Webtracking Gegenmaßnahmen

BesserAlsNix

Olaf Pichler

28. April 2017

Inhaltsverzeichnis

Kapitel 1

Allgemeines

1.1 Begriffe

1.1.1 Was ist Webtracking?

Webtracking ist das Verfolgen der Aktionen eines Internetnutzers über einen längeren Zeitraum. Dies geschieht unter der *missbräuchlichen* Verwendung von Webtechniken. Das Ziel ist es, aus dem Nutzverhalten persönliche Daten wie individuelle Interessen und Kaufkraft abzuleiten und ein Persönlichkeitsprofil aufzubauen. Das geschieht entweder durch Trackingcookies oder Fingerprinting.

1.1.2 Was sind Cookies?

Cookies sind kleine Textdateien, welche vom Browser gespeichert werden und von einer Webseite immer wieder ausgelesen werden können. Dies dient z.B. zur Speicherung von Logindaten und Warenkorbinhalten, kann aber auch zum Webtracking verwendet werden. Zum Verfolgen eines Nutzers wird in einem Cookie eine eindeutige Nummer gespeichert, welche der Webtracker auf jeder Seite wieder auslesen und somit der Nutzer eindeutig identifizieren kann.

1.1.3 Was ist Fingerprinting?

Fingerprinting bezeichnet eine Art des Webtrackings bei der das Gerät eines Nutzers anhand von an sich harmlosen Kenndaten, die in Summe einzigartig sind, immer wieder erkannt wird. Typische Kenndaten sind die Bilschirmauflösung, die verwendete Zeitzone, sowie installierte Schriften und Browsererweiterungen. Da immer mehr Nutzer Cookies löschen wird seit einigen Jahren vermehrt Fingerprintig zur Wiedererkennung des Gerätes und damit des Nutzers verwendet.

1.2 Tipps

1.2.1 Weniger ist oft mehr

Achten sie darauf welche Browsererweiterungen sie intalliert haben. Viele Erweiterungen machen den Browser eindeutig und/oder tracken selbst.

1.2.2 Mehrere Browser(-Profile) verwenden

Das Wechseln des Browser(-Profils) ist eine der einfachsten Methoden um Webtracker in die Irre zu führen. Cookies werden immer in einer Datenbank des Browser(-Profils) gespeichert und verschiedene Browser haben unterschiedliche Fingerprints. Durch das Verwenden mehrer Browser(-Profile) für unterschiedliche Anwendungsfälle kann das Verknüpfen der abgeschöpften Daten erschwert werden.

1.2.3 Ad-Blocker verwenden

Ad-Blocker verhindern das Nachladen bestimmter Elemente anhand von Block-Listen, in welchen die Adressen bekannter Werbeserver verzeichnet sind. Die meiste Werbung enthält auch Tracking-Code. Durch das Aktivieren mehrerer Anti-Tracking-Listen, werden Verbindungen zu bekannten Webtrackern verhindert. Ein empfehlenswerter Open-Source Ad-Blocker ist *uBlock Origin*.

1.2.4 Third-Party-Cookies verbieten

Third-Party-Cookies sind Cookies die von Drittseiten gesetzt werden. Nicht nur das Cookie der von ihnen besuchten Webseite, sondern auch Cookies von allen eingebundenen Werbeseiten und Trackern, werdenr auf ihrem Computer gespeichert. Das setzen dieser Drittparteicookies kann und sollte verhindert werden. Detailierte Anleitungen gibt es für Firefox unter Punkt 2.1 und für Chromium bzw. Google Chrome unter Punkt 3.1.

1.2.5 Browserdaten automatisch löschen

Um den Webtrackern das Wiedererkennen des Nutzers nach einem Neustart des Browsers zu erschweren, sollten unnötige Browserdaten beim Schließen des Browsers gelöscht werden. Detailierte Anleitungen gibt es für Firefox unter Punkt 2.2 und für Chromium bzw. Google Chrome unter Punkt 3.2.

1.2.6 JavaScript Blocker verwenden

Fingerprinting geschieht überwiegend mittels JavaScript, darum ist es empfehlenswert JavaScript nur von vertrauenswürdigen Seiten zuzulassen. Dies lässt sich mittels eines JavaScript Blockers erreichen welcher auch vor der Infektion mit Viren und Trojanern schützt. Dies erfordert allerdings die Pflege einer Whitelist und geht zu Lasten des Surfkomforts da sie vor allem anfangs viele Seiten zur Whitelist hinzufügen müssen. Die Whitelist speichert vertrauenswürdige Webseiten auf denen sie JavaScript zulassen möchten. Durch das Blockieren von JavaScript werden viele Seiten

