VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Octubre 2016

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- **Tu papel como usuario**
- **Contraseñas**
- **Actualizaciones**
- **Copias de seguridad**

Cuatro recomendaciones para mantenerse seguro

Resumen

La tecnología ha ganado un lugar importante en nuestras vidas, tanto como se ha vuelto más compleja. Tomando en cuenta la rapidez con que cambia, mantenerse al día con los consejos de seguridad puede ser un poco complicado y confuso. Parece que siempre existe una nueva guía sobre buenas prácticas y acciones que se deben evitar, sin embargo, si bien los detalles de cómo protegerse cambian con el tiempo, existen recomendaciones fundamentales que puedes seguir para protegerte. Independientemente de la tecnología que estés usando, te recomendamos cuatro consideraciones importantes a tomar en cuenta. Para obtener más información acerca de cualquiera de las siguientes sugerencias, te invitamos a revisar la sección de recursos al final de este boletín.

Editor Invitado

Ryan Johnson se dedica a asegurar que las organizaciones estén preparadas para responder a las inevitables brechas de seguridad e imparte Análisis Forense Avanzado de Redes en el Instituto SANS. Puedes encontrarlo en Twitter como **@ForensicRJ**.

1. **Tu papel como usuario**: Por principio y antes que nada, ten en cuenta que la tecnología por sí misma nunca será capaz de ofrecerte una protección absoluta. Los atacantes han aprendido que el método más fácil de evadir la tecnología más avanzada es atacándote. Si quieren tu contraseña, datos bancarios o personales, la forma más sencilla de obtenerlo es engañarte para que seas tú mismo quien proporcione esa información. Por ejemplo, pueden llamarte haciéndose pasar por personal de soporte técnico de Microsoft y argumentar que tu computadora está infectada, cuando en realidad son cibercriminales que solo quieren acceder a tu equipo. O quizás te enviaron un correo explicando que no fue posible entregarte un envío y solicitan que des clic en un enlace para confirmar tu dirección, cuando en realidad te engañan para que visites un sitio malicioso y por ese medio atacar tu computadora. Así es como los ataques de ransomware y la estafa del CEO se llevan a cabo. Al final, la gran defensa ante los atacantes eres tú, usando el sentido común puedes detectar y evitar la mayoría de los ataques.

2. **Contraseñas**: El siguiente paso para protegerte involucra el uso de una contraseña segura y única para cada una de tus cuentas y dispositivos. Una contraseña segura significa que no es predecible por un atacante o una herramienta automatizada. ¿Te molesta usar contraseñas complejas que son difíciles de memorizar o introducir? Mejor intenta usar una frase de acceso. En lugar de una sola palabra, utiliza una serie de palabras que sean fáciles de recordar,

Cuatro recomendaciones para mantenerse seguro

por ejemplo “¿Dónde está mi café?”. Entre más larga sea la frase, más fuerte es. Cuando se habla de una contraseña única nos referimos a evitar reciclar las credenciales en diferentes dispositivos o cuentas; de esta forma si una contraseña es expuesta, tus demás cuentas/dispositivos no serán afectados y estarán a salvo. ¿No puedes recordar todas las contraseñas? No te preocupes, tampoco nosotros podemos. Por eso te recomendamos usar un gestor de contraseñas, el cual es una aplicación para tu dispositivo móvil o equipo personal que tiene como objetivo almacenar de forma segura (cifrada) todas tus contraseñas.

Al seguir estas cuatro recomendaciones claves de seguridad, podrás protegerte al mismo tiempo que aprovechas la tecnología más reciente.

Finalmente, uno de los más importantes pasos que puedes realizar para proteger cualquier cuenta es habilitar la verificación en dos pasos. Las contraseñas por sí solas ya no son suficientes para proteger las cuentas, todos necesitamos algo más fuerte. La verificación en dos pasos es mucho más fuerte. Utiliza tu contraseña pero también añade un segundo paso, ya sea algo que eres (biométrico) o algo que tengas (por ejemplo, un código enviado a tu teléfono inteligente o una aplicación que genere el código). Activa esta opción en cada cuenta que puedas, incluyendo el gestor de contraseñas si es posible. La verificación en dos pasos es un proceso sencillo y el más importante que puedes tomar para protegerte, además es mucho más fácil de lo que piensas.

3. **Actualizaciones**: Asegúrate de que tus computadoras, dispositivos móviles, aplicaciones y todo lo que se conecta a Internet se encuentre en la versión más reciente del software. Los ciberdelincuentes constantemente buscan nuevas vulnerabilidades en los programas, y cuando las descubren hacen uso de programas especiales para explotarlas con el fin de conseguir acceso en los dispositivos que estás utilizando. Mientras tanto, las empresas que crearon el software para estos dispositivos están trabajando duro para reparar esas fallas y publicar actualizaciones. Al asegurar tus computadoras y dispositivos móviles a través de la instalación de estas actualizaciones harás más difícil que alguien pueda vulnerarlos; sólo tienes que habilitar la actualización automática siempre que sea posible. Esta regla se aplica a casi cualquier tecnología conectada a Internet, incluyendo televisores, monitores para bebé, enrutadores para el hogar, consolas de videojuegos o algún día tal vez incluso tu auto. Si los sistemas operativos o dispositivos son viejos y ya no son compatibles con las actualizaciones de seguridad, te recomendamos sustituirlos por otros nuevos que sean compatibles.

Cuatro recomendaciones para mantenerse seguro

4. **Copias de seguridad**: A veces no importa qué tan cuidadoso seas, existe la probabilidad de que seas atacado. Si ese es el caso, la única opción para garantizar que tu computadora o dispositivo móvil esté libre de malware es limpiarlo por completo y reconstruirlo desde cero. El atacante podría incluso impedir el acceso a tus archivos personales, fotos y otra información almacenada en el sistema vulnerado. A menudo, la única manera de restaurar toda tu información personal es a través de una copia de seguridad. Asegúrate que estás haciendo respaldos de seguridad periódicos de cualquier información importante y verifica que puedes restaurar a partir de ellos. La mayoría de los sistemas operativos y dispositivos móviles admiten copias de seguridad automáticas. Además, te recomendamos que las almacenes ya sea en la nube o fuera de línea para protegerlas contra ciberatacantes.

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

Tips de seguridad:	http://revista.seguridad.unam.mx/numero-01/tips-de-seguridad
Resguardar la información:	http://revista.seguridad.unam.mx/numero-10/medidas-resguardar-informacion
Contraseñas seguras:	https://revista.seguridad.unam.mx/numero-15/guia-para-contrasenas-seguras
Gestores de contraseñas:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_sp.pdf
Verificación en dos pasos:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_sp.pdf
Ingeniería Social:	https://revista.seguridad.unam.mx/numero-03/ingenieria-social-tecnica-de-ataque
Estafa del CEO:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201607_sp.pdf

Consejo editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traducción: Eric Castañeda, Leticia González y Katia Rodríguez

