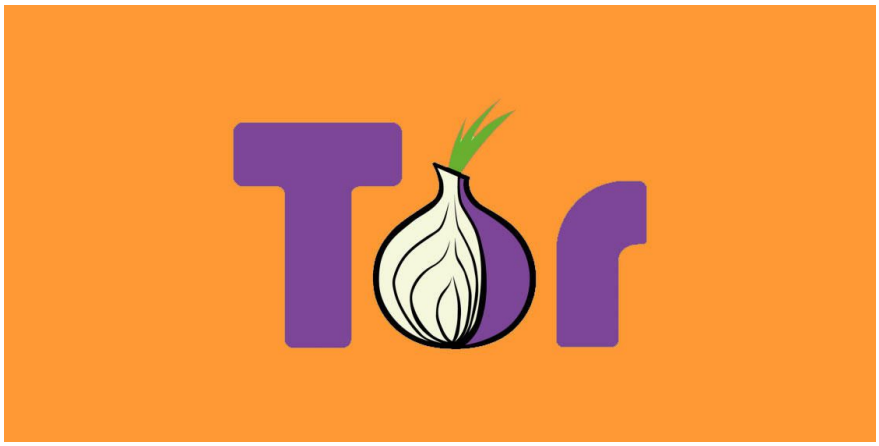
What is Tor? Your guide to using the private browser

We've got a beginner-friendly explainer on this privacy and security tool for online browsing, and how it works with VPNs.

If you're new to internet privacy and security, you've still probably already read references to something called Tor -- a widely hailed piece of internet-connected software with its own internet browser. Tor is embraced by privacy aficionados for its reliable encryption and its history of covering users' internet tracks.

At first glance, the terminology around Tor can seem intimidating and alien. Don't worry, though. It's simpler than it seems.



Here's everything you need to know about Tor.

What is Tor?

Back in the mid-'90s, when the US Navy was looking into ways to securely communicate sensitive intelligence information, a mathematician and two computer scientists emerged from the Naval Research Lab with something called "onion routing." It was a new kind of technology that would protect your internet traffic with layers of privacy. By 2003, The Onion Routing project, acronymed Tor, was in the hands of the public, where its vast network of users -- the engine enabling Tor -- has since continued to grow.

Today, thousands of volunteers all over the world are connecting their computers to the internet to create the Tor network by becoming "nodes" or "relays" for your internet traffic.

At a basic level, Tor is a type of internet-connected network with its own internet browser. Once you connect to the internet with the Tor browser, your internet traffic is stripped of its first layer of identifying information as it enters the Tor network, and is then sent bouncing through those relay nodes, which serve to encrypt and privatize your data, layer by layer -- like an onion. Finally, your traffic hits an exit node and leaves the Tor network for the open web.

Once you're in the Tor network, it's nearly impossible for others to track your traffic's manic pinballing path across the globe. And once you leave the Tor network via an exit node, the website you view (assuming it has HTTPS in front of its address) isn't sure which part of the world you're hailing from, offering you more privacy and protection.

How do I use Tor?

Normal web browsing is easy with Tor. Head to the official site and download the Tor browser. Follow the installation instructions as you would with any other program. When you open Tor for the first time, the program will ask you to either configure your connection (if you're in a country where Tor has been banned, like China or Saudi Arabia) or simply connect. Once you click connect, Tor may take a few minutes to find a set of relays to connect you through.

But once you're in, you can use Tor just as you would any other browser. You'll also be prompted to review your Tor browser security settings. If you're aiming for maximum privacy, I'd advise leaving the settings on their default selections.

If you start experiencing slower-than-normal speeds, you can nudge Tor into action by checking for a quicker connection path to the website you're trying to view. In the top right corner of the Tor browser, click the three-line menu icon and select **New Tor Circuit for this Site**.

The privacy-focused Brave browser also has an option to route traffic through Tor when inside a private window.

Are there any downsides to using Tor?

Because Tor is a volunteer-run network, speed can often be an issue. As your traffic moves from node to node, you're likely to notice more speed loss than you would, for instance, with most commercial virtual private networks. This becomes particularly noticeable if you try to watch streaming Netflix content over Tor or make voice-over-IP phone calls or video calls with an app like Zoom. Tor technology isn't necessarily built to provide seamless audio-video experiences.

Speaking of videos, there are also limits to the amount of privacy Tor can offer you if you enable certain browser media plugins like Flash. Likewise, your browser's JavaScript plug-in -- which enables you to view a lot of websites' embedded media -- can still leak your IP address information. Torrenting files with Tor also exposes you to privacy risks. Because of these risks, Tor's privacy settings have these kinds of plug-ins disabled by default.

If you're just looking to do general, daily internet perusal using a browser that will better hide your traffic from spying eyes, Tor probably isn't the best choice due to its slow speeds and incompatibility with most embedded media. But if you're concerned enough about privacy around a particular topic of internet research (and you don't

have a VPN), Tor is probably the best choice for you.

Will Tor work with a VPN?

In some cases, yes. Most of the time, however, it takes some know-how to be able to configure your VPN's connection to work in harmony with Tor. If you don't get it right, you can risk making both Tor and your VPN ineffective when it comes to protecting your privacy. We recommend getting familiar with both types of software before marrying the two.

On the plus side, however, a successful combination of the two can be useful. While Tor protects your internet traffic, your VPN can be set to encrypt the internet traffic of any other applications running on your device in the background.

To investigate VPNs further, check out our beginner-friendly guide to all the VPN terms you need to know and our directory of the best VPNs of 2020.