VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Octubre 2014

Boletín mensual de seguridad para usuarios de computadoras

OUCH!

En esta edición...

Cinco pasos para mantenerse seguro

Resumen

Conforme la tecnología gana terreno en nuestras vidas, manejarla se vuelve más complicado. Tomando en cuenta estos cambios, actualizarse en cuanto a recomendaciones de seguridad puede ser confuso. Sin embargo, mientras los detalles de cómo hacerlo pueden cambiar con el tiempo, existen cuestiones fundamentales con las que puedes protegerte. Independientemente de qué tecnología estés utilizando o en dónde la uses, te recomendamos seguir estos cinco pasos claves.

Editor Invitado

Lenny Zeltser se dedica a proteger las operaciones de TI de los usuarios en la corporación NCR y enseña cómo combatir malware en el instituto SANS. Lenny se encuentra en Twitter como **@lennyzeltser** y tiene el blog de seguridad **blog.zeltser.com**.

Cinco pasos claves

Cada uno de los cinco pasos mostrados a continuación es una descripción simple. Para aprender más acerca de cada paso, consulta la sección de recursos al final de este boletín.

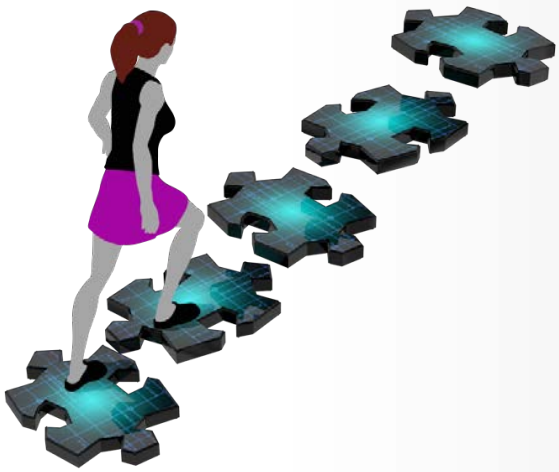
1. **Tú**: Primero y por sobre todo, ten en mente que la tecnología por sí sola no puede protegerte. Los atacantes han aprendido que la manera más fácil de sobrepasar la seguridad tecnológica es atacándote a ti. Si ellos quisieran tu contraseña o tu tarjeta de crédito, la manera más fácil es engañarte para que tú les des esa información. Por ejemplo, ellos pueden llamarte haciéndose pasar por el equipo de soporte de Microsoft y mencionar que tu computadora fue infectada, cuando en realidad son cibercriminales que quieren tener acceso a tu cuenta. Tal vez ellos te envíen un correo electrónico explicando que tu paquete no pudo ser entregado y te soliciten mediante un enlace confirmar tu dirección, realmente lo que ellos quieren es que visites un sitio web malicioso para tener acceso a tu computadora. La mejor defensa en contra de los atacantes eres tú. Duda utilizando tu sentido común, tú puedes detener la mayoría de los ataques.

2. **Actualízate**: Asegúrate de que tus computadoras, dispositivos móviles, aplicaciones, y todo aquello conectado a Internet, tenga la última versión de software. Los cibercriminales constantemente buscan vulnerabilidades en las tecnologías que ocupas. Cuando las descubren, utilizan programas especiales para atacar esa falla y poder entrar en cualquier tecnología que ocupes, incluyendo la red, la computadora y los dispositivos móviles. Mientras eso sucede, las compañías que crean esas tecnologías trabajan arduamente para mantenerte actualizado. Una

© The SANS Institute 2014

Cinco pasos para mantenerse seguro

vez que se conoce la vulnerabilidad, ellos crean una solución para arreglarlo y la liberan al público. Al revisar que tus computadoras y dispositivos móviles tengan estas actualizaciones, reduces el número de vulnerabilidades conocidas, así es mucho más difícil para alguien afectarte. Para mantenerte al día, activa las actualizaciones automáticas siempre que sea posible. Esta regla aplica para casi cualquier tipo de tecnología conectada a la red, incluyendo televisores inteligentes, monitores para bebés, routers caseros, consolas de videojuegos, y probablemente algún día, hasta tu auto. Si al sistema operativo de tu computadora, dispositivo móvil o cualquier otra tecnología que ocupes no se le está dando soporte y no recibe ninguna actualización, te recomendamos conseguir una versión que tenga soporte.



