



Sicherer im Internet surfen

Gläserne Werbekunden zu schaffen und damit möglichst viel Geld zu verdienen, ist ein Traum aller Unternehmer. Und allen voran Google, Facebook und Co. Das ist ihre Daseinsberechtigung. Damit verdienen diese Unternehmen Geld.



Wer sich vor den Datenkraken im Internet schützen will, sollte einige Sicherheitsmaßnahmen beachten. Internetbrowser zum Beispiel lassen sich so einstellen, dass die Chronik, die gespeicherten Cookies und Websitedaten automatisch gelöscht werden, sobald man das Fenster schließt, oder mit wenigen Klicks manuell zu säubern sind.

Es gibt die Tools, die die Datenkraken im Zaum halten. Nicht immer. Aber spürbar.

Wissen und Informationen brauchen Sie und noch wichtiger - das Wissen in die Praxis umsetzen. Sonst nützt das alles nichts. Ist dann erst mal alles an Sicherheitsmaßnahmen umgesetzt, gilt es trotzdem wachsam zu sein.

PCA Wrana zeigt, wie man mit wenigen Klicks und Apps, Firefox, Edge und Google Chrome abschottet.

Ihre eigene Einstellung zu diesem Thema läßt das Vorhaben „sicherer im Internet surfen“ wahr werden.

Probieren geht über Studieren. Handeln Sie! Alle hier genannten Add-Ons, Programme und Einstellungen verwende ich für mich selbst.

Ihr Othmar Wrana

Inhalt und Links zu den Videos

Inhalt und Links zu den Videos.....	1
Links zu den VIDEOS:.....	1
Browser Anonymisieren	2
Ghostery für Firefox (5 Schritte und Einrichten).....	4
Ghostery für Internet Explorer.....	9
Ghostery für EDGE (6 Schritte + Einrichten)	10
Ghostery für Chrome (3 Schritte und dann wieder wie auf Seite 7 beschrieben).....	12
Die Suchmaschine Startpage.....	15
Startpage für Browser einrichten.....	15
Bilder zu Startpage einrichten	15
Firefox-Browser Einstellungen für sicheres Surfen.....	17
Chrome-Einstellungen für sicheres Surfen.	20
Edge Einstellungen für sicheres Surfen im Internet.....	23
NOTIZEN	25
Impressum	26

Links zu den VIDEOS:

