Publicado en el 03/11/2016

Las extensiones para navegador también pueden vender tus datos comprometiendo tu privacidad

Internet no es gratis, y las redes sociales que se visitan a diario tampoco, puesto que se paga con los datos personales de cada usuario

Internet no es gratis, y las redes sociales que se visitan a diario tampoco, puesto que se paga con los datos personales de cada usuario. Este es un mensaje que se lleva varios años tratando de inculcar en la sociedad. Mucha gente es consciente de ello, e incluso la justicia está empezando a actuar los casos de servicios como Facebook o WhatsApp, pero esto es sólo la punta del Iceberg.

Algo tan aparentemente inocente como una extensión para un navegador también puede estar obteniendo y vendiendo tus datos personales. No sólo extensiones de baja calidad, sino, como ha destapado un medio alemán, también otras con tan buena calificación como la popular WOT: Web of Trust. Por lo tanto no se debe tener miedo a que Facebook pueda abusar de sus cookies, porque seguramente ya se les ha regalado los datos a quien menos nos se espera.

El caso de WOT no es ni el único ni el último del que sabremos, pero sí es un buen ejemplo de lo poco que a veces los usuarios se preocupan por la privacidad. Y es que con las extensiones no se tienen excusas de que nos de pereza leer largos términos de uso: al darle a instalar nos aparece un mensaje en el que lo único que se nos dice es que leerán todos los datos de nuestro historial.

¿Se baja la guardia con las extensiones?
Poco a poco se está concienciando de que las redes sociales cobran a partir de la privacidad. Pero igualmente se siguen utilizando igual, pero la preocupación de los usuarios hace que en algunos casos las autoridades decidan intervenir, lo que a su vez le da más voz al tema y hace que más gente se quiera informar de lo que pasa.

Si se cree que el riesgo es mínimo porque las extensiones no acceden a tantos datos volvemos al tema de WOT. Los periodistas alemanes les compraron datos que incluían diez millones de páginas web. El problema es que los datos no estaban del todo anonimizados, y en ellos había URLs que revelaban nombres de usuario, correos electrónicos o nombres propios. También direcciones de email de cuentas de PayPal o nombres de usuario de Skype.

Y es que las páginas que visitas dicen más de ti de lo que piensas. Por ejemplo, en este caso puntual pudieron saber información de investigaciones policiales o las preferencias sexuales de un juez. También obtuvieron el nombre de algunos que buscaban drogas o prostitutas online, e incluso la información financiera de algunas empresas.

¿Y qué podemos hacer?
Vale, es verdad que la mayoría de extensiones necesita estos datos para funcionar, pero por ello no

tenemos que bajar la guardia ni dejar de tomar precauciones. La primera siempre debería ser utilizar las extensiones oficiales de cada servicio, y no creernos que una lo es por poner entre paréntesis (by Google). Siempre fijémonos en el autor.

Esto no quiere decir que no se tengan que fiar de los pequeños desarrolladores o las nuevas aplicaciones alternativas, pero si se hace sí que se debería fijar en el número de usuarios, las opiniones de cada uno y, si la hubiera, la sección de ayuda para detectar posibles problemas. En definitiva cada usuario es la primera línea de defensa, y se tiene que saber instalar.

Como hemos dicho también es importante comprobar el tipo de permisos que se solicitan y pensar para qué se podrían utilizar. Por poner un par de ejemplos, leer o modificar todos los datos de los sitios que se visitan se podría servir para añadir publicidad, mientras que hacer lo propio con el historial les permitiría recopilar y vender nuestros hábitos de navegación.

La noticia Las extensiones para navegador también pueden vender tus datos comprometiendo tu privacidad fue publicada originalmente en Xataka

Datos de contacto:

Nota de prensa publicada en:

Categorías: Telecomunicaciones E-Commerce Premios