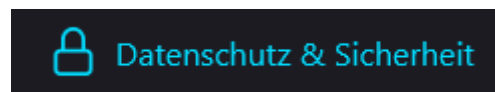
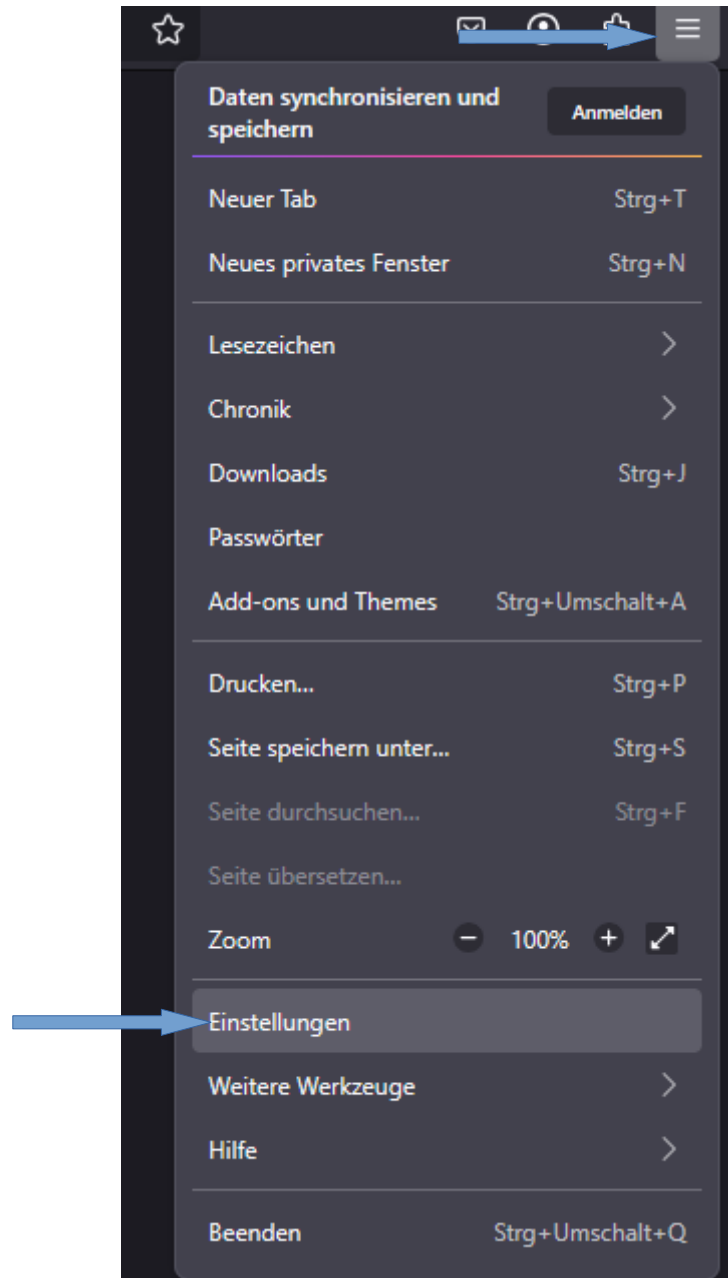


Firefox sicherer machen

Die in Firefox hinterlegten Einstellungen „Datenschutz & Sicherheit“ können durch gezielte Änderungen zur besseren Sicherheit beim browsen beitragen.

Vorgehensweise:

1. Einstellungen öffnen



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)
- Bekannte und vermutete Identifizierer (Fingerprinter)

⚠ Achtung!
Diese Einstellung kann dazu führen, dass einige Websites nicht korrekt Inhalte anzeigen oder funktionieren. Wenn eine Website defekt zu sein scheint, können Sie den Schutz vor Aktivitätenverfolgung für diese Website deaktivieren, um alle Inhalte zu laden. [Weitere Informationen](#)

Datenschutzinstellungen für Websites

Websites anweisen, meine Daten nicht zu verkaufen oder weiterzugeben [Weitere Informationen](#)
[Wir unterstützen das "Do Not Track"-Signal nicht mehr](#)

Cookies und Website-Daten

Die gespeicherten Cookies, Website-Daten und der Cache belegen derzeit 339 MB Speicherplatz. [Weitere Informationen](#)

Basierend auf Ihren Chronikeinstellungen löscht Firefox Cookies und Website-Daten aus Ihrer Sitzung, wenn Sie den Browser schließen.

Cookies und Website-Daten beim Beenden von Firefox löschen

Daten entfernen...
Daten verwalten...
Ausnahmen verwalten...

Keine Passwörter im Browser speichern

Passwörter

- Fragen, ob Passwörter gespeichert werden sollen [Ausnahmen...](#)
- Benutzernamen und Passwörter automatisch ausfüllen [Gespeicherte Passwörter](#)
- Starke Passwörter vorschlagen
- Firefox Relay-E-Mail-Masken zum Schutz Ihrer E-Mail-Adresse vorschlagen [Weitere Informationen](#)
- Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren [Weitere Informationen](#)
- Anmeldung am Gerät zum Ausfüllen und Verwalten von Passwörtern verlangen
- Hauptpasswort verwenden [Weitere Informationen](#) [Hauptpasswort ändern...](#)
Früher bekannt als Master-Passwort
- Windows Single Sign-on für Microsoft-, Geschäfts- und Schulkonten erlauben [Weitere Informationen](#)
Verwalten Sie Konten in Ihren Geräteeinstellungen.

