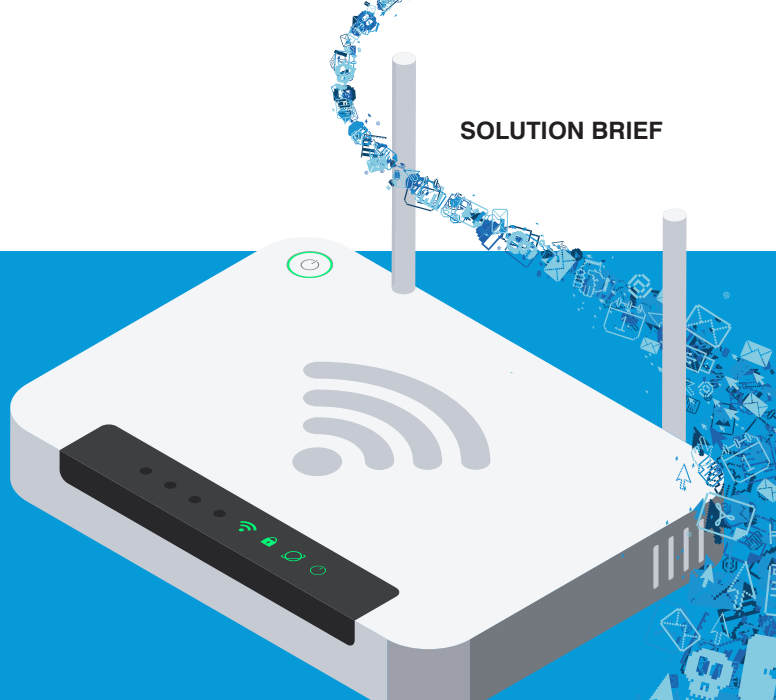


Tres pasos para actualizar la configuración de seguridad de redes Wi-Fi domésticas



Es posible que haya oído hablar de los peligros de conectarse a redes Wi-Fi abiertas y gratuitas. ¿Pero sabía que su red doméstica también puede presentar riesgos para sus datos personales? Si no ha tomado las precauciones de seguridad adecuadas, su red Wi-Fi puede ser tan vulnerable como la red inalámbrica abierta de la cafetería de la esquina. Sin las defensas necesarias, cualquiera puede acceder a su red, incluso personas con unas cuantas nociones básicas de ciberespionaje.

Nuestros expertos en seguridad de la información han identificado las tres medidas de seguridad más importantes para las redes Wi-Fi domésticas estándar. “Estas medidas de protección, afirmaron, resuelven normalmente el 99,99 % de los problemas para el 99,99 % de los usuarios”.

Lea las siguientes recomendaciones y comprométase a aplicar estas medidas para que su red sea más segura. La idea de actualizar las contraseñas predeterminadas y cambiar la configuración de la Wi-Fi puede sonar demasiado técnica, pero es más fácil de lo que imagina. Si alguna vez ha programado una videograbadora digital (o tradicional, VCR), también puede hacer esto.

1. Cambie la contraseña predeterminada del administrador de su enrutador y desactive la administración remota

La contraseña “admin” de su enrutador es totalmente diferente de la que utiliza para conectarse a la Wi-Fi. La contraseña de la Wi-Fi le permite conectarse a Internet utilizando el enrutador, mientras que la contraseña del enrutador le proporciona acceso a la configuración de la propia red Wi-Fi. (En la sección 3 encontrará más información sobre cómo definir o cambiar la contraseña de la red Wi-Fi).

El problema de no cambiar la contraseña predeterminada es que cualquiera, desde los hackers adolescentes poco experimentados hasta los ciberdelincuentes más sofisticados, puede encontrarla en Internet e utilizarla para acceder a su red. Cambiar las contraseñas predeterminadas ayuda a reducir los riesgos para la ciberseguridad. Siga estos pasos para cambiar la contraseña predeterminada:

- Localice en su enrutador la etiqueta que muestra la dirección IP predeterminada, y el nombre de usuario del administrador y su contraseña.
- Abra una nueva pestaña en su navegador.
- Escriba la dirección IP predeterminada (parecida a 123.456.7.8) en la barra de direcciones del navegador.

- Introduzca el nombre de usuario predeterminado y la contraseña correspondiente en la pantalla de inicio de sesión.
- Vaya a la zona de administración y cambie la contraseña admin. Cuanto más larga, mejor y es conveniente usar caracteres especiales. Una excelente opción es usar una frase de contraseña con información acerca de usted, pero difícil de adivinar para otros (por ejemplo, <3AlitasPolloPicante).
- A continuación, mientras está en esta pantalla, debe desactivar la administración remota. Cuando está activa la administración remota, es posible conectar con su enrutador desde fuera de su casa, por lo que mantenerla activa cuando no es necesario deja a su red en situación de vulnerabilidad ante ataques.
- Para desactivar esta función, busque una casilla o un botón parecido a “Activar administración remota” o “Desactivar administración remota”. Active o desactive la función, según corresponda, para asegurarse de que la administración remota no esté activada.