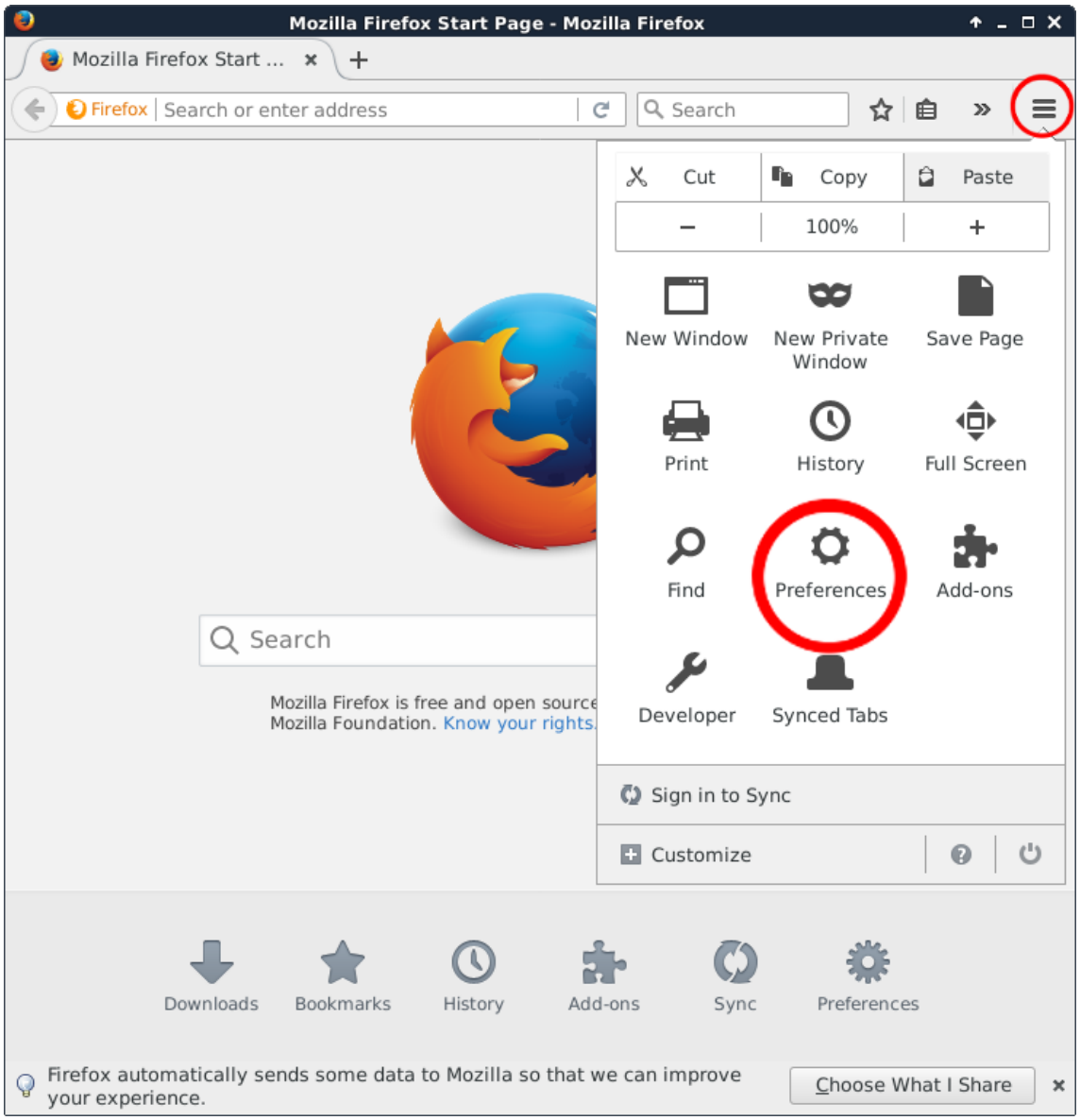
nicht mehr wie gewohnt dargestellt oder funktionieren nicht bis sie die Seite in Ihre Whitelist aufgenommen haben. Für den Firefox hat sich *NoScript* als Programm der Wahl erwiesen, für Chromium und Google Chrome steht mit *ScriptSafe* ein ebenso mächtiges Tool zu Verfügung. Nehmen sie sich Zeit und machen sie sich mit der Konfguration des jeweiligen Blockers vertraut und finden sie eine akzeptable Balance zwischen Schutz und Komfort.

