

Browser-Einstellungen

Einleitung

Programme (auch Browser genannt) mit denen wir im Internet surfen gibt es einige. Die am meisten verwendeten sind:

Edge von Microsoft

Chrome von Google

Firefox von Mozilla

Safari von Apple

Opera von Opera Limited

Allen gemeinsam ist, dass sie neben ihrer eigentlichen Aufgabe, uns die Daten im Internet sichtbar zu machen, auch Daten über uns und unser Verhalten sammeln und an allerlei Interessenten weitergeben.

Einige dieser, meist unerwünschten Verhalten kann man durch Einstellungen im Programm abstellen.

Eine weitere Möglichkeit unsere Privatsphäre zu schützen sind Zusatzprogramme zu den Browsern, sogenannte 'Add-ons'.

Aber Achtung! Auch einige dieser Zusatzprogramme werden zum Datensammeln missbraucht.

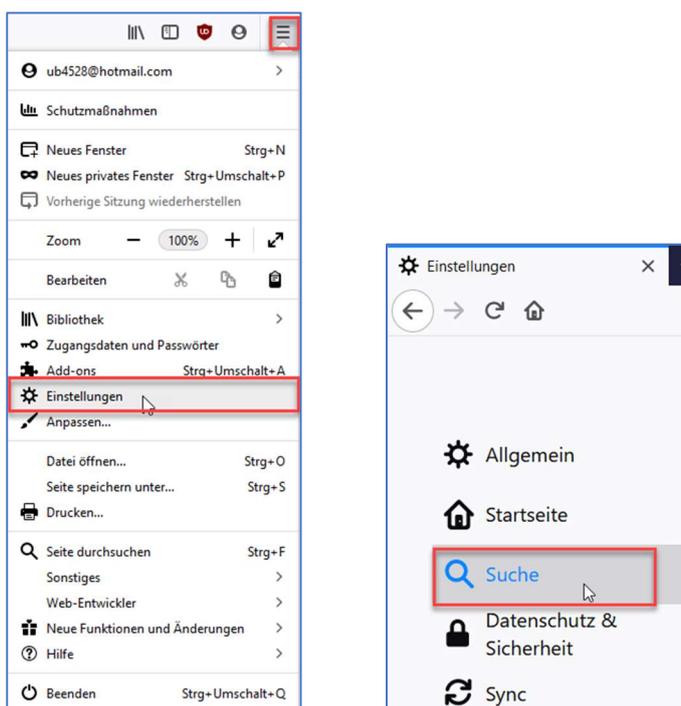
Beispiel einer Datensammlung durch Firefox

Tippen Sie folgendes in die Adresszeile: **about:telemetry**
Daten die der Browser täglich nach Hause sendet.

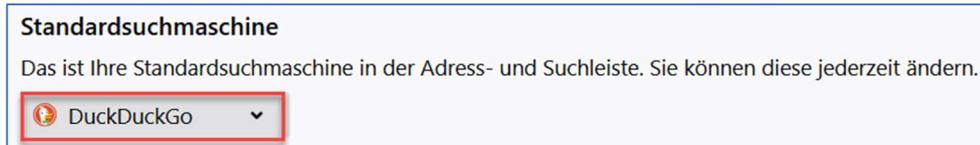
Firefox (Mozilla)

Standardsuchmaschine wählen

[Einstellungen – Suche]

