BROWSER REFERENCE DOCUMENT

Essential reference document for all workshops and activities related to the browser.

Contents

1. Comparing browsers

Increasing privacy in your browser can be done at several levels, but the first step is to decide which browser to use when you access the internet.

Chrome

Benefits

- Security: Chrome is among the best browsers out there.
- Flash is built in and automatically updated, which means that vulnerabilities are kept to a minimum (note however that security studies of Chrome were funded by Google in 2011, and a lot has changed since then).
- "Incognito Mode": Easy-to-use browsing 'mode' that prevents Chrome from saving your browsing history.
- Anti-tracking: Best selection of third-party ad- block solutions (close behind Chrome)

Limitations

- Privacy: Google makes most of its money through advertising. For this they use information they collect through their services, including Chrome, to find out what you do, where you are, what you buy, etc.
- Default settings: On Android, users are not able to change these.
- Not open source.

Firefox

Benefits

- Proven commitment to security, with a highly-paid bug bounty programmes.
- Has an easy to use Private Browsing mode, and privacy settings can also be customised.
- Anti-tracking: Great selection of third-party ad-block solutions (close behind Chrome).
- SSL certificate revocation: handles this better than any other browser.

- Data protection is a key issue: corporate manifesto states, "individuals' security and privacy on the Internet are fundamental and must not be treated as optional."
- The source code is available (Firefox is the only browser that is fully open source).
- Non-profit: Firefox is developed by Mozilla, a non-profit organisation that produces free, quality software. This means that the browser is not being used as part of larger profit-making agenda.
- New Private Window": Easy-to-use browsing 'mode' that prevents Firefox from saving your browsing history, and offers some protection against trackers.

Limitations

- Security still not as high as Chrome.

Safari

Benefits

- Security: Good choice for OSX. Good reputation for security and is an early adopter of new features.

Limitations

- Not fully open source.

Opera

Benefits

- Security: Known to adopt some new security features before others, and has a good reputation for patching security vulnerabilities faster than the others.

Limitations

- Completely closed source.

Internet Explorer

Limitations

- Worst reputation for security. (But if you use version 10 or greater, you can avoid the worst problems).
- Malware: Has the highest detection rate of malware.
- Security: There have been a lot of severe vulnerabilities exposed in its programming over the years.
- Completely closed source (and Microsoft has collaborated with the NSA).

2. Search engines

Privacy-friendly alternatives to Google Search or Bing:

- DuckDuckGo - https://myshadow.org/duckduckgo
- Searx - https://myshadow.org/searx
- StartPage - https://myshadow.org/startpage

3. Hands-On checklist: Browser

- Change your default search engine to one that respects your privacy.
- Change language to English (most widespread language - gives you a less unique browser fingerprint).
- Install Firefox and adjust settings: automatically clear all history, never accept third party cookies and clear history when Firefox closes. Find step-by-step instructions here: https://myshadow.org/how-to-increase-your-privacy-on-firefox
- Set cache disk to 0 MB: under menu --> preferences --> advanced --> network --> cached web content.
- Install plug-ins and add-ons. Find details here: https://myshadow.org/prevent-online-tracking.
- Log out of all commercial services like Gmail, Facebook and Twitter if you are not using them.

4. Tracking in the Browser: Visualisation tools

Trackography

Shows which third party trackers are present on media websites; the trace route from the website to the third party tracker servers; and the privacy policies of the most dominant trackers.

Lightbeam

Shows in real time which third party trackers are included in the websites the participants visit; draws connections between third party trackers across websites (e.g. Google Analytics).

5. Privacy and Security by Separation

This strategy involves increasing your privacy and security by using different browsers for different things - e.g. to use only Google services in the Chrome browser, Facebook in another browser, and do your normal browsing in Firefox.

6. Browser fingerprinting

A browser fingerprint consists of a detailed set of information about your device, font size, pixel, screen size, language, type of operating system, time zone, and whether cookies are enabled, among other things. The combination of these elements allows your device to be uniquely identified.

Panopticlick (https://panopticlick.eff.org/) allows you to test how unique your browser fingerprint is.