SyS Quest
Computación Corp,.S.A.

Cómo evitar que nos roben nuestra conexión WIFI

Hoy en día la gran mayoría de los usuarios de ADSL tienen un router con WiFi que permite a los usuarios conectarse a internet de forma inalámbrica. Esto, aunque tiene sus ventajas, también tiene inconvenientes como por ejemplo la facilidad que ofrece a los piratas informáticos de tener acceso a nuestra conexión, nuestra red e incluso si no estamos protegidos correctamente, a nuestros ordenadores y recursos compartidos.

La configuración que viene por defecto con los routers es práctica para empezar a funcionar cuanto antes pero queda bastante lejos de considerarse segura.

Si queremos poder utilizar nuestra conexión WiFi de forma segura y evitar que nos hackeen podemos seguir unos pequeños pasos para dificultar el acceso a los piratas informáticos.

Cambiar la contraseña del WiFi

Los routers suelen venir por defecto con una contraseña más bien débil y fácil de explotar. Junto a ello, múltiples vulnerabilidades que se han descubierto en los routers han permitido que los piratas informáticos creen diccionarios que simplemente introduciendo el nombre de la red WiFi nos devolverán la contraseña por defecto de dicho router.

Es muy importante cambiar la contraseña por defecto de nuestros routers para evitar que los piratas informáticos consigan acceder a ellos y comprometer nuestra seguridad.

En el siguiente artículo podemos ver los diferentes tipos de seguridad y cifrado que podemos habilitar.

Cambiar la contraseña de administración del router

La mayoría de los routers se gestionan a través de un pequeño servidor web al que accedemos escribiendo nuestra puerta de enlace en un navegador web (por defecto en la mayoría de los casos 192.168.1.1).

Es recomendable cambiar la contraseña de acceso de manera que si alguien no deseado consigue acceder a nuestra red WiFi no consiga acceder a este panel de configuración y modificar parámetros a sus anchas

Habilitar un filtrado MAC

Podemos configurar los filtrados MAC del router de 2 formas diferentes:

- Bloquear las direcciones MAC especificadas
- Permitir únicamente las conexiones MAC especificadas

Como cada dispositivo tiene una única dirección MAC personal e intransferible (aunque se pueden suplantar y modificar), una medida de seguridad muy efectiva es aplicar el filtrado MAC únicamente a las direcciones IP asignadas manualmente, introduciendo las nuestras en el router de manera que cualquier otro dispositivo que intente conectarse no podrá hacerlo.

Deshabilitar DHCP

Por defecto los routers vienen con un servidor DHCP para asignar direcciones IP automáticamente. Si una persona no autorizada se conecta a nuestra red lo más probable es que en primer lugar intente obtener una dirección IP válida de este servidor.

Si deshabilitamos el servidor DHCP el usuario que se conecte tendrá que asignar una dirección IP válida que permita tener conexión en la red, lo cual complica bastante el hecho de conseguir acceder a nuestra red y a nuestros recursos.

Desactivar la difusión de nuestra red

Podemos deshabilitar la difusión del SSID de nuestra red para que las demás personas que escaneen en busca de redes no vean la nuestra. De esta manera tendremos que introducir en los dispositivos el SSID manualmente para conectarnos y las personas que no lo conozcan simplemente desconocerán la existencia de dicha red.

Con estos pequeños pasos mejoraremos notablemente la seguridad de nuestras conexiones WiFi y evitaremos que piratas informáticos accedan a nuestra red sin nuestro permiso comprometiendo nuestra seguridad.