Video zu Startpage: <https://youtu.be/7aJxnyRjGBA>

Video zu Browser-Einstellungen: https://youtu.be/M_nu0RxnPU4

Video zu Ghostery und uBlock Origin: <https://youtu.be/fLtGkht0-SY>

Sicherer im Internet surfen

Browser Anonymisieren

gilt für alle Browser, weil eigenständiges kleines Programm und kein Add-on

Hier DOWNLOAD

<https://www.almisoft.de/?cont=anonymisierer>

Installation

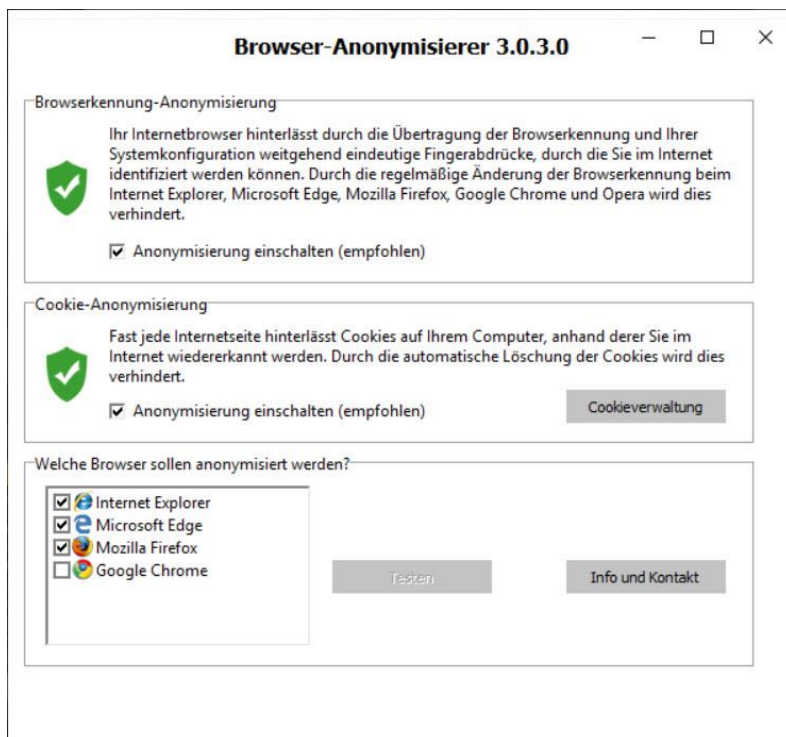
Wie ein Programm

Start

Mit Doppelklick auf das Programm-Icon auf dem Desktop

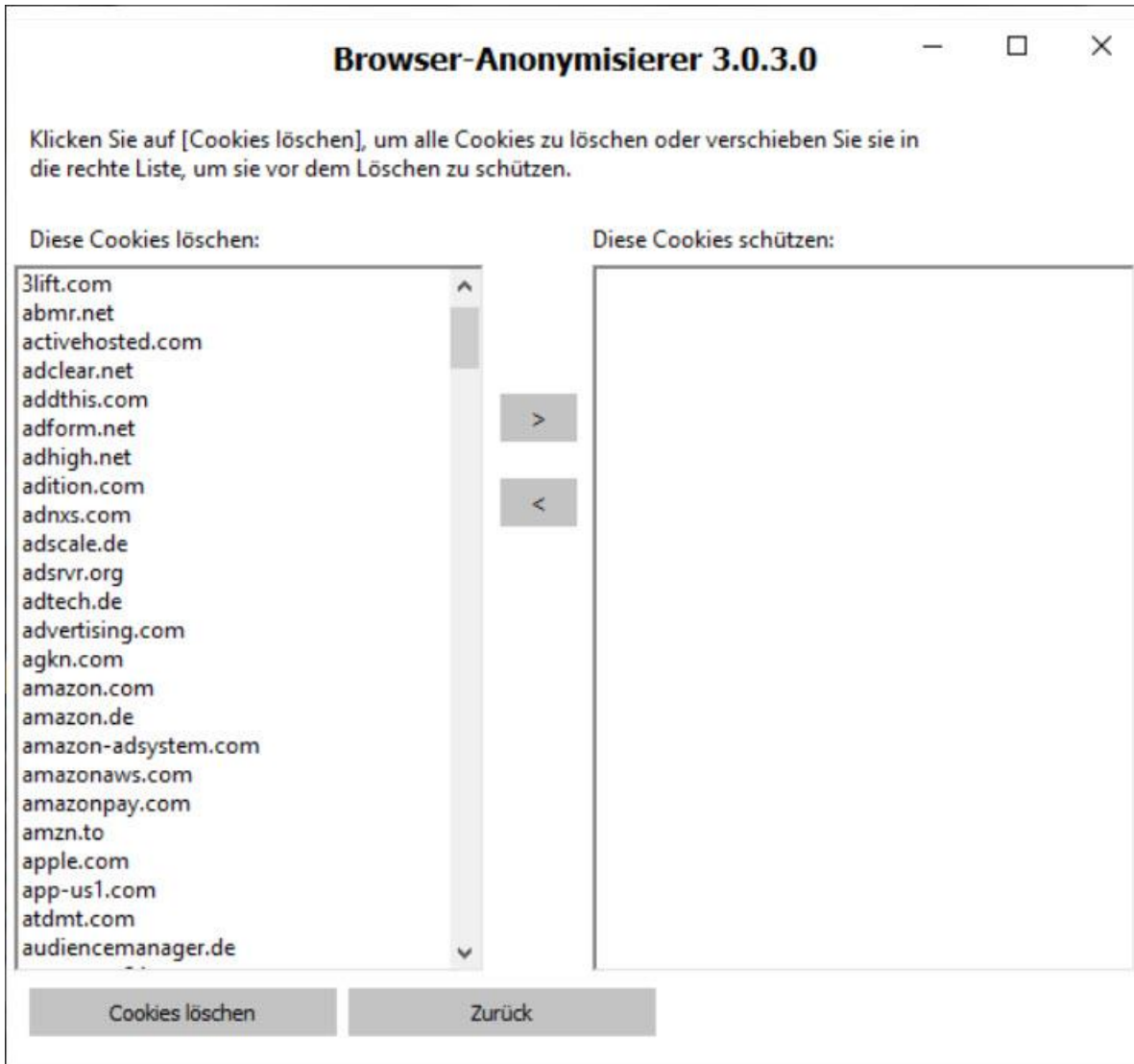


Einstellungen vornehmen



Cookieverwaltung

Wählen Sie die Einstellungen der Cookies so genau wie Sie Cookies benötigen. Ein paar Aktionen im Internet funktionieren nicht ohne Cookies und ein Löschen macht keinen Sinn. Aber nun können Sie ganz gezielt auswählen und speziell benötigte Cookies vor dem Löschen schützen.



