Protege tu conexión WIFI de intrusos

09/05/2015

Todos hemos oído alguna vez aquello de que el amigo de un amigo se puede conectar a la WIFI de algún incauto vecino usando algunos programas desde su ordenador o Smartphone. Y aunque existe mucho artículo y programa magufo, también existen herramientas avanzadas como WIFISlax, una distribución Linux Live DVD cargada de herramientas para capturar tráfico, analizar y envenenar o engañar a una red WIFI.

Por tanto, sí que existen herramientas que usadas **de forma malintencionada** pueden acabar sirviendo para que tu conexión WIFI sea la conexión gratis "de la comunidad de vecinos".

Además, en un porcentaje muy alto estos chupópteros del WIFI no tienen conocimientos sobre ingeniería informática, telecomunicaciones, sistemas o redes de computadores, simplemente utilizan vulnerabilidades descubiertas que son publicadas en internet en formato de "programa milagroso que te saca la WIFI del vecino dándole a un botón" lo que puede funcionar en algunos casos (cada vez menos), principalmente debido a la no actualización del software y hardware del Router de tu casa por parte de la operadora (que para eso tienen acceso a su configuración/actualización de forma remota)

Muchas de estas vulnerabilidades son corregidas por los proveedores rápidamente aunque con unos pequeños ajustes de seguridad y tips sobre el funcionamiento de tu router WIFI lograrás que el vecino "hacker" desista de su intento de intrusión.

Legalidad.

Si a estas alturas todavía hay quien piensa que "hackear la red del vecino" no está penado en España lamento decirle que se equivoca. Lo está tal como se indica en los artículos 255, 256 y 623.4. Básicamente es **como robar agua o electricidad a un vecino**. Si quieres saber más sobre la legalidad te recomiendo el siguiente artículo.

¿Existe algún riesgo de que alguien utilice tu conexión a internet?

Además de que tu conexión a internet irá más lenta ya que la estás compartiendo existen riesgos más importantes sobre todo en cuanto a privacidad o robo de información.

Una vez que un intruso está dentro de tu red puede capturar todo el tráfico (los datos) que pasan por ella para posteriormente analizarlos y extraer información delicada.

- Conexión a internet muy lenta.

- Datos disponibles para el análisis (Correos electrónicos, Usuarios y contraseñas, Servicios de mensajería, etc…)

- Usar tu conexión para realizar estafas, acusaciones delictivas a otras personas, etc… que te pueden acarrear un problema legal al ser el titular de la línea desde la que se realizó.

- Acceder tus dispositivos en red, discos duros, video cámaras, etc…)

¿Cómo consiguen conectarse a mi red WIFI?

Por regla general como ya te he comentado la forma de hacerlo es aprovechando algún tipo de vulnerabilidad del Router.

- **WIFI sin contraseña**. Si te gusta el riesgo.

- **Seguridad de tu Router anticuada**. Si todavía tienes una protección tipo WEP por favor configura tu Router para usar tipo WPA. Tener WEP es casi como tenerla sin contraseña.

- **Contraseñas WIFI por defecto**. Los fabricantes de Routers en ocasiones utilizan contraseñas estándar o que siguen cierto patrón.

- **Contraseñas débiles**. Contraseñas que **se pueden encontrar en un diccionario** sería considerado una contraseña muy débil.

- **Por fuerza bruta**. Esta forma será más o menos exitosa dependiendo de los puntos anteriores, pero básicamente se dispone de un equipo informático con una tarjeta de red WIFI preparada para escuchar el tráfico (tarjeta de red promiscua o en modo promiscuo) con la que se puede esnifar el tráfico WIFI para aislar y envenenar la Red con una técnica llamada Man-in-the-middle (Hombre en el medio) con la que se puede hacer creer a los equipos conectados a esa red que el Router es la tarjeta promiscua, haciendo pasar todo el tráfico por ella.

