

How to stay anonymous on the Internet?



If you are concerned about the privacy on the web. Then anonymous browsing is the best thing for you, Surfing the web without being tracked, you should definitely take a close look at the [Tor Browser](#).

The browser makes use of the Tor network to anonymize web browsing by connecting to the internet in a way that encrypts your connection, while also bouncing it around the internet via a series of relays run by volunteers all around the world.

Each Tor relay handles the task of decrypting one layer of encryption and then passes the data on to the next relay. When the data reaches the final relay, it decrypts the innermost layer of encryption and sends the original data without revealing the source IP address.

Websites can track your IP address, detect your geographical location and identify your device, operating system and even which browser you're using.

This offers protection against any sites you visit learning your actual IP address and location. It also allows you to access sites which may usually be blocked.

It should be noted that the Tor browser does not protect all of your internet traffic. Instead, it only protects the traffic sent through the browser. While other apps can be configured to use the Tor network, that is beyond the scope of this article.

While Tor does an excellent job of anonymizing your internet connection, there are still some rules you'll need to observe to protect the data you send and receive.

1. If possible, only connect to websites via SSL/TSL encryption (HTTPS).

If you access an unencrypted site, it is possible that your online activity could be monitored by the party running your Tor exit relay.

Luckily, the Tor browser has the HTTPS Everywhere add-on installed out of the box, which should take care of things - at least for websites that support HTTPS.

2. Don't enable or install any browser plugins.

The Tor Browser will automatically block plugins such as Flash, Quicktime and others. They can be used to reveal your real IP address.

3. Do not open any documents downloaded via the Tor browser while online.

Documents you download from the internet, such as Word documents or PDF documents, may contain resources that will be downloaded outside of the Tor browser when viewed. This could reveal your actual IP address.

Tor strongly recommends viewing such documents only when disconnected from the internet.

In addition to randomizing your IP address, the Tor browser also offers other protections. By default, the browser routes all searches through [DuckDuckGo](#), the search site that does not track you in any way - unlike Google or Microsoft's Bing search sites.

The Tor browser is also self-contained and lightweight, making it perfect for putting on a USB stick to use whenever you'd like, with no installation required.

It should be noted that the Tor browser is likely not a candidate for your daily driver browser, unless your daily needs include anonymous browsing.

The Tor network's methods of anonymizing your IP address does have a tendency to slow things down, so don't expect the same snappy internet experience you get with Chrome or Firefox.

Keep in mind that while the Tor browser also allows you to gain access to some of the, um, seedier parts of the web, it in no way protects you from any viruses or other malware you may encounter on your travels. So, be sure to practice safe browsing.

See Also -

- [**Hottest Careers In The World | 2018**](#)
- [**7 Must-Watch Inspirational Movies For Entrepreneurs**](#)



<https://www.tipslake.com/>

TipsLake is the best source of useful tips on topics like Health, Productivity, Technology, Internet, Fitness & Home medications etc. TipsLake not only provides tips, but also gives suggestions, solutions and provide ways for many problems that can be cleared with small efforts.