Cómo poner las cosas difíciles a alguien que pretenda robar tu WiFi

Quizá la principal preocupación de todo usuario que tiene una red de conexión WiFi instalada en su domicilio o negocio es que otros puedan acceder a esa red, bien para un uso gratuito de la misma, bien para realizar conexiones alternativas a un tercero que busque reali ...zar actividades ilegítimas, incluso (si se trata de una red wifi abierta) para acceder al procesador de nuestro ordenador y a los archivos de nuestro disco duro.

Si alguien fuese capaz de acceder a la red como administrador el problema de seguridad (especialmente de nuestros datos personales y datos confidenciales como claves bancarias) sería muy serio. De ahí que desde Consumer den una serie de sencillos consejos para evitar disgustos en este ámbito.

Una conexión WiFi envía paquetes de datos mediante ondas de radio según la capacidad del router y la antena. El alcance de las ondas es variable, pero generalmente es accesible más allá de las paredes del domicilio o la oficina. Si la conexión es abierta (y, por tanto, compartida de forma voluntaria) se corre el riesgo, además, de que esta quede colapsada en cuanto uno (o unos pocos) de los usuarios comience una descarga de archivos pesados.

Mejor una clave WPA que WEP

Los routers que proporcionan los proveedores suelen disponer de un 'login' y contraseña genéricos fáciles (cada vez más) de localizar en Internet. Cualquiera que sepa manejarse un poco por algunos foros o páginas determinadas puede dar con esas contraseñas. Si la encriptación

para proteger la señal WiFi utilizada es WEP, esta se puede romper de forma sencilla y se puede averiguar en pocos minutos ("Wired Equivalent Privacy" o Privacidad Equivalente a Cableado). Las claves proporcionadas, además, suelen seguir un patrón alfanumérico predecible, que hace más sencillo su acceso al dispositivo.

Consejos para remediarlo

Lo más recomendable es cambiar (siempre que los dispositivos la soporten) la encriptación del router a otra más segura como WPA ("Wi-Fi Protected Access" o Acceso Protegido Wifi) y hacer lo mismo con la contraseña para acceder a la señal WiFi. Hoy, muchos routers permiten configurar una clave WPA desde la página del router, a la que se accede al poner en la barra de direcciones la dirección IP desde la que se accede a la Red. Páginas como What's my IP Adress permiten conocerla.

También se debe cambiar la contraseña de administrador del router (avisando con antelación al proveedor de acceso ISP, ante posibles incidencias futuras en las que puedan actuar de forma remota). Páginas web como Bandaancha.eu y ADSLzone.net disponen de foros y wikis donde los usuarios pueden aprender a proteger su conexión según el modelo de router utilizado.

Si el usuario opta por una red abierta es necesario activar un cortafuegos en los equipos y no compartir carpetas y archivos. También se aconseja formar parte de algunas de las comunidades Wireless que crean y gestionan redes privadas gratuitas como alternativa a las gestionadas por empresas y que permiten conectarse a ellas en zonas y áreas concretas de la geografía, como Wifree, RedLibre o Guifi.net. También pueden utilizarse soluciones creadas desde proyectos comerciales como FON.