Estos cinco pasos clave cubren gran parte de la protección necesaria en tu interacción con la tecnología.

3. **Contraseñas**: El siguiente paso para protegerte a ti mismo implica el uso de una contraseña única y fuerte para cada uno de tus dispositivos, cuentas y aplicaciones en línea. Las palabras claves son únicas y fuertes. Tener una contraseña segura significa que un atacante o programa automatizado no la podrá adivinar fácilmente. En lugar de una sola palabra, puedes utilizar una frase larga de varias palabras con símbolos y números. Se debe usar una contraseña única para cada dispositivo diferente o para cada cuenta en línea. De esta manera, si una contraseña está en peligro, todas tus otras cuentas y dispositivos permanecen seguros. ¿No puedes recordar todas esas contraseñas únicas y fuertes?, no te preocupes, nosotros tampoco. Por eso te recomendamos utilizar un gestor de contraseñas, es una aplicación especializada para tu teléfono inteligente o computadora que puede almacenar con seguridad todas tus contraseñas de forma cifrada. Por último, si alguna de tus cuentas permite verificación de dos pasos, es muy recomendable habilitarla, esta es una de las formas más fuertes que existen para proteger tus cuentas.

4. **Cifrado**: Un cuarto paso que recomendamos es el uso de cifrado. El cifrado asegura que sólo tú o la gente de tu confianza acceda a tu información. Los datos se pueden cifrar de dos formas, en reposo y en movimiento. El cifrado de datos en reposo significa que los archivos se protegen cuando están almacenados en discos duros o memorias USB. La mayoría de los sistemas operativos permiten cifrar automáticamente todos los datos de uso con una característica llamada Full Disk Encryption. Te recomendamos activarla siempre que sea posible. El cifrado de datos en movimiento significa que los datos irán cifrados cuando se transmiten de una computadora o dispositivo a otro, por ejemplo cuando utilizas la banca en línea. Una forma sencilla de comprobar si el cifrado

Cinco pasos para mantenerse seguro

está activado es, al visitar un sitio web, verificar si la URL comienza con https: y si tiene una imagen de un candado cerrado al lado, entonces se está navegando de forma segura.

5. **Backups**: A veces no importa qué tan cuidadoso seas, alguno de tus dispositivos o cuentas puede verse comprometida. Si ese es el caso, a menudo la única opción para garantizar que tu computadora o dispositivo móvil esté libre de malware es limpiarlo por completo y reconstruirlo desde cero. Un atacante podría incluso impedir el acceso a tus archivos personales, fotos u otra información almacenada en tu sistema. La única opción podría ser restaurar toda la información personal por medio de una copia de seguridad. Debes asegurarte de que estás haciendo copias de seguridad periódicas de cualquier información importante y también comprobar que se puede hacer una restauración a partir de ellas. La mayoría de los sistemas operativos y dispositivos móviles admiten copias de seguridad automáticas.

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

Phishing por correo electrónico:	http://www.securingthehuman.org/ouch/2013#february2013
Cómo asegurar tu nueva tableta electrónica:	http://www.securingthehuman.org/ouch/2013#december2013
Contraseñas:	http://www.securingthehuman.org/ouch/2013#may2013
Gestores de contraseñas:	http://www.securingthehuman.org/ouch/2013#october2013
Verificación de dos pasos:	http://www.securingthehuman.org/ouch/2013#august2013
Cifrado:	http://www.securingthehuman.org/ouch/2014#august2014
Copias de seguridad y recuperación personal:	http://www.securingthehuman.org/ouch/2013#september2013

OUCH! es publicado por SANS Securing The Human y distribuido bajo licencia de Creative Commons BY-NC-ND 4.0.
Puedes distribuir este boletín o utilizarlo en tu programa de sensibilización de seguridad siempre y cuando no se modifique su contenido.
Para más información contáctanos en: ouch@securingthehuman.org

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducción al español por: Octavio Domínguez y Juan Pablo Colín

© The SANS Institute 2014