RMTELCOM
RM TELECOMUNICACIONES MOMPOS S.A.S
Te conecta con el mundo

Consejos para mejorar la seguridad de tu red WiFi

A veces no nos damos cuenta de la vulnerabilidad de nuestra red, y pensamos que al estar dentro de nuestra propia casa, no vamos a sufrir ningún ataque. Todo el mundo advierte que las redes wifi públicas pueden resultar inseguras, pero… ¿Qué hay de las redes wifi domésticas? Con el objetivo de ayudaros a comprender un poco más en qué consiste esto de la *seguridad wifi*.

1.- Cambiar la contraseña de la red

Es evidente que debes poner una contraseña, pero no la que viene por defecto. Incluso los móviles tienen aplicaciones capaces de descifrar la contraseña predeterminada. A los vecinos les será muy sencillo robarte el wifi, pero además no les será muy complicado acceder a tu información privada.

2.- Hacer que no sea visible la red WiFi

Si hacemos caso a este consejo, no nos va a ser tan sencillo, pero también va a resultar una red más segura. Consiste en ocultar nuestra ID de la red WiFi, o también llamada **SSID**. Ahora cada vez que tengamos que conectar un nuevo dispositivo, tendremos que meter primero la SSID, para más tarde introducir la contraseña. Eso si, una vez que lo tengamos configurado como predeterminado, ya no hará falta. Un pequeño paso que ayuda bastante.

3.- Cambiar la ID de la red wifi o SSID

Si no quieres ocultar el nombre de tu red porque te resulta demasiado incómodo, o simplemente no te convence, lo mejor es cambiar el nombre. Hay muchos que recomiendan que se pongan nombres disuasorios. Así el que quiere robarte información se lo piensa dos veces antes de hacerlo.

4.- Tener todo actualizado

Cada día salen nuevos programas de software maliciosos, con funcionalidades diferentes, que atacan a tus dispositivos. Para luchar contra ellos de manera efectiva, lo mejor es que tengas actualizado el antivirus, sistema operativo, y sobretodo el firmware. Al actualizarlo, se introducen las nuevas definiciones, nuevos parámetros, y nuestro sistema aumenta su seguridad. Los sistemas operativos sin soporte técnico (como Windows XP y anteriores), cada vez resultan más inseguros. Como recomendación extra, utilizad siempre páginas oficiales del fabricante, pues lo que puede parecer una actualización, nos puede jugar una mala pasada.

5.- Permitir la conexión solamente a unas direcciones MAC

El ordenador, el móvil, la consola,… todo tiene una dirección MAC. Esta dirección es la identificación de la tarjeta de red de cada uno. A través de la configuración, podremos limitar la conexión de la red, para que se conecte solamente a estas tarjetas. Es decir, que aunque supiéramos la ID de la red, y la contraseña, no podríamos acceder con otro dispositivo. Para lugares en los que no se suelen conectar nuevos dispositivos, puede ser una conexión válida, pero de lo contrario es algo incómoda, ya que deberemos configurarlo cada vez que queramos conectar algo nuevo.

6.- Desconectarlo cuando no sea necesario

A parte de ser un gasto energético innecesario, tener siempre encendido el router, incluso cuando no se utiliza, puede suponer un problema de seguridad. Esto es debido a los múltiples dispositivos que se conectan a través del mismo. Si cualquiera de ellos sufre una vulnerabilidad, podemos sufrir ataques en todo el sistema.

7.- No ser imprudente

Aunque sigas todas las recomendaciones sobre redes wifi, nunca estarás seguro al 100%. Siempre existen puntos débiles, y cualquiera puede estar expuesto a ellos. Hazte con un buen firewall, y se precabido. Aunque creas que los datos que hay en tu ordenador no son valiosos, pueden serlo para alguien que hace un mal uso de ellos.

Si tienes una empresa, y manejas información importante, lo mejor es que te pongas en manos de profesionales en seguridad informática. Ellos te asesorarán y te ayudarán a resolver y prevenir los problemas de seguridad.