*Tecnología Informática*

***Por el Dr. Raúl Alejandro Farías***

# Phishing

*Que la estafa no nos sorprenda.*

Generalmente vemos de atrás los adelantos tecnológicos que se producen en el mundo. A los que nos gusta la tecnología, en particular la relacionada con la informática, nos provoca no pocos suspiros y la sensación, por momentos, de estar fuera de ese mundo. Hay que reconocer que esos adelantos cada vez tardan menos en llegar. Sin embargo, la demora tiene su ventaja: podemos conocer con anterioridad los efectos positivos y negativos que producen sobre la sociedad los procesos que se valen de la nueva tecnología y, en la medida que nos informemos, estaremos prevenidos.
Internet, el revolucionario adelanto tecnológico de nuestro tiempo, tiene la particularidad de mostrar su crecimiento simultáneamente en todo el planeta. Y crece en todas sus facetas: la buena y la mala. Es un universo en constante desarrollo que ofrece miles de oportunidades tanto para hacer el bien como el mal.
A este ultimo catálogo se le suma un nuevo tipo de estafa, el ***Phishing*** que ha explotado, literalmente, durante el ultimo año en países con culturas tan distantes como sus geografías, tal el caso de Estados Unidos y China, pasando por Taiwan, Corea, Brasil, Alemania, Francia, Canadá, Australia y la lista sigue.

El ***Phishing***, contracción de "password harvesting and fishing" (cosecha y pesca de contraseñas), no es ni mas ni menos que un tipo particular de estafa que consiste en duplicar o clonar una página web para engañar al visitante, haciéndole creer que se encuentra en un sitio web legítimo, con el objeto de inducirlo a ingresar datos sensibles, tales como nombres de usuario y contraseña de acceso a la banca on-line o sitios de compras, números de tarjetas de crédito y demás datos de la persona en cuestión. Acto seguido, la estafa se perfecciona usando los datos “cosechados” para realizar transacciones, generalmente por Internet, suplantando la identidad de las víctimas.

El método que usa el ***phishing*** para capturar datos es bastante simple: El primer paso consiste en enviar a las potenciales víctimas mensajes de correo electrónico que simula proceder de entidades reales, por lo general bancos y negocios que venden por Internet. Estos mensajes son cuidadosamente diseñados al punto que se redactan con la tipografía típica de esos sitios incluyendo imágenes, logotipos exactamente iguales a los originales y banners (recuadros con imágenes publicitarias en movimiento). Estos mail pueden contener un formulario para que la víctima los rellene con los datos que se le intentan sustraer o bien y como segundo paso, contener un link o vínculo a un sitio clonado, igual al original, donde se le pedirá que ingrese los datos.

Si bien estos mail a primera vista aparentan provenir de una entidad legítima, en general bancaria, a poco de observarlos podrá advertir una serie de características que los delatan.
En primer lugar –suponiendo que provengan de un banco- se trata de mensajes masivos y no personalizados como los que acostumbran a enviar los bancos. Esto es, que en el encabezado del e-mail el indicador de destinatario permanece vacío o con la palabra “ninguno” en lugar de contener su nombre. Asimismo en el cuerpo del mensaje no aparece un saludo con su nombre.

Al ser de envío masivo muy probablemente pretenda venir de una entidad con la cual no se guarda ninguna relación.
En el cuerpo del mail se explica a la víctima que por seguridad, actualización de la base de datos, mejora en el servicio, o cualquier otra razón que guarde verosimilitud, debe actualizar sus datos, en particular nombre de usuario, contraseña, números de cuenta y de tarjeta de crédito. En muchos casos se advierte a modo de amenaza que de no actualizar los datos no podrá tener acceso a sus cuentas.
Muchos e-mail de este tipo contienen en su parte inferior un vínculo al sitio falso o bien un formulario para ingresar los datos que se intenta sustraer.
Estos vínculos también delatan la presencia del ***phishing*** ya que no guardan relación con el nombre oficial del sitio al cual dicen pertenecer, o bien están enmascarados detrás del nombre real. En otros casos se usan artilugios de programación para engañar al destinatario mostrando una apariencia cuasi real y valiéndose de ciertas vulnerabilidades de los navegadores de Internet. Por ejemplo, he podido ver un e-mail que decía provenir de la librería on-line Amazon.com en el cual urgía a ingresar en su página para actualizar información personal mediante el siguiente vínculo: http://www.amazon.com@mdelas.com/exec/.. Si mira con atención verá que esa dirección contiene un símbolo "@". Ello se debe a que debido a una vulnerabilidad de varios navegadores (browser) todo lo que está a la izquierda del símbolo "@" permanece oculto y sólo procesa lo que está a su derecha. Así se intenta que la victima del engaño, al ver que la dirección comienza como está acostumbrado a verla, siga ese vinculo, pero en realidad entrará a un sitio web falso, identificado con la dirección que está a la derecha del símbolo "@".
Otra forma de engaño consiste en poner en el e-mail una imagen con el logotipo de la supuesta entidad invitando ha hacer clic sobre el mismo para ingresar al sitio web falso. La imagen que verá tendrá aspecto de verdadera, pero el vínculo que contiene, escrito en el código de programación de las páginas de Internet, lo conectará con el falso sitio. En estos casos, antes de dar clic sobre el vínculo conviene deslizar el puntero del mouse por sobre el, sin apretar el botón, para ver en la base del mail (barra de estado) la dirección completa que contiene.
En los casos mas burdos, ni siquiera se intenta esconder el falso vinculo al que se induce a entrar y se presenta tal cual es, advirtiéndose enseguida que no guarda relación con el sitio al que refiere el resto del texto.

