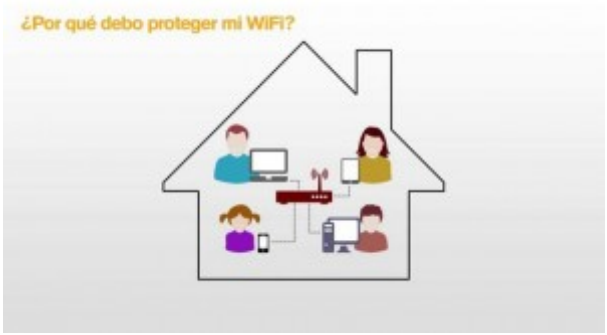
Descubre si te están robando el WiFi en dos pasos y cómo evitarlo



Para disfrutar de nuestra red hay que tenerla bajo control y reforzar su seguridad. Conexiones más lentas, páginas que no cargan, la señal de la radio online que se interrumpe justo cuando nuestro equipo va a marcar el gol de la victoria. Puede que sea un problema técnico, pero también puede que alguien nos esté robando el WiFi. Un 12,5% de los usuarios deja su red desprotegida y/o desconoce su estado, y casi un 26% ignora con qué sistema está asegurada, según el último Estudio sobre la Ciberseguridad y Confianza de los hogares españoles, realizado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) y el Instituto Nacional de Ciberseguridad (INCIBE).

¿Wi-fi público? Protégete

OSI / INCIBE

Los expertos de seguridad informática advierten que las redes Wi-fi disponibles en espacios públicos son un blanco fácil para los ciberdelincuentes, ya que muchas veces tienen una seguridad muy débil. Para defendernos, debemos eliminar el historial de las redes a las que nos conectamos. “Hay que tener el menor número posible de redes almacenadas, porque los atacantes las conocen y podrían suplantarlas. Se suelen poder borrar desde la pantalla de configuración”, explica Raul Siles, analista en Dinosec.

La Oficina de Seguridad del Internauta (OSI) sugiere también que evitemos comprar online e intercambiar datos sensibles a través de conexiones abiertas. Además, nos invita a comprobar que la señal a la que nos vayamos a conectar sea la oficial del lugar en el que estemos, a mantener nuestros dispositivos actualizados e intentar conectarnos a páginas provistas de certificado de seguridad (https://).

Víctor Domingo, presidente de la Asociación de Internautas, advierte que la cuestión va más allá de la molestia causada por tener una conexión más lenta. “El problema surge cuando los hackers convierten tu ordenador en un PC zombi: toman el control de tu dispositivo para hacer phishing, generar spam o cometer cualquier otro tipo de delito con nuestra dirección IP”, asegura.

El robo del WiFi representa una falta administrativa penada con una sanción pecuniaria solo cuando supera los 400 euros de facturación, explica Jorge Oria del despacho Abril Abogados. Sin embargo, si la conexión se usa cómo vehículo para cometer crímenes –sustraer números de tarjetas de crédito, suplantar la identidad o descargar pornografía infantil, por ejemplo–, el Código Penal prevé penas de reclusión de entre seis meses y tres años. Lo peor, explica Oria, es que se trata de circunstancias difíciles de detectar: "Generalmente lo descubrimos solo cuando nos vienen a detener".

Por todas estas razones es recomendable tener bajo control nuestra conexión, así como reforzar su seguridad para evitar sorpresas.

1. Cómo descubrir al intruso
Una conexión más lenta es solo una de las señales que nos deben de hacer saltar las alarmas. Marcos Gómez, subdirector de operaciones de INCIBE, explica que otro indicio nos lo dan los errores al cargar páginas con una alta disponibilidad de servicios, como Google. "Además, si no tienes ningún dispositivo conectado y el router parpadea mucho, preocúpate", alerta.

Herramientas gratuitas online. Para descubrir si alguien más está utilizando nuestra señal, Víctor Domingo aconseja rastrear nuestra red a través de una serie de softwares gratuitos. Existen métodos específicos para Microsoft Windows (Wireless Network Watcher o Microsoft Network Monitor), así como para Apple (Mac OS X Hints) y dispositivos móviles o Android (Fing, Network Discovery, Net Scan) e iOS (Fing, IP Network Scanner, iNet). La desventaja de estas herramientas es que detectan solo los equipos que están conectados a nuestra red en el preciso instante en el que realizamos la verificación.