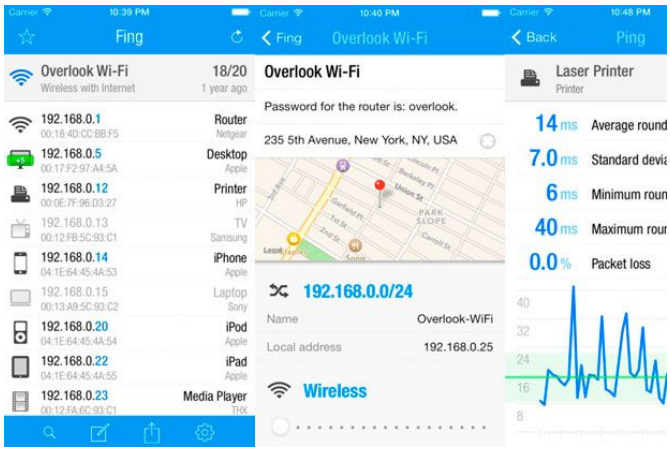
- **Atacando a la opción de tu Router WPS**. Esta opción básicamente permite conectar nuevos dispositivos al Router con una contraseña muy sencilla durante unos segundos. Existen vulnerabilidades en WPS ya conocidas que permitían obtener acceso a la red en un par de horas y recientemente se ha descubierto cómo hacerlo en segundos.

Te dejo con el siguiente video, un tanto cinematográfico (todo parece fácil y sencillo) pero que resume la idea de cómo es posible que alguien se acabe conectando a nuestra red.

https://www.youtube.com/watch?v=AM7GazNtoLM

Detectando intrusos

Ahora existen infinidad de programas que analizan tu red y te muestran todos los dispositivos que están conectados a la misma, ordenadores, smartphones, discos duros en red, etc… por lo que puedes verificar de un solo vistazo cuantos son los que están conectados a tu red.



Fing es una aplicación disponible para Android, iPhone y iPad que te permitirá obtener esta información

rápidamente.

Descargar para Android

Descargar para iPhone

Protégete

Te indico los tips a llevar a cabo para proteger tu WIFI de forma segura. Una vez has entrado en la configuración de tu Router:

- **Cambiar la contraseña para administrar tu Router**. Evitarás que si alguien se cuela en tu red pueda configurar tu router a su antojo.

- **Cambiar el nombre de la Red WIFI** por defecto (SSID http://es.wikipedia.org/wiki/SSID) evitando así que el atacante sepa de qué tipo de Router o compañía se trata.

- **Tipo de encriptación**. Utilizar tipo WPA2 si está disponible. Si no lo está al menos utilizar WPA.

- **Cambiar la contraseña por defecto** y colocar una contraseña compleja. (Mayúsculas, minúsculas, números y signos)

- **Filtrado por MAC**. Indicar explícitamente en la configuración del router la MAC de los dispositivos que pueden conectarse a la red. (Aunque esta también puede suplantarse)

- **Desactivando la función WPS**.

- **Y el que más fastidia** a los vecinos chupópteros. **Apaga el Router** cuando no estés en casa.

¡He encontrado WIFI sin contraseña!

¡Cuidado! Podemos estar conectándonos a la red de un Hacker que escuchará y analizará todo el tráfico que entre y salga de tu dispositivo (Hablaré de ello en otro artículo)

Conclusión.

Dedicar unos minutos a configurar tu Router aumentará tu seguridad y el riesgo de sufrir problemas de privacidad e incluso legales. Si tienes dudas puedes contactar con tu proveedor para que te ayude con esta configuración de seguridad y en última instancia esperar a la comida del domingo para pedirle ayuda al sobrino entendido.
PD. En Verkia Hosting y dominios ofrecemos correo electrónico profesional con SSL firmado (artículo sobre SSL), de esta manera tus correos estarán encriptados y aunque estos sean "esnifados" a su paso por la red estarán codificados (tanto los que recibes como los que envías) haciendo imposible (o casi) su lectura por alguien que los esté capturando en tu red.