Cómo saber si alguien se está conectado a tu red WiFi

osi.es /es/actualidad/blog/2014/03/17/como-saber-si-alguien-se-esta-conectado-tu-red-wifi

Saltar al área de contenido principal

Publicado el 17/03/14

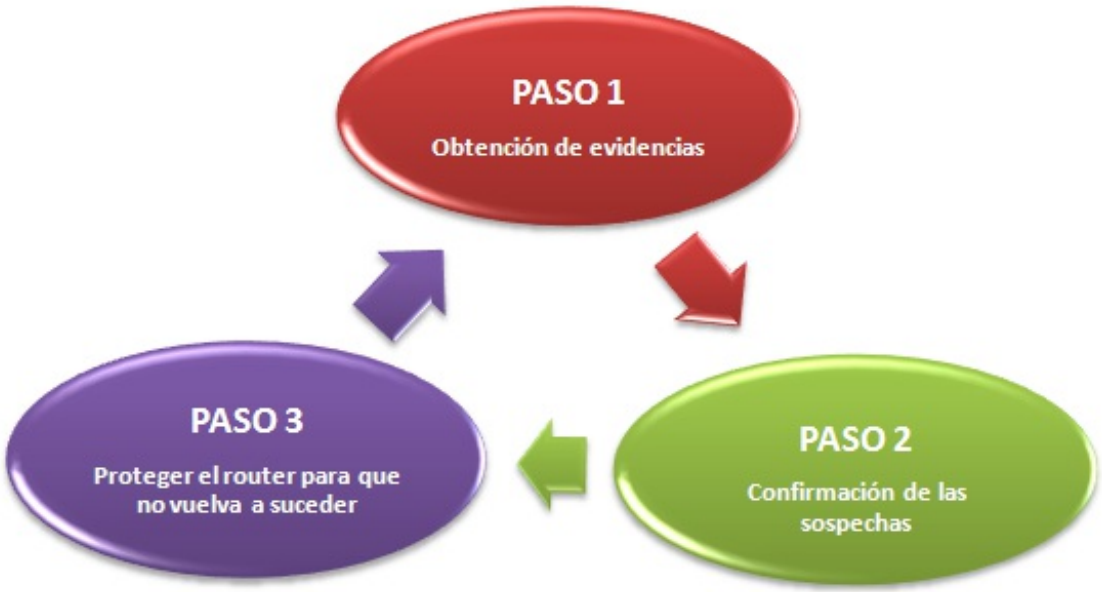
La facilidad de conexión, flexibilidad y movilidad que ofrecen las redes Wifi hacen que las usen millones de personas a diario. Debemos proteger la WiFi adecuadamente, para que los intrusos no intercepten nuestras comunicaciones.

¿Por qué motivo usas conexiones inalámbricas en casa?

La respuesta es fácil, sólo tienes que pensar en las ventajas que te ofrecen. Es muy práctico poder moverte por la casa con tus dispositivos sin necesidad de cables para estar conectado ¿verdad? Los cables son antiestéticos, molestan y cogen polvo. Además, reconoce que es muy útil poder conectar de forma simultánea varios dispositivos a la vez: el portátil de tu padre, el smartphone de tu amigo, la tableta de tu novia, la videoconsola de tu hermana, etc. Ahora bien, lo que no quieres bajo ningún concepto es que personas que no deseas se conecten a tu red WiFi. ¡Eso lo tienes claro! Y haces bien, porque podría acarrearte problemas de seguridad y privacidad.

Pero, ¿cómo puedes saber si un intruso está conectado a tu red WiFi?

¡Buena pregunta! Hoy despejamos todas tus dudas explicándote cómo detectar si hay algún intruso conectado en tu red y qué hacer para que no vuelva a producirse esa situación.



Cómo saber si un intruso está conectado a tu red WiFi

PASO 1: Obtención de evidencias

Desde CNMC comentan que si notas que tu conexión de Internet se vuelve más lenta a ciertas horas concretas del día, es un primer indicio de que alguien puede estar conectado a tu red. Puede que esa persona, por ejemplo, tenga el hábito de descargar cada noche un capítulo de su serie favorita desde tu WiFi.

