Browser und Erweiterungen

Wahl des Browsers

Empfohlener Webbrowser: **Mozilla Firefox**
Diese Anleitung bezieht sich auf die Desktop-Version von Firefox 77. Die Einstellungsmöglichkeiten und Menüführung in den Mobil-Versionen können abweichen.

- 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*** → **Startseite** (Unterpunkt ***Neue Fenster und Tabs***): **Startseite und neue Fenster: Leere Seite; Neue Tabs: Leere Seite**

≡ **Menübutton** → ***Einstellungen*** → **Startseite** (Unterpunkt ***Inhalte des Firefox-Startbildschirms***): alle nicht benötigten Elemente deaktivieren (insb. Empfehlungen von Pocket)

≡ **Menübutton** → ***Einstellungen*** → ***Suche***:
Suchvorschläge anzeigen deaktivieren, unter Ein-Klick-Suchmaschinen **weitere Suchmaschinen hinzufügen**, z.B. metaGer.de, StartPage.com, DuckDuckGo.com, Qwant.com und ***Standardsuchmaschine*** ändern

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

Seitenelemente blockieren:

- **Benutzerdefiniert** auswählen:
  - ***Cookies: Aktiviert; Alle Cookies von Drittanbietern auswählen***
  - ***Inhalte zur Aktivitätenverfolgung***: aktiviert; ***In allen Fenstern***
  - ***Heimliche Digitalwährungsberechner (Krypto-Miner): aktiviert***
  - ***Identifizierer (Fingerprinter):*** aktiviert
- ***Websites eine „Do Not Track“-Information senden***: ***Immer***

Cookies und Website-Daten:

- ***Cookies und Website-Daten beim Beenden von Firefox löschen***: aktiviert

Zugangsdaten & 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/)
- ***Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren***: deaktivieren

Chronik (optional):

- Firefox wird eine Chronik ***nach benutzerdefinierten Einstellungen anlegen***
- ***Optional: Die Chronik löschen, wenn Firefox geschlossen wird***: aktiviert; Details siehe Einstellungen

Datenerhebung durch Firefox und deren Verwendung:

- ***Firefox erlauben, Daten zu technischen Details und Interaktionen an Mozilla zu senden***: deaktiviert
- ***Firefox das Installieren und Durchführen von Studien erlauben***: deaktiviert

Sicherheit:

- ***Gefährliche und betrügerische Inhalte blockieren*** (Google Safe Browsing): deaktivieren (dadurch werden im Zweifel keine Daten an Google gesendet)

Erweiterungen / Add-ons & Plugins

≡ **Menübutton** → ***Add-ons*** → Suchleiste oben rechts ***Auf addons.mozilla.org suchen*** → Name des Add-Ons eingeben, Enter-Taste drücken:
(alle Add-ons können auch für die Ausführung in privaten Fenstern erlaubt werden)

- **uBlock Origin** (von Raymond Hill) blockiert Werbung und Tracker
- **Decentraleyes** (von Thomas Rientjes) ersetzt JavaScript-Bibliotheken von Online-Anbietern durch lokale
- **HTTPS Everywhere** (von EFF Technologists) ruft verschlüsselte Verbindung zu Websites auf, wenn verfügbar
- **Cookie AutoDelete** (von CAD Team) löscht Cookies automatisch nach dem Schließen von Browserfenstern und -tabs (die Einstellung *Automatisches Aufräumen* muss nach Installation aktiviert werden)

Add-ons für Fortgeschrittene:

- **NoScript** (von Giorgio Maone) blockiert die Ausführung von aktiven Inhalten und JavaScript-Programmen (Falls die manuelle Auswahl der Scripte zu mühselig ist, kann die Option *Top-Level Seiten vorübergehend auf VERTRAUENSWÜRDIG setzen* gewählt werden; Fortgeschrittene können in den Einstellungen alle Inhalte verbieten und die Whitelist leeren)
- **Smart Referer** (von meh., Alexander Schlarb) entfernt Referer;
- **uBlock Origin** im **Fortgeschrittenenmodus**: unter Einstellungen
    - Ich bin ein erfahrener Anwender (Pflichtlektüre beachten) aktivieren
    - *Freigabe der lokalen IP-Adresse via WebRTC verhindern* aktivieren
    - *CSP-Berichte blockieren* aktivieren
    - *Externe Schriftarten blocken* aktivieren
    - im Tab *Filterlisten* nach Bedarf die noch fehlenden Einträge unter *Werbung, Privatsphäre und Belästigungen* aktivieren
    - Weitere Einstellungen, siehe Blog von Mike Kuketz: https://www.kuketz-blog.de/firefox-ublock-origin-firefox-kompendium-teil2

- **uMatrix** (von Raymond Hill) 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:

- Das Add-on **Lightbeam 3.0** (von Princiya) zeigt von welchen Drittanbietern Inhalte nachgeladen werden (eine dauerhafte Aktivierung des Add-ons ist nicht ratsam, da es langsam ist)
- ≡ **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://wwwn.torproject.org/docs/documentation.html.e (Englisch)

Sonstiges

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

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