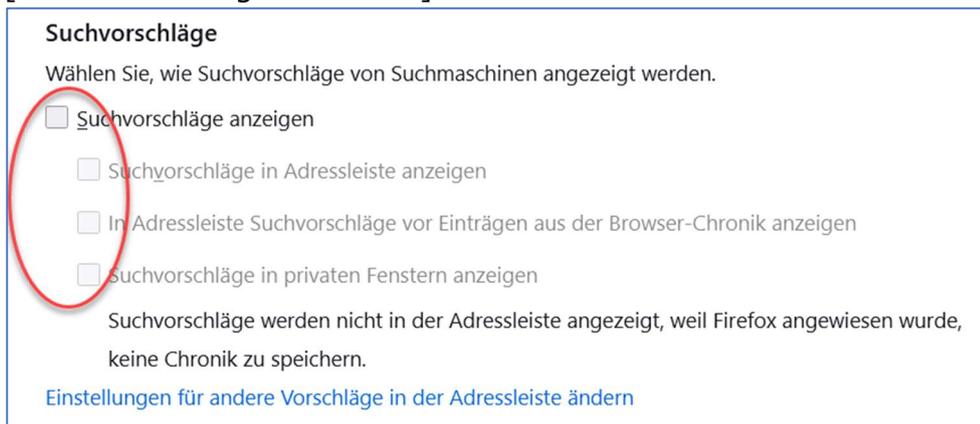


Auch die Standardsuchmaschine kann hier festgelegt werden.

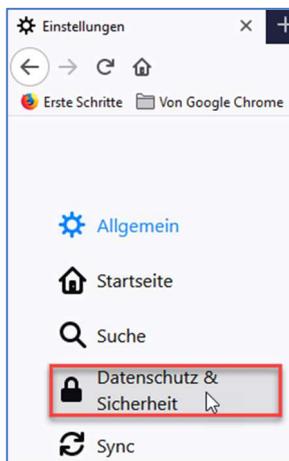


'Suchvorschläge anzeigen' deaktivieren

[☰ - Einstellungen – Suche]



[☰ - Einstellungen – Datenschutz & Sicherheit]



Browser Datenschutz

Browser-Datenschutz

Verbesserter Schutz vor Aktivitätenverfolgung

 Skripte zur Aktivitätenverfolgung folgen Ihnen und sammeln Informationen über Ihre Internet-Gewohnheiten und Interessen. Firefox blockiert viele dieser Skripte zur Aktivitätenverfolgung und andere böswillige Skripte. [Ausnahmen verwalten...](#)

[Weitere Informationen](#)

Standard ▼
Ausgewogen zwischen Schutz und Leistung. Seiten laden normal.

Streng
Stärkerer Schutz, einige Websites oder mancher Inhalt funktioniert eventuell nicht.

Firefox blockiert Folgendes:

- Skripte zur Aktivitätenverfolgung durch soziale Netzwerke
- Seitenübergreifende Cookies in allen Fenstern
- Inhalte zur Aktivitätenverfolgung in allen Fenstern
- Heimliche Digitalwährungsberechner (Krypto-Miner)
- Identifizierer (Fingerprinter)

Chronik ausschalten

Chronik

Firefox wird eine Chronik ▼

Firefox wird dieselben Einstellungen wie im Privaten Modus verwenden und keinerlei Chronik anlegen, während Sie Firefox benutzen. [Chronik leeren...](#)

Datenerhebung durch Firefox und deren Verwendung

Datenerhebung durch Firefox und deren Verwendung

Wir lassen Ihnen die Wahl, ob Sie uns Daten senden, und sammeln nur die Daten, welche erforderlich sind, um Firefox für jeden anbieten und verbessern zu können. Wir fragen immer um Ihre Erlaubnis, bevor wir persönliche Daten senden.

[Datenschutzhinweis](#)

Sie gestatten Mozilla nicht mehr, technische und Interaktionsdaten zu erfassen. Alle bisherigen Daten werden innerhalb von 30 Tagen gelöscht. [Weitere Informationen](#)

Firefox erlauben, Daten zu technischen Details und Interaktionen an Mozilla zu senden [Weitere Informationen](#)

Personalisierte Erweiterungsempfehlungen durch Firefox erlauben [Weitere Informationen](#)

Firefox das Installieren und Durchführen von Studien erlauben [Firefox-Studien ansehen](#)

Nicht gesendete Absturzberichte automatisch von Firefox senden lassen [Weitere Informationen](#)

Nur Verbindungen mit sichere Verschlüsselung erlaube

Nur-HTTPS-Modus

HTTPS bietet eine sichere, verschlüsselte Verbindung zwischen Firefox und den von Ihnen besuchten Websites. Die meisten Websites unterstützen HTTPS und wenn der Nur-HTTPS-Modus aktiviert ist, wird Firefox alle Verbindungen zu HTTPS aufrüsten.