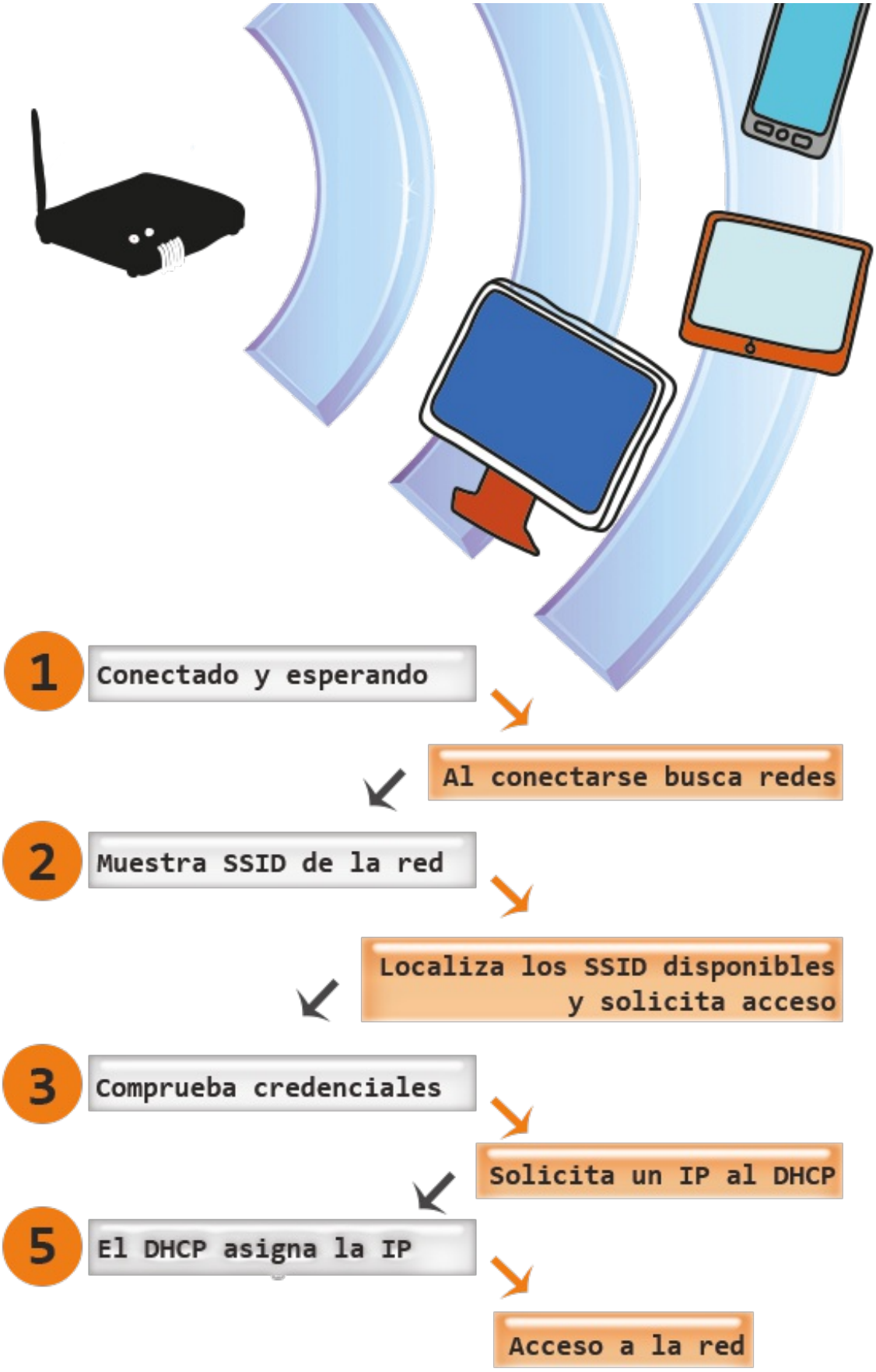
Otra evidencia que te podría hacer sospechar es que la luz del router continuase parpadeando tras apagar completamente todos tus dispositivos inalámbricos.

