ANONIMATO EN INTERNET

10 maneras de hacerse invisible y protegerse

SOBRE ESTE RECURSO

Cualquier actividad en Internet no pasa desapercibida.

Encontrar información, enviar correos electrónicos, visitar sitios web, comprar en línea y comunicarse en redes sociales, todo deja huellas que facilitan la búsqueda de la mayoría de los datos confidenciales del usuario. Y no hay forma de ocultar completamente el hecho de tu presencia en Internet: ¡es físicamente imposible!

Sin embargo, existen ciertas herramientas a través de las cuales puedes 'complicar' en gran medida el proceso de recopilación de información sobre ti de Internet, lo que hace que no sea rentable para los intrusos y otros "recolectores" de información confidencial.

EsGeeks

¿Quién Necesita Tus Datos Confidenciales?

Antes de hacer cualquier intento de "anonimizar" tus actividades en línea, debes definir claramente por qué necesitas personalmente el anonimato y de quién planeas proteger los datos confidenciales. Dado que esto determinará la elección de una herramienta de seguridad con la que protegerás tu anonimato en Internet.

Corporaciones

Quieren cualquier tipo de datos sobre los usuarios de Internet con los que puedan ganar más dinero.

Proveedores

Recopilan información de marketing (preferencias del consumidor) sobre sus clientes para venderla a varias corporaciones.

Motores de búsqueda

(Google, Yandex, Bing, Yahoo!). También recopilan datos de marketing para su venta posterior, pero también los usan para necesidades personales.

Atacantes

En el 98% de los casos, información financiera para robar dinero. El resto del porcentaje se distribuye entre la "vigilancia" y el capricho personal.

Las fuerzas del orden

En los estados regidos por el estado de derecho, la información se recopila para "garantizar la seguridad del país y sus ciudadanos", como insisten algunas subcláusulas de los documentos normativos.

10 maneras de permanecer anónimo en línea

Para proteger tus datos confidenciales de intrusos y volverse anónimo para los motores de búsqueda, las grandes corporaciones, el gobierno y otras agencias ocultas, no es necesario *auto-eliminarte* de la red. Es suficiente usar una o más herramientas a través de las cuales los usuarios experimentados de Internet ocultan su presencia en la red.

1) Proxies normales y SOCKS

Un servidor proxy (conexión) es un servicio intermedio intermediario entre la computadora del usuario e Internet. Es decir, proporciona anonimato al falsificar la dirección IP del suscriptor. Dependiendo del grado de seguridad, los servidores proxy se dividen en:

- **Servidores HTTP (regular)**: solo permiten que el tráfico HTTP pase a través de ellos mismos, agregando datos sobre el uso del proxy.
- **Servidores SOCKS**: permiten que el tráfico pase a través de ellos sin agregarle nada.

Estos servidores ayudan a mantener el anonimato para evitar varias restricciones regionales y proporcionar seguridad básica para la información confidencial. Esto es útil si deseas permanecer en anonimato para motores de búsqueda, corporaciones y atacantes sin experiencia. [**proxy6.net**]

10 maneras de permanecer anónimo en línea

2) Anonimizadores (CGI-proxy)

Los anonimizadores o CGI proxy son servidores creados en una forma en la que sus usuarios solo necesitan ingresar la dirección del sitio de interés y nada más. También crea tráfico anónimo al falsificar IP, pero nada más.

Los servicios de prueba son útiles para aquellos que desean evitar el bloqueo de empleadores, padres o estados. Sin embargo, no vale la pena usarlos para protegerse contra corporaciones o intrusos.

3) VPN

Virtual Private Network (VPN) o "Red Privada Virtual" es una tecnología mediante la cual se realizan una o más conexiones a través de otra red (por ejemplo, la Internet). En este caso, la conexión entre el suscriptor y el servidor VPN está cifrada, lo que crea el acceso más anónimo a Internet. Y así será no sólo para los recursos de la web, sino también para los proveedores. Si se utilizan servidores proxy, esto no se lograría.

