Boletín mensual de consejos de seguridad para usuarios de computadoras

OUCH!

EN ESTA EDICIÓN

- **Administración**
- **El nombre de tu red**
- **Cifrado y autenticación**
- **OpenDNS**

Asegura tu red Wi-Fi

EDITOR INVITADO

Raul Siles es el editor invitado para esta edición. Raul es fundador y analista sénior de seguridad de Taddong (www.taddong.com), es autor e instructor del SANS Institute, además de apasionado de la seguridad (www.raulsiles.com). Puedes seguir a Raul en Twitter @taddong y en su blog blog.taddong.com.

RESUMEN

Las redes Wi-Fi (conocidas por su nombre técnico: 802.11) permiten a las personas conectar dispositivos a Internet de forma inalámbrica, tales como smartphones, consolas de juegos, tablets y laptops. Debido a que son fáciles de configurar, muchas personas instalan sus propias redes Wi-Fi en casa. Sin embargo, muchas de ellas se configuran de forma insegura, lo que permite a extraños o personas no autorizadas acceder fácilmente a una red doméstica o, de forma anónima, abusar de la conexión a Internet. Para asegurarte de tener una red Wi-Fi segura y protegida, te presentamos algunos sencillos pasos a seguir.

Administración

Tu red Wi-Fi es controlada por algo llamado punto de acceso Wi-Fi. Éste es un dispositivo físico que puedes comprar en una tienda de electrónica, o incluso podría ya estar incorporado en tu router de Internet. El punto de acceso es lo que conecta a tus dispositivos de forma inalámbrica a Internet. Uno de los primeros pasos para proteger tu red Wi-Fi es limitar quién puede administrar el punto de acceso de ésta y cómo pueden acceder a ella. Te recomendamos seguir los siguientes pasos para configurar el punto de acceso de tu red Wi-Fi por primera vez.

- Para la mayoría de los puntos de acceso Wi-Fi, la cuenta por defecto del administrador, incluyendo su contraseña, no es privada. De hecho, estas cuentas por defecto suelen encontrarse listadas en Internet. Por lo tanto, asegúrate de cambiar el nombre de usuario y contraseña por defecto del administrador por algo que sólo tú conozcas.
- Para el acceso administrativo de tu punto de acceso Wi-Fi, te recomendamos deshabilitar el acceso inalámbrico y, en su lugar, establecer una conexión de red física, como el uso de un cable Ethernet. Si requieres tener acceso administrativo inalámbrico, al menos deshabilita el acceso HTTP y solicita HTTPS, ya que éste soporta el cifrado.

Configurar el nombre de la red Wi-Fi

Otra opción que tendrás que configurar es el nombre de tu red Wi-Fi (conocido como SSID). Este nombre se mostrará en tus dispositivos cuando busques la red local Wi-Fi. Te

Asegura tu red Wi-Fi

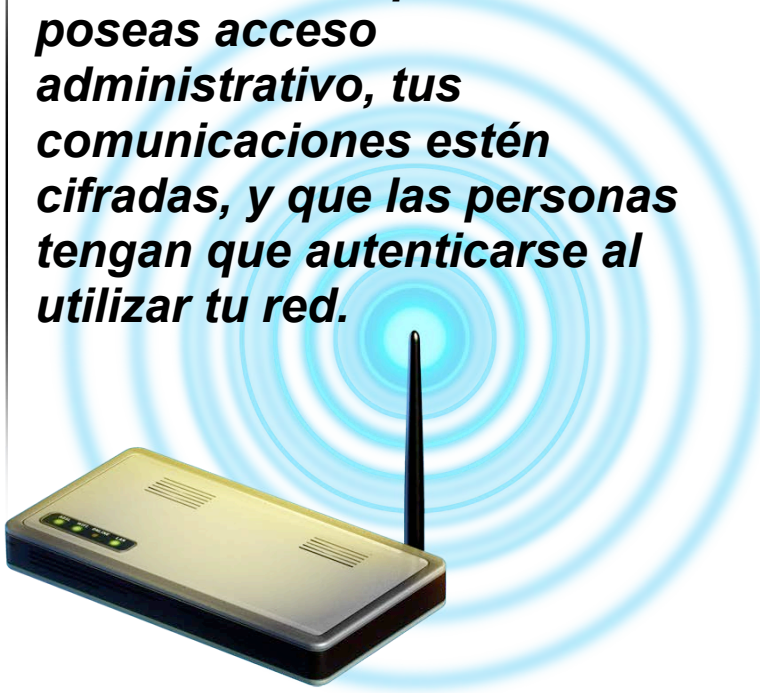
recomendamos cambiar el nombre que la red tiene por defecto. Asigna un nombre de red único que puedas identificar, pero asegúrate que no contenga ninguna información personal. Asimismo, considera que es poco útil que configures tu red Wi-Fi como oculta (o no compartida). Hoy en día, la mayoría de las herramientas de exploración Wi-Fi o cualquier atacante habilidoso, pueden descubrir los detalles de una red oculta. La opción más recomendable es dejar tu red Wi-Fi visible, pero segura; siguiendo el resto de los pasos mencionados en este boletín.

