OUCH! I Junio

SANS SECURITY AWARENESS

El Boletín Mensual de Concientización en Seguridad para ti

Creando un hogar ciberseguro

Resumen

En el pasado, construir una red doméstica era nada más instalar un router inalámbrico y varias computadoras. Hoy en día, debido a que muchos de nosotros trabajamos, nos conectamos o aprendemos desde casa, debemos prestar más atención para crear un hogar ciberseguro fuerte. Aquí hay cuatro pasos simples que te ayudarán a lograrlo.

Tu red inalámbrica

Casi todas las redes domésticas comienzan con una red inalámbrica (o Wi-Fi). Esto es lo que permite que tus dispositivos se conecten a Internet. La mayoría de las redes inalámbricas domésticas están controladas por el router de Internet o un punto de acceso inalámbrico separado y dedicado. Ambas trabajan de la misma manera: transmitiendo señales inalámbricas que permiten que los dispositivos de tu casa se conecten a Internet. Esto significa que asegurar tu red inalámbrica es una parte clave para proteger tu hogar. Recomendamos los siguientes pasos para asegurarlo:

- Cambia la contraseña de administrador predeterminada de tu router de Internet o punto de acceso inalámbrico, lo que sea que controle tu red inalámbrica. La cuenta de administrador es lo que te permite configurar los ajustes para tu red inalámbrica.
- Asegúrate de que solo los dispositivos en los que confías pueden conectarse a tu red inalámbrica. Haga esto habilitando una seguridad fuerte. Para hacerlo, se requiere una contraseña para conectarte a tu red doméstica y cifrar las actividades en línea una vez que esté conectado.
- Asegúrate de que la contraseña utilizada para conectarte a tu red inalámbrica sea una contraseña segura que sea diferente de la contraseña del administrador. Recuerda que tus dispositivos almacenan contraseñas, por lo que solo necesitas ingresar la contraseña una vez para cada dispositivo.

Si no estás seguro de cómo seguir estos pasos, consulta el sitio web de tu proveedor de servicios de Internet o consulta el sitio web del proveedor para tu router o punto de acceso inalámbrico.

Contraseñas

Usa una contraseña fuerte y única para cada uno de tus dispositivos y cuentas en línea. Las palabras clave son *fuerte* y *única*. Cuanto más larga sea su contraseña, más fuerte será. Intenta usar una serie de palabras que sean fáciles de recordar, como ***sol-donas-feliz***..

Una contraseña única significa usar una contraseña diferente para cada dispositivo y cuenta en línea. Usa un gestor de contraseñas para recordar todas esas contraseñas seguras, que es un programa de seguridad que almacena de forma segura todas tus contraseñas en una caja fuerte virtual cifrada.

Además, habilita la verificación en dos pasos siempre que esté disponible, especialmente para tus cuentas en línea. Utiliza tu contraseña, pero también agrega un segundo paso de autenticación, como un código enviado a tu teléfono inteligente o una aplicación en tu teléfono inteligente que genere el código para ti. Probablemente, este es el paso más importante que puedes hacer, y es mucho más fácil de lo que piensas.

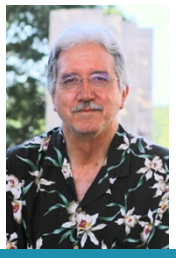
Tus dispositivos

El siguiente paso es saber qué dispositivos están conectados a tu red doméstica inalámbrica y asegurarte de que todos esos dispositivos sean confiables y seguros. Esto solía ser simple cuando solo tenías una computadora. Sin embargo, hoy en día casi cualquier cosa puede conectarse a tu red doméstica, incluidos tus teléfonos inteligentes, televisores, consolas de juegos, monitores para bebés, impresoras, bocinas inteligentes o incluso tu automóvil. Una vez que hayas identificado todos los dispositivos en tu red doméstica, asegúrate de que cada uno de ellos sea seguro. La mejor manera de hacerlo es cambiar las contraseñas predeterminadas y habilitar la actualización automática siempre que sea posible.

Respaldos

A veces, no importa cuán cuidadoso seas, te pueden hackear. Si ese es el caso, a menudo la única forma en la que puedes recuperar tu información personal es restaurar desde un respaldo. Asegúrate de realizar respaldos periódicamente de cualquier información importante y verifica que puedas restaurar a partir de ellos. La mayoría de los dispositivos móviles permiten respaldos automáticos en la nube. Para la mayoría de las computadoras, es posible que debas comprar algún tipo de software o servicio de respaldo, que es relativamente económico y fácil de usar.

Editor invitado



Randy Marchany es el CISO de Virginia Tech. También es instructor senior del SANS y enseña los cursos SEC566, SEC440, Implementación y auditoría de los controles críticos de seguridad. Sigue a Randy @randymarchany.

Recursos

Creando contraseñas simples: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Gestores de contraseñas: https://www.sans.org/security-awareness-training/resources/password-managers-0
Actualizaciones: https://www.sans.org/security-awareness-training/resources/power-updating
¿Hacer respaldos?: https://www.sans.org/security-awareness-training/resources/got-backups
Contraseñas predeterminadas en dispositivo: https://www.routerpasswords.com/

Traducido para la comunidad por: Célica Martínez Aponte, UNAM-CERT.