[Weitere Informationen](#)

Nur-HTTPS-Modus in allen Fenstern aktivieren [Ausnahmen verwalten...](#)

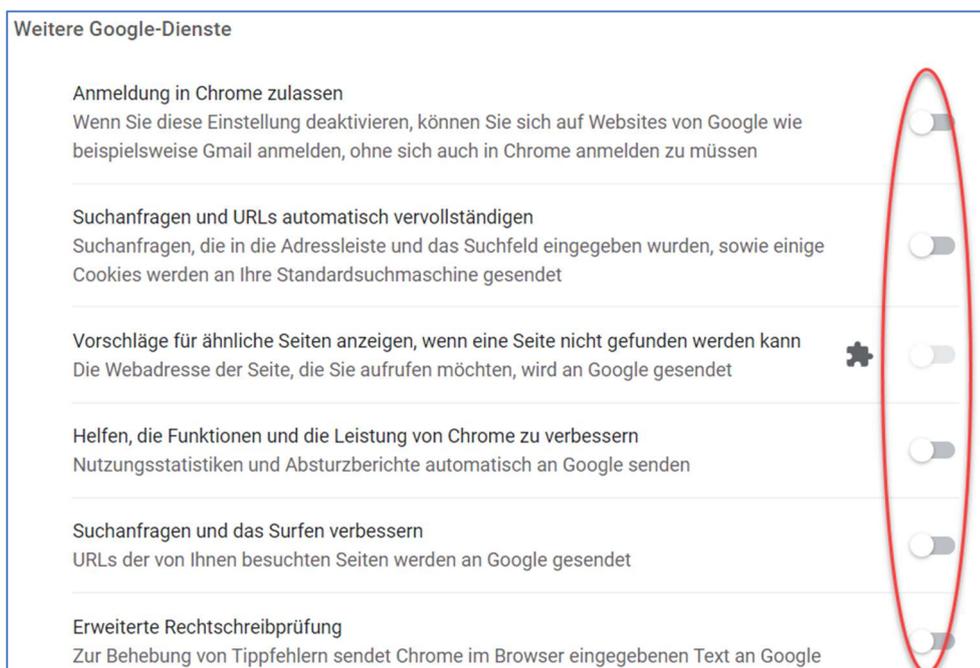
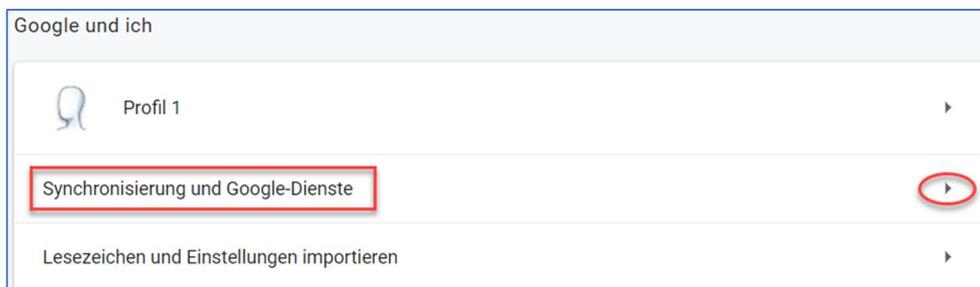
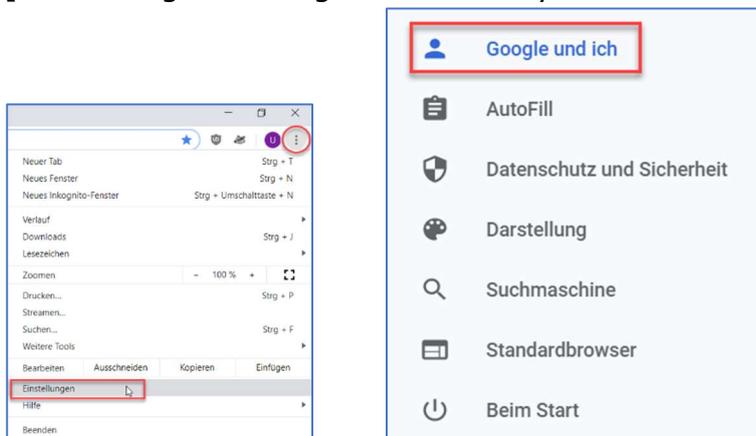
Nur-HTTPS-Modus nur in privaten Fenstern aktivieren