Cifrado y autenticación

El siguiente paso es asegurarte que sólo personas que conoces y de confianza, puedan conectarse y utilizar tu red Wi-Fi, y que estas conexiones sean cifradas. Lo más importante es asegurarnos que vecinos o extraños a la redonda no puedan conectarse o controlar tu red Wi-Fi. Afortunadamente, estos peligros son fáciles de mitigar habilitando la seguridad en tu punto de acceso Wi-Fi. En la actualidad una de las mejores opciones es utilizar el mecanismo de seguridad WPA2. Con sólo activar este mecanismo, las personas que se conecten a tu red Wi-Fi necesitarán una contraseña; y una vez que sean autenticadas esas conexiones, serán cifradas. Asegúrate de no utilizar métodos de seguridad obsoletos, como WEP, ni tampoco las llamadas redes Wi-Fi abiertas. Una red abierta permite que cualquiera pueda conectarse a esa red Wi-Fi sin ningún tipo de autenticación. El método de cifrado recomendable para WPA2 es únicamente AES, frente a otras opciones como TKIP o TKIP + AES.

Cuando configures la contraseña que las personas utilizarán para conectarse a tu red Wi-Fi, asegúrate de que sea diferente a la contraseña del administrador y que ésta no pueda adivinarse fácilmente, se recomienda que al

La clave para una red Wi-Fi casera segura es cerciorarse de que sólo tú poseas acceso administrativo, tus comunicaciones estén cifradas, y que las personas tengan que autenticarse al utilizar tu red.



menos tenga 20 caracteres de longitud. Esto puede sonar exagerado, pero recuerda que lo más probable es que lo introduzcas sólo una vez por cada uno de tus dispositivos, éstos almacenarán y recordarán la contraseña para acceder a la red en el futuro. Si tu punto de acceso de la red Wi-Fi está en una ubicación físicamente segura, y sólo los miembros de confianza de tu familia tienen acceso a ella, puedes optar por dejar escrita la contraseña del usuario debajo del punto de acceso Wi-Fi para consultarla fácilmente. Recuerda: alguien te dio la contraseña para tener acceso a tu red Wi-Fi; así que, de vez en cuando, sería bueno cambiarla.

Por último, te recomendamos apagar o deshabilitar WPS (Wi-Fi Protected Setup). WPS es una especificación

Asegura tu red Wi-Fi

diseñada para facilitar el proceso de configuración segura de tu punto de acceso Wi-Fi. Al momento de publicar este boletín, se encontraron vulnerabilidades recientes que permiten a un atacante tener acceso total a tu red inalámbrica si WPS está habilitada.

OpenDNS

Una vez que tu conexión Wi-Fi esté configurada, unos de los últimos pasos que recomendamos es configurar tu red para utilizar OpenDNS como tu servidor DNS. Cuando escribes el nombre en tu navegador, el DNS es como tu navegador, pues conoce a qué servidor de Internet se está conectando. OpenDNS es un servicio gratuito que ayuda a garantizar que te conectes solamente a sitios web seguros. Además, con OpenDNS puedes administrar los sitios web a los que tu familia se puede conectar. Si quieres bloquear y filtrar material ofensivo, éste es un gran recurso. El sitio web de OpenDNS te lleva paso a paso para configurar tu punto de acceso Wi-Fi para utilizar OpenDNS.

RECURSOS

Algunos de los enlaces mostrados a continuación, se redujeron para mejorar la legibilidad a través del servicio de TinyURL. Con el fin de mitigar problemas de seguridad, OUCH! siempre utiliza la característica de vista previa de TinyURL (preview), la cual muestra el enlace destino solicitando permiso antes de abrirlo.

- OnGuard Online Wi-Fi Security: http://preview.tinyurl.com/7u7qg6s
- ¿Crees que tu red inalámbrica es segura?: http://preview.tinyurl.com/6tl62z6
- Vulnerabilidad WPS: http://preview.tinyurl.com/8473vap
- OpenDNS: http://www.opendns.com/
- Wi-Fi: Guía rápida de consejos: http://preview.tinyurl.com/7kr54vq

MÁS INFORMACIÓN

Suscríbete al boletín mensual OUCH!, el boletín de consejos sobre seguridad. Accede a los archivos de OUCH! y aprende más acerca de las soluciones preventivas de seguridad que SANS tiene para ti. Visítanos en http://www.securingthehuman.org.

VERSIÓN EN ESPAÑOL

UNAM-CERT, equipo de respuesta a incidentes en México reconocido ante FIRST, es una referencia en seguridad de la información en este país. Sitio web http://www.seguridad.unam.mx, síguelo en Twitter @unamcert.

Consejo Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Versión en español a cargo de UNAM-CERT: Mayra Villeda, Francisco Martínez, Galvy Cruz, Edgar García