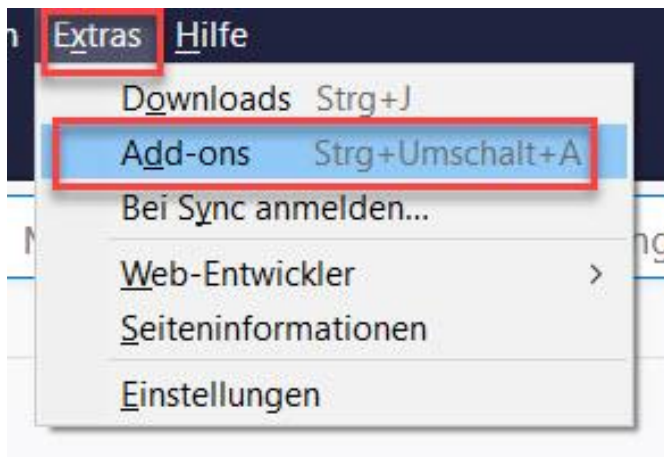
Ghostery für Firefox (5 Schritte und Einrichten)



Kein Download, aber hier schauen für mehr Informationen: <https://chrome.google.com/webstore/detail/ghostery-%E2%80%93-privacy-ad-blo/mlomiejdfkolichcflejclbcmpeanii?hl=de>

Installation Firefox

Schritt 1. Entweder im Menü unter EXTRAS – Add-ons (Bild 1)



Oder oben rechts im „Hamburger Menü“ die Add-ons auswählen (Bild 2)

