Boletín mensual de concientización en seguridad para ti

Compras en línea de manera segura

Resumen

La temporada de fiestas se acerca para muchos de nosotros y pronto millones de personas estarán buscando comprar los regalos perfectos. Muchos de nosotros compraremos en línea en busca de grandes ofertas y para evitar las grandes multitudes de personas. Desafortunadamente, los delincuentes cibernéticos estarán activos, creando sitios web de compras falsos y utilizando otras tácticas para estafar a la gente. En este boletín, explicaremos cómo puedes comprar en línea de forma segura y evitar convertirte en una víctima.

Tiendas en línea falsas

Los ciberdelincuentes crean tiendas en línea falsas que imitan el aspecto de sitios reales o utilizan nombres de tiendas o marcas conocidas. Cuando buscas las mejores ofertas en línea, puedes encontrarte con uno de estos sitios falsos. Al comprar en estos sitios web puedes terminar con artículos falsificados o robados, y en algunos casos, tus compras podrían nunca ser entregadas. Protégete de las tiendas en línea falsas:

Cuando sea posible, compra en tiendas en línea que conoces, confías y has hecho transacciones con anterioridad. Coloca en tus marcadores/favoritos de tu navegador las tiendas en línea que has visitado antes y en las que confías.

Mantente atento de los precios que son significativamente menores de los que se encuentran en las tiendas en línea establecidas. Si el precio suena demasiado bueno para ser verdad, puede ser falso.

Sospecha si el sitio web se parece al que has usado en el pasado, pero el nombre de dominio del sitio web o el nombre de la tienda es ligeramente diferente. Por ejemplo, puedes estar acostumbrado a comprar en Amazon, cuya dirección del sitio web es www.amazon.com, pero terminas comprando en un sitio web falso que tiene una dirección de sitio web similar, pero la letra "o" se sustituye por el número "0".

Escribe el nombre de la tienda en línea o su dirección web en un motor de búsqueda para revisar lo que otros han dicho al respecto. Busca términos como "fraude", "estafa", "nunca más" o "falso".

Utiliza contraseñas únicas para cada una de tus cuentas en línea. ¿No recuerdas todas tus contraseñas? Considera utilizar un gestor de contraseñas.

Defraudadores en sitios web legítimos

Mantén la guardia alta incluso cuando compres en sitios web de confianza. Las grandes tiendas en línea a menudo ofrecen productos vendidos por diferentes personas o empresas que podrían tener intenciones fraudulentas. Estas tiendas en línea son como los mercados del mundo real, donde algunos vendedores son más confiables que otros. Comprueba la reputación de cada vendedor antes de realizar el pedido. Ten cuidado con los vendedores que son nuevos en la tienda o que venden artículos a precios ridículamente bajos. Revisa las políticas de la tienda sobre compras con terceros. En caso de duda, compra artículos vendidos directamente por la tienda en línea, no por los vendedores de terceros que participan en el mercado en línea.

Pagos en línea para compras

Revisa regularmente los estados de cuenta de tu tarjeta de crédito para identificar cargos sospechosos. Si es posible, habilita la opción de notificaciones por correo electrónico, mensaje de texto o la aplicación para que se te notifique cada vez que se realice un cargo a tu tarjeta de crédito. Si encuentras alguna actividad sospechosa, llama a la compañía de tu tarjeta de crédito de inmediato y repórtala. Evita el uso de tarjetas de débito siempre que sea posible. Las tarjetas de débito toman dinero directamente de tu cuenta bancaria, por lo que en caso de que se cometa algún fraude con tu tarjeta, tardará un largo periodo de tiempo para que puedas recuperar tu dinero. Otra opción es el uso de servicios de pago más conocidos para compras en línea, como PayPal, que no requiere que reveles tu número de tarjeta de crédito al vendedor. Por último, considera el uso de una tarjeta de regalo para compras en línea.

El hecho de que una tienda en línea tenga un aspecto profesional y bien diseñado no significa que sea legítimo. Si el sitio web te incomoda, no lo uses. En su lugar, dirígete a un sitio conocido en el que puedas confiar o que hayas utilizado de forma segura en el pasado. Puedes no encontrar la oferta increíble, pero es mucho más probable que termines con un producto legítimo y evites ser estafado.

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

Editor Invitado

Lenny Zeltser *es oficial de seguridad de la información de Axonius, instructor senior y autor en el Instituto SANS. Puedes seguirlo en Twitter como* @lennyzeltser *y leer su blog en* zeltser.com.

Recursos

Ingeniería Social:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_sp.pdf
Estafas a través de redes sociales:	https://www.sans.org/sites/default/files/2019-09/201909-OUCH-September-Spanish_0.pdf
Creando contraseñas simples:	https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Spanish_0.pdf