3 pasos para actualizar la configuración de seguridad en redes WiFi domésticas

Es posible que haya oído hablar de los peligros de conectarse a redes WiFi gratuitas. Pero, ¿sabía que su red doméstica también puede ser peligrosa para sus datos personales? Si no ha tomado las precauciones de seguridad adecuadas, es probable que su WiFi doméstica sea tan vulnerable como la red inalámbrica abierta de su cafetería de la esquina. Sin las defensas adecuadas, su red podría ser accesible para cualquier persona con incluso un modesto conjunto de habilidades de cibernética de espionaje.

Expertos de infosec han identificado las 3 medidas de seguridad más importantes para las redes WiFi domésticas estándar. "Estas protecciones, deberían resolver el 99,99% de los problemas para el 99,99% de los usuarios", dijeron [1]

Lea los siguientes consejos y comprométase a seguir estos pasos para que su red sea más segura. Aunque la idea de actualizar las contraseñas predeterminadas y cambiar la configuración de WiFi puede sonar demasiado técnica para que la puedas manejar, es más fácil de lo que podría imaginar.

1. Cambie la contraseña predeterminada del administrador de su router y deshabilite la administración remota

La contraseña de "administrador" en su router es totalmente diferente de la contraseña que utiliza para conectarse a su red WiFi. Cuando su contraseña WiFi le permite conectarse a Internet utilizando su router, la contraseña de su router le da acceso a los ajustes de configuración settings reales de la propia red WiFi.

El problema con dejar una contraseña predeterminada en su lugar es que todo el mundo, desde hackers adolescentes aficionados a los ciberdelincuentes sofisticados pueden encontrar esa contraseña en algún lugar en línea y utilizarla para entrar en su red. Cambiar las contraseñas predeterminadas ayuda a reducir los riesgos de ciberseguridad.

A continuación, le explicamos cómo cambiar la contraseña predeterminada::

1. Busque la etiqueta en el router que enumera la dirección IP, predeterminada, el nombre de usuario del administrador y la contraseña de administrador.
2. Abra una nueva pestaña o ventana de su navegador web en su computador.
3. Ingrese la dirección IP predeterminada —se verá algo así como 123.456.7.8— en la barra de direcciones web.
4. Introduzca el nombre de usuario y la contraseña predeterminados en la pantalla de inicio de sesión.
5. Navegue al área de administración y cambie la contraseña del administrador. Más tiempo es mejor, y los caracteres especiales son una ventaja. Una frase de contraseña que significa algo para usted, pero sería difícil para otros adivinar es una gran opción (por ejemplo, I<3SpicyChickenWings).

1 Al igual que la mayoría de las redes, los sistemas WiFi pueden incluir diferentes tipos de equipos y diferentes configuraciones. Para los fines de este artículo, asumimos una configuración de red residencial relativamente común con un solo router inalámbrico con un point de acceso incorporado.

Lo siguiente que debe hacer mientras está en esta pantalla es deshabilitar la administración remota. Cuando la administración remota está habilitada, es posible conectarse a su router desde fuera de su casa; dejándolo encendido cuando no es específicamente necesario hace que su red sea vulnerable a ataques.

Para desactivar la función, busque un cuadro o botón que esté etiquetado con algo como "Habilitar administración remota" o "Desactivar administración remota." Marque o desmarque la característica según corresponda para asegurarse de que la administración remota no está activada.

Nota: Si no puede encontrar el lugar para cambiar su contraseña de administrador dentro de la interfaz, busque "cambiar <Marca del router> <Número de modelo> contraseña" en su navegador web favorito y debe encontrar rápidamente las direcciones.

2. Actualice el firmware de su router

Mientras esté en el área de administración, aproveche la oportunidad para mejorar el firmware de su router. Como es el caso con otros dispositivos electrónicos, los fabricantes de routers a menudo descubren errores y otros problemas que deben abordarse después de que los productos ya se han enviado e instalado.