Kapitel 2

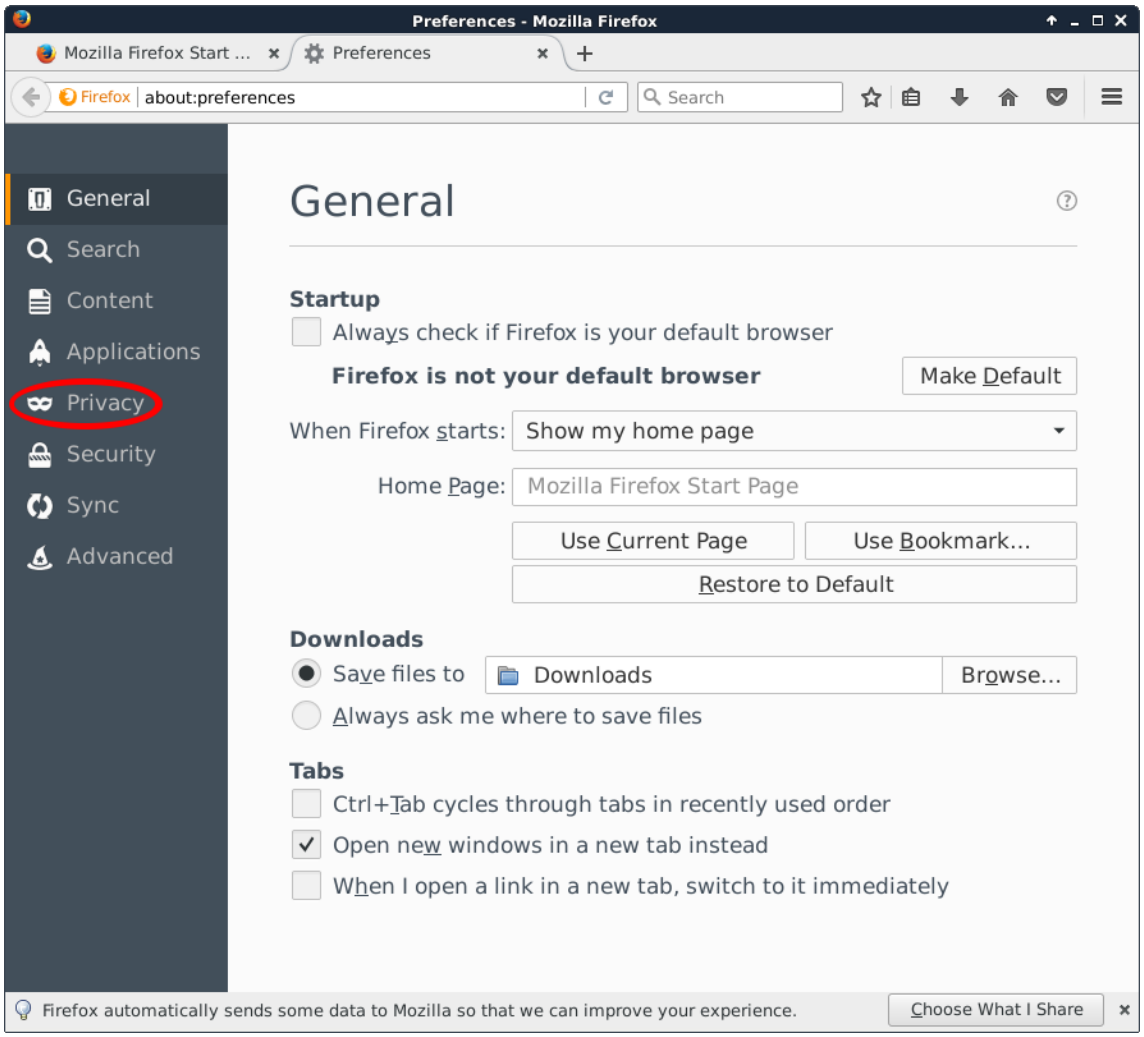
Firefox

2.1 Third-Party-Cookies verbieten

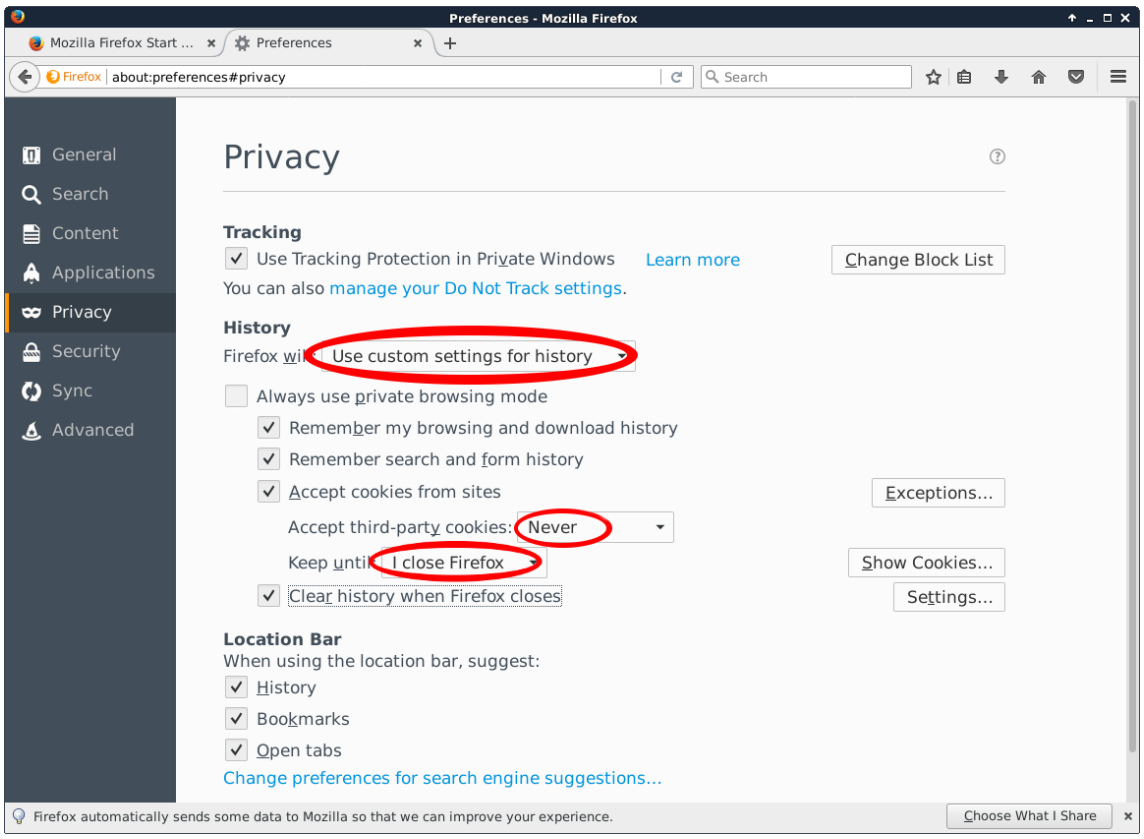
- Öffne die Einstellungen.



- Navigiere zu den Privatsphäreeinstellungen.

