Ma.Emilia del Barco
Abogada

FRAUDES EN INTERNET

1. PHISHING: ROBO DE DATOS PERSONALES.

Hoy en día se tornan cada vez más comunes, actividades como transacciones bancarias en línea, comercialización de bienes y acciones, compra de productos y servicios, así como el manejo de cuentas personales a través de sitios en la Web.

Si bien el fenómeno "INTERNET" hace que la conducción de dichas actividades sea más conveniente, también ha creado una nueva forma de fraude, de la cual las personas con malas intenciones, abusan cada vez más al obtener información personal como el número de tarjeta de crédito, contraseñas y otros datos confidenciales. Los delincuentes usan esta información para hacer compras con la tarjeta de crédito o debito bancaria robada, además de abrir cuentas fraudulentas o cometer otros delitos en nombre de la víctima.

A medida que avanza la tecnología, avanzan también nuevas y más complejas formas de fraude electrónico; una de la más reciente se denomina "PHISHING". En este tipo de fraude, el usuario recibe un mail que parece proceder de su banco de confianza.

La diferencia con otras formas de fraude o delitos electrónicos es que esta vez nadie intenta acceder a tu sistema con intenciones maliciosas, introduciéndote un virus que puede provocar el mal funcionamiento de tu computadora, o forzando la misma.

Con el *phishing*, es el propio usuario quien envía información personal y confidencial de forma voluntaria; eso si, animado mediante técnicas de ardid o engaño.

¿Alguna vez recibiste un mensaje de tu banco que te indica que debes verificar los datos de tu cuenta? Cuidado! No te confíes… es muy probable que se trate de un intento de Phishing.

2. ¿QUÉ ES EL PHISHING?

El **Phishing** no es más que la suplantación de sitios en Internet. Es una modalidad de estafa diseñada con la finalidad de robar la identidad.

El delito consiste en obtener información tal como número de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Los infractores envían millones de correos electrónicos en forma aleatoria, que parecen provenir de sitios Web populares o bien de tu banco o compañía de tarjeta de crédito, en fin: parecen provenir de fuente confiable; pero en realidad están diseñados para estafar al destinatario y conseguir que divulgue información confidencial.

Muchas veces los correos electrónicos incluyen un enlace URL que lleva al consumidor a lo que parece ser un sitio Web legítimo que sin embargo es realmente un sitio Web falso, y una vez que el consumidor está en este sitio Web falso, se le pide ingresar información personal que es transmitida al "fisher".

El término phishing significa "pescar", en inglés, ya que en realidad tiene cierta similitud con la pesca. Se lanza un cebo y se espera a que alguien "pique". La recompensa no puede ser más sabrosa: datos personales y claves de acceso a tus cuentas bancarias.

Alguna de las características más comunes que presentan este tipo de mensajes de correo electrónico son:

- **Uso de nombres de compañías ya existentes:** en lugar de crear desde cero el sitio de Web de una compañía ficticia, los emisores de correos con intenciones fraudulentas adoptan la imagen corporativa y funcionalidad del sitio de Web de una empresa ya existente, con el fin de confundir aún más al receptor del mensaje.
- **Factor miedo:** La ventana de oportunidad de los defraudadores es muy breve, ya que una vez que se informa a la compañía de que sus clientes están siendo objeto de este tipo de prácticas, el servidor que se aloja al sitio Web fraudulento y sirve para la recogida de información se cierra en el intervalo de unos pocos días. Por lo tanto es fundamental para el defraudador el conseguir una respuesta inmediata por parte del usuario. En muchos casos, el mejor incentivo es amenazar con una pérdida, ya sea económica o de la propia cuenta existente, si no se siguen las instrucciones indicadas en el correo recibido, y que usualmente están relacionadas con nuevas medidas de seguridad recomendadas por la entidad.

Utilizar el nombre de un empleado real de una empresa como remitente del correo falso. De esta manera, si el receptor intenta confirmar la veracidad del correo llamando a la compañía, desde ésta le podrán confirmar que la persona que dice hablar en nombre de la empresa trabaja en la misma.

¿CÓMO FUNCIONA EL PHISHING?

A través de un mensaje electrónico, simulando proceder de una fuente fiable (por ejemplo, de tu banco), se intentan recoger los datos necesarios para estafar al usuario. En realidad se trata de mensajes masivos. Los estafadores no saben cuál es tu banco y por ello crean un mail con la apariencia corporativa del banco escogido y se envía masivamente. La realidad es que alguno de esos mensajes llegará a alguien que pertenezca a ese banco.

Normalmente se trata de mensajes con textos como: "Por motivos de seguridad…", o "Su cuenta se debe confirmar…", o "usuarios del banco advierten", indicando al usuario que se están realizando cambios y que por seguridad debe introducir sus datos personales y códigos bancarios pinchando en un link que ellos te indican.