Nur-HTTPS-Modus nicht aktivieren

Chrome (Google)

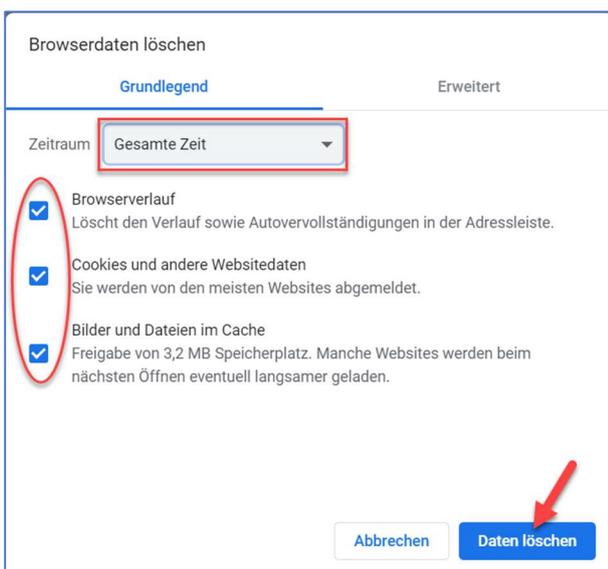
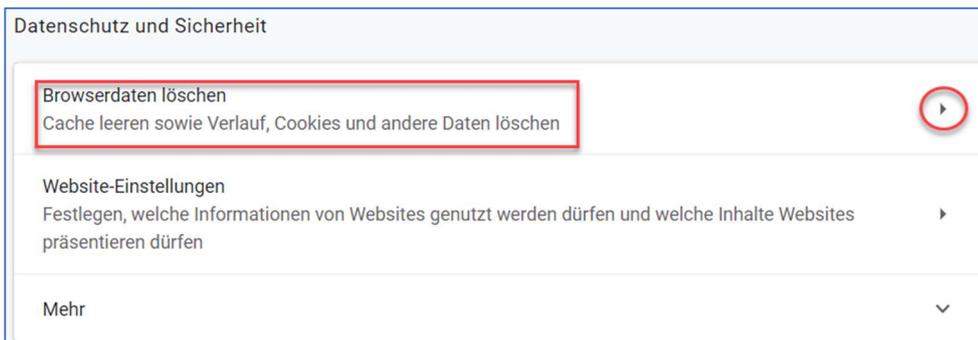
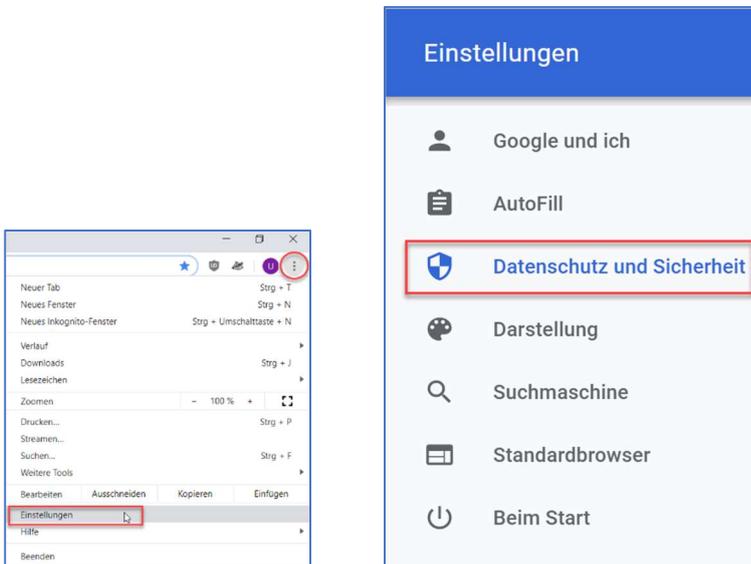
Alle 'Weitere Google-Dienste' ausschalten