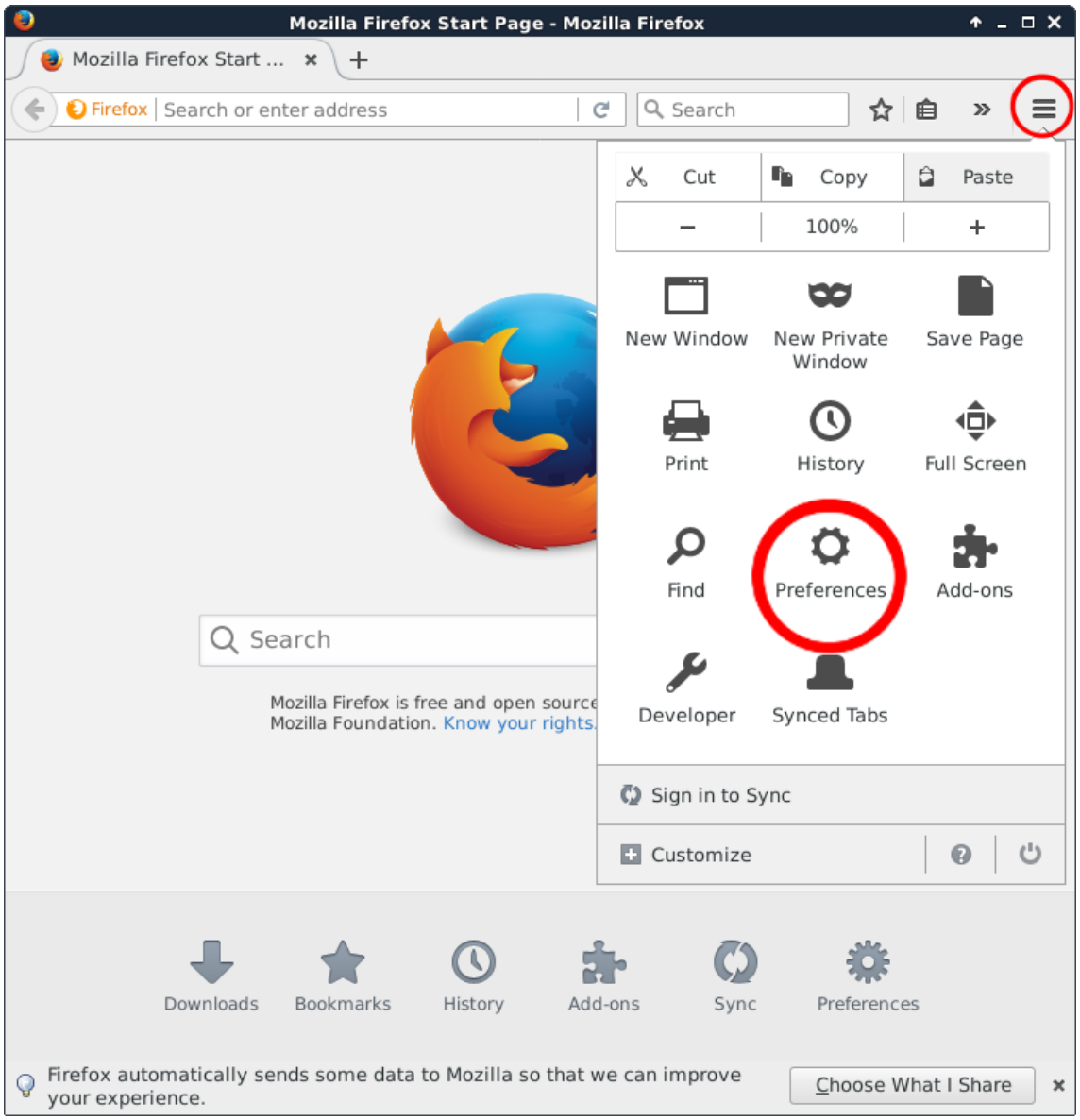


- Wähle „Historie nach benutzerdefinierten Kriterien anlegen“ und verbiete das Setzen von Third-Pary-Cookies.

