

CÓMO PREVENIR LAS ESTAFAS EN LA WEB

Por Walter S. Mossberg
Cortesía: Diario Reforma

Resumen

Los ladrones de identidad representan la amenaza de mayor crecimiento en Internet.

Si trabaja con una computadora que funciona con el sistema operativo Windows, necesita instalar una serie de programas de seguridad para protegerse de una oleada de invasores, tales como antivirus, firewall, antispam, entre muchos otros.

Pero el mayor problema es la llamada "ingeniería social" que consiste en las tácticas que tratan de hacer que los usuarios de PC revelen datos financieros importantes, que luego pueden ser usados por criminales para robar su dinero e incluso su identidad. Debe ser muy cuidadoso en sus actividades en línea.

La ingeniería social es un término amplio que incluye phishing, una técnica en la que los criminales crean correos electrónicos o páginas Web que aparentan provenir de fuentes confiables (P..ej. entidades bancarias) e intentan obtener datos confidenciales de los usuarios. Está directamente asociada a una recién creada categoría de software malicioso llamada crimeware – o programas que ayudan criminales a robar información financiera privada. La amenaza es real. Las reglas básicas para protegerse son:

1. No confíe en los correos electrónicos de las instituciones financieras. Los emails se pueden manipular con tanta facilidad que lo mejor es siempre considerar a todos los emails provenientes de instituciones financieras como ilegítimos. Nunca responda a esos mensajes, ni haga clic en ellos; hay una gran posibilidad de que se trate de un fraude bien preparado. El sitio también puede instalar sigilosamente en su PC un tipo de programa llamado key logger, que graba todo lo que usted digita en la computadora y envía la información a los estafadores.
2. Nunca conteste un email comercial no solicitado (spam). Tampoco haga clic en los enlaces de estos mensajes. Puede resultar en la instalación secreta de un key logger u otros software malicioso. La única respuesta adecuada a un spam es ignorarlo y borrarlo.
3. No descargue o utilice software gratuito a menos que esté seguro que es legítimo. Averigüe bien antes de descargarlos. Busque información sobre ellos en CNET y PC Magazine, que reseñan la mayor parte del software. Puede que pierda la oportunidad de tener algunos programas legítimos gratis, pero seguramente le evitará muchos dolores de cabeza.

Un programa antispyware no evitará que usted revele información privada a un sitio Web falso, pero puede bloquear la instalación y funcionamiento de un software espía que provenga de esta página. Un usuario Macintosh puede tontamente entregar los datos de su cuenta a un sitio Web, pero la mayoría del software malicioso que los criminales intentan instalar en computadoras privadas no funcionan en una Mac, es decir, resulta más segura.

Además, existen algunos nuevos programas de seguridad que combaten directamente los fraudes de la ingeniería social. El programa Site Advisor de McAfee, le informa si una página Web es sospechosa. Una nueva función del buscador FireFox (Shazou), puede decirle dónde se encuentra un servidor de un sitio Web, es decir, si piensa que está en el sitio de Bank of America, pero Shazou le informa que el servidor está en Rusia, es un claro indicio de que es una estafa. Symantec planea lanzar el Norton Confidential que le dirá si un sitio Web parece ser falso.

Sin embargo, la mejor protección contra los crímenes de la ingeniería social sigue siendo el estar siempre atento y se cuidadoso.

M.A. Enrique Tapia Padilla, CPP DSI