[Einstellungen – Google und ich – Synchronisierung und Google-Dienste]

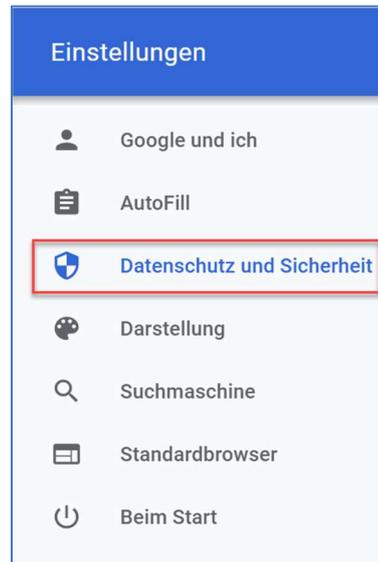
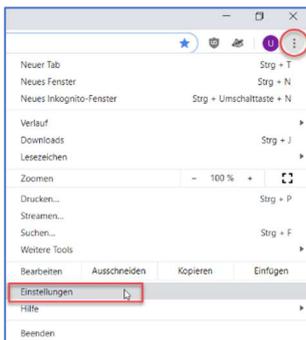


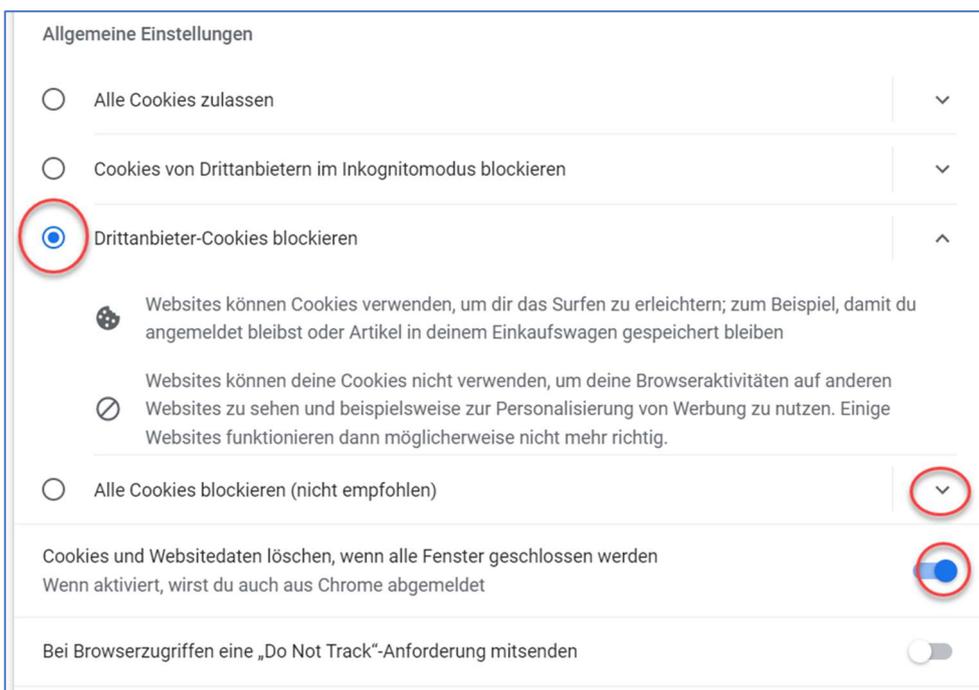
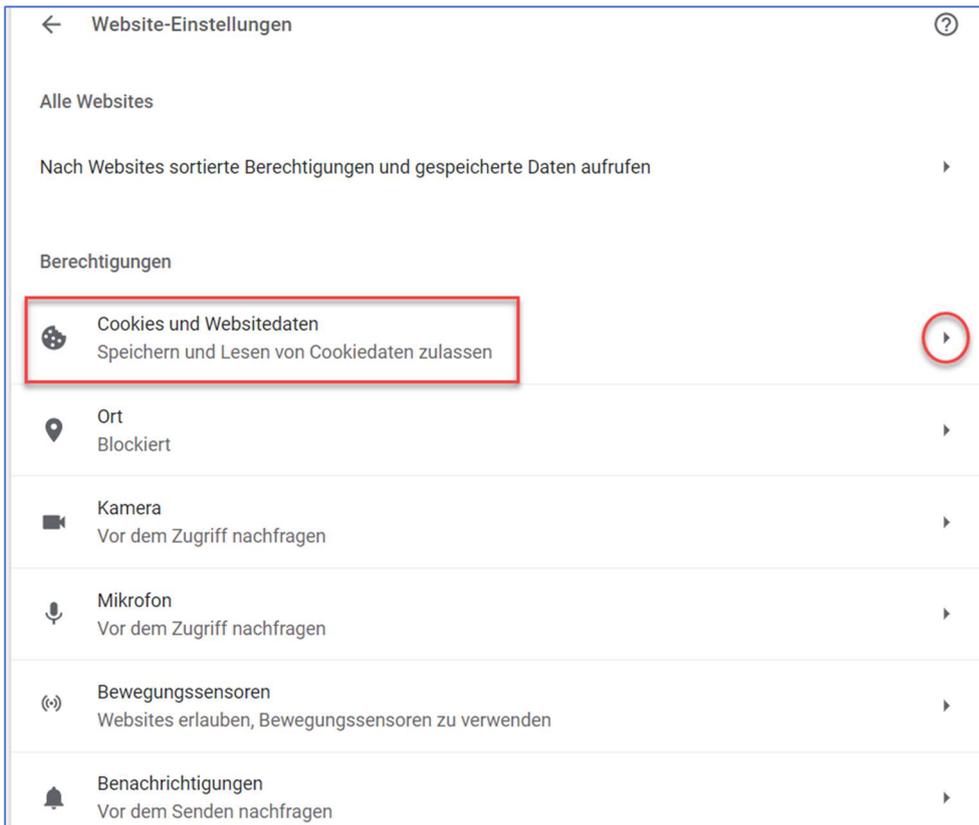
Browserdaten löschen