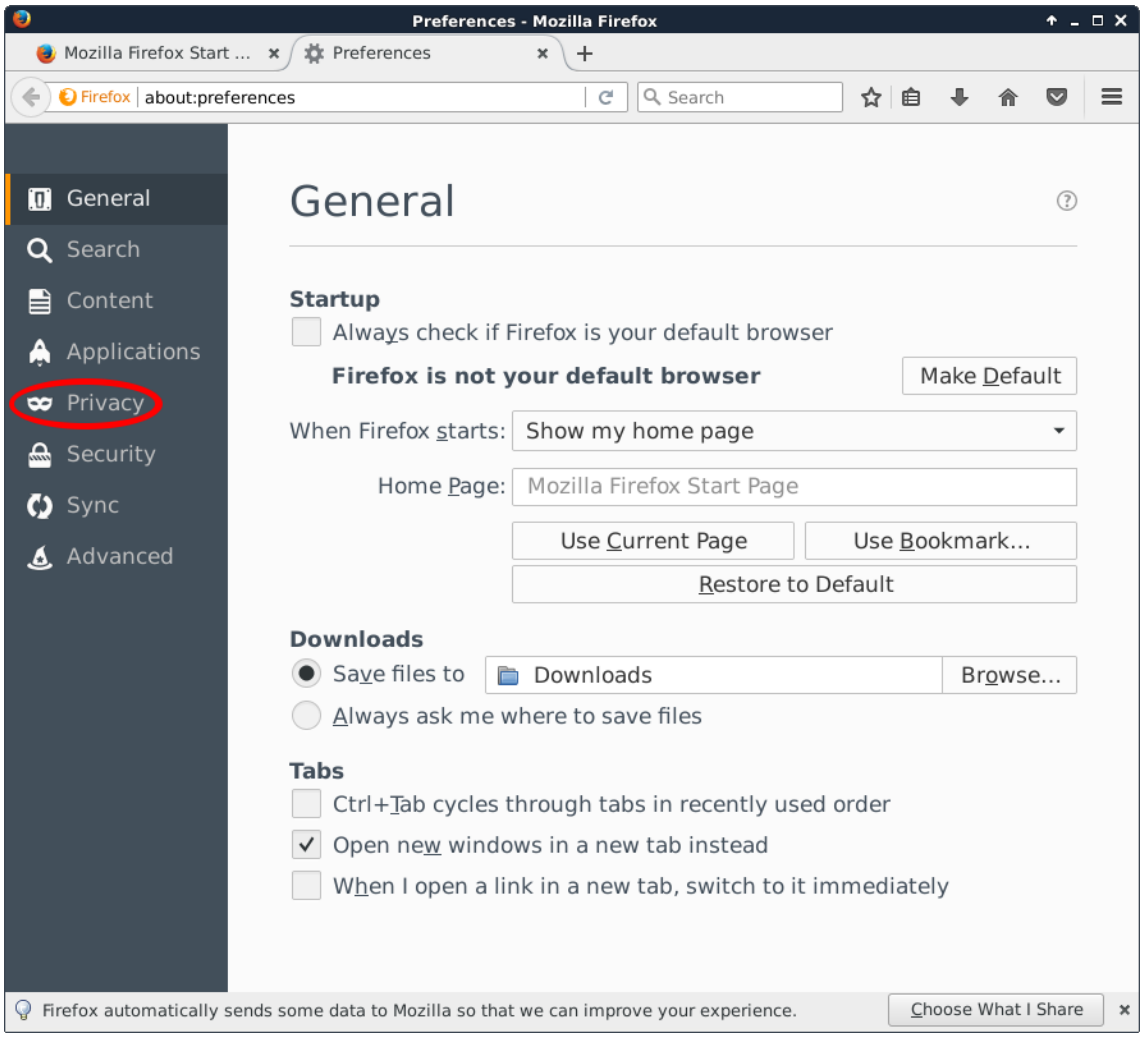


2.2 Browserdaten automatisch löschen

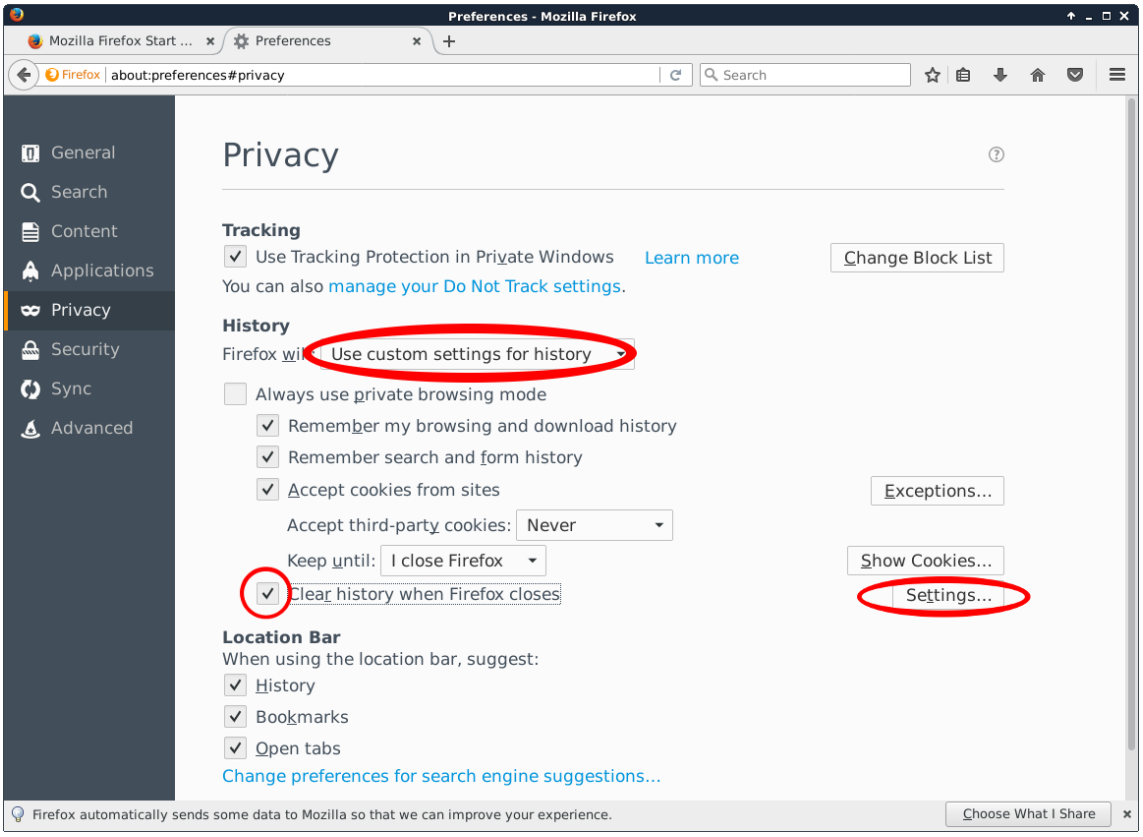
- Öffne die Einstellungen.



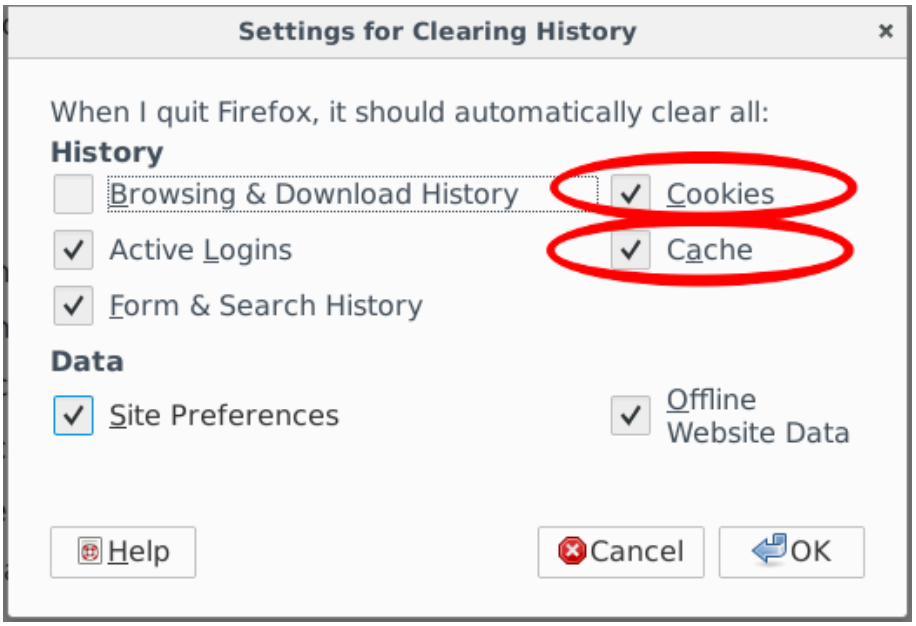
- Navigiere zu den Privatsphäreeinstellungen.