Nota: si no localiza dónde se cambia la contraseña admin en la interfaz, busque “cambiar contraseña de <marca del enrutador> <número de modelo>” en su navegador y encontrará las instrucciones rápidamente.

2. Actualice el firmware de su enrutador

Cuando esté en la zona de administración, aproveche la oportunidad y actualice el firmware de su enrutador. Al igual que ocurre con otros dispositivos electrónicos, los fabricantes de enrutadores con frecuencia descubren fallos y otros problemas que deben solucionarse una vez que los productos han sido entregados e instalados. Actualizar el firmware de su enrutador es como actualizar el sistema operativo de su smartphone o tablet, y es un paso que puede eliminar vulnerabilidades de ciberseguridad conocidas y mejorar el rendimiento.

Para efectuar la actualización, debe seleccionar las opciones “Actualización del firmware, Actualización del enrutador”, u otras similares, en la ventana del administrador. Si ve la opción para actualizar el firmware automáticamente (debe ser parecida a “Actualización automática del enrutador”), actívela para recibir automáticamente las actualizaciones de formato y de funciones en el futuro.

Como se ha indicado en la primera sugerencia, si no encuentra lo que necesita, puede buscar en Internet para identificar en dónde en la interfaz puede realizar la actualización.

3. Configure la seguridad de su Wi-Fi

Hay tres ajustes principales que se deben comprobar (y si es necesario, cambiar) en la configuración de su red Wi-Fi: su SSID (que es el nombre de su red inalámbrica), su método de cifrado y su contraseña de la Wi-Fi. El procedimiento es el siguiente:

- Busque una pestaña con el nombre “Configuración de Wi-Fi” o similar. (De nuevo, con una rápida búsqueda online puede identificar dónde se encuentra esta opción en el caso de su enrutador, si no está seguro).
- En primer lugar, compruebe el nivel de cifrado para redes inalámbricas. WPA3 es el último estándar de cifrado para redes inalámbricas, pero está aún dando sus primeros pasos. La mayoría de los enrutadores y dispositivos (como smartphones y laptops) no admiten todavía WPA3, por lo que es poco probable que esta opción esté disponible en su interfaz (a menos que haya instalado específicamente un enrutador compatible con WPA3). Hasta que el uso

de WPA3 esté más generalizado, elija cifrado WPA2 (ineludible), ya que otros protocolos de cifrado para Wi-Fi anteriores son mucho más vulnerables. Si hay varias opciones de WPA2, elija WPA2-PSK, WPA2-PSK (AES) o WPA2-Personal; las tres son básicamente lo mismo y ofrecen la mejor opción, aparte de WPA3, para el uso doméstico.

- Defina o cambie su contraseña para la red inalámbrica. (Si su proveedor de servicios le ha dado una contraseña, elija una nueva). Al igual que con su nueva contraseña de admin del enrutador, debe elegir una frase de contraseña que tenga un significado personal y un cierto grado de complejidad (caracteres especiales, números, etc.). NO utilice de nuevo su contraseña de admin.
- Cambie el SSID predeterminado por un nombre de su elección (“Inspección fiscal 1” podría ser divertido para sus vecinos, o es posible que les preocupe). Si conserva el SSID predeterminado, es posible que divulgue la marca y el tipo de su enrutador, y un ciberespía aprovecharía muy bien esa información para sus ataques.

Por otra parte, si le preocupa particularmente que haya extraños aprovechando su conexión a Internet, es decir, utilizando su red Wi-Fi en lugar de pagar ellos su propia conexión, desactive la difusión de SSID. (El uso no autorizado de redes inalámbricas suele ser un problema más habitual en áreas residenciales con más población, como bloques de departamentos y edificios).

Cuando se desactiva la difusión de SSID, el nombre de su red Wi-Fi no está visible para los dispositivos que exploran su zona en busca de redes inalámbricas disponibles. La ventaja de esto es que para personas ajenas es mucho más difícil conectarse a su red, ya que tendrían que adivinar su SSID y su contraseña para conseguir acceso. El inconveniente es que su SSID tampoco aparecerá en sus búsquedas, lo que significa que para conectarse tendrá que introducir de forma manual el nombre de su red en sus dispositivos.

Para desactivar esta función, utilice “Difusión de SSID” (o una opción similar) en el área de configuración de la red inalámbrica. Active (o desactive) la casilla o el botón, según corresponda, para desactivar la difusión.

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentran más de la mitad del Fortune 1000, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web.

Encontrará más información en www.proofpoint.com/es

proofpoint®