Fuente:OSI

Protege tu WiFi

¿Qué riesgos hay en que alguien utilice nuestra WiFi?

Tener la WiFi abierta implica tener nuestra conexión a Internet compartida, además de otros riesgos:

- **Reducción del ancho de banda**. Dependiendo del número de dispositivos intrusos y del uso que hagan de la red, pueden llegar a impedir la conexión de nuestros equipos.
- **Robo de la información transmitida**. Una configuración inadecuada de nuestra red inalámbrica puede permitir a un atacante robar la información que transmitimos.
- **Conexión directa con nuestros dispositivos**. Un intruso con los conocimientos suficientes, ayudado por un problema de seguridad o una instalación sin la seguridad apropiada, podría acceder a los equipos conectados a la red. Esto implicaría darle acceso a toda nuestra información.
- **Responsabilidad ante acciones ilícitas**. Cuando contratamos una conexión a Internet con un proveedor de servicios, ésta queda asociada a nosotros, asignándole una dirección IP que nos identifica dentro de Internet. Cualquier acción realizada desde esa dirección IP lleva a la persona que contrata el servicio: nosotros.

Somos los primeros responsables de las acciones cometidas bajo nuestra red WiFi

Por tanto, si un usuario no autorizado comete acciones ilegales mediante nuestra conexión WiFi, puede acarrearnos problemas muy serios.

¿Cómo lo hacen?

Para utilizar nuestra conexión WiFi, los intrusos aprovechan una incorrecta configuración de seguridad en el router. Según el método de seguridad que utilicemos, ofreceremos más o menos resistencia, pero conseguirán conectarse sin problemas si presentamos alguna de las siguientes debilidades:

- **WiFi abierta**. Ahora ya no es tan frecuente, pero aún es posible encontrar alguna red inalámbrica que no solicita clave de acceso y está disponible para cualquier usuario. En estos casos, cualquiera puede conectarse. Esto es un riesgo tanto para el propietario de la red como para quien decida conectarse a ella.
- **Seguridad obsoleta**. Algunos router venían configurados con un sistema conocido como WEP, que con el tiempo ha resultado débil e inseguro. Con unos conocimientos informáticos elevados se pueden descubrir las claves utilizadas en poco tiempo. Estas redes son casi tan inseguras como las abiertas.
- **Clave WiFi débil**. Es posible que la red cuente con un sistema de protección robusto y correcto pero también resultará vulnerable si la clave de acceso la WiFi no es lo suficientemente “compleja”.
- **Clave WiFi por defecto**. En ocasiones el sistema de seguridad es el adecuado e incluso la contraseña es aparentemente robusta, pero si es la que viene por defecto puesta por el

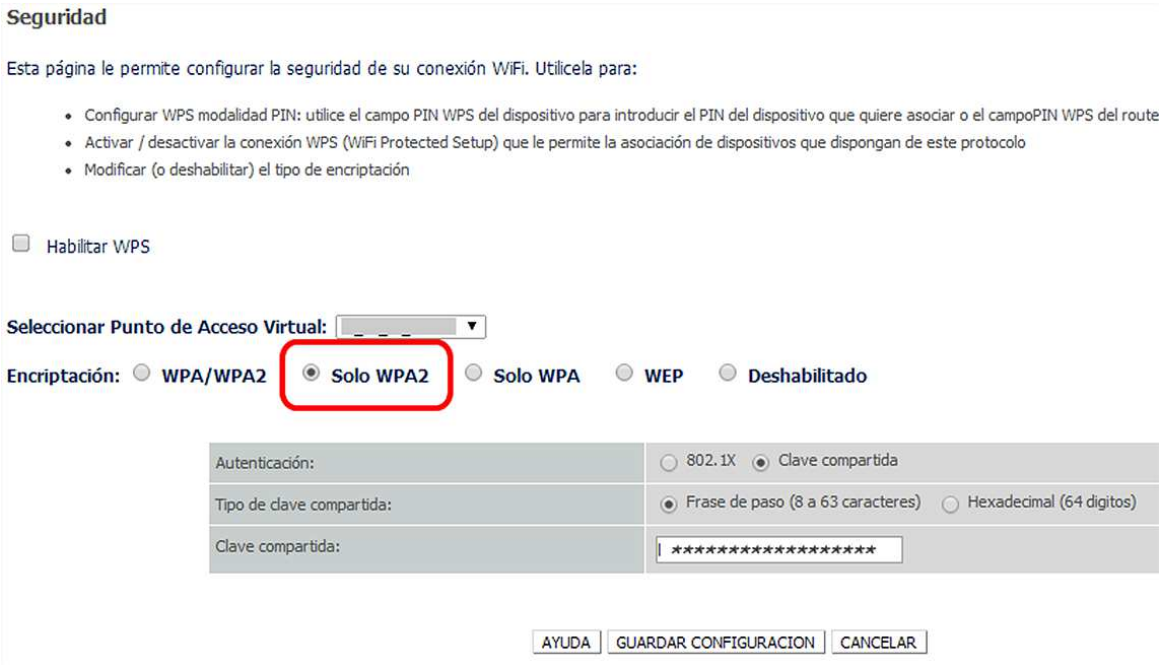
Fuente:OSI

proveedor antes o después será conocida en Internet. Es altamente recomendable cambiar la contraseña que viene por defecto.