Al pinchar se redirecciona a una página con gran similitud a la de tu banco habitual. La verdad es que esa página pertenece al estafador, quien no tiene más que copiar los datos que el usuario rellena. Al finalizar te confirma la operación y te quedas tranquilo pensando que esos datos los ha escogido tu banco sin menor problema.

Otras veces el mismo mail te pide que rellenes los datos y pulses "enviar", sin necesidad de redireccionarte a otra página.

La sorpresa en ambos casos llegará cuando encuentres que tu cuenta bancaria está cero, y tu banco te informe que has sido víctima de una estafa denominada "phishing"

Los principales daños provocados por el phishing son:

- Robo a la identidad y datos confidenciales de los usuarios.
- Pérdida de la productividad.
- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.)

Es importante tener en cuenta, que el phishing si bien es una nueva forma de delito electrónico, no se extiende únicamente a entidades financieras. Debemos ser cuidadosos y sospechar ante cualquier mail o ventana (aunque parezcan de fuente fiable) que nos pida datos bancarios.

Otros fraudes con mensajes engañosos se pueden encontrar en falsas ventanas o e-mails enviados a usuarios de Hotmail. También están siendo perjudicados los sectores de subastas y ventas on line.

¿COMO PUEDO RECONOCER UN MENSAJE DE PHISHING?

No resulta nada fácil el hecho de distinguir un mensaje de phishing de otro legítimo, para un usuario que haya recibido un correo de tales características, y especialmente cuando resulta ser cliente de la entidad financiera de la que "supuestamente" proviene el mensaje.

El campo De: del mensaje muestra una dirección de la compañía en cuestión. No obstante, es sencillo para el estafador, modificar la dirección de origen que se muestra en cualquier cliente de correo.

El mensaje de correo electrónico presenta logotipos o imágenes que han sido recogidas del sitio Web real al que el mensaje fraudulento hace referencia.

El enlace que se muestra parece apuntar al sitio Web original de la compañía, pero en realidad lleva a una página Web fraudulenta, en la que se solicitarán datos de usuarios, contraseñas, etc.

Normalmente estos mensajes de correo electrónico presentan errores gramaticales o palabras cambiadas, que no son usuales en las comunicaciones de la entidad por la que se están intentando hacer pasar.

Al usar Internet, es común que los consumidores provean información personal a

compañías y organizaciones legítimas. Sin embargo, alguna de estas compañías u organizaciones podrían compartir esa información personal con terceros.

Todos los usuarios del correo electrónico corremos el riesgo de ser víctimas de estos intentos de ataques. Cualquier dirección pública en Internet (que haya sido utilizada en foros, grupos de noticias o en algún sitio Web) será más susceptible de ser víctima de un ataque debido a los spiders que rastrean la red en busca de direcciones válidas de correo electrónico.

Ante este tipo de ataques, **la mejor defensa es la INFORMACIÓN**.

4. ¿COMO PUEDO PROTEGERME DEL PHISHING?

El fenómeno del phishing ha adquirido gran importancia a nivel mundial, tanto a nivel de usuarios como a nivel de empresas, incluido los propios bancos, que observan cómo no pueden hacer nada al respecto mientras sus clientes son estafados y además pierden confianza en la "banca online".

Actualmente, la única forma de evitar este tipo de estafas consiste en estar informados y concienciados. Por desgracia, ningún antivirus ni ningún sistema de seguridad pueden impedir estos ataques.

Proponemos los siguientes consejos para protegerse y preservar la privacidad de su información:

1. En primer lugar, nunca responda a solicitudes de información personal a través de correo electrónico: No conteste automáticamente a ningún correo que solicite información personal o financiera. Las empresas de prestigio nunca solicitan contraseñas, números de tarjeta de crédito y otro tipo de información personal por correo electrónico. Si recibe un mensaje que le solicita este tipo de información, no responda. Si tiene duda sobre la legitimidad del mensaje, comuníquese con la empresa por teléfono o a través de sus sitios Web para corroborar la información recibida.
2. Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones: si sospecha de la legitimidad de un mensaje de correo electrónico de la empresa de su tarjeta de crédito, banco o servicio de pagos electrónicos, no siga los enlaces que lo llevarán al sitio Web desde el que se envió el mensaje. Estos enlaces pueden conducirlo a un sitio falso que enviará toda la información ingresada al estafador que lo ha creado. Aunque la barra de direcciones muestre la dirección correcta no se arriesgue a que lo engañen. Los piratas conocen muchas formas de mostrar una dirección URL falsa en la barra de direcciones del navegador. Las nuevas versiones de Internet Explorer hacen más difícil falsificar la barra de direcciones, por lo que es buena idea visitar Windows Update regularme y actualizar sus software.
3. Observar si la dirección comienza con https: en lugar de solo http: (La "S" indica que la página está albergada en un servidor seguro). Las técnicas de phishing están aprendiendo rápidamente de este tipo de errores y los están perfeccionando. Consiste en crear una ventana emergente justo en la posición donde aparece la URL en la barra de dirección de Internet Explorer, de forma que se superpone y oculta la

dirección real del servidor Web del atacante donde realmente se encuentra el usuario, mostrando en su lugar la URL de la entidad bancaria. El mensaje incluye enlace que supuestamente le dirige a la Web de la entidad y que en la barra de direcciones de Internet Explorer aparece la URL correcta, incluyendo el prefijo **https://** como si estuviera en una conexión segura.

