

¡Protege tus datos personales cuando trabajes en Internet!

Escrito por ADICAE Centrales - 03/11/2014 13:08

Internet es ya una realidad de nuestro día a día: consultamos las noticias a través de medios online, comparamos productos de diferentes webs, operamos con la banca digital, etc. Estas conexiones las podemos realizar desde nuestra casa, a través de una red privada, o en un lugar público. En ambas situaciones debemos ser conscientes de que exponemos nuestros datos personales al conectarnos a Internet, unos datos que pueden ser robados por otros usuarios que sepan cómo. Por este motivo, debemos tener en cuenta una serie de consejos básicos para evitar que nuestra información personal acabe en manos de terceros.

Si al usar nuestro router nos percatamos de que la navegación es más lenta de lo normal, puede ser que alguien haya entrado en nuestra Wi-Fi al no estar bien asegurada. En estos casos, el propio router incorpora opciones para aumentar la seguridad de nuestra conexión, algo que podemos hacer manualmente o llamando al servicio técnico. Aún así, el consumidor puede seguir estas recomendaciones para prevenir el robo de datos en su propia casa:

Cambiar la contraseña que viene por defecto en el router Wi-Fi por una segura que combine números y letras. Es conveniente ir cambiando esta contraseña periódicamente.

Asignar las direcciones IP manualmente. Por defecto, no hay que configurar nada en nuestro dispositivo para que se conecte a una Wi-Fi, ya que recibe del router todos los parámetros necesarios. Para entorpecer la entrada de intrusos podemos desactivar esta asignación automática (llamada DHCP). En ese caso, cada dispositivo que se conecte al Wi-Fi deberá configurarse individualmente según los parámetros establecidos en el router.

Hacer invisible nuestro Wi-Fi o cambiarle el nombre -el SSID-. Ciertos nombres identifican el dispositivo con el operador que lo ha suministrado, lo que facilita que pueda conocerse la contraseña por defecto. Para evitarlo podemos ponerle a nuestra conexión otro nombre y además que no informe de su presencia cuando alguien busque redes inalámbricas. Para conectar nuestros dispositivos habrá que introducir manualmente el nombre exacto.

Protegiendo nuestra Wi-Fi dificultamos que alguien use nuestra conexión fraudulentamente e impedimos que acceda a nuestra información personal y bancaria.

En el caso de las redes públicas, como aquellas a las que te conectas en una cafetería o en un centro comercial, los datos que se transmiten pueden ser captados tanto por el administrador de la red como por el resto de usuarios conectados. En estos casos, no es recomendable conectarse a redes públicas cuando se va a operar con la banca online, hacer compras o realizar cualquier otra actividad que requiera ingresar una contraseña. En definitiva, conectarse a redes Wi-Fis desconocidas entraña unos riesgos pero podemos seguir estos unos sencillos trucos de seguridad:

Tener instalado y habilitado un cortafuegos o firewall que bloquee las conexiones entrantes a nuestro equipo.

Mantener actualizado un antivirus que no detecte solamente los programas dañinos para el equipo, sino también los intentos de ataque.

Actualizar los programas que tengamos instalados en el dispositivo. De no hacerlo, los atacantes pueden aprovechar los fallos de seguridad que tengan las aplicaciones y acceder a nuestra información.

Desactivar las sincronizaciones automáticas de las aplicaciones del dispositivo cuando estemos conectados a una red no segura.

Desactivar el sistema Wi-Fi cuando no lo estemos usando o estemos fuera del alcance de nuestras redes de confianza.

Limpiar de vez en cuando la lista de puntos de acceso memorizados. Cada vez que nos conectamos a una red Wi-Fi, queda memorizada en nuestro terminal. Conviene realizar una limpia de aquellas redes esporádicas a las que nos hemos conectado y dejar sólo las que son confiables.

Más información:

<http://blog.adicae.net/consumidores-2014/2014/11/03/protege-tus-datos-personales-cuando-trabajes-en-internet/>

=====