Security Best Practices - Part 2: Browsers

Travis - 2021-03-16 - Best Security Practices

Part 2: Browsers

TL/DR: Use an open-source browser with extensions such as HTTPS Everywhere, Disconnect, NoScript, Self-destructing Cookies, Bloody Vikings!, Clean Links, and LastPass (with 2FA)

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 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 of the four main browsers which can be viewed here. This analysis 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 (More information in Part Two: Browser Extensions.

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.

Chrome

- Developer: Google
- Open Source: No
- Update Frequency: 14 Days
- Security: Excellent
- Privacy: Poor

Background:
Chrome was launched in 2008 and is currently the most used browser with nearly 75% of people preferring to use it. Given the browser's reputation for speed and the prevalence of Google services in our lives, Chrome quickly became the most widely used browser.

Security:
Google has always been known as a leader for browser security. In addition to leading its competitors in update frequency and scanning for harmful downloads. Google also automatically updates Chrome to the latest version, ensuring its users are always enjoying the latest security improvements and browsing features. The latest version of Chrome also boasts the security test score and is only matched by the Chrome mobile version.

Privacy:
While the browser does offer the usual pop-up blocker and allows users to send a "Do Not Track" request along with their browser traffic, one simply cannot ignore that Chrome belongs to the company that makes millions from knowing everything about you. And although there are ways around this, it doesn't change the fact that Google is using Chrome to learn about you and then monetizing that information. Furthermore, since Chrome is a closed-source browser, it means that the source code is not able to be inspected to ensure that nothing is hidden in the code.

Firefox

- Developer: Mozilla Foundation
- Open Source: Yes

- Update Frequency: 28 Days
- Security: Excellent
- Privacy: Excellent

Background:
Of all the browsers featured in this ranking, Firefox is the only one that is developed by a nonprofit organization. The browser is well known for its customization options and has long been a favored alternative to Chrome and Internet Explorer. The TOR Browser is based on Firefox due to its open-source code, security, and privacy options.

Security:
Firefox offers a suite of security features that any internet user will appreciate: malware protection, blocking reported attack websites/web forgeries, and warning users when a site is trying to install add-ons. While it is still a step behind Chrome in this area, the difference is tiny. Firefox users can take solace in knowing their preferred browser is one the most secure offerings around.

Privacy:
Firefox was the first browser to introduce the 'Do Not Track' feature. Although a revolutionary feature when it was first introduced, this is now standard across major web browsers and still requires ad networks to honour the user's wishes to not be tracked. In keeping with the times, Firefox now also features 'Tracking Protection', allowing users to subscribe to tracking protection lists and protect themselves against cookie-dumping by third parties. Most important of all, Firefox is the only major web browser that is open-source. This means anyone can examine Firefox's source code, making sure there are no elements hidden in the source code.

Please Note: By default, Firefox is configured to run on a single processor. Enabling Multi-Processor support will result in a faster Firefox experience but this is not supported by Private Internet Access and may result in bugs and conflicts with add-ons.

To Enable Multi-Processor In Firefox:

1. Type about: config into the address bar and press Enter
2. Right-click any option and choose New --> Boolean
3. Type browser.tabs.remote.force-enable and press Enter
4. On the next screen select True and click OK
5. Type about: support into the address bar and press Enter
6. Check if Multiprocess Windows is enabled. If it is, success!

Internet Explorer

- Developer: Microsoft
- Open Source: No
- Update Frequency: 30 Days
- Security: Average
- Privacy: Average

Background:
Before the release of Chrome, Microsoft's Internet Explorer had a virtual monopoly on browser market share. Internet Explorer has taken a back seat to its Google rival but there is still a sizeable user base for Internet Explorer, at least for purposes of downloading Chrome on a new PC.

Security:
While it has made large strides to improve its security features, Internet Explorer's legacy will always include being one of the less secure browsers available. The browser also has adjustable security levels that allow users to beef up their online protection however the browser has yet to rise above and lead its competitors in terms of security.

Privacy:
Internet Explorer allows you to toggle pop-up blockers and send a 'do not track' request to both the sites you visit and the third parties whose content is featured on those sites. Internet Explorer features a 'Tracking Protection' feature that lets you subscribe to tracking protection lists. The browser will then prevent listed sites from dropping cookies onto your browser. Again, Internet Explorer is a closed source browser, so there's no telling what other sorts of surveillance widgets might be packaged into the browser itself.

Safari

- Developer: Apple
- Open Source: No
- Update Frequency: 58 Days
- Security: Excellent
- Privacy: Excellent

Background:
The name Safari may be foreign to most Windows users, but Apple's own web browser was actually featured on PC until 2012, after which it became available only on Apple devices. And although Safari is the default browser for Mac, it has largely suffered the same fate that befell Internet Explorer and is mainly used to download Chrome.

Security:
Although Safari doesn't upgrade often, it does a good job of protecting you while you use it. Safari prevents suspicious sites from loading and alerts you of the potential danger. By running web pages in separate processes, Safari prevents malicious code in one page from affecting the entire browser or accessing your data.

Privacy:
Safari also does quite well in terms of maintaining your online privacy. Like its peers, users can tell Safari to send a 'Do Not Track' request along with their browsing traffic. The browser also prevents third-party sites from leaving data in your cache by default, helping you stay anonymous online. However Safari is also closed source and it's "Do Not Track" requests do not necessarily guarantee privacy.

For more information about Browsers and their Extensions and Add-ons please continue on to Part Two B: Browser Extensions.

Tags
Security