Browser und Erweiterungen

Wahl des Browsers

Empfohlener Webbrowser: **Mozilla Firefox**
Diese Anleitung bezieht sich auf die Desktop-Version von Firefox 95. Die Einstellungsmöglichkeiten und Menüführung in den Mobil-Versionen können abweichen. In der Android-Version werden bisher nur einige wenige Add-ons unterstützt - darunter sind allerdings uBlock Origin, NoScript, HTTPS Everywhere und Decentraleyes. Die iOS-Version aufgrund Einschränkungen durch Apple keine Add-ons.

- Für 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. Suchmaschinen können auch hinzugefügt werden, wenn die gewünschte Suchmaschine im Browser aufgerufen und das Kontextmenü per Rechtsklick in der Adresszeile geöffnet wird.

≡ **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 (optional):

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

Zugangsdaten und Passwörter:

- ***Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen***: deaktiviert. Für alle gängigen Linux/Windows/macOS gibt es den Passwortmanager KeePassXC: https://www.keepassxc.org/, für Android KeePassDX: https://www.keepassdx.com/, für iOS KeePassium: https://keepassium.com.
- ***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
- **Nicht gesendete Absturzberichte automatisch von Firefox senden lassen**: deaktiviert

Sicherheit:

- **Gefährliche und betrügerische Inhalte blockieren** (Google Safe Browsing): deaktivieren (dadurch werden im Zweifel keine Daten an Google gesendet)
- **Nur-HTTPS-Modus**: Nur-HTTPS-Modus in allen Fenstern aktivieren.

Erweiterungen / Add-ons & Plugins

≡ **Menübutton** → ***Add-ons und Themes*** → 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
- **LocalCDN** (von nobody42) ersetzt beim Seitenaufruf Frameworks von externen Online-Anbietern durch lokale Varianten. Alternativ kann (insbesondere unter Android) auch **Decentraleyes** (von Thomas Rientjes) verwendet werden.
- **HTTPS Everywhere** (von EFF Technologists) ruft Websites über eine verschlüsselte Verbindung auf, falls möglich. Falls die Browser-Einstellung **Nur-HTTPS-Modus** aktiviert ist das Add-on nicht mehr notwendig.
- **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 und Einstellungen 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:** unter Einstellungen des Add-ons
    - unter *Privatsphäre* die Option *CSP-Berichte blockieren* aktivieren (evtl. schon voreingestellt)
    - unter *Standardverhalten* die Option *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

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** → ***Weitere Werkzeuge*** → ***Werkzeuge für Web-Entwickler*** → ***Netzwerkanalyse*** (oder Strg+Umschalt+E) zeigt beim Laden einer Website alle Anfragen als Liste

Tor Browser

Der Tor Browser ist ein modifizierter Firefox für Windows, Linux, macOS und Android, 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/de/

Für iOS gibt den inoffiziellen **Onion Browser**: https://onionbrowser.com/

Bitte beachtet die hilfreiche Dokumentation, da eure Anonymität im Tor-Netzwerk vor allen Dingen von eurem Surf-Verhalten abhängt: https://support.torproject.org/de/ (deutsch u.a.) und https://tb-manual.torproject.org/de/.

Wenn man doch mal einen chromiumbasierten Browser braucht …

Außer Firefox und dem Tor-Browser basieren heute fast alle Browser auf dem Google-Browser Chrome bzw. dessen quelloffener Variante Chromium. Für manche Anwendungen sind diese schneller. Google Chrome hat aber Tracking eingebaut, das sich nicht deaktivieren lässt. Nehmt in so einem Fall **Ungoogled Chromium** <https://ungoogled-software.github.io/> bzw. unter Android: **Bromite** <https://www.bromite.org/>.

Wer sich effektiv gegen Fingerprinting (siehe auch unter Sonstiges) wehren möchte, kann sich auch **Brave** ansehen. Leider telefoniert er selbst gern nach Hause. Mehr Infos: https://www.kuketz-blog.de/brave-datensendeverhalten-desktop-version-browser-check-teil1/

Sonstiges

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

Wie gut der eigene Browser gegen Fingerprinting geschützt ist, kann man anhand des Webdienstes **Cover Your Tracks** der EFF herausfinden: https://coveryourtracks.eff.org/

Wer dem ISP nicht vertraut, kann den datenschutzfreundlichen und **zensurfreien DNS-Server** von Digitalcourage auf dem eigenen Computer, Smartphone oder Router eintragen. Wer DNS-over-TLS (unter Android „privates DNS“ genannt) nutzen kann, trägt dort am besten **dns3.digitalcourage.de** (IPv4: 5.9.164.112, IPv6: 2a01:4f8:251:554::2, Port 853). Weitere Informationen unter https://www.kuketz-blog.de/empfehlungsecke/#dns und https://digitalcourage.de/support/zensurfreier-dns-server.