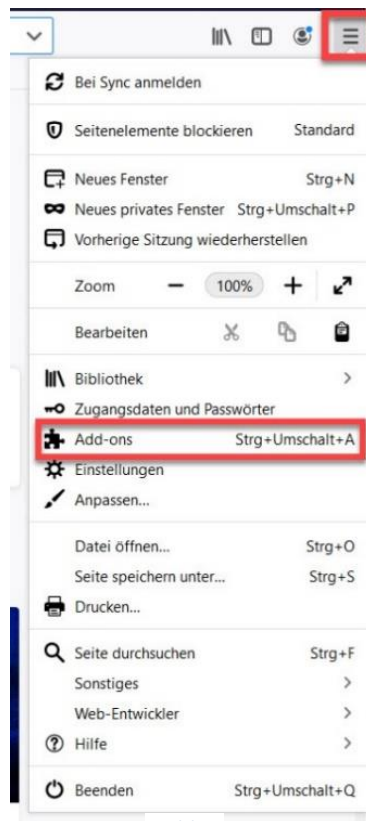


Bild 2

Sicherer im Internet surfen

Schritt 2, Punkt 1: Einstellungen wählen

Schritt 2, Punkt 2: In das Suchfeld Ghostery eintippen und mit ENTER suchen

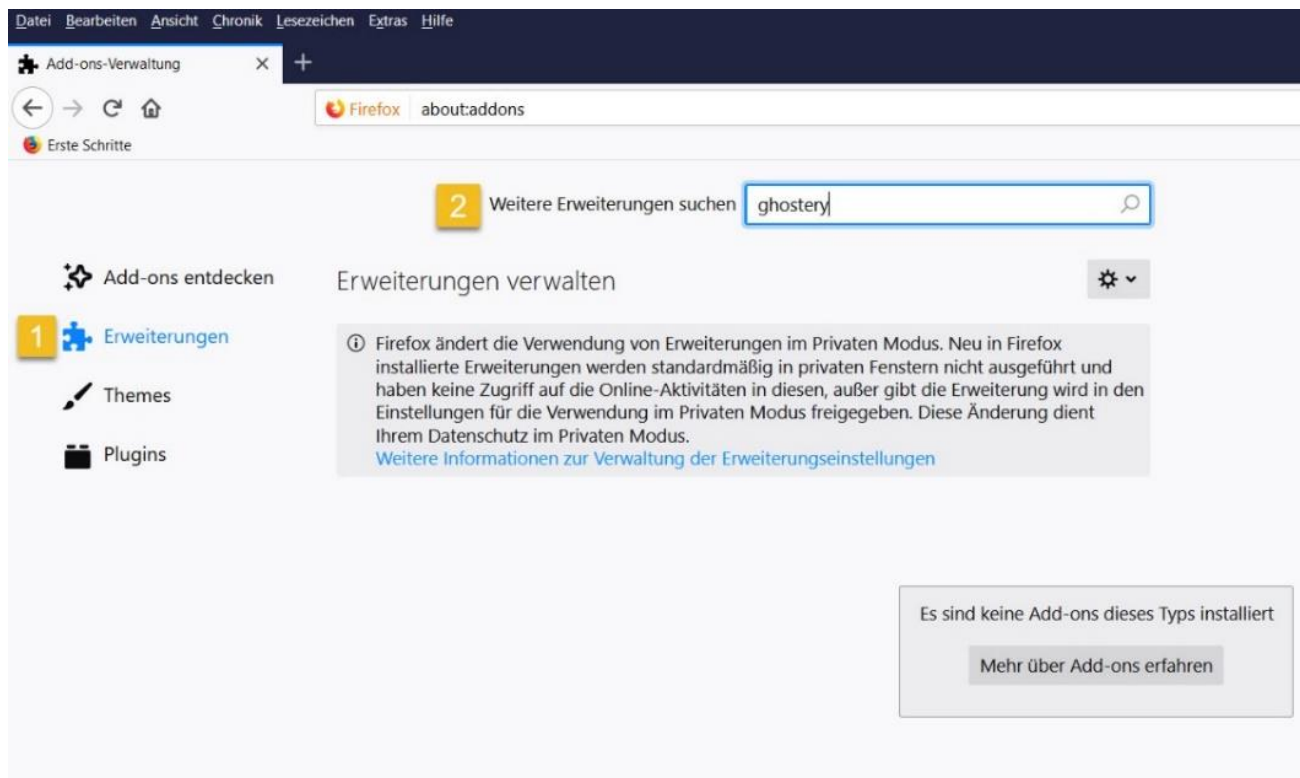


Bild 3

Schritt 3

Im darauffolgenden Fenster (Bild 4) klicken Sie auf Ghostery (Sie befinden sich damit in bester Gesellschaft)

