Browser und Erweiterungen

Wahl des Browsers

Empfohlener Webbrowser: **Mozilla Firefox** (diese Anleitung bezieht sich auf die Version 63)

- Für GNU/Linux, Windows und macOS: https://www.mozilla.org/de/firefox/new/
- Für Android & iOS: https://www.mozilla.org/de/firefox/mobile/
- In F-Droid [Android] als **Fennec F-Droid**: https://f-droid.org/de/packages/org.mozilla.fennec_fdroid/

Einstellungen

≡ Menübutton → *Einstellungen* → *Allgemein, Unterpunkt „Firefox-Updates“*:

- Suchmaschinen *nicht* automatisch aktualisieren

≡ Menübutton → *Einstellungen* → *Suche*:

- Alternative Suchmaschine (z.B. StartPage.com, MetaGer.de, DuckDuckGo.com) hinzufügen, Suchvorschläge deaktivieren und Standardsuchmaschine ändern

≡ Menübutton → *Einstellungen* → *Datenschutz & Sicherheit*:

- **Seitenelemente blockieren**:
  - *Alle erkannten Elemente zur Aktivitätenverfolgung*: Aktiviert & *Immer*.
  - *Cookies von eingebundenen externen Inhalten ("Drittanbieter")*: Aktiviert & *Alle Cookies von eingebetteten externen Elementen ("Drittanbieter")* auswählen
  - Websites eine "Do Not Track"-Information senden: *Immer*
- **Cookies und Website-Daten**:
  - *Blockieren von Cookies und Website-Daten* auswählen und unter „Zu Blockieren“ *Alle Cookies von Drittanbietern* auswählen
  - Behalten, bis: *Firefox geschlossen wird*
- **Formulare & Passwörter**:
  - *Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen:* Deaktiviert. Für alle gängigen Betriebssysteme gibt es den Passwortmanager KeePassX: https://www.keepassx.org/
- **Chronik:**
  - Firefox wird eine Chronik *nach benutzerdefinierten Einstellungen anlegen*
  - *Die Chronik löschen, wenn Firefox geschlossen wird*: Aktiviert
- **Datenerhebung durch Firefox und deren Verwendung:**
  - *Firefox erlauben, Daten zu technischen Details und Interaktionen an Mozilla zu senden*: Deaktiviert

Erweiterungen / Add-ons & Plugins

≡ Menübutton → *Add-ons* → *Erweiterungen* → *Suchleiste oben rechts „Auf addons.mozilla.org suchen“* → *Name des Add-Ons eingeben* → *Enter-Taste drücken*

- **uBlock Origin** blockiert Werbung und Tracker
- **HTTPS Everywhere** ruft verschlüsselte Verbindung zu Websites auf, wenn verfügbar
- **Cookie AutoDelete** löscht Cookies automatisch nach dem Schließen von Browserfenstern und -tabs (die Einstellung „Automatisches Aufräumen“ muss nach Installation aktiviert werden)

Add-ons für Fortgeschrittene:

- **NoScript** blockiert die Ausführung von Programmen bzw. JavaScript
- **uMatrix** unterbindet alle Drittanbieteraufrufe

Adobe Flash Player:

- Deinstallieren oder Deaktivieren (***Shockwave Flash*** unter ***Add-ons*** → ***Plugins***)
- Falls man auf Flash angewiesen ist: Nur auf Nachfrage aktivieren

Wirkung der Einstellungen und Add-ons überprüfen:

- Die Erweiterung **Lightbeam** zeigt, von welchen Drittanbietern Inhalte nachgeladen werden (eine dauerhafte Aktivierung des Add-ons ist nicht ratsam, da es langsam ist)
- Ohne Add-on: **≡ Menübutton** → ***Web-Entwickler*** → ***Netzwerkanalyse*** zeigt beim Laden einer Website alle Anfragen als Liste
- Den Browser-Fingerabdruck testen: https://panopticlick.eff.org/

Tor-Browser

Der Tor-Browser ist ein modifizierter Firefox, der über das Tor-Netzwerk im Internet surft – Erweiterungen zum Schutz der Privatsphäre sind bereits installiert. **Zusätzliche Add-ons oder gleichzeitige Benutzung eines VPNs können die Anonymität gefährden.** Weitere Informationen und Download unter: https://www.torproject.org/

Bitte beachtet die hilfreiche Dokumentation, da eure Anonymität im Tor-Netzwerk vor allen Dingen von eurem Surf-Verhalten abhängt:
https://www.torproject.org/docs/documentation.html.en (Englisch)

Sonstiges

Um zu sehen wie datenschutzfreundlich eine spezielle Webseite ist, kann die URL mit dem Webdienst **Webbkoll** geprüft werden: https://webbkoll.dataskydd.net/

Wer dem ISP nicht vertraut, kann den datenschutzfreundlichen und **zensurfreien DNS-Server** von Digitalcourage auf den eigenen Computern eintragen. IP: *46.182.19.48*
Weitere Informationen unter https://digitalcourage.de/support/zensurfreier-dns-server