SANS SECURITY AWARENESS
VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Noviembre 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Tiendas en línea falsas
- Tu computadora/dispositivo móvil
- Tu tarjeta de crédito

Compra en línea de manera segura

Resumen

La temporada de fiestas se acerca para muchos de nosotros y pronto millones de personas alrededor del mundo buscarán comprar los regalos perfectos. Muchos de nosotros elegiremos comprar en línea buscando grandes ofertas y evitando así largas filas y tumultos impacientes. Desafortunadamente, esta es también la temporada del año en la cual los cibercriminales crean tiendas en línea falsas para estafar y robar. A continuación, explicamos los riesgos de comprar en línea y cómo obtener esa asombrosa oferta de manera segura.

Editor Invitado

Lenny Zeltser construye productos de seguridad en Minerva Labs y enseña a combatir malware en el Instituto SANS. Lenny es activo en Twitter a través de la cuenta **@lennyzeltser** y escribe en un blog de seguridad en **zeltser.com**.

Tiendas en línea falsas

Mientras muchas tiendas en línea son legítimas, existen algunos sitios falsos establecidos por cibercriminales. Ellos crean estos sitios falsos replicando la apariencia de sitios reales o usando los nombres de tiendas o marcas reconocidas. Después, usan estos sitios fraudulentos para captar a la gente en busca de ofertas. Cuando se buscan los precios más bajos en línea podrías ser dirigido a uno de estos sitios falsos. Al seleccionar un sitio donde hacer una compra, se debe tener cuidado de sitios que muestran productos exageradamente más baratos que cualquier otro sitio o sitios que ofrecen productos agotados. La razón por la cual sus productos son baratos o están disponibles es porque lo que se recibirá no es legítimo, podría ser clonado o robado, o en algunos casos nunca es entregado. Protégete de la siguiente manera:

- Si es posible, compra en sitios que ya conozcas, en los cuales confíes y con quienes hayas hecho alguna transacción con anterioridad.
- Verifica que el sitio tenga una dirección de correo legítima y un número telefónico para ventas o dudas referentes a soporte. Si el sitio luce sospechoso, llama y habla con una persona de la tienda, si no puedes hablar con nadie, esta debe ser la primera señal de que estás frente a un sitio falso.
- Busca señales obvias de alerta, por ejemplo, ofertas que son demasiado buenas para ser verdad, o una gramática y redacción pobre.
- Sospecha de un sitio web si parece ser una réplica exacta de otro sitio reconocido que hayas usado en el pasado pero que tenga el nombre de dominio o nombre de la tienda ligeramente diferente. Por ejemplo, podrías estar acostumbrado

Compra en línea de manera segura

a realizar compras en línea en Amazon, cuyo sitio web es https://www.amazon.com. Entonces deberías sospechar si te encuentras en sitios web que pretenden ser Amazon como http://store-amazoncom.com

- Teclea el nombre de la tienda o la URL en un motor de búsqueda y ve lo que la gente ha dicho sobre el sitio en el pasado. Busca los términos “fraude”, “engaño”, “nunca” o “falso”. La falta de reseñas puede ser también una señal que indica que el sitio es muy nuevo y podría no ser confiable.
- Antes de comprar cualquier producto, asegúrate de que tu conexión esté cifrada. La mayoría de los navegadores muestran las conexiones cifradas con un candado y/o las letras HTTPS en color verde justo antes del nombre del sitio web.

Protégete a ti mismo comprando solo en sitios web con una reputación establecida.

Recuerda: solo porque el sitio luzca profesional no significa que es legítimo. Si no te sientes cómodo con el sitio, no lo uses. En cambio, encuentra un sitio reconocido en el que puedas confiar o que hayas usado de manera segura con anterioridad. Quizás no puedas encontrar una oferta increíble, pero es más seguro que obtengas un producto legítimo y que evites que tu información personal o financiera sea robada.

Tu computadora/ dispositivo móvil

Además de comprar en sitios web legítimos, debes asegurarte de que tu computadora o dispositivo móvil sea seguro. Los cibercriminales intentarán infectar tus dispositivos de manera que puedan obtener tus cuentas bancarias, información de tus tarjetas de crédito y contraseñas. Realiza los siguientes pasos para mantener tus dispositivos seguros:

- Si tienes niños en casa, considera tener 2 dispositivos, uno para tus hijos y otro para los adultos. Los niños son curiosos e interactúan con la tecnología, como resultado son más propensos a infectar su propio dispositivo. Usando una computadora o tablet por separado, solo para transacciones en línea (tales como banca y compras) puedes reducir la probabilidad de infectar tu equipo.
- Siempre instala las últimas actualizaciones y ejecuta software antivirus actualizado. De esta forma es mucho más complicado que un cibercriminal logre infectar tu equipo.

Tu tarjeta de crédito

Revisa con regularidad los estados de tu tarjeta de crédito para identificar cobros sospechosos, especialmente luego de

Compra en línea de manera segura

usar tus tarjetas para efectuar compras en línea o usar un nuevo sitio en línea. Algunos proveedores de tarjetas de crédito te proporcionan la opción de notificarte por medio de correo electrónico o mensajes de texto cada vez que un cobro es cargado a tu tarjeta o cuando los cobros exceden el límite establecido. Otra opción es tener otra tarjeta de crédito solo para compras en línea, de esa manera si la tarjeta es comprometida, puedes fácilmente cambiar la tarjeta sin afectar ninguna de tus otras actividades financieras. Si piensas que se ha cometido un fraude con tu tarjeta de crédito, contacta inmediatamente a tu banco. Por esta razón deberías considerar usar tarjetas de crédito para todas tus compras por Internet, evita usar tarjetas de débito si es posible. Las tarjetas de débito toman dinero directamente de tu cuenta bancaria, si un fraude ha sido cometido puede ser muy complicado obtener tu dinero de vuelta. Finalmente, considera utilizar tarjetas de crédito que generen un número único de tarjeta cada vez que compras en línea, tarjetas de regalo o servicios de pago reconocidos, como PayPal, que no requieren que proporciones 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: securingthehuman.sans.org/ouch/archives

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

Ingeniería social: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_sp.pdf

Cuatro recomendaciones para mantenerse seguro:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201610_sp.pdf

Asegurando tu red doméstica: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201602_sp.pdf

Consejos prácticos de seguridad para proteger los datos bancarios al comprar en línea:
https://revista.seguridad.unam.mx/numero-28/consejos-practicos

Consejo editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: Fernando Castañeda González y Oscar Iván Flores Ávila