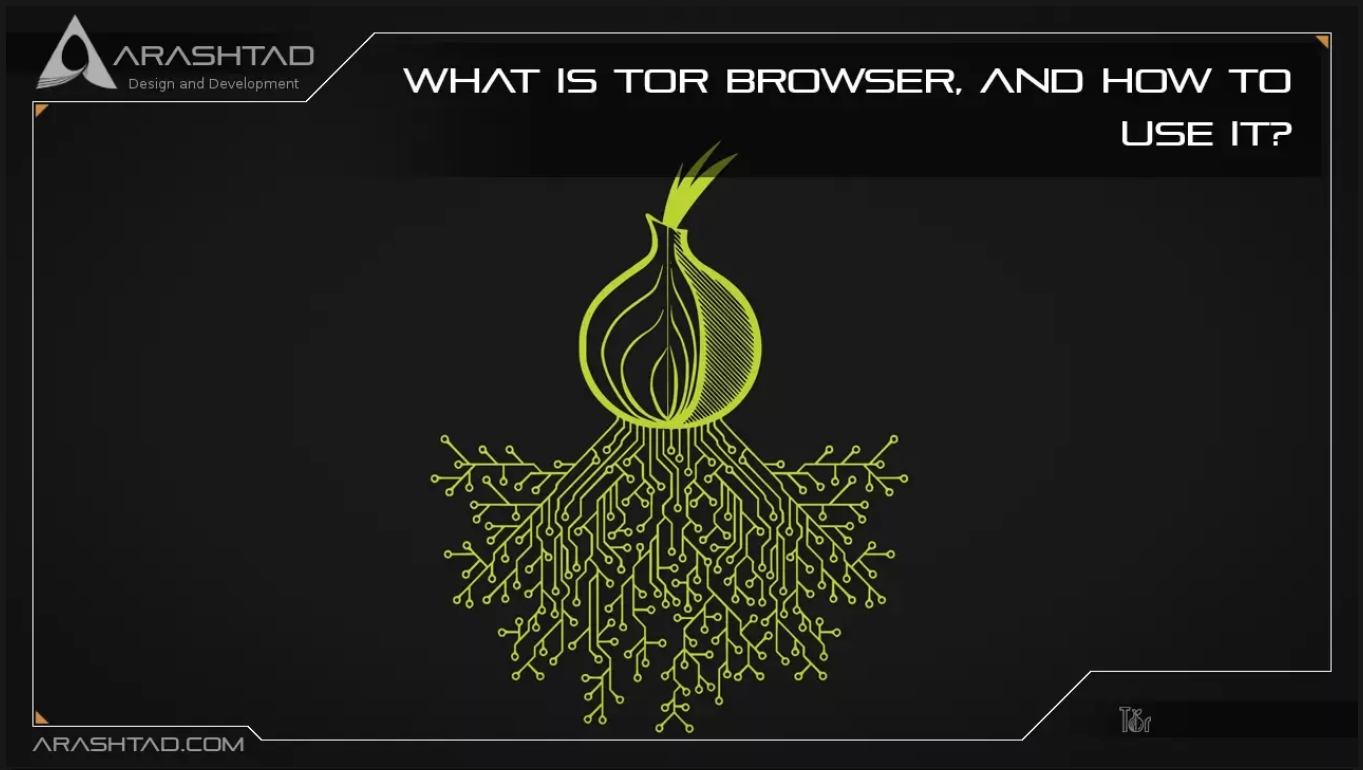
What Is Tor Browser, and How to Use it?

No comments



Today's Tor Browser offers the best anonymity on the web, and researchers are constantly working to improve its anonymity features. The Tor dark web browser lets you access the unindexed part of the internet known as the dark web. But how does it work, and is it safe? In this article, you learn about the Tor browser and its pros and cons.

Tor Browser Definition

An open-source privacy network, Tor—short for Onion Routing—enables anonymous web browsing. It uses secure, encrypted protocols to protect the privacy of users online. In the Tor network, users' digital data and communications are shielded by layers that resemble the layers of a nested onion. As part of the U.S. Navy's efforts to protect sensitive government communications, Tor was initially developed and solely used. However, it has been made available to the public as an open-source platform, meaning that its source code can be accessed by anyone. Tor's source code is upgraded and enhanced by volunteer developers within the Tor network.

