VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2013

Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- Tiendas en línea
- Tu computadora
- Tu tarjeta de crédito

Compras seguras en línea

Época de cautela

La temporada navideña está cerca y pronto millones de personas alrededor del mundo estarán buscando comprar los regalos perfectos. Muchas personas optan por comprar en línea, intentando conseguir el mejor precio o para evitar las largas filas y multitudes. Desafortunadamente, los sitios web falsos también aprovechan estas fechas para estafar a los compradores con la venta de productos falsificados al robar información de tarjetas de crédito o simplemente al no entregar el producto. En este boletín vamos a cubrir algunos de los peligros de las compras en línea y las formas de protegerse.

Editor Invitado

Lenny Zeltser es el editor invitado para esta edición. Lenny se centra en la protección de TI de los clientes de NCR Corp y enseña análisis forense de malware en el SANS Institute. Lenny está en Twitter como **@lennyzeltser** y escribe un blog de seguridad en **blog.zeltser.com**.

Tiendas en línea

Un estafador puede crear fácilmente un sitio web que parezca ser una tienda legítima, simplemente copiando el aspecto de otras tiendas famosas. Una vez que estos sitios web falsos se encuentran disponibles, los estafadores se aprovechan de las personas que buscan el precio más bajo posible. Los compradores muchas veces comienzan buscando en Google o Bing los productos que les gustaría comprar y después agregan palabras como “barato” o “precio más bajo”. Como resultado, el buscador presentará cientos de sitios web que venden el artículo, muchos de ellos podrían ser falsos.

Cuando selecciones un sitio web para comprar el artículo de tu interés, ten cuidado con las tiendas en línea que ofrecen un precio que es considerablemente más barato que cualquier otra. La razón por la que puede ser tan barato es porque, después de comprar el artículo, lo que realmente recibas es un artículo falsificado o robado, incluso en algunos casos, simplemente nunca lo envían. Estos pueden ser indicadores de sitios web fraudulentos:

- No hay un número de teléfono para llamar donde se atiendan dudas relacionadas con las compras o para recibir soporte.
- El nombre de dominio del sitio web es diferente que el nombre de dominio que se utiliza para las direcciones de correo electrónico o de otra información de contacto.
- La página web tiene errores de gramática o de ortografía.

Compras seguras en línea

- El sitio web es una réplica exacta de un sitio web muy conocido que utilizabas en el pasado, pero el nombre de dominio del sitio web o el nombre de la tienda es ligeramente diferente.

Recuerda, solo porque el sitio se vea profesional no quiere decir que sea legítimo. Si algún aspecto del sitio te parece extraño, tómate el tiempo para verlo más de cerca. Por ejemplo, llama al número de teléfono que aparece en la sección “contacto” del sitio web para confirmar que el número es válido. Adicionalmente puedes escribir el nombre o la URL de la tienda en un buscador y ver lo que otras personas han dicho sobre ese sitio web. Si todavía no estás seguro de que el sitio es legítimo, no lo uses. En su lugar, compra en un sitio web que sea conocido o en el que se pueda confiar, de preferencia uno que tú, tus amigos o miembros de la familia hayan utilizado en el pasado. Los precios pueden no ser tan baratos pero recibirás un producto más fiable y es menos probable que te estafen.

La mejor forma de protegerse en línea es ir de compras en las tiendas en línea de confianza y que tienen una reputación establecida.

Tu computadora

Además de hacer compras en sitios web legítimos, necesitas asegurarte de que la computadora que estás usando para las compras en línea es segura. Si tu computadora está infectada, un criminal cibernético en alguna parte del mundo puede capturar las pulsaciones del teclado y tus archivos. Esto podría permitir a los criminales robar tu usuario y contraseña de acceso a las tiendas en línea, números de tarjetas de crédito, información bancaria y otros datos sensibles. Asegúrate de que solo tú tengas acceso a la computadora que estás utilizando y que esté conectada a una red de confianza. Esto significa que se hayan instalado las últimas actualizaciones de seguridad y se esté ejecutando el software antivirus, por lo menos.

Si hay niños en casa, considera tener dos computadoras, una para tus hijos y una solo para los adultos. Los niños son muy curiosos e interactivos con la tecnología y como resultado de ello, es más probable que infecten su propia computadora. Mediante el uso de una computadora separada solo para transacciones en línea, como la banca en línea y compras, se reduce el riesgo de que tu computadora se infecte. Si dos equipos no es una opción, por lo menos ten cuentas separadas en el equipo compartido y asegúrate de que tus hijos no tengan privilegios de administrador.

Compras seguras en línea

Tu tarjeta de crédito

Se cuidadoso con tu tarjeta de crédito. Esto implica mantenerte al pendiente de tus estados de cuenta de la tarjeta de crédito para identificar cargos sospechosos. Debes revisar tus estados de cuenta al menos una vez al mes. Algunos proveedores de tarjetas de crédito incluso te dan la opción de notificarte vía correo electrónico o con una alerta a tu teléfono cuando se realizan cargos o cuando se excede una cantidad fija.

Si crees que te han cometido fraude, como no recibir tu paquete a pesar de que has tratado de ponerte en contacto varias veces o recibes cargos extraños a tu tarjeta de crédito, llama a tu compañía de tarjeta de crédito de inmediato y explica tu situación. Esta es la razón por la que las tarjetas de crédito son mejor opción para compras en línea que las tarjetas de débito. Las tarjetas de débito entregan dinero directamente de tu cuenta bancaria y, si se han cometido fraudes, es mucho más difícil obtenerlo de vuelta. Varias tarjetas de crédito te dan la opción de generar un número de tarjeta único para todas las compras en línea, o quizás puedas considerar un servicio como PayPal, donde no tienes que exponer tu tarjeta de crédito con cada compra en línea. Revisa su compañía de tarjeta de crédito para ver cuáles son los servicios adicionales que ofrecen para las compras en línea.

Conoce más

Suscríbete al boletín mensual de conciencia sobre seguridad OUCH!, consulta los archivos OUCH! y aprende más acerca de las soluciones de seguridad SANS visitando: http://www.securingthehuman.org

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.

Sitio web: http://www.seguridad.unam.mx

Síguelo en Twitter @unamcert

Recursos

Consejos para mantenerse seguro en las compras en línea:	http://disc.unam.mx/2012/img/presentaciones/davidRamirez.pdf
Compras seguras por Internet:	http://revistadelconsumidor.gob.mx/?p=33457
Cómo comprar en línea de forma segura:	http://www.samsung.com/es/article/consejos-para-hacer-compras-seguras-con-el-movil
Compras seguras utilizando un Smartphone:	http://www.viruslist.com/sp/glossary
Glosario de términos de seguridad:	http://www.viruslist.com/sp/glossary
Tip del día del Instituto SANS:	http://www.sans.org/tip_of_the_day.php
Consejo del día SSI UNAM-CERT:	http://www.seguridad.unam.mx/usuario-casero/consejos/

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Sarahí Díaz, Pedro Guerrero, Nora Cozaya