- Wähle „Historie löschen wenn Firefox geschlossen wird“ aus.



- Wähle in den Einstellungen dieses Punkts mindestens die Cookies und Cachedaten aus.

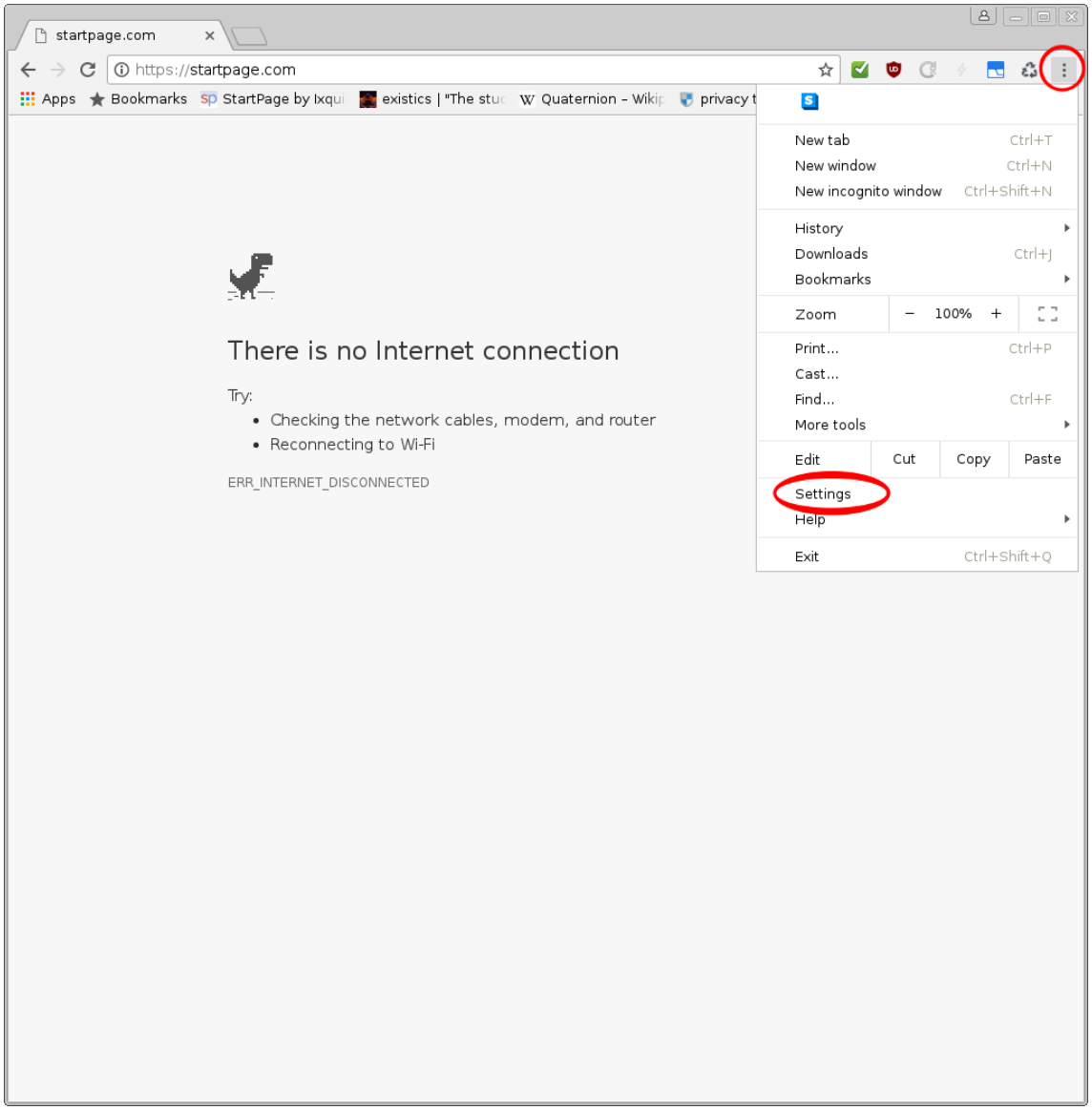