De una u otra forma, si es que el e-mail dentro de su cuerpo no contiene un formulario para ingresar los datos que se intenta sustraer, la víctima de ***phishing*** es guiada a una página web falsa que en la mayoría de los casos imita con gran calidad al sitio verdadero, donde se le pedirá que ingrese sus datos de cuentas, tarjetas y contraseñas en un formulario para así capturarlos.
A estos falsos sitios también se los puede reconocer por una serie de detalles que es bueno tener en cuenta: Si se mira la barra de dirección, enseguida se advertirá que no comienza con la autentica dirección del sitio que pretende ser, aunque en ella figure todo o parte del nombre autentico, pero en distinto orden del original.
Los sitios web de entidades bancarias poseen "zonas seguras" desde las que se puede realizar una variada gama de transacciones que van desde la mera consulta de saldos hasta el pago de tarjetas y servicios con débito en cuenta. Estas zonas seguras se identifican de dos formas: desde la barra de dirección y por el icono de un candado amarillo cerrado o llave, dependiendo del navegador que se use.
En la barra de dirección se puede observar que la URL (Localizador Universal de recursos o dirección de Internet) comienza con http**s**, por ejemplo https://www.bancoxxxxxx.com.ar/cgi-bin/preprd.dl... . Normalmente las URL comienzan con **http**. La **"**s" final que se agrega indica que se está en conexión con un "servidor seguro", esto significa que el intercambio de información hacia y desde el sitio se realizará bajo encriptación, en la actualidad de 128 bits. El candado cerrado o llave

que aparece en el extremo inferior derecho de la ventana en la que se ve la página indican lo mismo.
Sin embargo, que se trate de un sitio seguro no significa que sea legítimo. Para comprobar la legitimidad del sitio se debe examinar cuidadosamente el certificado digital expedido por una Autoridad de Certificación que acredita que el sitio que lo posee es el que dice ser. Para ver el certificado digital se debe hacer doble clic sobre el icono del candado o la llave.
Por lo general existe en las páginas un logotipo de la Autoridad de Certificación que permite hacer la comprobación de autenticidad con mayor facilidad.
Es así que podrá comprobar si ha sido "*direccionado*" a un sitio falso mediante el chequeo previo de estos ítem.
Por ultimo, se han registrado casos en que la página a la cual se *direcciona* desde los vínculos contenidos en los e-mail, utiliza un código en JavaScript para abrir el sitio auténtico del banco de referencia mientras que al mismo tiempo abre una segunda ventana que muestra un formulario para el ingreso de datos. Si se rellena ese formulario y se envían los datos, el "ciber-delincuente" se habrá hecho con la identidad de la víctima y podrá usar su tarjeta de crédito o transferir sus fondos a otras cuentas.

**Cómo proceder:**
Si bien alarma el rápido crecimiento que este delito ha tenido durante el ultimo año en Estados Unidos, Asia y Europa, los estafadores criollos parecen no haberlo adoptado aun en forma masiva. Personalmente, conozco un solo caso de *phishing* usando una página falsa de un banco nacional de primera línea. En todo caso para que no nos sorprenda conviene prevenirse:

1. Las claves de usuario y contraseña tanto de la banca electrónica como de sitios web de compras solo deben ingresarse en sitios seguros, es decir aquellos cuyas direcciones comienzan con http**s**:// y muestran el icono de un candado cerrado amarillo o de una llave en la parte inferior del navegador.
2. Tenga en cuenta que el ingreso al sitio web de un banco se hace mediante un servidor normal, cuya su dirección comenzará con http:// , pero el ingreso del nombre de usuario y contraseña que da paso a la página personal de transacciones on-line solamente debe hacerse en servidores seguros.
3. Antes de ingresar cualquier información confidencial, como claves, contraseñas o números de tarjetas de crédito, revise la autenticidad del sitio examinando su certificado digital. Si no lo tiene o guarda dudas sobre su autenticidad no use ese servicio hasta estar seguro.
4. No ingrese datos confidenciales en formularios que aparezcan dentro de ventanas independientes sobre sitios legítimos
5. Los nombres de usuario y contraseña no deben ser dados a nadie ni colocado en mensajes de e-mail aunque tengan un formulario. En caso que ello hubiera ocurrido debe cambiarse la clave inmediatamente.
6. Desconfíe de los e-mail en que se solicitan datos confidenciales, más aun si contienen formularios ya que ninguna entidad bancaria solicita datos confidenciales vía e-mail.
7. Lea atentamente el contenido de los vínculos que ofrecen. Si se trata de iconos, deslice el mouse sobre ellos para leer en la parte inferior de la pantalla la dirección web a la que lo enviará.

En artículos anteriores les hablé sobre las diversas formas en que se obtienen datos personales sin autorización y se espía nuestra actividad en la web. También les conté sobre estafas un poco más "inocentes". La de hoy parece ser mas seria y sofisticada que las anteriores. Pero esto no debe asustar al "internauta". Internet es un mundo maravilloso y salvaje, prácticamente sin reglas, donde -hoy por hoy- son los propios usuarios quienes ejercen el control. Los delitos que se realizan mediante la web no

difieren, en esencia, de los de la calle. Por eso, como en la calle, es necesario estar alerta para que la estafa no nos sorprenda.

Firmado digitalmente por Raúl Alejandro Farías
Nombre de reconocimiento (DN): CN = Raúl Alejandro Farías, O = Política de Certificación de Correo Electrónico, OU = Persona no verificada - No amparado bajo el Decreto 427/98 de la IFDAPN
Motivo: Artículo creado por Dr. Raúl A. Farías para "Sintesis Forense"
Ubicación: San Isidro, Pcia. de Buenos Aires
Fecha: 2005.03.18 00:56:18 -03'00'