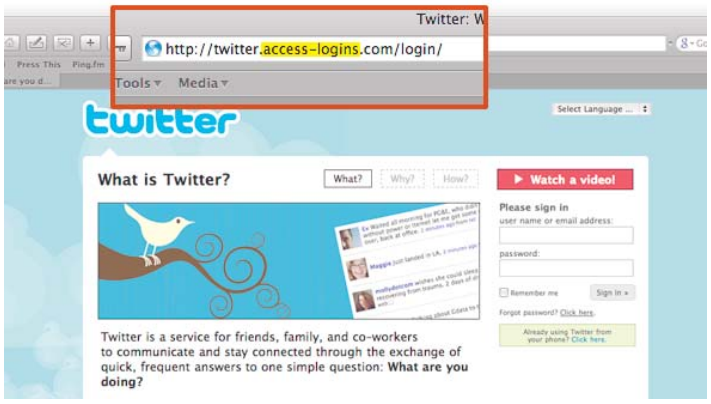

Figura 2. Es necesario verificar la URL del sitio sospechoso

- Evitar seguir los enlaces que llegan por correo electrónico o msn. Como por ejemplo invitaciones de redes sociales. Si llega un correo que dice que “fulanito” te agrego en Facebook, no hagas click en la dirección te puede llevar a una página falsa.
- Evite rellenar formularios en correos electrónicos que le soliciten información financiera personal.
- Verificar que en la barra de direcciones la URL, comienza por https:// para asegurarnos de que nos estamos conectando con un servidor Web seguro pues podríamos introducir información confidencial, lo ideal es escribir la dirección directamente en el navegador y no mediante enlaces.
- Igualmente podemos comprobar la veracidad del protocolo de seguridad; para ello, podemos clic dos veces en el candado de la parte inferior de la página, y nos aparecerá una ventana en la que se identifica a la compañía de certificación y al titular del protocolo, así como su validez.
- Ninguna entidad financiera sería nos pedirá ni por e-mail ni en una llamada telefónica (y ojo que este tipo de fraude muchas veces lo obviamos), ni en cualquier otra forma en la que se pongan en contacto con uno, la numeración de la Tarjeta, su caducidad, su usuario o contraseña, su número PIN.
- Cambiar la contraseña de forma periódica y usar contraseñas seguras. Claves como “12345678”, “qazxsw” son las más comunes. Usa combinaciones de números, letras y caracteres especiales.
- Consultar con regularidad los estados de las cuentas, y del modo más sencillo, y seguro, mejor a través de los Servicios Online de la entidad financiera.

  No usar la misma contraseña para varios sitios web.
- Cuando una organización se dirige a sus usuarios suele hacerlo de manera personalizada. Ya sea nuestro banco u otras organizaciones conocidas se dirigirán a nosotros con nuestro nombre. Si lo hacen de forma genérica, por ejemplo "Estimado usuario" podemos sospechar de que sea un phishing.

- Usar sitios Web seguros. Cuando las organizaciones nos piden información confidencial suelen utilizar tecnologías seguras para asegurarnos que nadie la puede interceptar y ser objeto de fraudes. La tecnología que se suele utilizar se conoce como SSL, y es una tecnología que los atacantes de phishing no acostumbran a utilizar. Por eso, si te piden información confidencial (por ejemplo, financiera) y no utilizan SSL puede tratarse de un caso de phishing.
- Mantener el sistema muy bien actualizado, tanto el sistema operativo, como el resto de aplicaciones, especialmente el navegador que se utilice y los últimos parches de seguridad instalados para las transacciones electrónicas.
- Debemos contar con una solución antivirus actualizada, ya que también proliferan los gusanos, troyanos y keyloggers (o programas que capturan las pulsaciones de teclado) destinados a robar los datos de los usuarios para poder acceder a la banca electrónica y a otros sitios con información confidencial.

3.1. ¿Navegadores más seguros?

La usurpación de datos personales se ve favorecida por la vulnerabilidad de los navegadores, incapaces de certificar la autenticidad de la URL (dirección de Internet). Tanto Internet Explorer, como Mozilla (y Mozilla Firefox) u Opera padecen esta debilidad que facilita la verosimilitud de enlaces falsos y páginas ilegítimas. Microsoft ofrece detallada información sobre el 'phishing' y consejos contra la falsificación de la URL, e Hispasec Sistemas facilita una página para que el usuario compruebe si su navegador es vulnerable a la falsificación de la URL.

3.2. ¿Qué se puede hacer si se detecta el phishing o hemos sido defraudados a través de esta técnica?

En ambos casos, la mejor solución es denunciarlo directamente a la entidad bancaria de la que es cliente, así como a la policía Ambas, pondrán todos los medios a su disposición para la búsqueda y captura de los autores, así como para restituir los daños que le hayan podido ser ocasionados.

4. CONCLUSIONES

El 'phishing' es una estafa que consiste en el envío de correos electrónicos y proponen que se acceda a páginas web falsas que simulan ser del organismo suplantado, y en las que se propone la actualización de datos o el acceso al servicio.

Al acceder a tales páginas los incautos ceden sus datos financieros, tales como identificador (usuario) y password, número de cuenta bancaria o de tarjeta de crédito.

Lo más importante de todo es estar pendientes y si notas algo raro en la página no introduzcas tus datos, asegúrate primero de estar en el sitio correcto, para no ser victimas de estos estafadores.

Además debemos contar con políticas que protejan a los usuarios, entidades fingieras, organismos, etc. De este tipo de fraudes informáticos, pues en nuestro país no contamos con estas políticas de protección.

5. REFERENCIAS

[1]http://technet.microsoft.com/es-es/

[2]http://www.dragonjar.org/category/informatica-forense

[3]www.mir.es/policia/bit/index.htm

[4]http://www.laflecha.net/canales/seguridad/noticias/

[5]Antonio Toca - elblogsalmon.com

[6]http://es.wikipedia.org/wiki/Phishing

[7]http://seguridad.internautas.org/html/451.html

[8]http://en.wikipedia.org/wiki/Phishing

[9]http://www.msnbc.msn.com/id/6416723/