TOR: Myths and Facts

Tor is a service that helps protect your anonymity while using the internet by obfuscating your online behavior and by obscuring your identity from unwanted surveillance by other users, governments, or corporations. When you use Tor, your IP address remains hidden, and it appears that your connection is coming from the IP address of a Tor exit relay, a computer on the Tor network which can be anywhere in the world. Tor also allows access to .onion services, which allow people to publish information or run web services while hiding their location.

Tor is comprised of two parts

- **Software** you can download that allows you to use the internet anonymously (Tor Browser)
- **A Volunteer network of computers** that make it possible for the software to work

MYTH: Tor is for criminals who want to make illegal transactions free from law enforcement's prying eyes.

FACT: Tor is and can be used by anyone who would benefit from online anonymity: people who do not want companies to market to them based on their browsing data, individuals who live in countries with censored internet access, journalists who need to protect their sources, or businesses that want to keep their strategies confidential. Without Tor, a person's IP address and browsing history can be tracked whenever they go online, and normal everyday internet use creates an absurdly detailed profile of their reading habits and rough location.

EFF

MYTH: Tor does not provide protection from U.S. government surveillance because it was developed by the U.S. military and is funded in part by the U.S. State Department.

FACT: The initial development of Tor was funded by the U.S. Navy, and the U.S. State Department currently funds Tor because the freedom-enhancing software is used to circumvent censorship in countries that block access to parts of the internet. However, there is no evidence that the software includes a backdoor, and the code has been audited to look for vulnerabilities. All Tor projects are completely open-source and transparent in their design and implementation.

MYTH: Tor will completely protect one's online activity.

FACT: The Tor software does not anonymize one's identity. It anonymizes where internet traffic originates. While the government has been able to exploit vulnerabilities in the software to target Tor users and identify some Tor-related traffic, leaked government documents revealed that the core Tor technology continues to be a barrier to mass surveillance. Indeed, according to the NSA, "Tor Stinks." If someone on the Tor network does not want their identifying information to be found online, then she should use encryption and discretion in her online communications and keep the Tor Browser up-to-date. Keep in mind that if you log into a website using the Tor Browser or fill out forms with personally identifying information, that website will be able to identify you and may know that you're using Tor. Similarly, keep in mind that your local network administrator or ISP can also see that you are using Tor, but not what you are using it for. However just using Tor alone may be enough to raise suspicion, especially if you are the only one using it.

MYTH: Tor is hard to use.

FACT: The Tor Browser is as easy to install and use as any web browser. The concern about difficulty may arise because the browser can access both the regular web that you're used to, as well as special ".onion" sites that only live on the Tor network. Unlike traditional websites, which have a public IP address, a .onion address is hidden, unique, and provides end-to-end encryption. These sites won't show up on a Google search.

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org