Actualizar el firmware de su router es similar a la actualización del sistema operativo en su smartphone o tablet, y este paso puede ayudar a eliminar las vulnerabilidades de ciberseguridad conocidas y mejorar el rendimiento.

Para completar la actualización, busque y seleccione "Actualización de firmware", "Actualización del enrutador" o una opción similar en la ventana del administrador. Si no ve la opción para habilitar las actualizaciones automáticas de firmware (busque una función de alternancia como "Actualización automática del enrutador" o similar), actívela para asegurarse de recibir automáticamente actualizaciones de seguridad y características en el futuro.

Como se señaló en el primer consejo, si no puede encontrar lo que está buscando, una búsqueda en línea puede ayudarte a identificar dónde ir dentro de la interfaz para completar la actualización.

3. Configure la configuración de seguridad WiFi

Hay tres configuraciones clave para comprobar (y, si es necesario, cambiar) dentro de la configuración de red WiFi: su SSID (que es el nombre de su red inalámbrica), su método de cifrado y su contraseña WiFi.

A continuación, le explicamos cómo hacerlo:

1. Busque una pestaña denominada "Configuración inalámbrica" o similar. (Una vez más, una búsqueda rápida en línea puede ayudarle a identificar la ubicación exacta para su router específico si no está seguro).
2. En primer lugar, compruebe su nivel de cifrado inalámbrico. WPA3 es el estándar de cifrado inalámbrico más reciente, pero actualmente está en sus primeros días.
   La mayoría de los routers y dispositivos (como teléfonos inteligentes y portátiles) todavía no son compatibles con WPA3, por lo que es poco probable que sea una opción disponible en su interfaz (a menos que haya instalado específicamente un router compatible con WPA3). Hasta que WPA3 se vuelva más común, elija el cifrado WPA2 — una necesidad, ya que los protocolos de cifrado WiFi anteriores son mucho más vulnerables. Si hay varias opciones WPA2, elija WPA2-PSK, WPA2-PSK (AES) o WPA2- Personal; los tres son esencialmente lo mismo y ofrecen la mejor opción fuera de WPA3 para uso en el hogar.
3. Establezca o cambie la contraseña de la red inalámbrica. (Si su proveedor de servicios le dio una contraseña, elija una nueva). Al igual que con su nueva contraseña de administrador del router, opte por una contraseña más larga que tenga un significado personal y al menos algún grado de complejidad (caracteres especiales, números, etc.). NO reutilice su contraseña de administrador.
4. Cambie el SSID predeterminado al nombre de su elección (algo así como "VIGILANCIA 1" es probable que deje a sus vecinos entretenidos o preocupados). Si mantiene el SSID predeterminado, es probable que transmita la marca y el tipo de router que está utilizando, y estos son pedazos de información que un fisgón cibernético puede utilizar en su contra.

En una nota relacionada, si usted está particularmente preocupado por los forasteros "piggybacking" en su acceso a Internet, es decir, el uso de su red WiFi en lugar de pagar por su propia conectividad, deshabilite la difusión SSID. (El uso inalámbrico no autorizado tiende a ser un mayor preocupación en áreas residenciales más pobladas como complejos de apartamentos y edificios).

Cuando la difusión SSID está desactivada, el nombre de la red WiFi no será visible para los dispositivos cuando busquen redes inalámbricas disponibles en su área. El beneficio de deshabilitar la radiodifusión es que se hace mucho más difícil para los forasteros conectarse a su red porque tendrían que adivinar su SSID y su contraseña para obtener acceso. La desventaja de esto es que su SSID tampoco aparecerá en sus escaneos, lo que significa que tendrá que introducir manualmente su nombre de red en sus dispositivos cuando se conecte.

Para desactivar esta función, busque "SSID Broadcast" (o similar) en el área de configuración inalámbrica. Marque (o desmarque) la casilla o el botón según corresponda para desactivar la radiodifusión.