Tor Browser and the Dark Web

A lot of people associate Tor with the dark web - an unindexed part of the internet that is accessible only with certain browsers. The connection between Tor and the dark web began with Silk Road, the first dark web marketplace where drugs and other illegal items could be purchased. Tor was the only way to access the notorious online marketplace when it was in operation.

Tor's anonymity features appeal to dark web participants. Although the dark web is more than just a haven for illicit activities, criminals like to use the onion browser to access it. While Tor was not designed with criminality in mind, or to be used as the "dark web browser", it is a legitimate and effective online privacy tool used by many people who value their online privacy.

Who Uses Tor and Why

Despite Tor's illicit reputation, many Internet users are using it for legitimate reasons. Here's a closer look at who uses Tor and why:

1. Government agencies: Tor can be used to protect sensitive government data and share it securely.

2. For-profit enterprises: Using Tor can increase privacy and security for businesses.

3. Illicit organizations: Criminals sometimes hide their online activities using Tor.

4. Private individuals: Users of the this browser can benefit from better online privacy and cybersecurity. Journalists, activists, and people facing censorship may use Tor as a way to communicate online.

How to Use Tor

To use Tor's privacy and security features, you need to install it. You can download Tor from the Tor website. You should have an Internet connection and a compatible operating system to do so. The Tor browser is installed just like any other app on your device. You can view tutorials to learn how to use it. While Tor lets users customize their privacy settings, the standard settings are generally considered sufficient for most users. Modifying Tor to be more secure can affect certain websites' functionality.

How Tor Works

In Tor, web traffic is rerouted and encrypted through the onion network, after it has been secured inside multiple layers of encryption. Your data is transferred through a series of nodes, called onion routers. The routers peel away layers of

encryption until the data reaches its final destination. Three layers of international proxy servers make up the Tor circuit that anonymously transmits encrypted data. Let's take a closer look at each layer:

1. Entry/Guard node: Your data is first introduced into the Tor network by a publicly known entry node.

2. Middle nodes: Data is encrypted here. It's then decrypted by a series of middle nodes. Each middle node knows only the identity of the node that preceded it.

3. Exit node: Once the last layer of encryption is peeled off, data will leave Tor via the exit node to reach its final destination.

The Tor Browser encrypts and decrypts web traffic through an entry node (blue), a middle node (green), and an exit node (orange).

Does the Tor Browser Hide Your IP Address?

By using onion routing technology, this Browser conceals your IP address from network surveillance and traffic analysis extremely well. As well as relaying your data through network nodes to hide your location and identity, onion routing protects your data even further with multilayered encryption. When internet traffic reaches its destination, its origin is wholly obscured because Tor-encrypted data is "peeled" through over 7,000 independent network relays before it is fully decrypted. With this elaborate process, Tor protects your data and hides your IP address from websites, your internet service provider, and even the government.

Is Tor Browser Anonymous?

While Tor Browser hides your location and browsing activity, it also has limits. Your ISP can still see that you are using Tor even though they are not able to see your browsing activity or Tor-encrypted data. You can also be identified if you log into an online account or provide details to a website while using Tor.

Image source: tor.stackexchange.com

What Is Tor Browser and How to Use it?

Is Tor Browser Legal?

Most countries allow the use of this Browser, although it may be stigmatized due to its association with dark web criminality. Although it has a sometimes shady reputation, the dark web is host to many legitimate resources like dark web Wikipedia, secure email services, and research databases. Providing you are not involved in illicit activities, it is not a crime to protect your privacy on the dark web.

Tor can still draw undue attention to your web activity—which could be counterproductive if you're trying to maintain

your privacy. Your ISP may slow down your connection and even contact you if you use Tor. And your government may also monitor your activity if you use Tor. It is illegal to use Tor in some countries. China bans anonymous browsing - making it illegal to use Tor. Russia and Venezuela actively try to prevent their citizens from using Tor. You should first check if Tor or VPNs are legal in your country if you are interested in anonymous browsing.