Kapitel 3

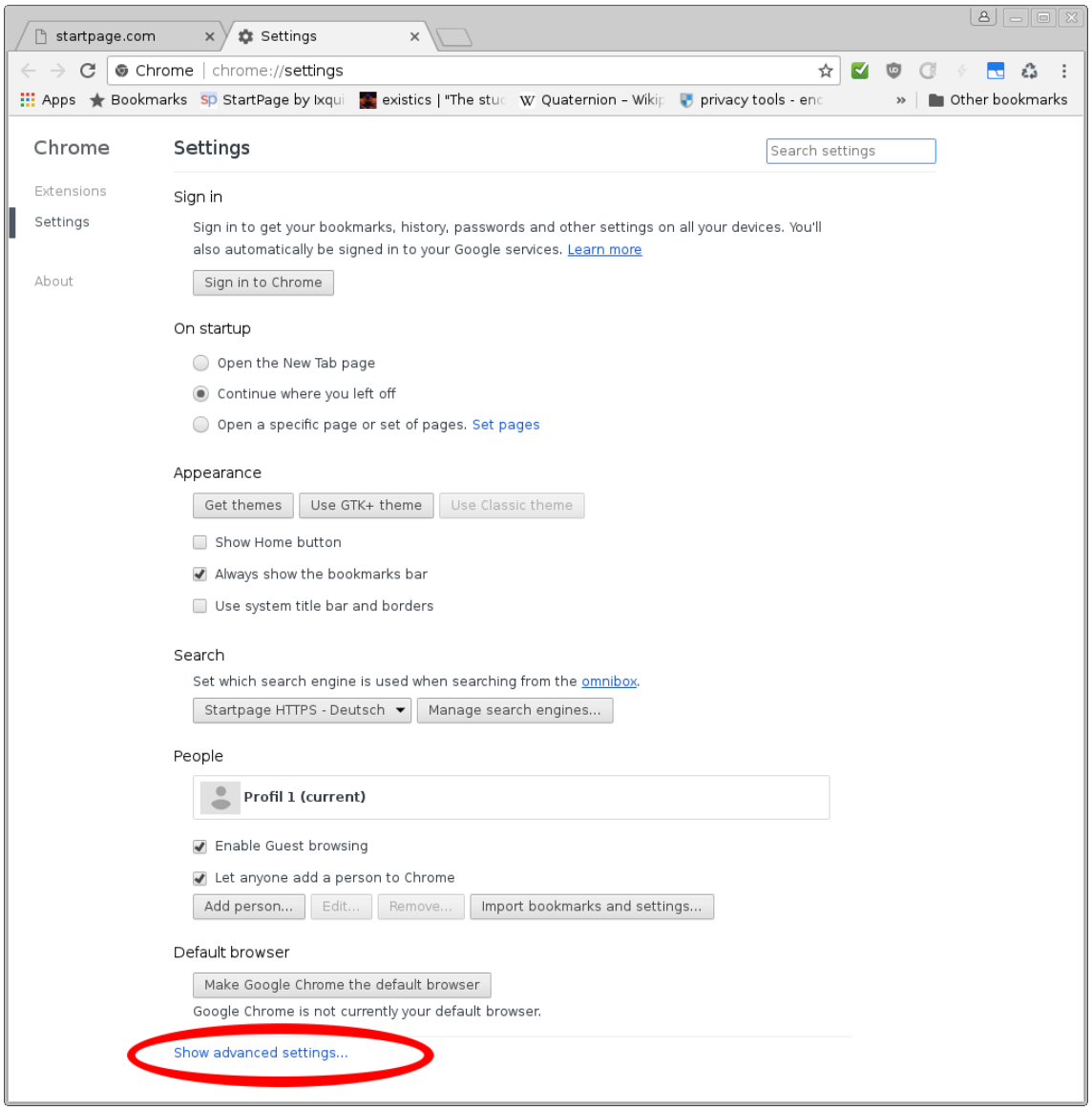
Chrome und Chromium

3.1 Third-Party-Cookies verbieten

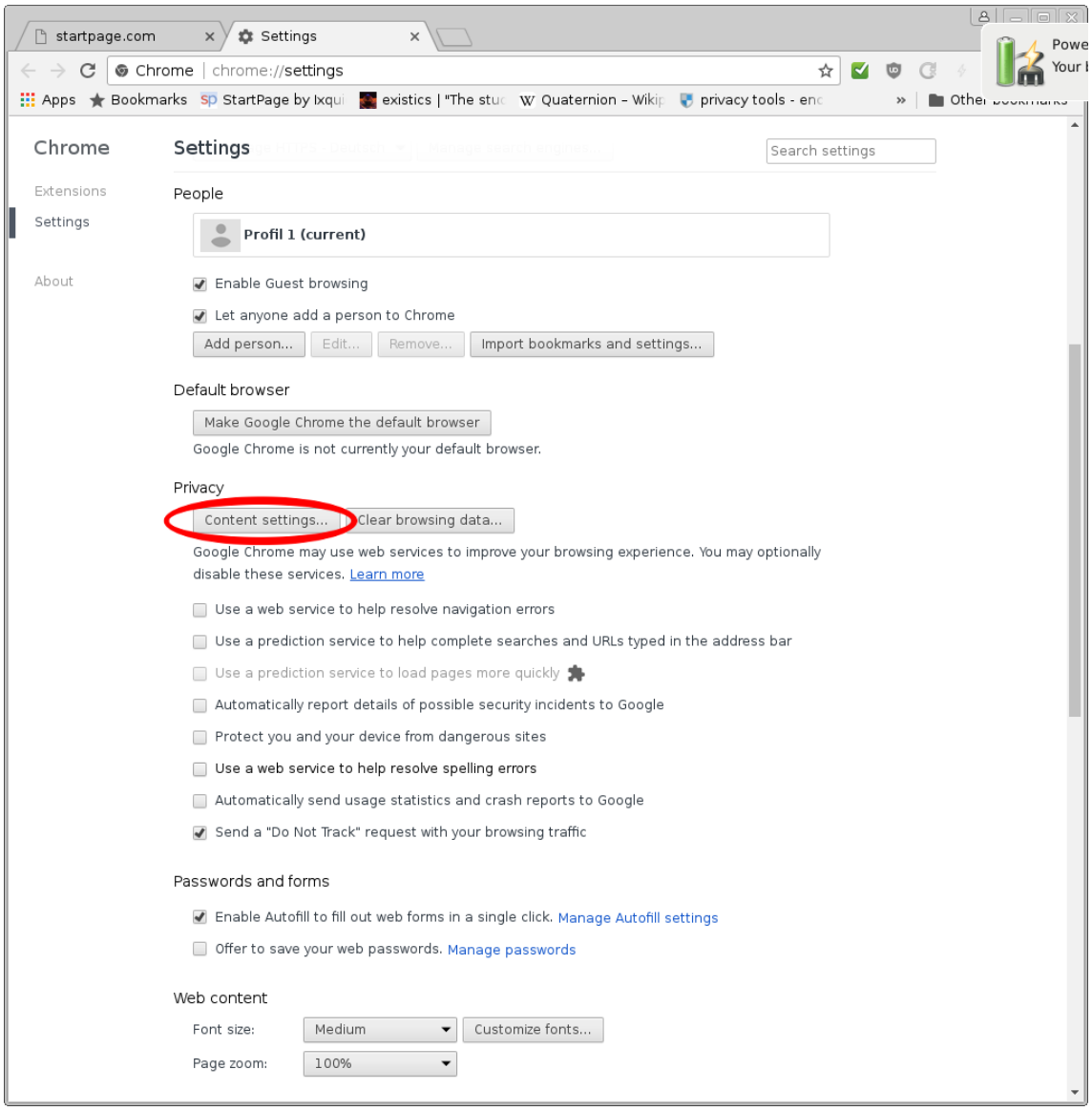
- Öffne die Einstellungen.