¿Cómo protegernos?

Si queremos minimizar la probabilidad de ser víctimas de un ataque que pueda poner en riesgo nuestra red WiFi debemos comprobar su configuración de seguridad.

La configuración por defecto del router no siempre es la más apropiada.



El router debe incorporar al menos el protocolo WPA entre sus medidas de seguridad. Si es anterior a esta opción de seguridad debemos sustituirlo. Para conocer qué protocolo utiliza, lo primero es acceder a la configuración de nuestro router. Si no sabemos cómo hacerlo, podemos consultar el manual o buscar información sobre nuestro modelo en Internet.

En la mayoría de ellos podremos acceder utilizando nuestro propio navegador de Internet y escribiendo los números 192.168.1.1 en la barra de direcciones. Los números finales pueden variar según el modelo concreto. También necesitamos la clave de administración para entrar a la configuración del router. Ésta viene con el kit de instalación en una pegatina o en la documentación adjunta. Tengamos en cuenta que para entrar en la configuración del router debemos estar conectados a la red.

Las medidas de seguridad recomendables son:

- **Asignar el sistema de seguridad más avanzado: WPA2**. Buscaremos las opciones de seguridad para configurar un sistema de cifrado o encriptación WPA2 con un cifrado AES.

Fuente:OSI

- **Cambiar la contraseña por defecto**. Un sistema de seguridad robusto deja de serlo si la contraseña es trivial o fácilmente identificable. Debemos establecer una clave de acceso a la red WiFi de al menos 12 caracteres con mayúsculas, minúsculas, números y símbolos.
- **Cambiar el nombre de la WiFi o SSID**. Normalmente el SSID o nombre de la red viene definido por defecto. Éste debe ser sustituido por uno que no sugiera cuál es nuestro operador y que no guarde relación con la contraseña de acceso a la red.
- **Modificar la contraseña para cambiar la configuración**. Para acceder al panel de configuración necesitamos conocer la contraseña de acceso, que viene en la documentación de nuestro dispositivo. Suelen ser muy sencillas, como “1234” o “admin”. Conviene sustituirla para evitar que si alguien logra conectarse, pueda configurar el router a su antojo.
- **Apagarlo si nos ausentamos varios días**. Si no vamos a estar en casa y no necesitamos la conexión WiFi, lo mejor es apagar el router. Además del pequeño ahorro energético que supone, evitaremos que se intenten aprovechar de nuestra conexión.

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

- **Ocultar el SSID**. Una vez establecido, el nombre de la red se puede ocultar. Así se le indica al router que no debe “anunciar” el nombre de la red a los dispositivos móviles. 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.
- **Habilitar restricción MAC (o dirección física)**. Una de las características de seguridad que nos permiten los routers es la restricción del acceso a la red tan solo a aquellos equipos o dispositivos con una dirección MAC concreta.

  La MAC es el identificador único de cada dispositivo de red. Podemos averiguar en cada uno de ellos su MAC y añadirlo en el router como dispositivo seguro, impidiendo así el acceso de cualquier otro dispositivo no memorizado.