Is Tor Browser Safe?

In general, Tor is considered safe and secure due to the onion routing protocol that hides your IP address and encrypts your data. Tor, however, does have some vulnerabilities, and Tor users remain vulnerable to online threats, like malware and phishing scams. To safely use Tor, you need to use it along with other cybersecurity tools, so set up a VPN to take advantage of end-to-end encryption. Install firewalls and antivirus software to protect your network.

The Disadvantages of Tor Browser

Despite Tor's sophistication, it has several disadvantages - some of which counterbalance its cybersecurity advantages.

Slow Speeds

In Tor, web traffic is encrypted and routed through network nodes – this is good for privacy, but the elaborate process results in slow speeds. Even though there are ways to speed up Tor, you cannot significantly boost its speed.

Stigma

The Tor browser has acquired the unfortunate stigma of being illegal on the dark web. ISPs and governments may monitor their users. For those seeking privacy, Tor may cause the opposite effect.

Blocking

Tor is often blocked by network administrators. Some websites also monitor and block Tor exit node traffic. Tor bridges or VPNs can mask node usage.

Vulnerabilities

Despite Tor's anonymity features, the onion network is vulnerable at its entry and exit points. Since internet traffic is not encrypted at these points, your data could be an interception and your IP address could be discovered.

Conclusion

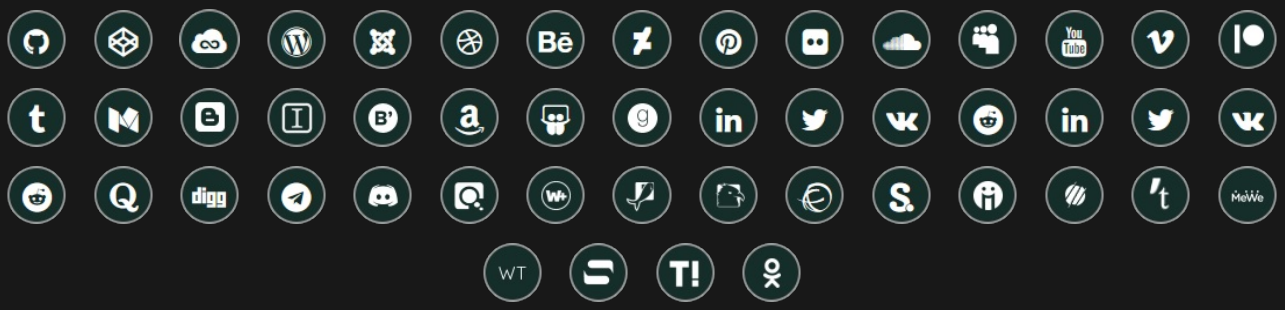
You may want to use Tor and the Tor Browser if you wish to protect your privacy and anonymity online as much as possible. Tor offers access to a wide range of services, including avoiding surveillance and censorship from internet service providers and government agencies. It is widely used and well-studied. Onion hidden services, which are used for avoiding oppressive regimes (and, occasionally, less-noble activities as well).

There are several security and privacy concerns you need to consider when using Tor effectively, as outlined earlier in this article. To keep your browsing anonymous, you may need to take aggressive measures, some of which can make browsing inconvenient based on your threat model – which potential threats you want to be protected against.

Join Arashtad Community

Follow Arashtad on Social Media

We provide variety of content, products, services, tools, tutorials, etc. Each social profile according to its features and purpose can cover only one or few parts of our updates. We can not upload our videos on SoundCloud or provide our eBooks on Youtube. So, for not missing any high quality original content that we provide on various social networks, make sure you follow us on as many social networks as you're active in. You can find out Arashtad's profiles on different social media services.



Get Even Closer!

Did you know that only one universal Arashtad account makes you able to log into all Arashtad network at once? Creating an Arashtad account is free. Why not to try it? Also, we have regular updates on our newsletter and feed entries. Use all these benefitial free features to get more involved with the community and enjoy the many products, services, tools, tutorials, etc. that we provide frequently.

SIGN UP | NEWSLETTER | RSS FEED