PASO 2: Confirmación de las sospechas

Llegado a este punto, lo que te interesa es comprobar de alguna forma si tus sospechas son ciertas o no y la forma más fácil de obtener esta información es instalando en tu dispositivo alguna herramienta qué te permita saber que dispositivos son los que están conectados a tu red WiFi de casa. Dependiendo del sistema operativo del ordenador o la plataforma de tu dispositivo móvil, podrás usar una herramienta u otra:

PASO 3: Proteger el router para que no vuelva a suceder

- **Cambia la contraseña WiFi que trae "de fábrica" el router.** Los operadores suelen utilizar un patrón conocido para crearlas, y es muy fácil descubrirla por fuerza bruta. Para una mayor seguridad, te recomendamos modificar esta contraseña por una que elijas tú y asegurándote que cumple los requisitos mínimos de seguridad.
- **Modifica la contraseña que te da acceso a la administración del router.** El panel de administración de los routers vienen siempre protegidos con una contraseña por defecto, que generalmente, suele ser la misma para un mismo modelo de router y, además, suele ser muy sencilla: "1234", "admin", "abcd", etc. Para evitar que nadie acceda a la administración de tu router, deberás cambiar esta contraseña.
- **No uses el protocolo de cifrado WEP bajo ningún concepto.** WEP es un protocolo decifrado para redes WiFi que no es seguro, ya que han aparecido fallos de seguridad que provocan que se pueda saltar fácilmente. Tener configurado el protocolo WEP en tu router es como tener la WiFi abierta a cualquiera. Si tu router es algo antiguo y sólo trae este protocolo, te recomendamos que contactes con tu operadora de telefonía para que te reemplace el router por uno que incorpore el protocolo WPA2 (protocolo de cifrado más seguro que WEP) o bien compres uno nuevo.
- **Utiliza IP estáticas.** Cuando tu dispositivo trata de conectarse a una red, ha de tener una dirección IP, que es una serie de números que identifican a tu ordenador de forma unívoca dentro de la red.¿Quién se encarga de asignar esa dirección IP a tu ordenador? El servidor DHCP que por defecto, viene activado en el router y configura los ajustes de la dirección IP automáticamente, evitando que los tengas que introducir manualmente. Si deshabilitas DHCP en el router, cuando un nuevo dispositivo solicite una dirección IP, éste, no se la dará.



Cómo se realiza la conexión de un nuevo dispositivo

- **Deshabilita WPS si el router dispone del mismo.** El protocolo WPS (WiFi Protected Setup), que permite conectar los dispositivos utilizando un PIN en lugar de la clave WPA, es vulnerable, se ha demostrado que un atacante podría obtener el PIN. Por este motivo, te recomendamos

que lo deshabilites.

- **Apaga el router o punto de acceso cuando no lo utilices.** Es obvio que, si apagas el router, reducirás las probabilidades de éxito de un ataque contra la red inalámbrica y por lo tanto de su uso fraudulento.

Hay otras configuraciones del router que si bien son recomendables, a nivel de seguridad no son efectivas:

- **Oculta el SSID (nombre de la red) para que no esté visible** , es decir, para que otros dispositivos no vean tu router. Aunque esta medida es aplicada por muchos usuarios, es importante saber que no se trata de una medida de seguridad, ya que es relativamente fácil encontrar redes inalámbricas con SSID ocultos.
- **Filtra por dirección MAC**. La dirección MAC es un valor que los fabricantes asignan a cada componente de una red, y que los identifica de forma unívoca. Digamos que es como el DNI de los dispositivos (routers, USB WiFi, tarjetas de red, impresoras, etc.) Es posible configurar el router para que filtre por direcciones MAC, para que sólo los dispositivos que tú desees se conecten a tu red wifi. Sin embargo, a día de hoy, con los conocimientos necesarios, es posible falsear esa dirección para ponerse una permitida. ¿Cómo? Mirando por ejemplo, la dirección MAC que tienen los dispositivos conectados en un momento dado. Por tanto, aunque aplicar esta medida es bueno, no es una garantía de seguridad.