11 Cosas Que Debes Y No Debes Hacer Con Tor

TOR es un software gratuito, que usa una red abierta con la finalidad de permitir a las personas mejorar su privacidad y seguridad en la Internet. ***TOR*** es la solución perfecta en el caso que te preocupes, por el rastreo de tus datos por parte de alguna agencia gubernamental de tu pais. **TOR encripta los datos que envías**, y los transporta a través de de diversos puntos, con esto oculta la verdadera fuente de donde inicio la comunicación; dando así seguridad y protección a tus datos y tu ubicación. Por eso, te compartimos **11 Cosas Que Debes Y No Debes Hacer Con Tor**.

Red TOR

Con los siguientes consejos puedes tener mayor control sobre la **seguridad de tu identidad y datos en la web**, esperamos que te sean utiles.

1. Usa TOR

Cualquier persona preocupada por la privacidad en la web, debe de preocuparse por aquellas personas que estan detras de este servicio , tales como proveedores de Internet , agencias gubernamentales , proveedores de servicios web, etc. La red TOR es bien conocido por proporcionar el anonimato en la web , y esa es la mayor razón por la que se debe usar.

TOR puede ser utilizado por cualquiera y para todo tipo de navegación sensible, pero sin limitarse a , casos de abuso y corrupción; actividades comerciales serias, las comunicaciones

de datos sensibles de los gobiernos; y toda aquella informacion que dañe directa o indirectamente a una persona.

2 . No usar TOR en Windows

Windows no es simplemente la mejor elección de la plataforma para usar TOR, esto, debido a los fallos de seguridad y vulnerabilidades presentes en el sistema puede poner en peligro su privacidad, incluso cuando se utiliza TOR.

Es por eso que no se debe navegar por sitios web a través de **TOR** en sistemas Windows. TOR tambien se ejecuta en sistemas linux, los cuales son algo mas seguros que los Sistemas Windows, ademas la configuración en Linux puede ser mas flexible.

3. Actualiza tu Software

Cliente Tor es simplemente un software que se ejecuta en la capa superior de tu Sistema Operativo, lo que significa, que la seguridad que pueda brinda el, depende directamente de los programas y el Sistema Operativo que use. Con esto, debemos actualizar nuestro Sistema Operativo, navegador web, cliente de mensajería y todo aquel software que use TOR.

4. No usar sitios con

HTTP

The Onion Router (**TOR**), como su nombre indica, es sólo un router tráfico y no una herramienta para cifrar el tráfico de red a través de Internet. Eso significa que TOR oculta el origen de su tráfico de red y encripta todo **dentro de la red Tor**, pero no cifra el tráfico de Internet fuera de la red.

TOR es mas inseguro en la salida de los datos, ya que estos no están envueltos en ninguna encriptación. Es por eso que siempre se debe utilizar el cifrado tanto en el que envía, como en el que lo recibe, algo como SSL o TLS cuando se hace las comunicaciones sensibles, y que requiere del uso de **HTTPS** en los sitios web. También debe considerar el uso de complementos tales como HTTPS y así cambiar automáticamente a la navegación por HTTPS-mode para los sitios web compatibles.

5. Encripta tus datos locales

TOR, solo encripta el trafico que sale y entra de la web, no los archivos que recibes ni los que envias. Para esto existen herramienta para la encriptacion de archivos. **LUKS** ó **TrueCrypt** se pueden utilizar para cifrar los archivos y así protegerse de diversas amenazas. **LUKS** ofrece una protección de datos razonablemente seguro en sistemas Linux, mientras que TrueCrypt también ha demostrado ser útil en la protección de sus datos.

6. No utilizar el

Navegador web de TOR

Recientemente el FBI ha cerrado un servidor denominado como el **Freedom Hosting** (un servicio de alojamiento web en el anonimato se ejecuta como un servicio oculto en la **red Tor**). El rastreo que hizo este ente gubernamental fue a través del navegador que nos brinda la herramienta TOR. Si fueron capaces de rastrear un servidor «anonimo», por que no podrían rastrear tus datos?**7. Desactive JavaScript, Flash y Java**

Estas tecnologias son de cierta manera independientes, ya que ciertamente se ejecutan con con permisos especiales en el navegador, como tambien usan sus propias configuraciones en cuanto al proxy. Desactivandolas, nos aseguramos de que la privacidad de nuestra navegación sea mas fuerte.

7. Desactive JavaScript, Flash y Java

Estos complementos son de cierta forma independientes de las configuraciones que nos brinde **TOR**. Lo cual nos dara un hueco de seguridad, desactivandolas, nos aseguramos de minimizar los rastreos atraves de estas tecnologias.

8. No usar P2P

P2P no se debe usar en **TOR**, ya que este no se creo para el intercambio de archivos **peer-to-peer**. Al usar servicios como torrents, cargamos la red de usuarios de la red TOR, ya que esta red no fue creada para dar un soporte eficiente para las

descargas de grandes archivos. Por otra parte, el uso de **TOR** con **BitTorrent** no es segura y es una amenaza para su anonimato en línea.

9. Elimine cookies y datos locales del Sitio

Las **cookies** sirven no solo para analizar búsquedas y preferencias de sitios, sino también para reunir información del navegante. Eliminandolas, nos aseguramos de que nuestros datos no sean expuestos. Considere la instalación de **una extensión** que elimine automaticamente las **cookies**.

10. No use su Correo Electronico personal

De nada sirve usar una red que proteja la información que envies y recibas, una red que te oculta del rastreo indiscriminado de datos; mientras usas tu identidad «real». Es como si usaras una mascara en un evento, pero llevas tu nombre es una escarapela. Crea una identidad virtual, una que solo uses para cuando navegues o quieras anonimato total. Procura no usar tus datos cuando crees algo así.

11. No uses Google

Google reúne información de los navegantes con la finalidad de mejorar sus formatos de publicidad. Por ende, al usar este navegador, nos aseguramos de dar información sensible de nosotros. Para esto, hay alternativas como **Startpage y DuckDuckGo**.