Three security steps prevent Internet providers from tracking you

But if you want your ISP to stand up for advertisers, here are three easy steps you can take right now.

Recently, the US Senate has approved allowing Internet service providers to sell web access history and other data to third parties. This action has not yet been approved by the White House but if this is actually done, it means that those who are interested in privacy will have to protect themselves against data collection from their ISP.

Some privacy-conscious people have started working on this but many are not. But if you want your ISP to stay out of advertisements for advertisers, here are three simple steps you can take right now.

Use HTTPS Everywhere

The Electronic Frontier Foundation's add-on HTTPS Everywhere is one of the first tools you need to install. This extension requires all web connections with your browser to use SSL / TLS encryption. This means that the content you are viewing will be protected from passive storage by your ISP. The extension does not require HTTPS when the page you are connecting to does not support the protocol.

This extension starts working as soon as you install it. However, it will not prevent ISP from seeing the pages you visit. Only your contact content will be protected. So ISPs will know every time you visit YouTube, but you can't see what content you have viewed there or the specific pages visited.

HTTPS Everywhere is available for Firefox (desktop and Android), Chrome, and Opera.

Using virtual private network for a fee

The next step to do is to register a virtual private network service for a fee because they will keep all your information, not the free service that collects and sells your data to third parties for analysis. or used for advertising. You will need to spend about $ 40 to $ 60 a year for a VPN to store your data in private mode.

VPN is like an encrypted tunnel between users and the Internet. You connect directly to your VPN (the connection will see your ISP) then all Internet browsers go through the VPN server and block third parties from monitoring. Once selected and set up VPN configuration, set it to start automatically and put all your Internet traffic in it.

Choosing VPN should be a bit tricky because you need a provider to collect and store a minimum amount of data about your browser. Freedome VPN is committed not to record your traffic and is run by F-Secure, a reputable provider in the field of Internet security. In addition, some VPN providers also have useful extras, such as an Internet connection blocker that immediately prevents computer access to the Internet as soon as your VPN is disconnected.

In the next step, we will prevent DNS leaks.

Adjust DNS

DNS (Domain Name System) is a way for a computer to translate a website's name so that people can read it, such as NYTimes.com to a computer-friendly Internet Protocol address. It is like the phone book of the Internet.

The problem is that PCs are often installed to use DNS for ISPs, meaning your ISP will see all your browser requests. VPNs often configure the PC to use DNS, and it is often a DNS leak protection feature that prevents the computer from bypassing VPN and using the default DNS settings.

However, to make sure that you don't use ISP's DNS, the best way is to install a PC using a third-party DNS provider such as OpenDNS.

Summary

Now you have started protecting your data from ISP spies. Although it is not easy to do that, you have taken some important steps. When installing, refer to IPLeak.net or DNS Leak Test to ensure you do not disclose any unwanted data.

Now all you need to do is expect ISP not to block or control your traffic whenever you use paid VPN.

You finished reading the article "**Three security steps prevent Internet providers from tracking you**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com