# Consejos para mejorar la seguridad de tu WiFi

## 1- Comprender los conceptos básicos del WiFi.

El centro de las comunicaciones WiFi "caseras" es el router. El router en su interior posee un pequeño sistema operativo que gestiona la comunicación y el intercambio de los datos de la red, por lo tanto si queremos modificar los parámetros de nuestra red tendremos que acceder a él.
La mayoría de los routers vienen con una configuración de fabrica, cierto es que cada vez estas configuraciones son más robustas pero es aconsejable modificarlas y adecuarlas a nuestras necesidades: contraseñas, aperturas de puertos, velocidad…
El panel de configuración de cada router es un mundo diferente, por lo tanto investiga un poco la estructura del tuyo y los parámetros que te permite modificar.
Seria conveniente que ampliaras un poco tus conocimientos sobre cifrado WiFi y sobre el funcionamiento básico de la tecnología.

## 2- Modificar configuración por defecto.

Una vez que hemos aprendido un poco más sobre nuestro router, debemos cambiar su configuración inicial. La configuración inicial de un router lo hace vulnerable aunque esta sea una configuración robusta ya que le aporta al atacante una información valiosísima sobre la red a la que esta accediendo.
Los aspectos básicos a modificar serian:

- Nombre de la red (SSID).
- Tipo de cifrado y contraseña.
- Limitar el número de direcciones IP asignables.
- Si tenemos problemas con las interferencias con otras redes podemos modificar el canal.

Ningún cifrado está a prueba de ataques criptográficos, pero si elegimos las tecnologías más robustas, la probabilidad de que nuestra red sea invadida por extraños se reduce bastante.

## 3- Intentar hackearnos a nosotros mismos.

Para vencer hay que conocer al enemigo y a uno mismo, es un principio que también se aplica la seguridad informática: para impedir que alguien supere las defensa de tu red hay que saber qué herramientas se usan para hackear redes Wifi.
Actualmente hay cientos de aplicaciones para ello, se puede hacer desde el dispositivo móvil con un par de clicks, yo recomiendo que te descargues alguna de ellas e intentes hackearte a ver cual es el resultado.

## 4- Control de cobertura de tu red WiFi.

La señal de una red inalámbrica se propaga hacia todas las direcciones desde el router. Si tu punto de acceso se encuentra al lado del apartamento del vecino, este disfrutará de casi la mitad de tu señal. Es una invitación a disfrutar de tu red WiFi. Para evitar que la señal se extienda a lugares desde los que no conectarás, debes pensar en dónde situar el punto de acceso.

Los escapes de señal son inevitables cuando se vive en lugares pequeños, pero es posible minimizarlas alejando el router de la calle y de los vecinos.
Y si no aprovechas la velocidad del protocolo 802.11n, usa el b o el g: tienen menos alcance.

## 5- Nombre de red anónimo, gracioso, agresivo…

Como ya hemos mencionado cambiar el nombre de la red es un paso importantísimos, como decíamos no cambiar este parámetro aporta información valiosa al atacante.
Cambiar el nombre de tu punto de acceso no hará que tu red esté a salvo, pero sí será un mensaje para quien explore las redes. Le estas diciendo a los potenciales ladrones que conoces tu router y que te has preocupado por hacer de tu red sea más segura.

## 6- No descuides la seguridad intramuros.

Por muy segura que sea la configuración del router, debes tener una segunda línea de defensa en la que refugiarte en caso de que alguien consiga acceder a tu red y tenga malas intenciones (o simplemente curiosidad). Si el cifrado de la conexión WiFi falla y no tienes un cortafuegos en tu PC, cualquiera podrá acceder a tus carpetas compartidas.

El muro más importante que debes levantar es el cortafuegos / firewall. Todos los sistemas operativos incluyen uno, y hay utilidades que facilitan su puesta a punto. Por otro lado, en nuestro especial sobre detección de intrusos en redes WiFi recomendamos varias utilidades para detectar e identificar visitas inesperadas.

## 7- Seguridad en su justa medida.

Llenar tu router de contramedidas, en lugar de ser beneficioso, puede causarte problemas. Es lo que se conoce como el fenómeno "Me he quedado fuera de mi castillo". El filtrado de direcciones MAC es un ejemplo de medida de seguridad ineficaz y peligrosa, puesto que es tremendamente fácil quedar excluido de la propia red por un pequeño error.
O dicho de otra forma: no te vuelvas paranoico. El 99% de las personas que intentan entrar en redes WiFi solo quieren ver vídeos en YouTube y descargar el correo; usan herramientas semi-automáticas, y, si estas fallan, se dan por vencidos al instante y buscan otras redes más sencillas de hackear.

## 8- Apaga el WiFi si no lo vas a usar.

La última recomendación es de sentido común: si no vas a conectar a tu red a través de una conexión WiFi, desactiva esa funcionalidad en tu router. Una red cableada es más segura, rápida y fiable que una inalámbrica.

Y si vas a estar fuera de casa por un largo periodo, apaga el router. Todavía no tenemos noticia de que alguien haya conseguido hackear un router apagado...