Accede al registro del router. Para acceder a la interfaz de administración del router, hay que teclear su dirección IP en

la barra del navegador. Esta –normalmente 192.168.1.1– se encuentra en la información proporcionada por el fabricante; en alternativa la podemos averiguar dándole al botón inicio y tecleando cmd en el espacio donde aparece la lupa. En el recuadro que se abre, introducimos el comando ipconfig /all y después intro. Los números que se corresponden a la voz puerta de enlace predeterminada son la dirección IP de nuestro router. En un dispositivo Apple, en la lupa digitaremos la palabra terminal y luego netstat –r. La dirección aparecerá bajo la voz gateway. Llegados a este punto, copiamos la dirección en la barra del navegador. Se abrirá la interfaz de configuración del router. El nombre de usuario y contraseña suelen estar apuntados en el manual del router o en la pegatina que está debajo de ello. Si no los encontramos, podemos buscarlos en las páginas que los recopilan según la marca y modelo del router.

Ahora viene el momento de buscar el historial de los dispositivos que se hayan conectados a nuestro Wi-Fi. Lo encontraremos, generalmente, en el apartado DHCP o en el registro de los equipos asociados a la red. Ya que la IP de nuestros aparatos puede cambiar, hay que identificar al intruso a través de la dirección MAC, es decir, la dirección física de cada dispositivo. Este número, de 12 caracteres entre cifras y letras, ya nos ha aparecido anteriormente al ejecutar el comando ipconfig /all bajo la voz dirección física –para que aparezca en Apple, tras digitar netstat –r, tendremos que escribir ifconfig seguido por el nombre de la tarjeta asociada (que aparece bajo la voz netif) y buscar el número asociado a la palabra ether–. Otra forma para averiguar este código, tanto en ordenadores como en móviles y tabletas, es entrando a las opciones avanzadas de las propiedades de la tarjeta de red.

2. Fortalece la seguridad de tu conexión
Cambia el nombre y la contraseña de la red. Raul Siles, exalumno de la Escuela Técnica Superior de Ingenieros

Informáticos y fundador de la empresa de seguridad informática Dinosec, sugiere que cambiemos el nombre de nuestra red (SSID) —por defecto proporcionado por el fabricante—, así como su contraseña. “En lugar de una palabra, es mejor una frase superior a los 20 caracteres. Por ejemplo: estaeslaclavedeseguridaddemicasa. Será más difícil de averiguar y más fácil que nos acordemos de ella”, sugiere. Para aumentar aún más la seguridad, Siles aconseja modificar también la contraseña de acceso a la interfaz de administración del router.

Refuerza el protocolo de seguridad. El mejor sistema para proteger nuestra red doméstica es el protocolo WPA2-PSK, recomienda Siles. “Éste se selecciona en la interfaz del router. Si la configuración nos permite modificar también el encriptado, tenemos que elegir la opción AES”, añade.

Usa el filtro MAC. La empresa de seguridad informática Kaspersky aconseja incluir en el panel de administración del router las direcciones MAC de nuestros dispositivos, de modo que sean los únicos “autorizados” a conectarse a la red. El inconveniente de este sistema es que tendremos que cambiar la configuración del aparato todas las veces que tengamos que conectar un nuevo dispositivo, por ejemplo cuando algún huésped nos pida utilizar nuestra señal.

Inhabilita la administración remota y oculta tu red. Marcos Gómez, de INCIBE, sugiere modificar la configuración del router para que podamos acceder a su interfaz solo a través del cable LAN y no por red inalámbrica. Antes habrá que averiguar si nuestros dispositivos tienen puerto de acceso para el cable, ya que las tabletas y algunos modelos de portátiles no disponen de ello. “También puedes elegir ocultar tu router, para que nadie lo vea”, añade Gómez: “Y, si te vas de vacaciones, apágalo, por si hay algún listo que quiere aprovechar de que te has ido para hacer lo que quiera”.

Fuente: El País