ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Defending Freedom on the Electronic Frontier eff.org

How to Help Protect Your Online Anonymity Using Tor

WHAT IS TOR?

Tor is free software and an open network that helps you to circumvent Internet censorship and aids in protecting your anonymity online. The Tor network provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

Who Uses Tor?

People use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like, if local Internet providers have blocked by them. Tor's hidden services allow users to publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses. Journalists use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization.

HOW DOES TOR WORK?

Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing your transactions over several places on the Internet, so no single point can link you to your destination. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination.

How Do You Get Started?

You can start by downloading the Tor Browser Bundle from https://www.torproject.org/download/download-easy.html.en. The Internet is much, much bigger than the Web, but many of us access websites, read our email, chat with our friends, and use social media through a web browser. Browsing the web using the Tor Browser allows you to do all of these things while protecting your privacy and anonymity.

Tor will encrypt your traffic to and within the Tor network, but the encryption of your traffic to the final destination website depends upon that website. To help ensure private encryption to websites, the Tor Browser Bundle includes the HTTPS Everywhere browser extension, developed by the Electronic Frontier Foundation, to force the use of HTTPS encryption with major websites that support it. However, you should still watch the browser URL bar to ensure that websites you provide sensitive information to display a blue or green URL bar or button, include **https://** at the beginning of the URL, and display the proper expected name for the website.

The Tor Browser will also block browser plugins such as Flash, RealPlayer, Quicktime, and others: they can be manipulated into revealing your IP address. Installing additional add-ons or plugins into the Tor Browser is not recommended because they may bypass Tor or otherwise harm your anonymity and privacy.

BEYOND THE BROWSER BUNDLE

The Tor Project has developed other tools to help you use the Tor network to protect your privacy and anonymity.

- Orbot is a Tor client for your Android phone: https://guardianproject.info/apps/orbot/
- Tails is a complete operating system that fits on a USB stick which is pre-configured with privacy and security in mind, which includes running all applications through the Tor network: https://tails.boum.org/
- Obfuproxy is an application that disguises your Tor traffic so that eavesdroppers cannot see that you are using Tor: https://www.torproject.org//projects/obfsproxy.html.en