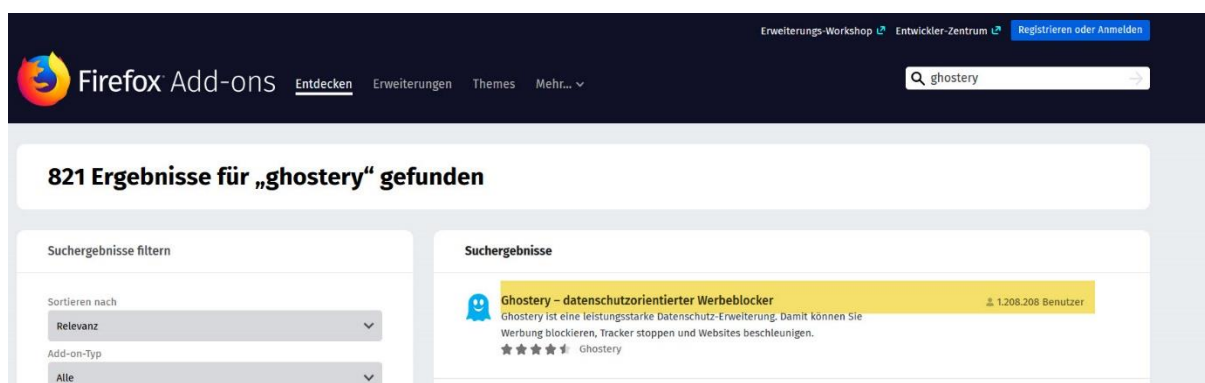


Bild 4

Schritt 4: zu Firefox hinzufügen

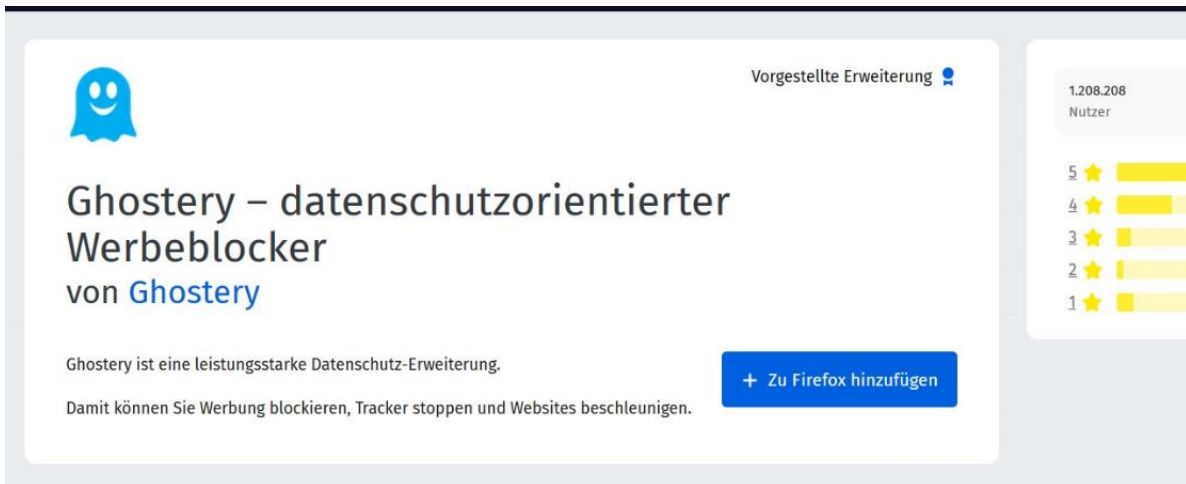


Bild 5

Schritt 5: wieder auf Hinzufügen klicken

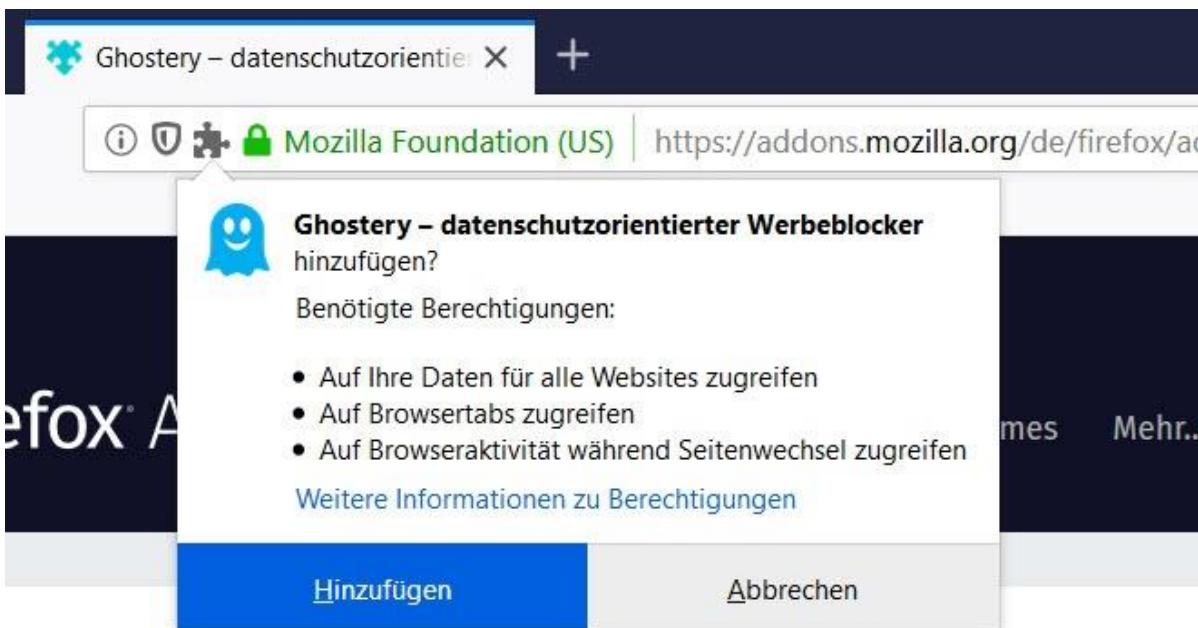


Bild 6

Letzter Schritt: Ghostery für FireFox fertig einrichten und sich mit Ghostery anfreunden

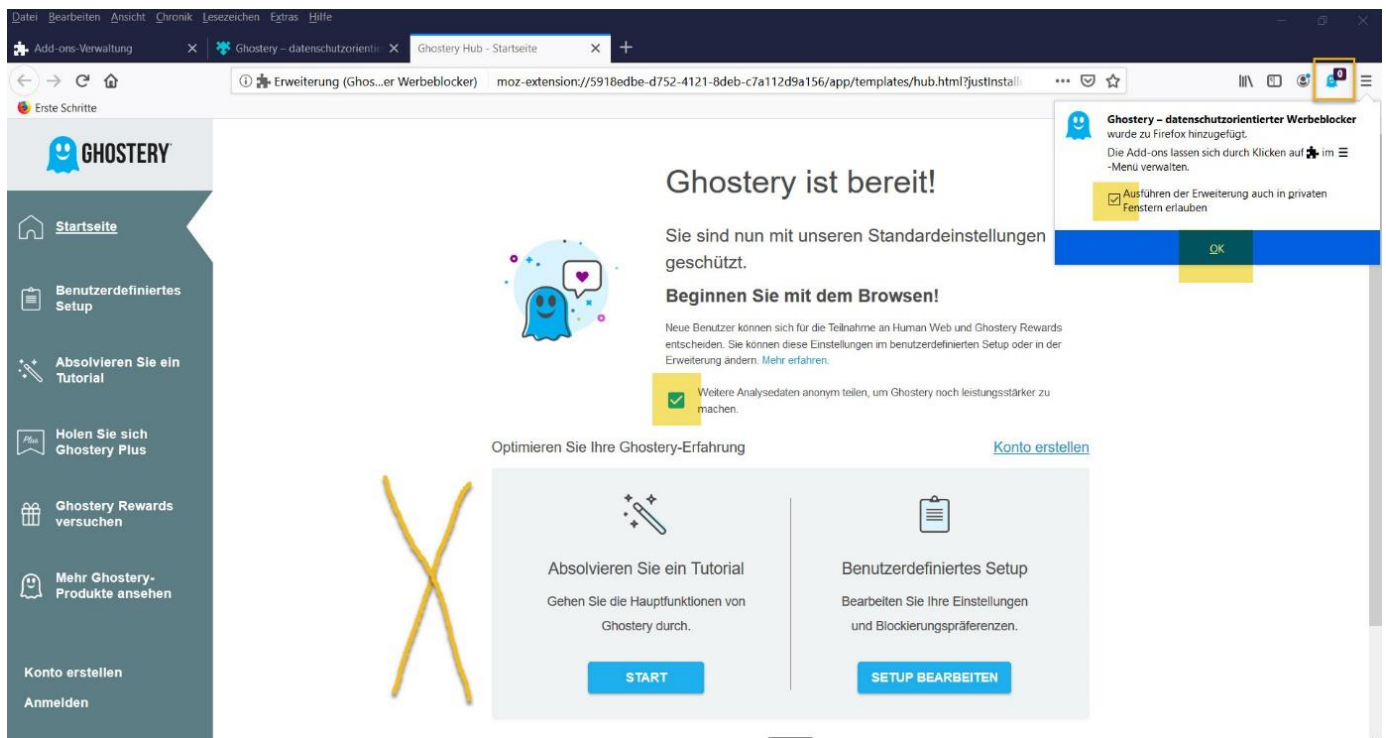
Beschäftigen Sie sich mit Ghostery. Schauen Sie sich die kurze Einführung von Ghostery an. Rufen Sie Ihre Lieblingsseite zum Einkaufen auf. Einmal mit Ghostery und anschließend ohne Ghostery. Dafür brauchen Sie Ghostery nur zu pausieren.

