SANS SECURITY AWARENESS
VERSIÓN EN ESPAÑOL
UNAM CERT

OUCH! | Enero 2018

Boletín mensual de seguridad para todos

OUCH!

En esta edición...

- **Tu red inalámbrica**
- **Tus dispositivos**
- **Contraseñas**
- **Respaldos**

Crear un hogar ciber seguro

Resumen

Años atrás, crear un hogar ciber seguro era simple, la mayoría de los hogares consistían en solo una red inalámbrica y varias computadoras. Hoy en día, la tecnología se ha vuelto mucho más compleja y está integrada en cada una de las partes de nuestra vida, desde los dispositivos móviles y las consolas de videojuegos hasta el termostato y quizás también tu refrigerador. Aquí encontrarás cuatro simples pasos para crear un hogar ciber seguro.

Editor Invitado

Matt Bromiley es consultor en respuesta a incidentes, ayuda a clientes de todos los tamaños a lidiar con problemas de seguridad de la información. Es también instructor del Instituto SANS e imparte FOR508, el curso avanzado de forense digital y respuesta a incidentes. Sigue a Matt en twitter **@mbromileyDFIR**.

Tu red inalámbrica

Casi todas las redes domésticas comienzan con una red inalámbrica o Wi-Fi. Esto es lo que permite a tus dispositivos conectarse a Internet. La mayoría de las redes inalámbricas son controladas por un enrutador de Internet o por un punto de acceso inalámbrico dedicado y separado. Ambos trabajan de la misma manera al transmitir señales inalámbricas, los dispositivos en tu casa se conectan a través de estas señales. Esto significa que asegurar tu red inalámbrica es una de las claves para proteger tu hogar. Te recomendamos seguir los siguientes pasos para asegurarla.

- Cambia las contraseñas de administrador que están por defecto en el enrutador de Internet o de tu punto de acceso inalámbrico, cualquiera que controle tu red inalámbrica. La cuenta de administrador es la que te permite ajustar las configuraciones de tu red inalámbrica.
- Asegúrate de que solo personas de confianza puedan conectarse a tu red. Haz esto habilitando una seguridad sólida. Actualmente la mejor opción es utilizar el mecanismo de seguridad llamado WPA2. Para habilitarlo, es necesaria una contraseña para que las personas se puedan conectar a ella y una vez conectadas sus actividades quedan cifradas.
- Asegúrate de que la contraseña que utilizas para conectarte a la red inalámbrica sea fuerte y diferente a la de administrador. Recuerda que solo tienes que ingresar tu contraseña una vez para cada dispositivo, pues ellos almacenan y recuerdan tu contraseña.
- Muchas redes inalámbricas soportan lo que conocemos como red de invitados. Esta permite la conexión a Internet de visitantes, pero protege tu red doméstica ya que no pueden conectarse a ningún otro dispositivo de tu red. Si agregas este tipo de red, asegúrate de habilitar WPA2 así como una única contraseña para esta red.

Crear un hogar ciber seguro

¿No estás seguro de cómo realizar estos pasos? Pregunta con tu proveedor de servicio de Internet, revisa la documentación que viene con tu enrutador o access point inalámbrico o consulta sus respectivos sitios web.

Sigue estos cuatro simples pasos para crear un hogar ciber seguro; asegura tu red Wi-Fi, habilita las actualizaciones automáticas, utiliza contraseñas únicas y realiza respaldos.

Tus dispositivos

El siguiente paso es saber qué dispositivos están conectados a tu red inalámbrica doméstica y asegurarte que todos ellos sean seguros. Esto es sencillo cuando solo tienes una computadora o dos. De cualquier manera, hoy en día casi cualquier dispositivo se puede conectar a tu red doméstica, incluyendo tu teléfono inteligente, televisión, consolas de videojuego, monitores para bebés, altavoces, y quizás hasta tu automóvil.

Una vez que hayas identificado estos dispositivos, cerciórate de que todos ellos sean seguros. La mejor manera para hacer esto es asegurarte de que las actualizaciones estén habilitadas de manera automática siempre que sea posible. Los ciber atacantes están constantemente buscando nuevas debilidades en diferentes dispositivos y sistemas operativos. Al habilitar las actualizaciones automáticas, tu computadora y dispositivos cuentan con el software más actual, lo que lo hace mucho más difícil de ser vulnerado.

Contraseñas

El siguiente paso es utilizar una contraseña fuerte y única para cada uno de tus dispositivos y cuentas en línea. Las palabras clave aquí son fuerte y única. ¿Estás cansado de contraseñas complejas que son difíciles de teclear? También nosotros. Utiliza frases en vez de eso. Este es un tipo de contraseñas que utiliza una serie de palabras fáciles de recordar, como ¿Dónde está mi café? o no-vivo-para-comer-como-para-vivir. La longitud de las contraseñas es lo que las hace fuertes. Una única contraseña significa utilizar una contraseña para cada uno de tus dispositivos y cada cuenta en línea. De esta manera, si una contraseña es comprometida, todas tus otras cuentas y dispositivos estarán seguros. ¿Puedes recordar todas esas contraseñas fuertes y únicas? No te preocupes, tampoco nosotros. Por eso te recomendamos utilizar un gestor de contraseñas, que es un software que te permite almacenar todas tus contraseñas de manera segura en una caja fuerte cifrada y virtual.

Finalmente, habilita la verificación en dos pasos siempre que esté disponible, especialmente para tus cuentas en línea. Este tipo de verificación es mucho más fuerte. Utiliza tu contraseña, pero siempre agrega un segundo paso, como un código enviado a tu teléfono inteligente o una aplicación en tu móvil que genera el código para ti. La verificación en dos

Crear un hogar ciber seguro

pasos es probablemente el paso más importante que puedes tomar para protegerte a ti mismo en línea y es más fácil de lo que crees.

Respaldos

Algunas veces, no importa lo cuidadoso que seas, probablemente serás hackeado. Si este es el caso, a menudo la única forma en la que puedes recuperar tu información es restaurar desde tu respaldo. Asegúrate de respaldar periódicamente tu información importante y verifica que puedes recuperarla. Muchos dispositivos móviles soportan respaldos automáticos en la nube. Para muchas computadoras, es posible que tengas que comprar algún tipo de software o servicio de respaldo, que son relativamente económicos y fáciles de usar.

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

Frases de acceso:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201704_sp.pdf
Gestores de contraseñas:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201709_sp.pdf
Protege tu inicio de sesión:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201712_sp.pdf
Respaldo y recuperación:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201708_sp.pdf

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