What Is Tor and How Does it Work?

The Onion Router (Tor) is a popular distributed network of global relays that provides anonymity against network surveillance and traffic analysis. Originally developed for the United States Navy, Tor is a free, open-source tool run by volunteers that helps users keep their browsing habits and physical locations private. Tor can be used for web browsers, instant messaging clients, mobile operating systems, and more.

Who Might Use Tor, and Why?

Tor has a diverse group of users around the world, although the United States and Western Europe make up the largest user base with the highest usage ratio. Tor users include military personnel, law enforcement officers, journalists, activists, and whistle-blowers, as well as businesses, family, and friends. At colleges and universities, faculty and researchers use Tor to protect their research and keep information confidential. Security professionals can use Tor to anonymously investigate websites or networks. Students may use Tor to prevent websites from tracking their browsing habits or for more sensitive communications.

The Benefits of Using Tor

The primary benefit of using Tor is to reduce the risk of network surveillance for an individual while providing the user with control over their privacy and the means to keep personal or sensitive information confidential when it is being transmitted from one place to another.

According to the Electronic Frontier Foundation (EFF) Tor on Campus page, some institutions contribute to the Tor Project by hosting Tor nodes, which helps expand and diversify the network and provide better anonymization for the general community of Tor users. (EFF also notes that some students may already be running Tor relays on campus.)

Risks to Consider When Using Tor

Although Tor provides users with anonymity, it should not be the only tool used for online privacy and security. This is especially true if Tor is used incorrectly or inconsistently, or software is not updated regularly. Tor users also need to understand that they can still be vulnerable to timing attacks, side-channel attacks, or traffic correlation attacks.

Some organizations do not allow employees to use Tor and choose to block or monitor Tor. Firewalls can be configured to block Tor relay servers using publicly available IP addresses and traffic patterns, but the list of IPs are constantly changing, which can make this approach challenging.

Tor is composed of volunteer-operated relay servers known as nodes. Network traffic enters Tor at an entrance node. This traffic bounces between a number of transit nodes before returning to the regular Internet at a server known as an exit node. Organizations running exit nodes should be aware that all Tor traffic exiting their node will appear to have originated on their network. This could result in interactions with law enforcement investigating illegal activities that were committed through the exit node. This could also present a challenge during any forensic investigations at an institution.
Additional Resources about Tor

- EFF: Tor on Campus
- Gizmodo: 7 Things You Need to Know About Tor
- MIT News: How to Stay Anonymous Online
- The University of Texas at Austin Center for Identity: Identity Theft and the Underground Economy

Sustain and Improve Your Privacy and Information Security Programs

The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs.