Security Best Practices- Part 2b: Browser Extensions

Travis - 2022-08-16 - Best Security Practices

Part 2B: Browser Extension

As we stated in Part Two: Browsers, we have opted to discuss the big four browsers that specialize in security and privacy, though there are many different offshoot browsers of these four. This can be seen in examples such as Brave(based on Chromium), Ice Dragon (based on Firefox), and TOR Browser (based on Firefox).

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

We've posted an analysis on a number of features through extensions or add-ons which will further enhance your privacy and/ or security on the four main browsers which can be viewed here. This analysis features an overlook of different Browser extensions and add-ons that can be used on Chrome, Firefox, Internet Explorer and Safari.

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 are kept as a priority.

Browser Extensions

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 use less data (which is great for people on metered connections).

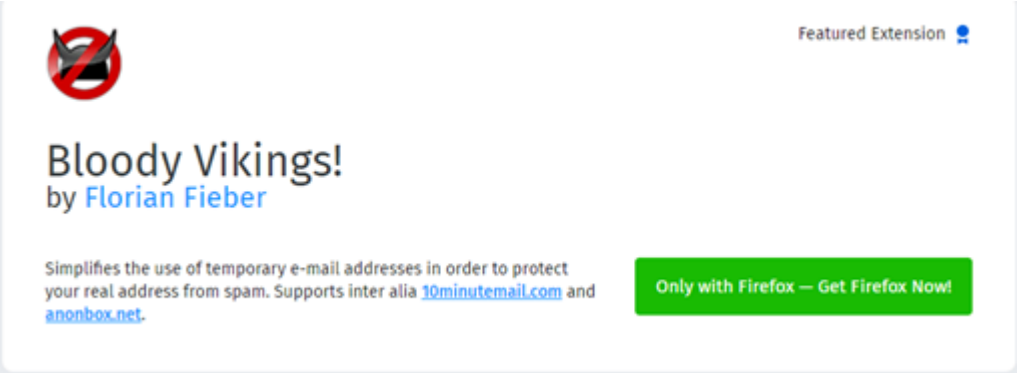
NoScript

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

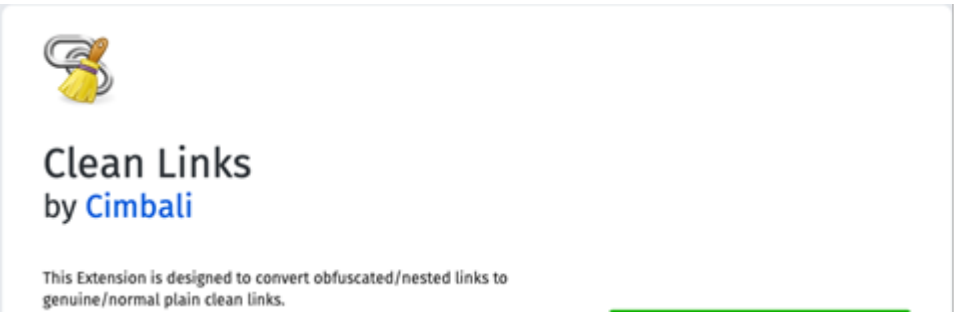
Self-destructing Cookies automatically removes cookies when they're no longer used by an active browser. By removing unused cookies, you're removing potential lingering sessions and tracking information collected on your browsing habits. Self-destructing cookies also allows for automatic deletion of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

Bloody Vikings!



Bloody Vikings! is an extension that 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.

Tags

Security