Phishing

El "Phishing" es una forma de estafa financiera, basada en el envío de mensajes electrónicos fraudulentos.

¿En qué consiste?

Básicamente el "Phishing" es una forma de correo electrónico no solicitado, que pretende obtener información confidencial mediante la suplantación de las páginas de acceso a un servicio con el propósito de engañar a los usuarios e inducirlos a que revelen información sensible.

De esta manera capturan información personal, datos financieros, números de tarjetas de crédito, nombre de usuarios y contraseñas de acceso haciendo efectivo el robo de su identidad.

¿Cuándo ocurre el Phishing?

Cuando un usuario recibe un correo electrónico que parece proceder de una compañía financiera de buena reputación, con un mensaje que solicita la actualización de su información personal haciendo clic en un mensaje que parece auténtico.

En algunos casos, para ganar la confianza del destinatario y lograr que éste responda, acompañan el mensaje de advertencias de fraudes: "*Estimado Cliente. Queremos informarle que personas inescrupulosas están solicitando información a nuestros clientes en nombre de nuestra Institución, por consiguiente, para verificar si su cuenta fue afectada ingrese en los siguientes campos su número de Tarjeta y contraseña...* ". Al pinchar el link adjunto en el comunicado direcciona al destinatario a una página que es una réplica exacta de la original.

¿Cómo evitarlo?

Estar informado acerca de esta modalidad de fraude electrónico es la mejor arma para no convertirse en una víctima. Sea cuidadoso cuando suministre información personal o financiera a través de Internet. A continuación, le presentamos una lista de recomendaciones que debe seguir para evitar este ataque:

- Sospeche de todo correo electrónico con un requerimiento urgente de entrega de información financiera personal.
- Nunca haga clic en enlaces incluidos en un correo electrónico. Verifique la información contactando telefónicamente a la compañía que lo está enviando y que seguramente ofrecerá sus teléfonos o dirección.
- Evite llenar formularios, planillas anexas o formas incluidas en estos mensajes de correo electrónico, las cuales preguntan por información financiera personal.

- Verifique que su navegador haya establecido una conexión segura cuando entregue información a través de Internet.

- Verifique regularmente las transacciones de sus cuentas y tarjetas de crédito para asegurarse que éstas son legítimas y llevar un control regular de las mismas.

- Asegúrese de contar con la última versión de su navegador y actualice los parches de seguridad liberados para éste.

- Siempre reporte a Mercantil Seguros los intentos de Phishing, con esto contribuirá a alertar a la Institución para que ésta tome medidas al respecto.

Keylogger

El Keylogger o Capturador de Teclas son herramientas de software o hardware que permiten grabar el texto que escribe una persona en su teclado.

Características

- Permite al usuario saber qué es lo que otros están haciendo con su computadora, sin necesidad de estar presente.
- Permite establecer las opciones "Arrancar en modo oculto" y "Ocultar en la lista de tareas" para que el programa sea invisible a cualquiera, de este modo toda la actividad que se realice en el mismo será guardada en un archivo al cual sólo puede acceder el administrador, a través del ingreso de un password.
- Es una herramienta de fácil adquisición, instalación y uso, ideal para los usuarios de banca hogareña.
- Pequeño y con bajos requerimientos de sistema.
- Permite el envío de archivos por e-mail.
- Su atractivo se centra en el ahorro de tiempo previniendo los daños y pérdidas accidentales de datos que son frecuentemente causadas por el uso de Internet y que el usuario puede recuperar sin importar el tiempo en que fue ingresada toda la información, días e incluso semanas anteriores.

Tipos

Actualmente la herramienta está disponible tanto en software como hardware:

- En el caso del software, es un programa disponible que puede ser instalado en cualquier computadora, el cual intercepta y guarda en un archivo toda la información que se ingresa desde el teclado.
- Estos programas se instalan y funcionan de manera 'invisible' sin que el usuario del PC se percate de su existencia, ya que está diseñado para trabajar de modo oculto y aparecer al ingresar una combinación de teclas específicas (clave) presionadas por su administrador y así obtener la información allí registrada de manera clara, sencilla y fácil de leer así como cada evento que ha ocurrido en ese PC.
- En el caso del hardware, el keylogger se presenta como unos dispositivos USB y PS2 que se conectan entre el PC y el teclado a través de los puertos, los cuales graban en una memoria interna el texto digitado en el computador. De este

modo, toda la actividad que se realizó en un determinado PC está ahora en manos de su administrador.

Uso malintencionado del keylogger

- Por ser una herramienta de fácil adquisición, instalación y uso, atractiva a los ojos de los usuarios de banca hogareña, se convierte en blanco para que personas malintencionadas que no necesitan ser expertas en la materia, cometan fechorías y fraudes sorprendiendo a los usuarios de la banca en línea.

- El keylogger captura todo lo que escribe la víctima y lo envía a una dirección de correo electrónico configurado por su administrador recibiendo contraseñas, números de tarjetas, cuentas y demás datos financieros que al ser utilizados por personas malintencionadas el titular de éstas puede ser víctima de una estafa sin darse cuenta.

