¿No quieres que te espíen? Tendrás que navegar sin ruido

HOJADEROUTER.COM :: 23/11/2013

Navegar por internet de forma completamente anónima es prácticamente imposible, pero lo de Snowden demuestra que hay que estar atentos. Algunos consejos

¿Que Google nos espía? ¿Facebook también? Todas las grandes empresas de internet tienen un acceso casi ilimitado a nuestros datos e información personal, y eso es algo que no gusta mucho a la gente. Sin embargo, tenemos que tener en cuenta una cosa: la gran mayoría de esa información se la hemos dado nosotros voluntariamente.

Lo hacemos todos los días cuando nos registramos en páginas web, cuando subimos fotos a las redes sociales, cuando opinamos sobre un producto concreto en un foro. El problema, sin embargo, viene cuando información que consideramos privada (el contenido de un correo electrónico) también queda al descubierto. En la era actual es complicado permanecer en un anonimato absoluto cuando se navega por la Red, y nadie nos puede asegurar que no haya grandes empresas o gobiernos espiando. Sin embargo, sí es posible dificultar la tarea de los fisgones teniendo un poco de cuidado con nuestros hábitos al tratar la información y usando las herramientas adecuadas.

Software de código abierto

Los sistemas operativos mayoritarios en el entorno doméstico, como Windows o Mac, son software de código cerrado al que el usuario no tiene acceso, con lo que no puede supervisarlo ni, por supuesto, modificarlo. El problema está justamente ahí. Los equipos que funcionan sobre estas plataformas pueden incorporar programas o código malicioso que 'secuestren' nuestro ordenador, nos espíen o sencillamente recopilen nuestros datos. Sin ir más lejos, Microsoft llegó a admitir que colaboró con la NSA (Agencia de Seguridad Nacional de EEUU) durante el desarrollo de Windows.

Mientras los usuarios no tengan acceso al código, nunca podrán estar seguros de que ningún programa está recabando sus datos personales. Es por eso que usar un sistema operativo de código abierto podría ser un refuerzo para nuestra privacidad.

Utilizar un navegador basado en software libre

De la misma manera que un sistema operativo de código cerrado puede contener programas maliciosos, las aplicaciones también pueden hacerlo, y más las que se utilizan para conectarse a la Red. Internet Explorer, Opera o Safari pueden contener procesos ocultos que compartan más datos de los que nosotros queremos. Y no hay manera de comprobarlo. Sin embargo, navegadores de código abierto como Firefox nos proporcionan un plus de seguridad al navegar por internet. Eso sí, ojo con los complementos que instalamos, que ahí sí puede haber problemas.

Buscadores que no monitorizan tu actividad

Ha tenido que llegar Edward Snowden para que la gente se diera cuenta de la cantidad de información personal que fluye entre las empresas de internet como Google y los gobiernos, más concretamente el estadounidense. Google siempre ha querido enseñarnos su cara amable y el 'don't be evil' (no seas malo), pero el tiempo ha demostrado que los de Mountain View juegan con las mismas cartas marcadas que la competencia en lo que respecta a la privacidad de sus usuarios. Incluso les han caído multas.

Actualmente, la principal polémica acerca de Google es el 'tracking' (rastreo) al que somete a sus usuarios. Desde que abre su Gmail hasta que hace una consulta en el buscador, Google está almacenando información sobre gustos, dudas, o miedos de cada persona. Esos datos se utilizan luego para adaptar la publicidad o incluso, como se ha especulado a raíz de las revelaciones de Snowden, para informar al Gobierno de EEUU de lo que hacen sus ciudadanos.