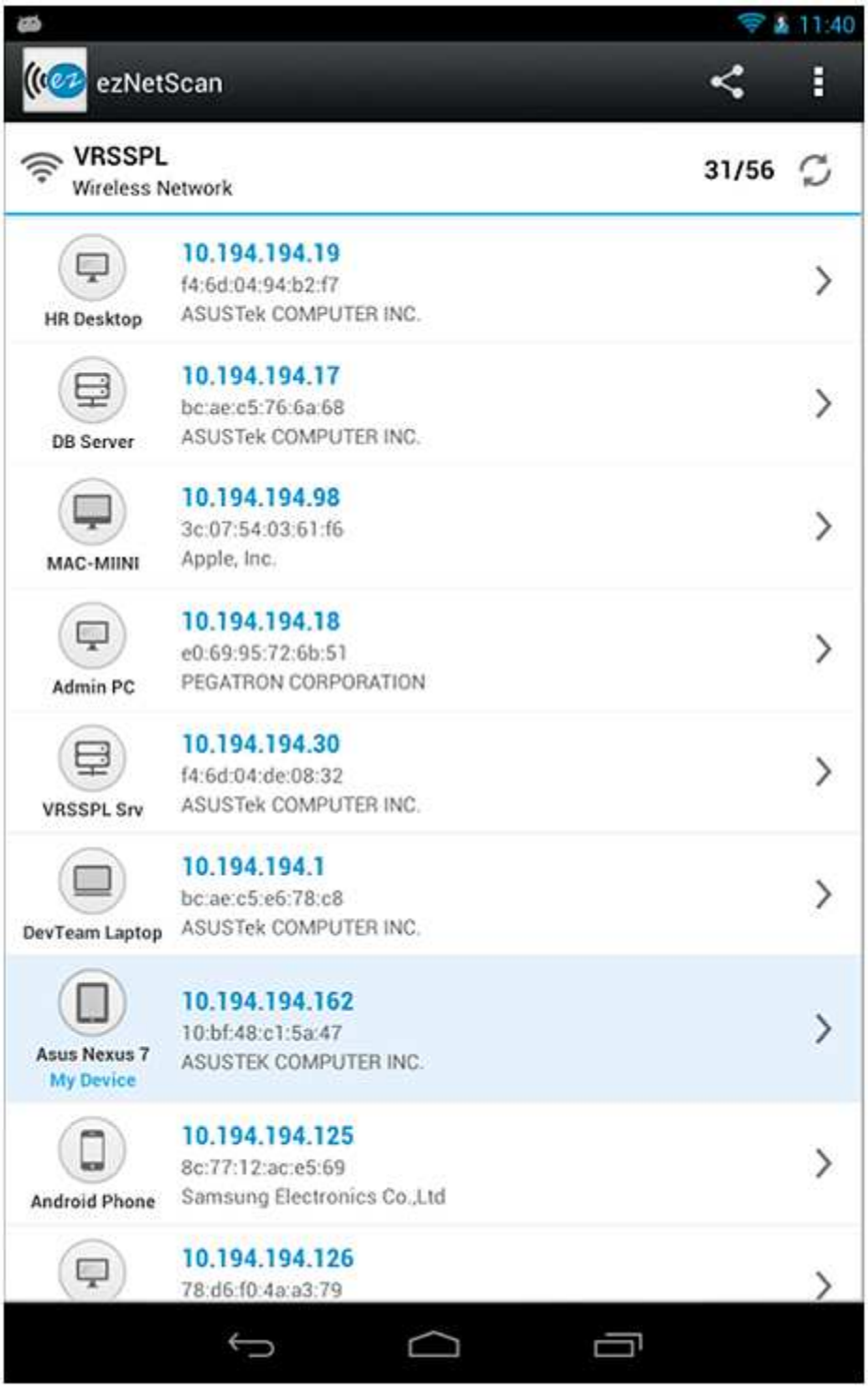
  Es decir, es posible configurar el router para que filtre por direcciones MAC, para que sólo los dispositivos que deseemos se conecten a nuestra red WiFi. Sin embargo, a día de hoy, con los conocimientos necesarios, es posible falsear esa dirección para ponerse una permitida. ¿Cómo? Mirando por ejemplo, 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.

¿Cómo detectar a un intruso?

Una de las formas de saber si alguien está utilizando nuestra WiFi es apagar completamente todos nuestros equipos y comprobar el parpadeo de las luces del router. Si continúan parpadeando es posible que otras personas estén utilizando nuestra conexión sin nuestro consentimiento.

Además, podemos revisar el estado de nuestra red fácilmente: desde un PC con Windows podemos descargar y utilizar Wireless Network Watcher y desde un dispositivo con Android, la aplicación ezNetScan.

Fuente:OSI



Consejos finales

Aunque nos parezca que estas cosas solo les pasan a los demás y que nuestra red WiFi nunca va a ser objetivo de un atacante, debemos ser prudentes y mejorar nuestro sistema de seguridad. Que un intruso utilice nuestra WiFi puede causarnos, además de incómodos fallos de funcionamiento, importantes problemas con la justicia.

Sólo necesitamos ponernos al día y aplicar unas recomendaciones básicas:

Fuente:OSI

- Mejorar el cifrado de la red a WPA2.
- Cambiar las claves por defecto, tanto de la red como la del acceso al panel de control, y utilizar siempre claves robustas.
- Verificar periódicamente quién se conecta a nuestra red. Con la aplicación adecuada podemos comprobar que se están conectando a nuestra red sólo nuestros dispositivos.