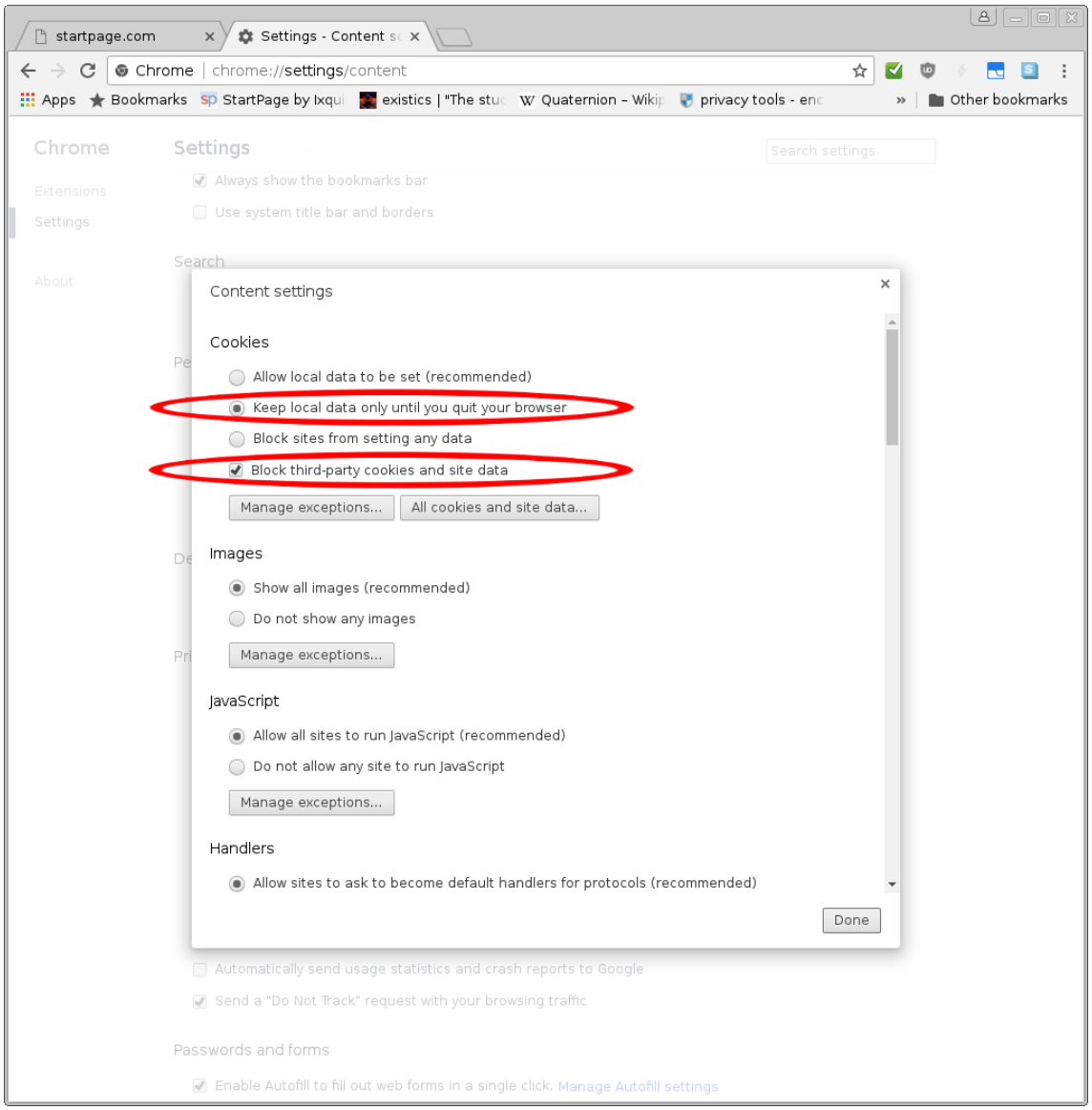
- Navigiere zu den Privatsphäreeinstellungen.



- Öffne die Inhaltseinstellungen



- Verbiete das Setzen von Third-Party-Cookies.



3.2 Browserdaten automatisch löschen

- Installiere die Erweiterung *Auto History Wipe*.
- Öffne die Optionen durch einen Rechtsklick auf das Auto History Wipe Symbol und Aktiviere mindestens die Cookies und Cachedaten.