Automatisch ausfüllen

- Adressen speichern und ausfüllen [Weitere Informationen](#) [Gespeicherte Adressen](#)
- Zahlungsmethoden speichern und ausfüllen [Weitere Informationen](#) [Gespeicherte Zahlungsmethoden](#)
Einschließlich Kredit- und Debitkarten
- Anmeldung am Gerät zum Ausfüllen und Verwalten von Zahlungsmethoden verlangen [Weitere Informationen](#)

Chronik

Firefox wird eine Chronik [niemals anlegen](#) [▼](#)

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

Pop-up-Fenster blockieren

[Ausnahmen...](#)

Warnen, wenn Websites versuchen, Add-ons zu installieren

[Ausnahmen...](#)

Datenerhebung durch Firefox und deren Verwendung

Wir bemühen uns, Ihnen die Wahl zu lassen und nur die Daten zu sammeln, die notwendig sind, um Firefox für alle zu verbessern. [Datenschutzhinweis ansehen](#)

Daten zu technischen Details und Interaktionen an Mozilla senden

Dies hilft uns, die Funktionen, Leistung und Stabilität von Firefox zu verbessern. [Weitere Informationen](#)

Personalisierte Erweiterungsempfehlungen erlauben

Erhalten Sie Empfehlungen für Erweiterungen, um Ihr Surferlebnis zu verbessern. [Weitere Informationen](#)

Studien installieren und durchführen

Probieren Sie Funktionen und Ideen aus, bevor sie für alle freigegeben werden. [Firefox-Studien ansehen](#)

Täglichen Nutzungs-Ping an Mozilla senden

Dies hilft Mozilla, aktive Benutzer zu schätzen. [Weitere Informationen](#)

Absturzberichte automatisch senden

Dies hilft Mozilla bei der Diagnose und Behebung von Problemen mit dem Browser. Die Berichte können persönliche oder sensible Daten enthalten. [Weitere Informationen](#)

Sicherheit

Schutz vor betrügerischen Inhalten und gefährlicher Software

Gefährliche und betrügerische Inhalte blockieren [Weitere Informationen](#)

Gefährliche Downloads blockieren

Vor unerwünschter und ungewöhnlicher Software warnen

Nur-HTTPS-Modus

Erlaubt nur sichere Verbindungen zu Websites. Firefox wird nachfragen, bevor eine unsichere Verbindung hergestellt wird.

[So funktioniert Nur-HTTPS](#)

[Ausnahmen verwalten...](#)

Nur-HTTPS-Modus in allen Fenstern aktivieren

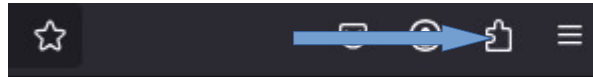
Nur-HTTPS-Modus nur in privaten Fenstern aktivieren

Nur-HTTPS-Modus nicht aktivieren

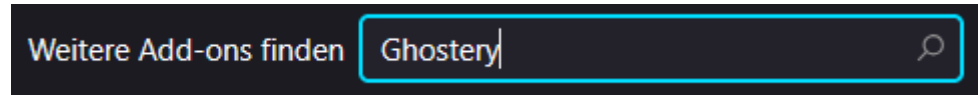
Firefox könnte trotzdem einige Verbindungen ändern [Weitere Informationen](#)

Installation eines Adblockers (z.B. Ghostery) – blockiert unerwünschte Webeinhalte -

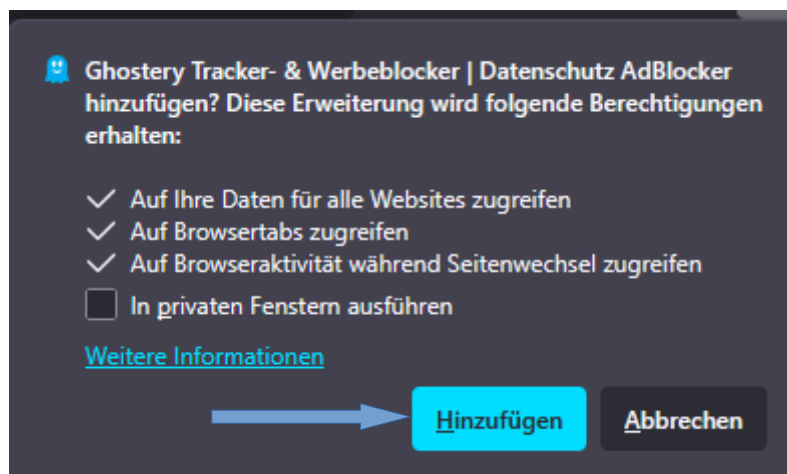
Symbol anklicken




Ghostery eingeben



Auf Eintrag klicken



 Ghostery Tracker- & Werbeblocker | Datenschutz AdBlocker wurde hinzugefügt.

Add-ons und Themes können über das Anwendungsmenü verwaltet werden.

OK