Browser and Extensions

Browser – which one should I use?

We recommend **Mozilla Firefox.** These instructions refer to the desktop version of Firefox 70. The setting options and menu navigation in the mobile versions may differ.

- For GNU/Linux, Windows and macOS: https://www.mozilla.org/en-US/firefox/new/
- For Android and iOS: https://www.mozilla.org/en-US/firefox/mobile/
- In F-Droid [Android] as **Fennec F-Droid**: https://f-droid.org/en/packages/org.mozilla.fennec_fdroid/

Settings

≡ **Menu button** → ***Settings*** → ***General*** (Subsection ***Firefox Updates***): Deactivate „Automatically update search engines“

≡ **Menu button** → ***Settings*** → ***Search***: Add alternative search engine (e.g. startpage.com, MetaGer.de, Searx.me), deactivate ***Provide search suggestions*** and modify ***Default Search Engine***

≡ **Menu button** → ***Settings*** → ***Privacy & Security***:

Blocking page elements:

- Select **Custom (!! selecting means blocking)**
  - select ***Tracking content*** & ***In all windows***
  - select ***Cookies***: & ***All third-party cookies (may cause websites to break)***
  - select ***Cryptominers*** & ***Fingerprinters***
- ***Send Websites a „Do Not Track“ signal that you don‘t want to be tracked***: ***Always***

Cookies and Site Data:

- ***Delete cookies and site data when Firefox is closed***: activated

Logins and Passwords:

- deactivate ***Ask to save logins and passwords for websites***. (The password manager KeePassX is available for all common operating systems: https://www.keepassx.org/)
- deactivate ***Show alerts about passwords for breached websites***

History:

- Firefox will ***Use custom settings for history***
- *optional:* select ***Clear history when Firefox closes,*** see ***Preferences*** for details

Firefox Data Collection and Use:

- deactivate ***Allow Firefox to send technical and interaction data to Mozilla***

Security:

- deactivate **Block dangerous and deceptive content** (Google Safe Browsing) to avoid sending data to Google

Add-ons & Plugins

≡ **Menu buttons** → ***Add-ons*** → ***Extensions*** → search bar top right ***Search addons.mozilla.org*** → type name of add-on and press Enter (all add-ons can also be allowed for execution in private windows)

- **uBlock Origin** (by Raymond Hill) blocks ads and trackers
- **Decentraleyes** (by Thomas Rientjes) replaces JavaScript online libraries with local ones
- **HTTPS Everywhere** (by EFF Technologists) forces an encrypted connection to websites if available

- **Cookie AutoDelete** (by Kenny Do) deletes cookies automatically after browser windows and tabs are closed (the button Auto-clean must be enabled after installation)
- **NoScript** (by Giorgio Maone) blocks execution of external content and JavaScript (advanced users can enable restrictions globally in the settings and clear the white list)

Add-ons for advanced users:

- **Smart Referer** (by meh., Alexander Schlarb) removes referer, strict mode should be activated
- **uBlock Origin** (by Raymond Hill) in advanced mode, see preferences:
    - activate *I am an advanced user. (Required reading)*
    - activate *Prevent WebRTC from leaking local IP addresses*
    - activate *Block CSP reports*
    - activate *Block remote fonts*
    - if necessary activate *Filter lists* and activate missing entries concerning *Ads, Privacy* and *Annoyances*
    - for further settings see Mike Kuketz' blog: https://www.kuketz-blog.de/firefox-ublock-origin-firefox-kompendium-teil2 (German)
- **uMatrix** (by Raymond Hill) blocks all third-party requests

Adobe Flash Player:

- uninstall or deactivate (in case you should find ***Shockwave Flash*** in ≡ Menu button → ***Add-ons*** → ***Plugins***)

Check the effect of settings and add-ons:

- ≡ Menu button → **Web *Developer*** → ***Network*** shows all requests as a list when loading a website
- Test the browser fingerprint: https://panopticlick.eff.org/

Tor Browser

The Tor browser is a modified Firefox that browses the internet over the Tor network - privacy enhancements are already installed. Be careful: Additional add-ons or simultaneous use of a VPN can compromise anonymity! Further information and download at: https://www.torproject.org/

Please read the helpful documentation, as your anonymity in the Tor network depends primarily on your surfing behavior: https://www.torproject.org/docs/documentation.html.en

Miscellaneous

To see how privacy friendly a particular website is, the URL can be checked with the web service Webbkoll: https://webbkoll.dataskydd.net/

If you do not trust the ISP, you can setup your connection to use the data protection-friendly and censorship-free DNS server from Digitalcourage on your own computer. **IP: 46.182.19.48.** Further information is available at https://digitalcourage.de/support/zensurfreier-dns-server