Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Sitios web falsos

EDITOR INVITADO

Arrigo Triulzi es el editor invitado para este número. Es Instructor Certificado por el Instituto SANS y consultor de seguridad independiente a las fueras de Ginebra, Suiza.

RESUMEN

Una de las ventajas de comprar en línea es la posibilidad de encontrar el producto o servicio que quieres, pero a menor costo. Los criminales saben esto y tomarán ventaja de tu deseo de encontrar una oferta en línea. Crearán sitios web falsos que parezcan legítimos, pero venderán productos falsificados o incluso peor, simplemente no entregarán nada. En éste boletín daremos un ejemplo de este tipo de ataques y explicaremos cómo puedes protegerte de fraudes similares.

EJEMPLO DE UN SITIO WEB FALSO

Supongamos que necesitas comprar una carriola para niños, quizá como regalo para un amigo o un familiar que tenga un recién nacido. Decidiste buscar una oferta en línea y hacer una búsqueda de carriolas, específicamente de la MARCA X, ya que sabes que es la marca preferida de tu amigo. Cuando realizas la búsqueda de la carriola MARCA X, rápidamente descubres que muchos sitos venden la misma carriola; sin embargo, los precios varían enormemente. Seleccionas el sitio web que tiene los precios más bajos y compras el producto en línea. Varias semanas después, recibes el producto, pero descubres que no luce bien; algunas de las piezas están mal, el material es defectuoso o el producto no es nuevo. Intentas llamar al sitio web para devolver el producto y te encuentras con que no hay número telefónico. Entonces envías un correo electrónico al sitio web, pero ninguna de tus quejas obtiene alguna respuesta. Todo apunta a que compraste un producto pirata (o robado) en un sitio web falso.

Lo que sucedió es que un criminal simplemente copió el sitio web legítimo del fabricante original (en este caso la carriola MARCA X), publicó este sitio web bajo un nuevo nombre de dominio que él controla y después bajó significativamente los precios para incitar a las personas a comprar en su sitio. Los productos que entrega son productos falsificados, robados o usados, en ocasiones simplemente no te entregan nada en absoluto. En consecuencia, todo lo que cobran es ganancia pura para ellos.

PROTEGIÉNDOSE A SÍ MISMO

Sabemos y entendemos que buscas aprovechar Internet para tener la mejor experiencia de compra posible. A continuación, se listan varios pasos que puedes seguir para protegerte de ataques como este:

© The SANS Institute 2012

Sitios web falsos

1. Si el precio parece demasiado bueno para ser verdad, debes desconfiar.
2. Llama a su número de asistencia. Espera… ¿no hay número de asistencia o ningún número al cual llamar? Otra señal de alerta.
3. Comúnmente, los criminales que establecen estos sitios falsos no son hablantes nativos del lenguaje del sitio web. Los correos que te envían suelen tener una gramática pobre o errores básicos de ortografía. En el caso del sitio web de una carriola falsa, uno de sus correos iniciaba con "*We wish to welcome you to BRAND X baby carrier, Cheap baby carrier BRAND X, on sale,Free shipping*." ("Queremos darle la bienvenida a carriola MARCA X, Carriola barata MARCAX, a la venta,Envío gratuito"). Los negocios respetables tienen sus correos revisados y corregidos antes de enviarlos a sus clientes. Cuando veas mala gramática u ortografía, debes desconfiar.
4. Los criminales a menudo usarán el nombre de la marca de los productos que estás usando en la URL para aparentar legitimidad. Sin embargo, también cambian frecuentemente las URL de sus sitios falsos, haciendo difícil clausurarlos. Debido a esto, los criminales frecuentemente usarán nombres de dominio y direcciones de correo diferentes durante el proceso de compra. Por ejemplo, en nuestro caso del sitio web de la carriola, los cibercriminales pueden tener un nombre de dominio para el sitio web como www.carriolasmarcax.com, otro dominio para los correos que te envían como ventas@ofertascarriolasmarcax.com y un tercer nombre de dominio para correos de asistencia al cliente como asistencia@marcaxcarriolas.com Todos estos diferentes dominios son otra importante señal de alerta.

Si un sitio web vende productos o servicios a precios demasiado buenos para ser verdad, desconfía, el sitio web puede ser falso

5. Organizaciones legítimas deberían siempre utilizar cifrado durante el proceso de compra. Si no se usa cifrado durante el proceso de transacción de la compra en línea, entonces no uses el sitio web. Puedes determinar si el sitio web está usando cifrado si la URL contiene HTTPS y tu navegador muestra el símbolo de un candado.
6. Haz una búsqueda del nombre o URL de la tienda en línea, ve si alguien más ha publicado cualquier queja acerca del sitio web indicando fraude. Por

© The SANS Institute 2012

Sitios web falsos

ejemplo, si estás comprando artículos de www.carriolamarcax.com, haz una búsqueda de esa URL primero y ve si otros se han quejado de productos fraudulentos.

7. Utiliza PayPal u otros mecanismos que no revelen información de tu tarjeta de crédito al comerciante. Por ejemplo, algunos proveedores de tarjetas de crédito pueden darte números de tarjeta de crédito de un solo uso. Otra opción es usar tarjetas de regalo.
8. Considera usar software de seguridad que ayude a evaluar el nivel de confianza de los sitios web que visitas.
9. Si estás preocupado por no poder determinar si un sitio web es legítimo o no, no utilices el sitio, compra el producto en un sitio en el que confíes. Puede que no obtengas la mejor oferta, pero te sentirás tranquilo con el producto y con la política de devolución.
10. Si caes víctima de fraude en línea, repórtalo a la agencia de procuración de justicia correspondiente en tu país. Además, llama a tu proveedor de tarjeta de crédito para cancelarla, protegerte de algún otro fraude en línea y para que te proporcione una nueva.

RECURSOS

Algunos de los enlaces mostrados a continuación se redujeron para mejorar la legibilidad a través del servicio TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! Siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino, solicitando permiso antes de abrirlo.

Monitoreo de estafas por Internet: http://www.denunciaestafaporinternet.com/

SiteAdvisor: https://www.siteadvisor.com/

Reportar sitios de ventas falsos:
http://www.profeco.gob.mx/Servicios/quejas_denun.asp
http://www.econsumer.gov/espanol/

Términos de seguridad en español:
http://www.viruslist.com/sp/viruses/glossary

Tip del día en seguridad del Instituto SANS:
http://preview.tinyurl.com/6s2wrkp

Consejos UNAM-CERT: http://seguridad.unam.mx/usuario-casero/consejos/

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país.

Sitio web http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

OUCH! es publicado bajo el programa Securing The Human de SANS y es distribuido bajo la licencia Creative Commons BY-NC-ND 3.0. Se concede el permiso para distribuir este boletín siempre y cuando se referencie la fuente, la distribución no sea modificada ni usada con fines comerciales. Para traducción o más información, por favor contacte a: ouch@securingthehuman.org

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Sergio Becerril, Tonatihu Sánchez, Célica Martínez, Jazmín López