VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Octubre 2017

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- Descripción general
- Cinco sencillos pasos
- Seguridad para niños al visitar a otros

Ayuda a otros a asegurarse

Descripción general

Muchos nos sentimos cómodos con la tecnología, incluso sabemos cómo se usa de manera segura y protegida. Sin embargo, nuestros amigos o familiares pueden no sentirse de esta manera. De hecho, pueden estar confundidos, intimidados o incluso asustados por ella. Esto los hace muy vulnerables a los ciberataques de hoy. La ciberseguridad no tiene por qué provocar miedo, ya que es realmente sencillo entenderla una vez que se conocen los conceptos básicos. Seguramente solo necesitan un guía como tú para ayudarlos a comprender lo esencial.

Editor Invitado

Randy Marchany (Twitter: **@randymarchany**) es el jefe de seguridad de la información para Virginia Tech e instructor certificado del Instituto SANS.

Cinco sencillos pasos

Aquí se presentan cinco sencillos pasos que puedes tomar para ayudar a otros a superar sus miedos y aprovechar al máximo la tecnología de hoy. Para más información sobre cada uno de los puntos, consulta la sección de referencias al final de este boletín.

1. **Ingeniería social**. La ingeniería social es una técnica común empleada por los ciberatacantes al engañar o confundir a las personas para que hagan algo que no deberían, como dar a conocer su contraseña, infectar su equipo o compartir información sensible. Esto no es nada nuevo, las estafas y estafadores han existido por miles de años. La única diferencia es que ahora esos chicos malos están aplicando los mismos conceptos al Internet. Puedes ayudar a otros explicándoles las trampas más comunes de un ataque de ingeniería social, como cuando alguien crea un enorme sentido de urgencia, cuando algo es demasiado bueno para ser verdad, o cuando un ciberatacante pretende ser alguien que conoces, pero sus mensajes no suenan como tu amigo. Comparte ejemplos de ataques comunes de ingeniería social, como los correos de phishing o las “supuestas” llamadas telefónicas de soporte técnico de Microsoft. Por lo menos, asegúrate de que los miembros de la familia entiendan que nunca deben dar su contraseña a nadie ni permitir el acceso remoto a su equipo.
2. **Contraseñas**. Las contraseñas fuertes son la clave para proteger tanto los dispositivos como las cuentas en línea. Habla con los miembros de tu familia sobre cómo crear contraseñas seguras. Recomendamos el uso de frases de contraseñas, ya que son más sencillas de teclear y recordar. Las frases de contraseñas no son más que contraseñas elaboradas con múltiples palabras. Adicionalmente, ayúdales a instalar y usar un gestor de contraseñas. Es importante

Ayuda a otros a asegurarse

tener una contraseña única para cada uno de los dispositivos y cuentas. Si el gestor de contraseñas es abrumador, entonces enséñales a escribir sus contraseñas y después almacenarlas en un lugar seguro. Finalmente, para cuentas importantes, ayúdales a habilitar la verificación de dos pasos (a menudo llamada autenticación de dos factores). La verificación de dos pasos es uno de los elementos más importantes que puedes tomar para asegurar una cuenta.

Ayuda a otros a aprovechar al máximo la tecnología compartiendo con ellos estos cinco sencillos pasos.

3. **Actualizar**. Mantener los sistemas totalmente actualizados es un paso clave que cualquiera puede tomar para asegurar sus dispositivos. Esto no solo es verdad para las computadoras y dispositivos móviles, si no para cualquier cosa conectada a Internet, como consolas de juegos, termómetros o incluso luces o altavoces. La forma más sencilla de asegurar que todos los dispositivos están al día es habilitar la actualización automática siempre que sea posible.
4. **Antivirus**. La gente comete errores, a veces damos clic o instalamos cosas que probablemente no deberíamos tener y que podrían infectar nuestros sistemas. Los antivirus están diseñados para protegernos de esos errores. Mientras que un antivirus no puede detener todo el malware, ayuda a detectar y bloquear los ataques más comunes. Como tal, asegúrate de que todos los equipos tienen un antivirus instalado y que se encuentra actualizado y activo. Adicionalmente, muchas de las soluciones antivirus de hoy en día incluyen otras tecnologías de seguridad como firewalls o protección para el navegador.
5. **Respaldos**. Cuando todo lo demás falla, los respaldos son a menudo la única forma de recuperarse de errores como la eliminación errónea de archivos o de ciberataques como el ransomware. Asegúrate de que tu familia y amigos tienen un sistema automatizado de respaldos. A menudo, las soluciones más simples son los respaldos almacenados en la nube que hacen respaldos de tus dispositivos cada hora o cada que cambia un archivo. Esas soluciones hacen fácil no solo respaldar la información, sino recuperarla.

Seguridad para niños al visitar a otros

Si estás cómodo con la tecnología, lo más probable es que no solo te asegures a ti mismo, sino también a tus niños. Sin embargo, cuando los niños visitan a alguien que no se siente cómodo con la tecnología, como los abuelos, esos amigos o parientes pueden no estar conscientes de cómo proteger mejor a los niños cuando están en línea o según tus expectativas. Aquí hay algunos pasos que se pueden tomar para proteger a los niños cuando visitan a otros, especialmente a la familia.

- **Reglas**. Asegúrate de que los otros saben de la existencia de alguna regla o de lo que esperas acerca de la seguridad de los niños. Por ejemplo, ¿existe alguna regla sobre cuánto tiempo pueden estar en línea, con quién

Ayuda a otros a asegurarse

pueden hablar, cuáles juegos pueden o no jugar? Créenos, no esperes que los niños expliquen las reglas a otros miembros de la familia. Una idea es contar con una "hoja de reglas" y compartirla con aquellos a quienes tus niños visitan frecuentemente.

- **Control**. Si un niño entiende la tecnología mejor que sus cuidadores, pueden tomar ventaja de esto. Por ejemplo, los niños pueden solicitar o ganar privilegios administrativos en el equipo de sus abuelos y entonces hacer lo que quieran, como instalar un juego con el que no quieres que jueguen. Asegúrate de que sus cuidadores entiendan que no deben dar acceso adicional a los niños más allá del que ya se ha establecido.

Finalmente, sugiere a las personas que se suscriban a recursos como el boletín OUCH! para que puedan seguir aprendiendo por su cuenta. Este boletín es publicado mensualmente de forma gratuita en más de 20 idiomas. Únete en: https://securingthehuman.sans.org/ouch.

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

Ingeniería social:	https://securingthehuman.sans.org/ouch/2017#january2017
Frase de contraseña:	https://securingthehuman.sans.org/ouch/2017#april2017
Gestores de contraseñas:	https://securingthehuman.sans.org/ouch/2017#september2017
Verificación en dos pasos:	https://securingthehuman.sans.org/ouch/2015#september2015
Respaldo y recuperación:	https://securingthehuman.sans.org/ouch/2017#august2017
Proteger a los niños en sus actividades en línea:	https://securingthehuman.sans.org/ouch/2017#may2017

Consejo editorial: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traducción: Angie Aguilar Domínguez, Raúl Abraham González y Célica Martínez Aponte.