Security Best Practices - Part 2: Browsers

2. Browsers


Love them or hate them, browsers are an integral part of our online experience. There are four main browsers, Chrome, Firefox, Internet Explorer and Safari, each with their respective strengths and weaknesses but how well does each perform behind the scenes to protect your security and privacy? What can be done to improve security and privacy? Why are these things important?

We've opted to discuss the big four as browsers that specialise in security and privacy are often offshoots of these 4. This can be seen in examples such as [Brave](https://brave.com/) (based on Chromium), [Ice Dragon](https://addons.mozilla.org/en-US/firefox/addon/ice-dragon/) (based on Firefox) and [TOR Browser](https://www.torproject.org/) (based on Firefox).

It's entirely possible to run a standardised program with a few options altered to enhance your security and privacy and with the addition of a few plugins be as secure as using a dedicated and specialised program with the added bonus of frequent updates.

We've posted an analysis of the main browsers which can be viewed here. This features an overlook of Chrome, Firefox, Internet Explorer and Safari. In addition to choosing a browser, you can also add a number of features through extensions or add-ons which will further enhance your privacy and/or security.

Whilst we understand that a browser is a personal choice with people often using Chrome, we advise using a well maintained open source browser to ensure your privacy and security is kept as a priority.

*The following extensions can also be installed to further enhance your privacy and security:*

**HTTPS Everywhere**

HTTPS Everywhere encrypts your traffic over SSL encryption eliminating potential Man-in-the-middle attacks and eavesdropping. This means that visiting any sites allows you better security because the HTTPS Everywhere extension fixes these problems by rewriting all
requests to sites to use HTTPS even if the default is the HTTP protocol.

**Disconnect**

Disconnect disables over 2000 third party tracking sites that will record your browsing habits. As a result of blocking tracking cookies and code, sites load up to nearly a third faster and uses less data (which is great for people on metered connections).

**NoScript**

NoScript adds additional security by disabling JavaScript, Java and other executable content on all sites unless you give them permission (as simple as right clicking and choosing Allow or Temporary Allow). This prevents XSS (cross-site scripting) attacks, CSRF (router hijacking) attacks and clickjacking attempts. It also implements the DoNotTrack option as default.

**Self-Destructing Cookies**

Self-destructing Cookies automatically removes cookies when they're no longer used by an active browser. By removing unused cookies, you're removing potential lingering sessions and tracking information collected on your browsing habits. Self-destructing cookies also allows for automatic deletion of Evercookies by enabling 'Automatic Cache Cleaning' in the options.

**Bloody Vikings!**

Bloody Vikings! is an extension which allows for the easy creation of temporary email addresses which can be used during account creation to eliminate spam to your actual email address and improves your privacy. Once you start using it, you'll wonder how you did without it.

**Clean Links**

Clean Links is an extension which is used to convert "obfuscated" and/or nested links to genuine plain clean links. This removes any referrer or redirect links and sends you directly to where you want to go.

**Last Pass**

As described in Part One: Passwords, using a password manager is a secure way to operate online ensuring your passwords are hard to crack and your security and privacy is maintained to high standards. The LastPass extension allows for communication with the LastPass service in a secure and encrypted fashion. All encryption and decryption is handled locally (on your machine) so nothing of use can be intercepted or listened to.

For the sake of clarity and transparency, I personally use Firefox with the extensions named above.
Related Pages

- Security Best Practices