4. En caso de duda, se puede pasar el cursor por encima del enlace que lleva adjunto el correo. Muchas veces la dirección no es la misma que aparece en el mensaje.
5. Otra manera de reconocer estos mensajes es que no van personalizados. Normalmente llevan el titular de: "Estimado cliente".
6. Procure no dirigirse a sus Web financieras de confianza a través de enlaces facilitados o direcciones de Internet cuyo origen es desconocido.
7. También puedes confirmar que en la parte baja del navegador se vea un candado entero (no roto). Este símbolo indica un certificado de autenticidad y si pinchamos sobre él, se mostrarán los datos del certificado. Podremos comprobar que no esté caducado y que el propietario del mismo corresponde a la página que estás viendo.
8. Use software antivirus y antispam para protegerse contra las amenazas del Internet. Busque una solución integrada de seguridad que lo proteja de piratas informáticos, códigos maliciosos, spam, spyware, invasiones a la privacidad y otros tipos de fraudes en línea. Asesórese en seguridad informática.

Cumplidos todos estos requisitos, el usuario puede proporcionar su información con una razonable seguridad de que ésta no será utilizada contra sus intereses.

La mejor manera de protegerse del phishing es entender el modo de actuar de los proveedores de servicios financieros y otras entidades susceptibles de recibir este tipo de ataques. La regla principal que estas entidades no infringen es la solicitud de información sensible a través de canales no seguros, como por ejemplo el correo electrónico.

REPERCUSIONES SOBRE PHISHING.

En la actualidad, los casos más graves de phishing se han producido en Estados Unidos, aunque las mafias se han dado cuenta de sus gran potencial, por lo que su expansión se está produciendo a nivel mundial, sobre todo en los países de habla inglesa donde se encuentra ahora más concentrado.

La empresa Gartner ha analizado el problema del Phising y realizó un intereante estudio sobre este fenómeno en Estados Unidos. A continuación exponemos las conclusiones más revelantes:

- Los intentos de fraude contra consumidores en Internet, mejor conocido como phishing, se han vuelto tan comunes que se estima que 57 millones de estadounidenses han recibido algún tipo de correo fraudulento, de acuerdo con un nuevo estudio presentado por Gartner. Las pérdidas directas del fraude de identidad contra estas víctimas relacionadas con ataques tipo phishing, costaron a

los bancos y compañías de tarjetas de crédito alrededor de 1,200 millones de dólares el año pasado.

- Basados en una encuesta aplicada a 5,000 adultos que usan Internet, los analistas de Gartner estiman que aproximadamente 30 millones de adultos usuarios de la Web creen que definitivamente han experimentado un ataque phishing, mientras que otros 27 millones creen que han observado lo que parece ser un intento de fraude.

"Las instituciones financieras, proveedores de servicios de Internet y otros proveedores de servicios deben de tomar en cuenta seriamente este tipo de fraudes", dijo Avivan Litan, vicepresidente y director de investigación de la firma. "Estos proveedores de servicios deben tomar acciones y aplicar soluciones que dramáticamente minimicen o erradiquen la amenaza, incluso si los proveedores de servicios no son blancos directos. Eventualmente, todos los involucrados en el comercio electrónico de Internet se verán afectados por una falta de confianza del consumidor en sus transacciones si los fraudes no son reducidos en forma significativa de los niveles en que actualmente se encuentran". Sitio Departamento de Comunicación: www.recoverylabs.com

El ataque tipo phishing ocurre cuando un ciberpirata manda un correo electrónico que contiene una liga a un sitio de red fraudulento donde se le solicita al usuario que provea información sobre su cuenta personal. El correo electrónico y el sitio de red están típicamente disfrazados simulando ser el de uno de los proveedores de servicios de confianza, institución financiera o comercio en línea de los usuarios.

Basándose en los resultados de la encuesta Gartner estima que alrededor del 19% de los atacados o casi 11 millones de estadounidenses adultos que usan Internet, han dado clic a un correo de intento de fraude. Peor aún, 3% de los atacados o un estimado de 1.78 millones de adultos, reportan haber dado a los defraudadores su información financiera o personal.

En Estados Unidos se ha creado la "Antiphishing Working Group" (APWG). Se trata de una asociación de industrias cuyo principal objetivo es finalizar con el robo de identidad y fraudes resultantes del creciente problema del phishing en correos electrónicos fraudulentos.

Para obtener más información acerca de otras formas de fraudes o delitos electrónicos puede visitar las siguientes páginas:

- www.antiphishing.org
- www.segu-info.com.ar
- www.identidadrobada.com
- www.densi.com.ar

Ma. Emilia Del Barco