

Presentan:

RECOMENDACIONES DE SEGURIDAD PARA LAS REDES WIFI

1. Averiguen qué tipo de seguridad ya tiene su WiFi de casa.

¿Sus amigos necesitan introducir una contraseña para entrar en la red cuando visitan su casa por primera vez y solicitan utilizar su WiFi? Si no lo hacen, la red no es tan segura como podría ser. Incluso si necesitan introducir una contraseña, existen algunos métodos diferentes para hacer segura su red, y algunos son mejores que otros.

Comprueben qué tipo de seguridad tiene la red en su casa mirando la configuración WiFi. Es posible que su red no sea segura o que esté protegida con WEP, WPA o WPA2. WEP es el protocolo de seguridad inalámbrica más antiguo, y es bastante débil. WPA es mejor que WEP, pero WPA2 es el mejor.

2. Cambien la configuración de seguridad de red a WPA2.

Su router inalámbrico es la máquina que crea la red WiFi. Si no tienen su red protegida con WPA2, tendrán que acceder a la página de configuración del router para hacer el cambio. Pueden consultar el manual de usuario de su router para encontrar la manera de acceder a esta página, o buscar instrucciones en línea para su router específico.

Cualquier dispositivo con la marca WiFi vendido desde 2006 debe tener soporte para WPA2. Si tienen un router que se fabricó antes, les sugerimos actualizar a un nuevo router que sí ofrezca WPA2. Es más seguro y puede ser mucho más rápido.

3. Establezcan una contraseña segura para su red WiFi.



Para configurar su red con WPA2 tendrán que crear una contraseña. Es importante que elijan una contraseña única, con una larga combinación de números, letras y símbolos para que otros no puedan adivinarla fácilmente. Si están en un espacio privado, como su casa, está bien que escriban esta contraseña para que puedan recordarla, y manténganla en un lugar seguro para no perderla. También podrían tenerla a la mano en caso de que sus amigos vengan de visita y quieran conectarse a Internet a través de su red. Así como no le darían la llave de su casa a un extraño, sólo deberían darle la contraseña de su WiFi a las personas de confianza.

4. Hagan su router seguro también, para que nadie pueda cambiar la configuración.

El router tiene su propia contraseña, separada de la contraseña que utilizan para proteger su red. Los routers vienen sin una contraseña, y si la tienen, es una contraseña simple que viene por defecto y que muchos criminales en línea ya conocen. Si no cambian la contraseña del router, los delincuentes en cualquier parte del mundo tienen una manera fácil de lanzar un ataque contra la red, los datos compartidos en la misma y los equipos conectados a la red. En muchos routers pueden cambiar la contraseña desde la página de configuración del router.

Esta contraseña sólo deben conocerla ustedes y debe ser distinta a la que utilizan para conectarse a la red WiFi (como se describe en el paso 3). Si estas contraseñas son iguales, entonces cualquier persona que tenga la contraseña para conectarse a la red también será capaz de cambiar la configuración del router inalámbrico.

5. Si necesitan ayuda, busquen las instrucciones.

Si han extraviado el manual del router, escriban el número de modelo de su router en un buscador, ya que en muchos casos la información está disponible en línea. De lo contrario, pónganse en contacto con la empresa que fabrica el router o con su proveedor de servicios de Internet para obtener ayuda.