Ahora los proveedores comerciales ofrecen a sus suscriptores los siguientes protocolos VPN: OpenVPN (protocolo abierto), SSTP, L2TP + IPSec o PPTP (no tan seguro).

10 maneras de permanecer anónimo en línea

4) Túneles SSH

El túnel SSH es una tecnología para crear conexiones anónimas a Internet a través del protocolo SSH. Su característica especial es que la información se codifica en un extremo del túnel y se descifra en el otro. Los recursos de la web aquí se utilizan sólo para la transferencia de tráfico.

Cabe señalar aquí que los túneles SSH, por regla general, se utilizan a través de VPN, manteniendo así la seguridad de datos confidenciales y proporcionando el acceso más anónimo a los recursos web.

5) Navegador Tor

TOR (del inglés The Onion Router) es un navegador de código abierto que utiliza un sistema de routers capa por capa, con la ayuda de los cuales se establece una conexión anónima entre el usuario y recursos web con protección contra escuchas. No recopila registros, no transmite ninguna información sobre el usuario a Internet y utiliza una conexión TLS bidireccional.

Es perfecto? No. (1) Hay servidores de control; (2) baja velocidad; (3) el tráfico que viene del otro lado no está cifrado.

10 maneras de permanecer anónimo en línea

6) Navegadores y Plug-ins para ellos

También es posible pasar desapercibido en la Internet utilizando los navegadores convencionales, si tienen la modalidad de "incógnito" o tienen una extensión especial (add-on).

El principal inconveniente es la falta de aclaraciones sobre la seguridad de dicha conexión (falta de términos), por ello recomendamos **DuckDuckGo**.

7) Sistemas Operativos Seguros

La siguiente forma de proporcionar acceso anónimo a Internet es instalar un sistema operativo especial. Hay muchos de ellos, pero los más confiables son: **Whonix**, **Tails** y **Liberté Linux**.

8) Redes Anónimas

Las redes anónimas o descentralizadas son redes informáticas que se ejecutan sobre Internet principal. Tienen sus propios sitios, foros, uso compartido de archivos y otros recursos web, pero no usan direcciones IP. El acceso a ellos se proporciona mediante software de código abierto que crea un túnel especial al Internet alternativo, cifra el tráfico y oculta la IP.

I2P, GNUnet, Bitmessage, RestroShare, Freenet, OneSwarm.

10 maneras de permanecer anónimo en línea

9) Anonimato Financiero

Hablando sobre cómo mantener el anonimato en Internet, también debería mencionarse las criptomonedas. Porque gracias a ellos, puedes hacer pagos en línea sin temor a que alguien se entere. Después de todo, las criptomonedas no están controladas por los estados, ni son análogos virtuales de unidades monetarias reales.

La criptomoneda es una moneda digital descentralizada, cuya emisión se produce a través de operaciones informáticas realizadas en los dispositivos de sus usuarios. Al mismo tiempo, la información sobre sus usuarios puede abrirse o cerrarse (a solicitud), y los datos sobre todas las transacciones se transmiten a todos los usuarios para garantizar la seguridad de la criptomoneda verificando estos datos.

10) Tarjeta SIM Adicional

Al registrarse en una red social, debes indicar tu número de teléfono o dirección de correo electrónico. Obtén una tarjeta SIM por separado para estos fines. Esto hace que sea mucho más fácil y seguro confirmar o restaurar el acceso a las cuentas. No publiques ese número de teléfono en ningún lugar y no se lo des a nadie.

Palabras Finales

En resumen, vale la pena señalar que las soluciones anteriores permiten, en un grado u otro, proporcionar acceso anónimo a Internet y asegurarlo.

Al tomar medidas de seguridad relativamente simples y al mismo tiempo suficientes, puede aumentar significativamente el nivel de tu anonimato en línea, evitar el robo de información confidencial, recuperar el acceso a los recursos bloqueados por el proveedor y protegerse de los anuncios intrusivos.

Usa Internet al máximo y cuídate.

- Alexgeeks

Descargar más recursos