Browser Security [1]

Key Actions

Always run an up-to-date version of your web browser. Use Qualys’ BrowserCheck [2] to confirm your browser, plug-ins and system are patched.

Browser Privacy Settings - Vendor information regarding browser privacy settings.

- Chrome [3]
- Firefox [4]

Tips for safe Internet browsing

Exploiting browser vulnerabilities has become a popular way to compromise computers. There are several easy ways to secure your preferred browser, through individual browser settings and add-ons. Browsers aim for a balance of performance and security. Features added by the manufacturer to improve performance may make the browser (and the computer) less secure. In addition, the more add-ons you have installed, the more your browsing experience may be impacted or slowed.

Best Practices

1. Install and use an ad blocker such as AdBlock Plus [8] or uBlock Origin [6] (for Chrome [7] or Firefox [8]). It's best to use one or the other not both.
2. Do not use the "remember my password" function of a browser or website. Instead, use the LastPass password management service [9] (premium version available free to all Duke faculty, staff and students). Download LastPass [10] install it and create an account, the activate the premium version available at Duke’s LastPass page [11]. To remove data that may have already been saved see: Chrome [12] and Firefox [13].
3. Ensure the pop-up blocker in your browser is enabled (instructions available for Chrome [14] and Firefox [15]).
4. Consider private browsing using Chrome Incognito mode [16] or Firefox private browsing [17]. These options are starting to be available for mobile browsers as well. Firefox has created Focus [18] as a privacy focused browser.
5. If you have Adobe Flash or Oracle Java plugins installed, consider uninstalling them. Many content providers have moved away from these platforms due to ongoing security issues with both. If you need Flash, it's built into Chrome. If something needs Oracle Java,
remember it needs to be updated on a regular basis. They continue to be two of the top programs leveraged by malware to compromise computers.

For advanced users

The items listed below will add additional security to your web browsing, but from time to time may need adjusting for a site to function. You should read what these extensions do, and research each before deciding if they are the right tools for you. They may be available for other browsers, we've only provided links for Chrome and Firefox here. Users should be comfortable with managing Chrome extensions [19] and Firefox add-ons [20] as a prerequisite to using any of the items in this list. Extensions also add to the overall resource use by your browser. Mobile users will find some of these have App corollaries as well.

1. NoScript Firefox [21] only - Allow active content to run only from sites you trust, and protect yourself against XSS and Clickjacking attacks, "Spectre", "Meltdown" and other JavaScript exploits.
2. UMatrix Chrome [22] and Firefox [23] - Point & click to forbid/allow any class of requests made by your browser. Use it to block scripts, iframes, ads, facebook, etc.
3. IP Whois & Flags Chrome [24] and Firefox [25] - Displays server's location of all websites, and provides Geo location and WHOIS info on toolbar click
4. Privacy Badger Chrome [26] and Firefox [27] - Protects you from trackers as you surf the web.
5. Ghostery Chrome [28] and Firefox [29] - A powerful privacy extension. Block ads, stop trackers and speed up websites. Creating an account allows settings to be shared between machines and browsers.
6. Web of Trust [30] Chrome [31] and Firefox [32] - Instantly know which websites to trust! WOT protects you while you browse, warning you against dangerous sites that host malware, phishing, and more. Creating an account allows settings to be shared between machines and browsers. Can use a users Google credentials for login.

Source URL: https://security.duke.edu/browser-security

Links
[1] https://security.duke.edu/browser-security
[3] https://support.google.com/chrome/answer/114836?hl=en&amp;co=GENIE.Platform%3DDesktop
[9] https://security.duke.edu/news-alerts/privacy-tips-windows-10
[12] https://support.google.com/chrome/answer/95606
[14] https://support.google.com/chrome/answer/95472?co=GENIE.Platform%3DDesktop&amp;hl=en
[16] https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&amp;hl=en