Es wird Webseiten geben, die Sie bitten, diesen Adblocker auszuschalten. Wenn Sie das nicht wollen, werden Sie die Inhalte nicht sehen. Ansonsten pausieren Sie Ghostery. Ihr Browser ist völlig in Ordnung, nur Ghostery kommt seiner Aufgabe nach.

Pausieren erklärt sich von selbst – Ghostery ist kurzfristig deaktiviert – und auf Knopfdruck wieder einzuschalten.

Deinstallation:

Rechtsklick auf Ghostery-Symbol in der Menüleiste und „Erweiterung entfernen“ wählen.





Ghostery für Internet Explorer

Lieber nicht den Internet Explorer verwenden. Ein Browser aus der alten Zeit. Ghostery Erweiterung für den alten Browser wird keine mehr angeboten, wie dem Bild zu entnehmen ist. Ein Grund mehr, sich jetzt endlich zu verabschieden.

Lade die Ghostery Browser-Erweiterung herunter

GHOSTERY BROWSER-ERWEITERUNG

 Clizq 8.1 Erweiterung Clizq	 Firefox 8.4.0 Erweiterung Firefox	 Chrome 8.4.0 Erweiterung Chrome	 Opera 8.4.0 Erweiterung Opera
 Edge 8.4.0 Erweiterung Edge	 Safari 5.5.0 Erweiterung Safari		

GHOSTERY LITE


Safari 1.0
Erweiterung Safari

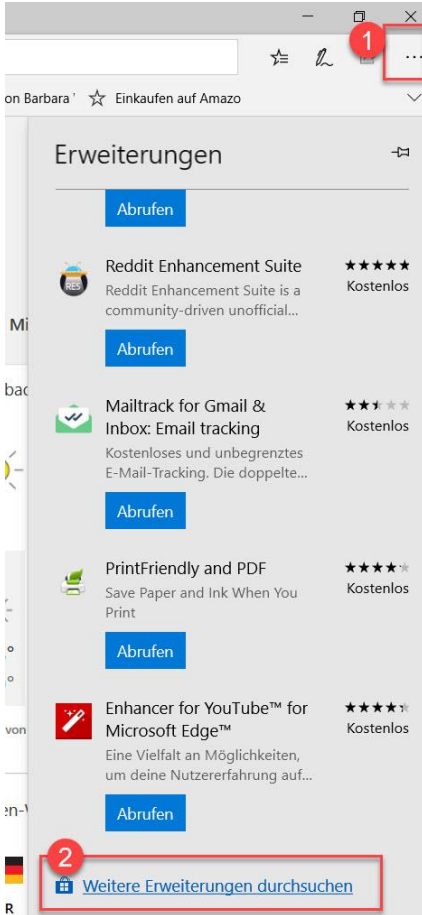
GHOSTERY MOBILER BROWSER

 Android 2.2  	 iOS 2.0.2 
--	---



Ghostery für EDGE (6 Schritte + Einrichten)

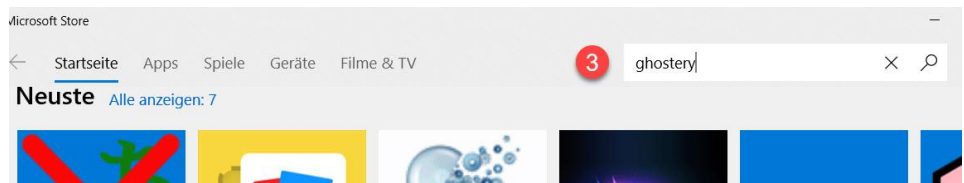
Installieren:



