Consumer Reports WebWatch
Proyecto para prevenir delitos en línea (Web)
Hoja informativa #3: No permita que obtengan sus datos personales

Este es el tercer artículo de una serie de hojas informativas editado por *Consumer Reports WebWatch*, con una subvención de la Oficina de la Procuraduría General del Estado de Nueva York.

¿Le ha pasado esto alguna vez? Recibe un correo electrónicco que aparenta ser de eBay, PayPal o Citibank, pidiéndole qua actualice su cuenta. ¡Pero no haga clic tan deprisa! Pudiera acabar en un sitio Web compuesto por estafadores que obtienen información de su computadora y consiguen un récord de todas sus contraseñas para enviar la información al extranjero. Millones de personas han sido víctimas de estafas como éstas – aún si no hacen negocio con la compañía que les envió el correo. Los correos electrónicos para obtener datos o información confidencial sin autorización (*phishing*) normalmente pretenden provenir de compañías de servicios financieros, proveedores de servicios de internet o negocios minoristas. Inclusive, en una ocasión unos estafadores atrevidos usaron fraudulentamente el nombre de la Comisión Federal de Comercio, agencia encargada de enjuiciar a aquellos que cometen fraude por correo electrónico.

Dependiendo de con quién hable, la explosión en las estafas de datos confidenciales no va en aumento, pero las técnicas de los estafadores para perpetrarlas están mejorando. Entre las técnicas populares que engañan al consumidor se encuentran: asociar el mensaje electrónico con un día feriado o evento, tal como la Copa Mundial; hacer como si el que lo envía es parte de la compañía con la que usted trabaja; o enviar un correo diciendo que su cuenta bancaria ha sido comprometida y urgiéndolo a que envíe información confidencial a un sitio fraudulento que aparenta ser el de su banco.

Para evitar ser víctima de la pesca de datos confidenciales, siga las siguientes recomendaciones:

1. Sea cauteloso con cualquier mensaje y evite usar hiperenlaces en sus correos electrónicos. Éstos pueden mostrar una dirección pero enviarlo a otra. Borre cualquier mensaje que trate de mandarlo a una página Web mediante un enlace que se encuentre allí. Los correos electrónicos legítimos le pedirán que vaya a un sitio Web específico – escribiendo la dirección en su navegador o usando su propio marcador de sitios favoritos. Las instituciones financieras están aumentando su vigilancia contra la pesca fraudulenta de datos. Bank of America y Vanguard les piden ahora a sus clientes que seleccionen una imagen o frase personalizada que aparece cuando entran al sitio, para corroborar que es el sitio legítimo de la institución.

2. En las páginas Web, ponga el apuntador de su mouse (ratón) sobre la dirección de Internet para ver si la que aparece abajo en su navegador guarda relación con la página o el sitio que usted espera visitar. Al llegar al sitio, verifique que la dirección que aparece en la barra de dirección del navegador sea la correcta. Preste atención a la parte de la dirección entre "http:// " (or https://) y la siguiente marca. Tenga cuidado con trucos como el uso de un cero en lugar de la letra O. Verifique la dirección y después márquela en su navegador o use un marcador favorito ya almacenado en su navegador.

3. Fíjese en errores de ortografía o gramática incorrecta, una de las señales más comunes de estafas y obtención fraudulenta de información confidencial.

4. Reporte la obtención fraudulenta de información confidencial. Si recibe un e-mail de este tipo, envíelo al grupo contra phishing, Anti-Phishing Working Group, a la Comisión Federal de Comercio y a la compañía u organización que está siendo imitada. También puede enviar una queja al Centro de Quejas para Delitos de Internet del FBI en www.ic3.gov.

5. Use un navegador Web con herramientas para verificar el sitio, tal como Firefox, o software como McAfee's Site Advisor, que verifica el sitio y le permite bajar los resultados gratuitamente.

Para más información y para mantenerse al día sobre lo último en estafas de información confidencial y recursos para el uso del consumidor, marque como favorito el sitio de Consumer Reports WebWatch.