- La experiencia internacional indica que la tasa de estos delitos crecerá a medida que aumenten los usuarios de banca hogareña (Home Banking), ya que vulnerar la seguridad de la computadora de un banco o una emisora de tarjetas de crédito es un desafío sólo posible para hackers muy expertos. Leer las claves mientras viajan por la red hacia la computadora del banco es casi imposible, dado que están encriptadas. En cambio, "meterse" en una PC hogareña es más accesible para estafadores que no necesariamente tienen grandes conocimientos de informática.

- De acuerdo a los expertos, en la actualidad, uno de los métodos más usados es infiltrar en las PCs estos software llamados keyloggers ó registradores de teclas.

- Este programa también puede llegar a la PC hogareña a través de Internet, adjunto a un mensaje de e-mail, o escondido dentro de ciertos utilitarios (por ejemplo, un software de DVD) que se ofrecen gratuitamente en la web como el Caballo de Troya esconden un enemigo; por eso se les conoce con el nombre "troyanos".

Cómo prevenirlo

- No realice transacciones en línea desde computadores o lugares poco seguros, como centros de Internet. Si lo hace, asegúrese que sea de su entera confianza.

- Instale en la computadora de su uso frecuente un **firewall**, ya que es la mejor manera de evitar controlar todo lo que entra y sale de su computador.

- No se convierta en víctima, cuando ingrese a Internet recuerde que muchos de estos programas espía se auto instalan durante su conexión introduciéndose en su PC y obteniendo toda la información.

Pharming

¿En qué consiste?

Es una nueva modalidad de fraude online que consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para direccionar al usuario a una página web falsa. Como toda amenaza nueva expandible y peligrosa, la prevención y una solución antivirus eficaz, son las mejores armas.

Si hasta ahora uno de los fraudes más extendidos era el *phishing*, consistente en engañar a los usuarios para que efectúen operaciones bancarias en servidores web con el mismo diseño que un banco online, el *pharming* entraña aún mayores peligros. Consiste en la manipulación de la resolución de nombres en Internet, llevada a cabo por algún código malicioso que ha sido introducido en el equipo intencionalmente.

¿Cómo actúa?

Cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores **DNS** (Domain Name Server).

En ellos se almacenan tablas con las direcciones IP de cada nombre de dominio. A escala menor, en cada computador conectado a Internet hay un fichero en el que se almacena una pequeña tabla con nombres de servidores y direcciones IP, de manera que no haga falta acceder a los DNS para determinados nombres de servidor, o incluso para evitarlo.

El *pharming* consiste en modificar este sistema de resolución de nombres, de manera que cuando el usuario crea que está accediendo a su banco en Internet, realmente está accediendo a la IP de una página web falsa.

Si el *pishing* debe su éxito a la ingeniería social, aunque no todos los usuarios caen en estos trucos y su éxito está limitado. Además, cada intento de *pishing* se debe dirigir a un único tipo de servicio bancario, por lo que las posibilidades de éxito son muy limitadas. Por el contrario, el *pharming* puede atacar a un número de usuarios muchísimo mayor.

El *pharming* no se lleva a cabo en un momento concreto, como lo hace el *pishing* mediante sus envíos, ya que la modificación de DNS queda en un ordenador, a la espera de que el usuario acceda a su servicio bancario. De esta manera, el atacante no debe estar pendiente de un ataque puntual, como hemos mencionado antes.

Un antivirus

Como hemos mencionado en los demás temas relacionados con el fraude electrónico, la solución inmediata es tener instalado un antivirus robusto, el cual reducirá al mínimo los riesgos de esta nueva amenaza, ya que para llevar a cabo el *pharming* se requiere que alguna aplicación se instale en el sistema a atacar (un fichero .exe, un *script* , etc.).

La entrada del código en el sistema puede producirse a través de cualquiera de las múltiples vías de entrada de información que hay en un sistema como por ejemplo el e-mail que es una de las más frecuentes, descargas por Internet, copias desde un disco o CD, etc. En todas y cada una de estas entradas de información, el antivirus debe detectar el fichero con el código malicioso y eliminarlo.

La prevención como mejor solución

Actualmente nos movemos en un escenario en el que el *malware* ha adquirido una velocidad de propagación muy elevada, y los creadores son más y ofrecen los códigos fuente para que introduzcan variaciones y puedan crear ataques nuevos.

Los laboratorios de virus no disponen de tiempo suficiente para efectuar la detección y eliminación del *malware* para todos los nuevos códigos antes de que lleguen a propagarse en unos pocos computadores. A pesar de los esfuerzos y la mejora de los laboratorios, es imposible que se elabore una solución adecuada y a tiempo para algunos códigos malignos que se propagan en cuestión de minutos.

La solución para este tipo de amenazas también la podemos encontrar en la instalación de un sistema mediante el cual se detecten no sólo los ficheros en función de firmas víricas, sino también mediante las acciones que se llevan a cabo en el computador. De esta manera, cada vez que se intente realizar un ataque al sistema de DNS del computador, como es el caso de las aplicaciones para *pharming,* sea reconocido el ataque y detenido, así como bloqueado el programa que lo ha llevado a cabo.