1. Menü

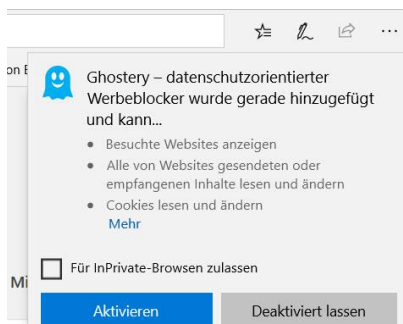
2. Weitere Erweiterungen durchsuchen

3. Ghostery eingeben und mit ENTER suchen



4. Klicken Sie Installieren (kein Bild)

5. Klicken Sie starten (kein Bild)



6. Aktivieren

7. Letzter Schritt wie auf Seite 7

Deinstallation - mit Rechtsklick auf Ghostery-Symbol in der Menüleiste - VERWALTEN – DEINSTALLIEREN

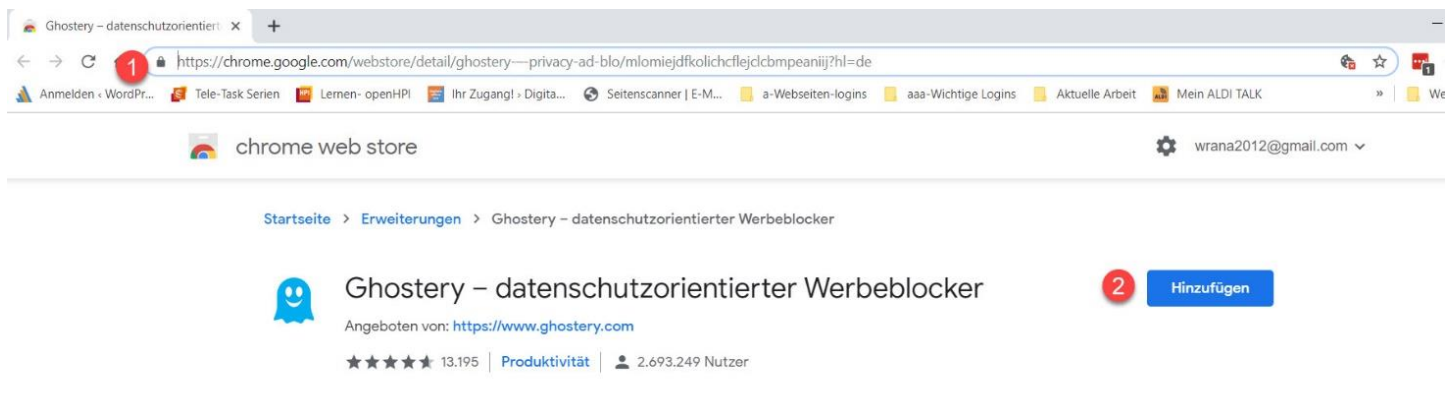
Ghostery für Chrome (3 Schritte und dann wieder wie auf Seite 7 beschrieben)



1. Rufen Sie in Chrome diese Seite auf (Punkt 1 im Bild):

<https://chrome.google.com/webstore/detail/ghostery---privacy-ad-blo/mlomiejdfkolichcfejlclcbmpeanii?hl=de>

