Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

Siete pasos para tener una computadora segura

EDITOR INVITADO

El editor invitado para esta publicación es Guy Bruneau. Guy tiene la certificación GIAC Security Expert (GSE) y completó satisfactoriamente el programa Cyber Guardian del SANS (Blue team). Es instructor certificado del SANS, además de realizar manejo de incidentes en el Storm Center del SANS. Para más información síguelo en su cuenta de twitter @guybruneau

RESUMEN

Mientras que los dispositivos móviles, tales como teléfonos inteligentes y tablets, nos ofrecen nuevas formas para poder aprovechar la tecnología, las computadoras siguen siendo la principal herramienta que utilizamos en nuestra vida profesional y personal.

Como resultado, tu computadora, ya sea en el trabajo o en casa, sigue siendo el objetivo principal de los criminales cibernéticos. Al seguir los siete pasos descritos a continuación puedes ayudar a asegurar tu computadora y protegerla contra los ataques más conocidos.

1. PRIMER PASO

Para tener una computadora segura, el primer paso es comenzar con una computadora en la que puedas confiar. Si adquiriste un equipo nuevo directamente de un proveedor conocido, entonces deberías poder confiar en él y en el software preinstalado. Si compraste una computadora usada, entonces no deberías hacerlo. El equipo usado pudo haber sido accidentalmente (o intencionalmente) infectado por su dueño anterior. Intentar asegurar una computadora que ya ha sido infectada no es bueno. El primer paso a seguir después de adquirir una computadora usada es formatear el disco duro y reinstalar el sistema operativo (asegúrate de pedir ayuda a alguien de confianza si no estás seguro de cómo hacerlo).

2. ACTUALIZACIÓN

El siguiente paso es la actualización del equipo. Los atacantes cibernéticos siempre identifican nuevas vulnerabilidades en las computadoras y sus aplicaciones. Cuando los proveedores de computadoras y software tienen conocimiento de estas nuevas vulnerabilidades desarrollan y liberan soluciones, llamadas actualizaciones o parches que solucionan el problema. Cuando compras una computadora nueva o reinstalas el sistema operativo, es muy probable que tu computadora requiera actualizaciones. Por lo tanto, el primer paso que debes realizar es conectarte a Internet y actualizar el sistema operativo. Asegúrate que cuando te conectes a Internet, el nuevo equipo se encuentre protegido por un firewall o un punto de

Siete pasos para tener una computadora segura

acceso Wi-Fi de hogar. Además, la mayoría de los sistemas operativos, incluyendo Windows, OS X, e incluso muchas aplicaciones, tienen una función de actualización automática integrada. Habilita esta función para comprobar si hay actualizaciones al menos una vez al día, esto te ayuda a asegurar que tu equipo se mantenga actualizado y seguro. Si un proveedor libera un parche que tienes que instalar manualmente, asegúrate de que sea lo antes posible.

3. SOFTWARE DE SEGURIDAD

Una vez que tu computadora está actualizada, quieres asegurarte de que tienes software de seguridad instalado y habilitado. Los dos tipos más comunes de software de seguridad son los firewalls y los antivirus. Los antivirus ayudan a identificar archivos infectados que pudiste haber descargado o compartido con otros y los detienen para que no dañen tu computadora. Los firewalls actúan como policías virtuales, determinando quienes pueden o no hablarle a tu computadora. Ahora, muchos proveedores de seguridad ofrecen kits de software de seguridad que incluyen firewall, antivirus y otras opciones de software. Es recomendable que consideres la compra de un paquete de seguridad completo.

4. CUENTAS

Cada persona que tiene acceso autorizado a tu computadora debe tener su propia cuenta protegida por una contraseña única y robusta. Nunca compartas cuentas. Si usas una computadora en casa crea cuentas para cada miembro de tu familia, especialmente para los niños. De esta forma puedes aplicar diferentes controles para cada usuario (como control parental para niños) y rastrear quien hizo qué. Además, otorga a cada usuario los privilegios mínimos que necesitan para usar la computadora. Nunca

Siguiendo estos sencillos pasos puedes ayudarte a tener una computadora segura

des a alguien privilegios de administrador a menos que realmente los necesite, incluyéndote. Usa privilegios de administrador cuando los necesites. Por ejemplo, al instalar software o cambiar configuraciones del sistema.

5. SEGURIDAD PORTATIL

Si tu computadora es portátil, como una laptop, puedes considerar el cifrado de disco duro completo (FDE por sus siglas en inglés). El cifrado ayuda a asegurar que los datos en tu computadora están protegidos aún si la pierdes. También podrías asegurarte de que la pantalla del ordenador esté bloqueada por contraseña, de esta forma las personas no podrán acceder a tu sistema cuando estés lejos de tu computadora. Finalmente, algunas computadoras ahora soportan localización y/o borrado remoto, para ayudarte a localizar una laptop perdida o borrar permanentemente datos sensibles si no puedes recuperarla.

Siete pasos para tener una computadora segura

6. USANDO LA COMPUTADORA

No hay tecnología suficiente que pueda proteger a tu equipo contra todas las amenazas. Todo lo que hemos cubierto hasta ahora ayudará a proteger tu computadora, pero el último elemento que tenemos que asegurar eres tú, el usuario de la computadora. Debes saber y entender que hay personas que siempre estarán tratando de engañarte. Si recibes un mensaje que luce extraño o sospechoso, no des clic sobre ninguna liga o archivo adjunto. Si alguien te habla diciéndote que tu computadora está infectada y necesitas instalar software, probablemente es una estafa. En muchos sentidos, tú eres la mejor defensa para tu computadora, no la tecnología.

7. RESPALDOS

Finalmente, aún si adoptas todos los pasos que hemos cubierto, siempre hay una oportunidad de que tu computadora sea hackeada, tenga una falla en el disco duro o sufra alguna otra catástrofe. Tu última defensa son los respaldos. Te recomendamos que realices regularmente copias de seguridad de toda tu información importante (documentos, imágenes, videos, etc.) ya sea en un disco duro externo o utilizando un servicio de respaldo en la nube, o tal vez ambas cosas.

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 tu permiso antes de abrirlo.

Antivirus gratuitos:
http://preview.tinyurl.com/d8kyhoa

Seguridad de Microsoft:
http://preview.tinyurl.com/culyajg

Seguridad de Mac OS X:
http://preview.tinyurl.com/cwmq386

Términos comunes de seguridad:
http://preview.tinyurl.com/6wkpae5

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

Consejo del día UNAM/CERT:
http://preview.tinyurl.com/8fpbhtw

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

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Sandra Atonal, Carlos Colio, Célica Martínez, Jazmín López, Gustavo Villafán