[Einstellungen – Datenschutz und Sicherheit – Browserdaten löschen]

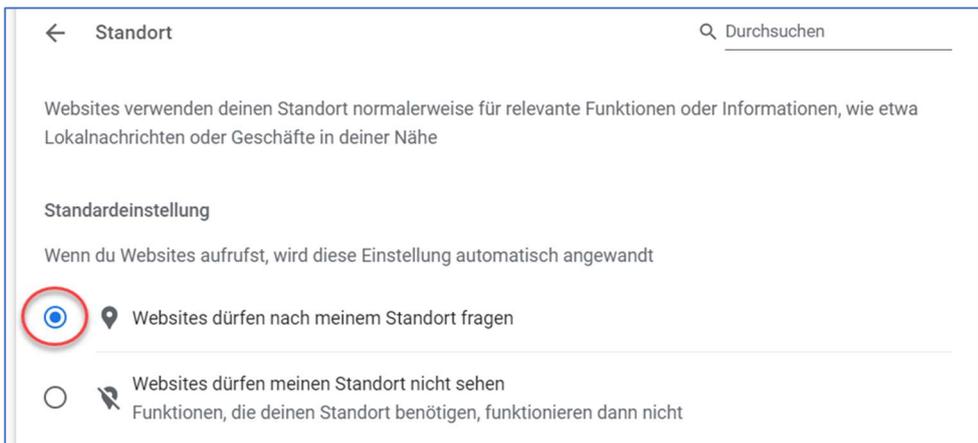
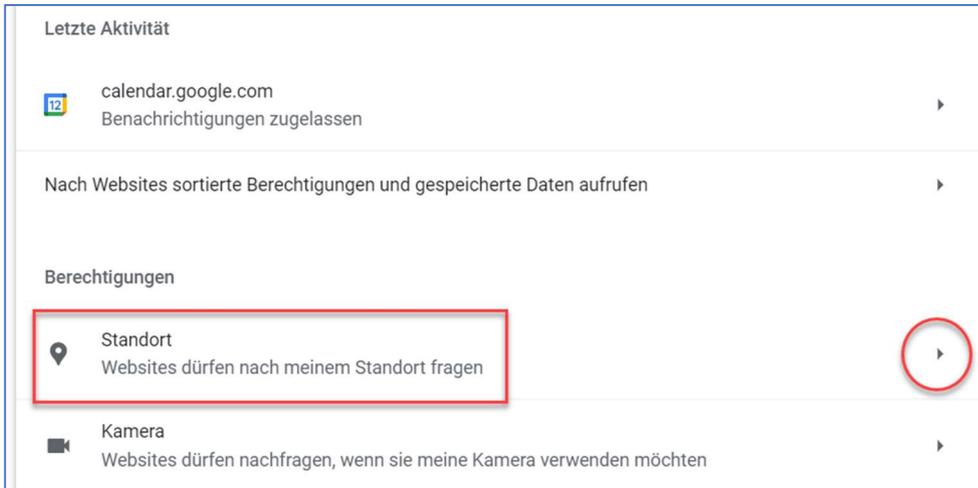


