VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2015

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

- **Tiendas en línea falsas**
- **Tu equipo de cómputo / dispositivo móvil**
- **Tu tarjeta de crédito**

Comprando en línea de forma segura

En esta temporada, sé precavido

La temporada navideña está cerca y pronto millones de personas alrededor del mundo buscarán comprar los regalos perfectos. Muchos de nosotros elegiremos comprar en línea tratando de encontrar una buena oferta, evitando largas filas y multitudes impacientes. Desafortunadamente, también es la época favorita de los criminales para cometer fraudes financieros o en línea. Este mes explicaremos los peligros de comprar en línea y las maneras en las que puedes protegerte.

Editor Invitado

Jonathan Homer (**@JonathanLHomer**) es un reconocido líder en el área de la concientización en seguridad cibernética y labora tanto en el gobierno como en el sector privado. Jon se especializa en el compromiso de audiencias y técnicas innovadoras de capacitación.

Tiendas en línea falsas

Aunque la mayoría de las tiendas en línea son legítimas, algunas no lo son. Existen sitios web falsos elaborados por criminales, los cuales copian la apariencia o usan el nombre de tiendas de prestigio. Después, utilizan esos sitios para engañar a las personas que buscan la mejor oferta posible. Cuando buscas en línea por el precio más bajo, puedes ser dirigido a alguno de estos sitios falsos.

Al seleccionar un sitio web para comprar un producto, sé precavido de aquellos que anuncien precios exageradamente más baratos que cualquier otro lugar o que ofrezcan productos que se encuentren agotados a nivel nacional. La razón por la que sus productos sean tan baratos o estén disponibles puede deberse a que lo que recibirás no es legítimo, es falso, es un producto robado o, en algunas ocasiones, nunca lo recibirás. Protégete a ti mismo haciendo lo siguiente:

- Verifica que el sitio web tenga una dirección de correo legítimo y un número telefónico para ventas o dudas al consumidor. Si el sitio parece sospechoso, busca los datos de contacto, llama y habla con una persona.
- Busca señales de advertencia obvias como una mala ortografía o gramática.
- Sospecha bastante de algún sitio web que parezca ser una réplica exacta del portal web de alguna tienda de prestigio que hayas usado anteriormente, pero que el nombre de dominio o nombre de la tienda sea un poco diferente. Por ejemplo, quizás usaste el sitio web https://amazon.com para hacer todas tus compras Amazon, pero puede ser muy sospechoso si te encuentras algún sitio web pretendiendo ser Amazon con la URL http://store-amazon.com.

Comprando en línea de forma segura

- Escribe el nombre de la tienda o URL en algún motor de búsqueda y examina qué han dicho otras personas acerca del sitio web en el pasado. Revisa términos como “estafa”, “nunca más”, o “falso”. La falta de comentarios tampoco es una buena señal ya que indica que el sitio web es muy reciente.

Recuerda, sólo porque el sitio parezca profesional no quiere decir que sea legítimo. Si existe cualquier cosa en el sitio que te de señales de advertencia, tómate tu tiempo para investigar. Si no te sientes a gusto con el sitio web, no lo uses. En vez de eso, busca algún sitio web de una tienda de prestigio en la que puedas confiar o hayas usado de forma segura anteriormente. Quizás no encuentres una gran oferta o algún producto de moda, pero te asegurarás de terminar con un producto legítimo o un estado crediticio limpio.

Protégete a ti mismo en línea comprando sólo en sitios web confiables con una reputación establecida.

Tu computadora / dispositivo móvil

Además de comprar en un sitio web legítimo, debes verificar que tu computadora o dispositivo móvil es seguro. Los cibercriminales tratarán de infectar tus dispositivos para recolectar cuentas bancarias, información crediticia y contraseñas. Considera los siguientes pasos para mantener tus dispositivos seguros:

- Si tienes niños en casa, considera tener dos dispositivos: uno para ellos y otro para los adultos. Los niños son curiosos e interactúan con la tecnología y, como resultado, son más propensos a infectar sus dispositivos. Usando una computadora o tableta por separado, sólo para las transacciones en línea como la banca o compras en línea, reduces la posibilidad de infección. Si separar dispositivos no es una opción, entonces ten cuentas separadas para una computadora compartida y asegúrate que los niños no tengan privilegios administrativos.
- Conéctate sólo a redes inalámbricas que tú administres, como la red de tu casa, o redes conocidas en las que puedas confiar para hacer transacciones financieras. Usando una red Wi-Fi pública, como la que te conectas cuando compras en una cafetería, puede ser excelente para leer noticias pero no para acceder a tu cuenta bancaria.
- Siempre instala las últimas actualizaciones de tu sistema operativo y mantén actualizado tu software antivirus. Esto hace mucho más difícil que un cibercriminal infecte tu dispositivo.

Tu tarjeta de crédito

Mantente atento de tus cuentas bancarias para identificar cargos sospechosos. Puedes revisar tus cuentas regularmente, como mínimo una vez al mes. Algunos proveedores de tarjetas de crédito te dan la opción de notificarte vía correo

Comprando en línea de forma segura

electrónico o mensaje de texto cada vez que un cargo es hecho en tu tarjeta o cuando éste excede alguna cantidad. Otra opción es tener una tarjeta de crédito sólo para compras en línea; de esta manera, si la tarjeta es comprometida, puedes fácilmente cambiar la tarjeta sin impactar cualquier otra actividad de pago. Si crees que se ha cometido algún fraude, llama a la compañía de la tarjeta de crédito inmediatamente y explica la situación. También es importante que consideres que las tarjetas de crédito son mejores para compras en línea que las tarjetas de débito. Las tarjetas de débito toman el dinero directamente de tu cuenta bancaria, si un fraude ha sido cometido puede ser mucho más difícil tener tu dinero de vuelta.

Finalmente, existe nueva tecnología que te permite pagar sin exponer tu número de tarjeta. Considera tarjetas de crédito que generen un único número de tarjeta en cada compra en línea, o usa servicios de pago bien conocidos, como PayPal, la cual no requiere que reveles tu número de tarjeta de crédito al vendedor.

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

Tips para evitar fraudes en línea:	http://revista.seguridad.unam.mx/numero-02/tips-para-evitar-fraudes-en-l%C3%ADnea
Cómo protegerte de fraudes a tarjetas bancarias:	http://www.seguridad.unam.mx/noticia/?noti=1924
¿Cómo enfrentar de manera segura el comercio electrónico?:	http://www.seguridad.unam.mx/img/20121115comercioelectronico.png
Cinco pasos para mantenerse seguro:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción: Pablo Lorenzana y Katia Rodríguez