# 10 Ways to Make Web Browsing Faster and Safer

*François Briatte*

*June 8, 2018*

This document is part of the "Computing Advice for Students" series. Specifically, it expands Tip #4 of "10 Computing Tips and Tricks for Students" ("Use a proper Web browser").

***Note*** – Since we start with security and privacy, an important thing to know is that using a secure browser on an *insecure* network makes you only marginally less vulnerable to attacks.

## 1. Choose your Web browser wisely

The rest of this document assumes that you are using Google Chrome, because it is likely to be more secure to alternatives like Apple Safari or Microsoft Internet Explorer, or even privacy-aware browsers like Mozilla Firefox and Brave.

Whatever browser you end up using, always keep it up to date, *with no delay*.

***N.B.*** Chrome supports many extensions, e.g. Google Docs Offline to use Google Docs, Sheets and Slides without an Internet connexion. Make sure, however, that you know what you have installed, from where and whom, in your `chrome://extensions`, and that you know which extensions will try e.g. to access your microphone and camera, such as appear.in (an alternative to Skype).

## 2. Use HTTPS Everywhere

Use HTTPS Everywhere to encrypt your Web connexions whenever possible.

***N.B.*** An encrypted *connexion* can still lead to an insecure *website* – do *not* assume that a website is secure just because it can be accessed via HTTPS.

## 3. Disable Flash

Flash is a highly insecure media plugin: go to `chrome://settings/content/flash` from within Chrome to inspect your Content settings, and make sure that Flash is blocked from running.

The panel opened by the address above can also be accessed by opening `chrome://settings` and by finding it in the 'Advanced' settings. Make yourself familiar with Chrome Settings panel right now.

***Related*** – Media autoplay is evil. Thankfully, Chrome now blocks some of it by default.

## 4. Use a password manager

Tip #5 of "10 Computing Tips and Tricks for Students" recommends that you use the Dashlane password manager, which will prevent you from saving passwords in your browser.

***N.B.*** Make sure to protect your password manager with a long, random passphrase, and remember the following paragraph from Tip #5:

> Your passwords do not protect you against network attacks: *never* log on to a sensitive website, such as one that stores your credit card details, from an insecure connexion like airport or hotel Wi-Fi.

## 5. Use a blocker

Web browsing will expose you to a virtually infinite amount of undesirable ads and trackers that will put both your security and your privacy at risk. For those, you need a 'blocker' extension.

The most efficient blocker is uBlock Origin. If you are using another blocker like Adblock Plus or Disconnect, remove it and use that one instead.

On top of that, you might also want to consider adding:

- Privacy Badger, to block trackers that uBlock might have missed
- Decentraleyes, to block tracking via content delivery networks

## 6. Erase your past Web sessions

Your Web sessions are going to leave traces on your disk. Limit those:

- Use Limit History Lifetime to make your Web history last only a few days.
- Use Vanilla Cookie Manager to allow cookies only on chosen (trusted) websites.
- Use Don't add custom search engines to do what precisely what its name says.

All extensions above are available for Google Chrome only.

***Note*** – Limiting cookies makes you less trackable and prevents some security issues, while also helping to stay logged out from (and hopefully, less engaged with) social media accounts.

## 7. Use browser tabs

Your browser works with tabs, which you can easily navigate through keyboard shortcuts. Pinning some of your browser tabs will help organising your work, and saving large collections of opened tabs helps save memory and segment your Web sessions into shorter periods.

Two recommendable extensions to handle tabs are

- OneTab, to save all opened browser tabs for later use
- Tab Pinner, to pin or unpin a tab via a keyboard shortcut

## 8. Focus on content

Reading long articles online, especially from media websites, can be tiresome due to the distracting layout and modal windows that those websites often run.

To get rid of those annoyances, install Mercury Reader and try it on this example article.

## 9. Save valuable content

Web content can easily be relocated or erased, with no guarantee that it will have been saved by the Internet Archive before disappearing.

If you are going to use the Web for research, use some backup tools:

- Archive.is and Perma.cc to save Web pages (as well as, for the latter, PDF files)
- Pinboard-fu, to access the Pinboard bookmark service via a keyboard shortcut
- Save It Offline and Video DownloadHelper to save videos and audio/video streams
- Tumblr, to publish all sorts of media to a blog

***Note*** – The services above have different user formulas: for instance, individual Perma.cc accounts are limited to 10 archived links per month, while paid Pinboard accounts will bookmark *and* save the content of Web pages. As for Archive.is, there is little information as to who runs the service, and why.

## 10. Go under the hood

Web browsing is built on a stack of technologies that can be fun to learn about and experiment with:

- Learn to use Chrome DevTools to inspect how Web pages work and what resources they load.

- Advanced Chrome controls, such as `chrome://discards` and `chrome://media-engagement`, can be accessed at `chrome://flags`. Some of them can be useful, e.g. to speed up Web rendering.
- If you know what you are doing, Tampermonkey is a great way to inject Javascript code into Web pages in order to run helper scripts. Use it *very* carefully, and disable it after use.

---

***Final note*** – The Markdown version of this document, which can be found in its repository, contains links to the source code of most (though not all) of the Chrome extensions recommended above.