'Cookies und Webseitendaten beim Beenden von Chrome löschen' einschalten
und
'Drittanbieter-Cookies blockiere' einschalten
[Einstellungen – Datenschutz und Sicherheit – Webseite-Einstellungen – Cookies und Webseitendaten]





Ort 'Vor dem Zugriff nachfragen' einschalten
[Einstellungen – Datenschutz und Sicherheit – Weitere Einstellungen – Standort]



Edge (Microsoft)

[. . . – Einstellungen]



[Datenschutz, Suche und Dienste]

Verhindern der Nachverfolgung ?

Websites verwenden Tracker, um Informationen über Ihr Surfverhalten zu sammeln. Websites nutzen diese Informationen unter Umständen, um Verbesserungen durchzuführen und Inhalte wie personalisierte Werbeanzeigen anzuzeigen. Einige Tracker sammeln und senden Ihre Informationen an Websites, die Sie nicht besucht haben.

Tracking-Verhinderung

Einfach

- Lässt die meisten Tracker auf allen Websites zu
- Inhaltsinformationen und Werbeanzeigen werden wahrscheinlich personalisiert
- Websites werden wie erwartet funktionieren.
- Blockiert bekannte schädliche Tracker

Ausgewogen
(Empfohlen)

- Blockiert Tracker von Websites, die Sie nicht besucht haben
- Inhalte und Werbeanzeigen sind wahrscheinlich weniger stark personalisiert
- Websites werden wie erwartet funktionieren.
- Blockiert bekannte schädliche Tracker

Streng

- Blockiert die meisten Tracker von allen Websites
- Inhalt und Anzeigen verfügen wahrscheinlich über eine minimale Personalisierung
- Teile von Websites funktionieren möglicherweise nicht.
- Blockiert bekannte schädliche Tracker

Blockierte Tracker >
Websites anzeigen, für die das Tracking blockiert wurde

Ausnahmen >
Alle Tracker auf Websites zulassen, die Sie auswählen

Beim InPrivate-Browsen immer die strenge Tracking-Verhinderung nutzen

Datenschutz

Wählen Sie Ihre Datenschutzeinstellungen für Microsoft Edge aus. [Weitere Informationen](#)

„Nicht verfolgen“-Anforderungen (Do not track) senden

Zulassen, dass Websites überprüfen, ob Sie Zahlungsmethoden gespeichert haben

Erweiterungen

uBlock Origin (blockiert Werbung)



uBlock Origin
Endlich ein effizienter Blocker, der wenig Prozessorleistung und Arbeitsspeicher verbraucht.

[Details](#) [Entfernen](#)

AdBlock



AdBlock – der beste Ad-Blocker
★★★★★ (1'008) | BetaFish

Blockieren Sie Werbung und Pop-ups auf Facebook, YouTube, Twitch und Ihren...

[Entfernen](#)

Privacy Badger



Privacy Badger

www.eff.org [Vorgestellt](#)

Privacy Badger lernt automatisch, unsichtbare Tracker zu blocken.

★★★★★ 1.684 Produktivität