



internet

NUEVOS MÉTODOS PARA ROBAR DATOS PERSONALES EN INTERNET

Eduardo Fainé Celis *

Phishing.

Este término es una deformación de la palabra inglesa *fishing*, que quiere decir pescar, siendo su propósito atraer posibles presas hacia una carnada con la suposición que mientras la mayoría de éstas no hará caso del cebo, al menos algunas se verán tentadas y picarán.

En nuestro caso, este es el acto de enviar un e-mail a un usuario, fingiendo ser una empresa legalmente establecida. Por ejemplo, su proveedor de Internet, banco, servicio de pago en línea o incluso una entidad gubernamental, en un intento de llevar al destinatario a entregar su información privada que será usada para robar su identidad.

El e-mail dirige al usuario a visitar un sitio web donde se le solicita actualizar su información personal como passwords, números de tarjetas de crédito, números de cuentas bancarias u otros igualmente sensibles que esa organización ya posee. El sitio web, sin embargo, es falso y está destinado sólo para robar la información de la víctima. Por ejemplo, durante el año 2003, se vio una proliferación de una trampa de *phishing* en la que los usuarios recibían un supuesto e-mail de eBay informando que su cuenta sería cerrada, a no mediar que se hiciera clic

sobre un vínculo dentro del mensaje y actualizara la información de su tarjeta de crédito, la que en el verdadero sitio web de eBay ya existía.

Dado que es relativamente fácil imitar la apariencia de un sitio comercial legítimo copiando su código HTML, la trampa confiaba en convencer a sus víctimas que realmente estaban siendo contactadas por eBay y luego eran redirigidas al sitio de esa empresa para actualizar la información de su cuenta. Mediante el envío de correos spam a grandes grupos de personas, el creador del *phishing* contaba con que al menos un porcentaje de sus destinatarios que leyeron el correo tendrían cuentas registradas en eBay y accederían a entregárselos mediante este engaño.

Cómo evitar este tipo de estafa.

- Si se recibe un mensaje, o en Internet aparece una ventana pop-up que solicita información personal o financiera, no responda o cliquee el vínculo del mensaje. Las compañías legítimas no hacen estos requerimientos por e-mail. Si tiene dudas acerca de la solicitud, contacte a la organización empleando una línea conocida de atención al cliente, o bien use el sitio web de esa empresa,

* Capitán de Fragata. Oficial de Estado Mayor. Máster en Diseño y Comunicación Multimedia.

digitando personalmente la dirección IP. No copie y pegue el link del mensaje.

- No envíe su información por e-mail. Este no es un método seguro para transmisión de información personal. Si requiere enviar sus datos por Internet, verifique que el sitio contenga indicadores acerca de su seguridad, como un candado en la ventana del navegador o la sigla "https" al inicio de la dirección. La "s" indica que se trata de un sitio seguro. Desafortunadamente, ningún icono es garantía de seguridad total, algunos estafadores han falsificado íconos de seguridad.
- Use un antivirus actualizado. Algunos mensajes de *phishing* contienen programas espías (spyware) que detectan sus actividades en la red o bien pueden contener virus que destruyan su información. En caso de poseer banda ancha, un cortafuegos (firewall) es esencial. Ayuda a mantenerse invisible en Internet y bloquea los intentos de acceso no autorizados desde el

exterior. Finalmente, mantenga actualizado su sistema operativo, instalando los parches gratuitos que se pueden bajar de los sitios corporativos.

- Siempre sea cauto al momento de abrir o descargar cualquier archivo adjunto de correos electrónicos que reciba, sin importar la fuente que se lo envió.

Lo mencionado anteriormente puede parecer cercano a la paranoia, pero estas medidas no tienen otra finalidad que dar algo de tranquilidad mientras se aprovecha todo lo bueno que ofrece Internet en sus muchas aplicaciones, sin correr el riesgo de caer en manos inescrupulosas que sacan partido de las deficiencias del sistema para su propio beneficio.

Fuentes:

Comisión Federal de Comercio para el Consumidor, <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

Enciclopedia en Internet "Webopedia", <http://www.webopedia.com/TERM/p/phishing.html>

* * *