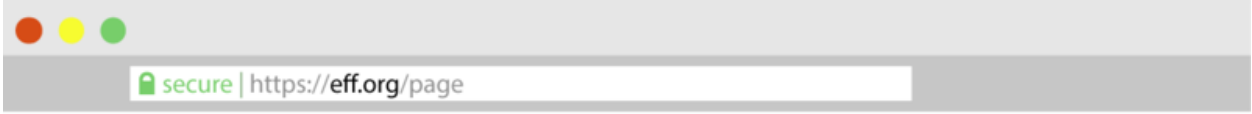
An Overview of Web Browsing Security

We use our web browsers to communicate, shop, get directions, research, and ask questions we are too embarrassed to ask a person. It's no wonder that "How do I protect my web browsing?" is one of the most common questions people ask when they start learning about digital security. The various methods for protecting your browser security can be confusing, and can work together in counterintuitive ways. Here we'll go over a few common, effective ways to protect your web browsing information, including their respective pros, cons, and differences.

HTTPS vs. HTTP



There are two ways for a website to get to your browser: HTTP and HTTPS. The difference is that "S," which stands for "secure."

When you see "https" and a little green lock next to the web page address in the top of your browser, that means you are using a secure connection. You have probably seen this when shopping online or entering credit card information. For a long time, website owners only offered HTTPS on pages that requested sensitive information like usernames and passwords or credit card numbers.

Now, however, the web is in the middle of a large shift to using HTTPS for *all* webpages. This is because HTTP lacks any meaningful security, and HTTPS comes secure by default. Webpages that come to you over HTTP are vulnerable to eavesdropping, content injection, cookie and credentials stealing, targeted censorship, and other problems.

If someone is spying on the network and trying to see what websites users are visiting, an HTTP connection offers no protection. An HTTPS connection, on the other hand, hides which specific page on a website you navigate to—that is, everything "after the slash." For example, if you are using HTTPS to connect to www.eff.org/ssd, an eavesdropper can only see "www.eff.org". With HTTPS, an eavesdropper cannot see what part of a website you're visiting.

VPNs

Virtual Private Networks (or VPNs) hide your Internet traffic all the way from your local computer to whatever VPN service provider you choose. Instead of traveling over your Internet service provider's (ISP's) connection, your traffic will pass through your VPN provider's servers. If someone is spying on your local network and trying to see what websites users are visiting, they will be able to see that you're connecting to a VPN, but will *not* be able to see what websites you are ultimately visiting.

Using a VPN essentially shifts your trust from your ISP to the VPN, so it's important to make sure you trust your VPN provider to protect your privacy.

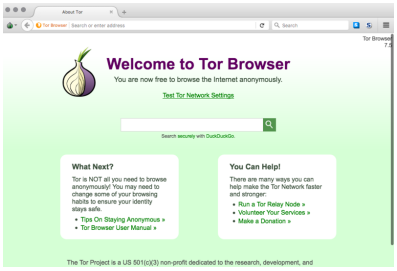
While using a VPN hides your traffic from your ISP, it also exposes all your traffic to the VPN provider itself. The VPN provider will be able to see, store, and modify your traffic. Using a VPN essentially shifts your trust from your ISP to the VPN, so it's important to make sure you trust your VPN provider to protect your privacy.

Although it's a common question at security trainings, recommending VPNs is a tricky task. It's generally better to explain how VPNs work and share key questions to ask rather than make a one-and-done tool recommendation. That's because VPN services are changing all the time, and it is hard to guarantee any privacy promises they make. Different VPNs also offer different pros and cons for different threat models, making it hard to choose the right VPN for a particular audience or individual. If you do share the name of a particular VPN, be sure to explain why you trust them. Has it been around a long time? Does it have a good reputation, and with whom? What makes you believe it will stick to the privacy promises it makes? What do you use it for—privacy protection, censorship circumvention, or something else?

Additional resources to learn about VPNs include That One Privacy Site's guide and TorrentFreak's 2018 VPN review.

Tor Browser

Tor Browser is an anonymous browser designed to protect your identity and location while browsing the web. Instead of connecting you directly to the website you want to visit, Tor will bounce you around a network of volunteer computers (called "**nodes**") on your way to your final destination. This bouncing around masks who you are and where you are connecting from. This makes it harder for people monitoring you to know what you are doing online, and harder for people monitoring certain sites to know who is using them and where they are connecting from.



The welcome page of Tor Browser.

It's important to remember that Tor will protect your privacy and anonymity *only* for activities inside Tor. Having Tor installed on your computer does *not* make other things you do on your device, like web browsing on another browser like Chrome or Firefox, more private or anonymous. It also does not hide the fact *that* you're using Tor. Your web navigation may be anonymous, but it will be clear that you're using the Tor software.

Tor also does not encrypt your web traffic—you'll need HTTPS for that. That's why it's key to visit websites that support HTTPS within Tor, so that the two can work together to give you both security and anonymity while you browse. This infographic demonstrates what kinds of information HTTPS and Tor protect separately, and what kinds information they protect when used together.