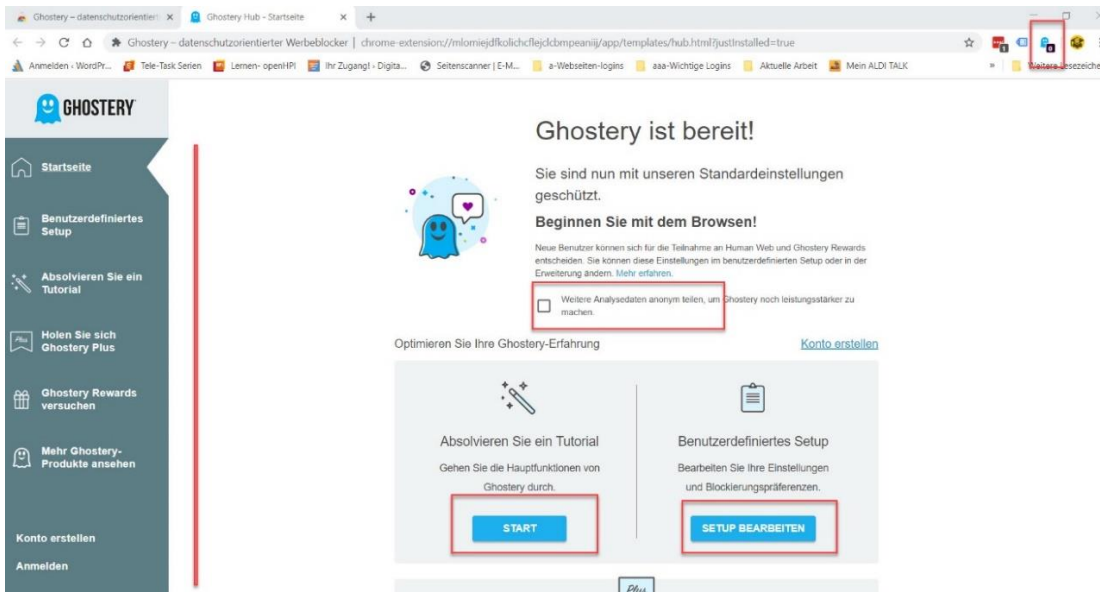
2. Klicken Sie auf Hinzufügen



3. Erweiterung hinzufügen



Letzter Schritt wie auf Seite 7. Beschäftigen Sie sich mit Ghostery.



Die Suchmaschine Startpage

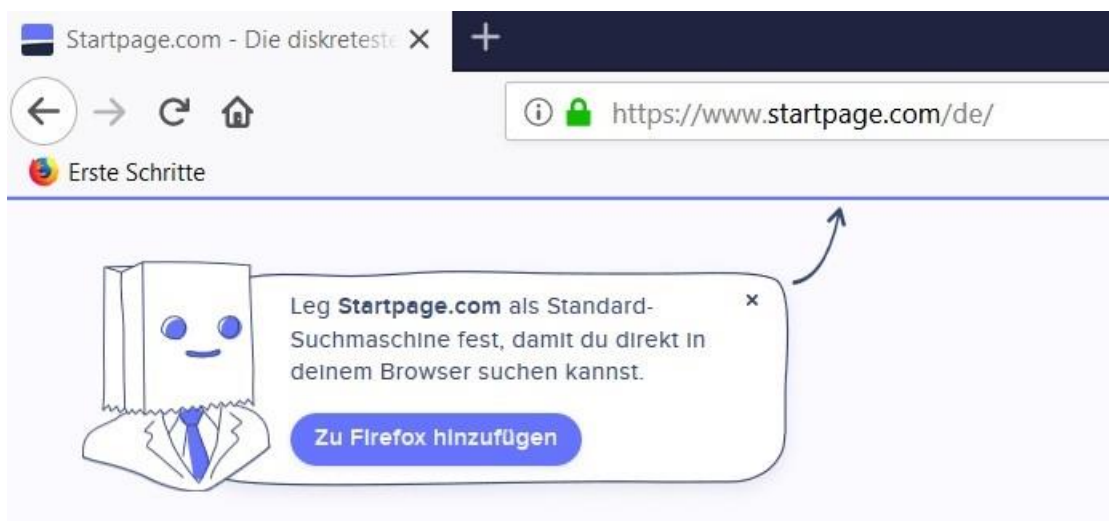
Startpage ist eine weniger neugierige Suchmaschine als Google. Startpage war früher Ixquick! Ixquick wird seit 2016 nicht mehr unterstützt.

- „...Startpage erfasst im Gegensatz zu Google keine [IP-Adressen](#) der Nutzer. Es werden auch keine [Cookies](#) zur Identifizierung der Nutzer benutzt. Des Weiteren werden Daten nicht gespeichert und nicht an Dritte weitergegeben. Es besteht die Möglichkeit, eine verschlüsselte Verbindung zu benutzen. Ein kostenloser [Proxy](#)-Service ermöglicht außerdem ein anonymes Surfen im Internet...“
mehr zu diesem Thema in [Wikipedia nachzulesen](#).
Quelle: Aus Wikipedia

Startpage für Browser einrichten

- Starten Sie den Browser Ihrer Wahl und wählen Sie diese Internet-Adresse
- <https://www.startpage.com/de/>
- Für Firefox und Chrome folgen Sie den Dialogen und installieren Startpage als Standardsuchmaschine. Edge arbeitet etwas anders. Dort sehen Sie nicht diesen Papiertütenkopf, sondern scrollen etwas nach unten um dort einen Button zu drücken. Sie werden es erkennen. Alles wird gut beschrieben und mit welchem Browser Sie gerade unterwegs sind, wird automatisch erkannt. Ja, manchmal hat’s auch was, wenn man erkannt wird.
- Später kontrollieren Sie, ob Startpage tatsächlich als Standard-Suchmaschine eingestellt ist.

Bilder zu Startpage einrichten



Firefox-Browser Einstellungen für sicheres Surfen

Hinweis: im Folgenden nur die wichtigsten Einstellungen

Über EXTRAS – EINSTELLUNGEN sofern Sie die Menüleiste sichtbar haben oder



Hamburger Menü oben rechts und dann EINSTELLUNGEN

Linke Seite: Datenschutz & Sicherheit

Seitenelemente blockieren: Standard

Do not track: immer

Cookies und Website-Daten wie im Bild



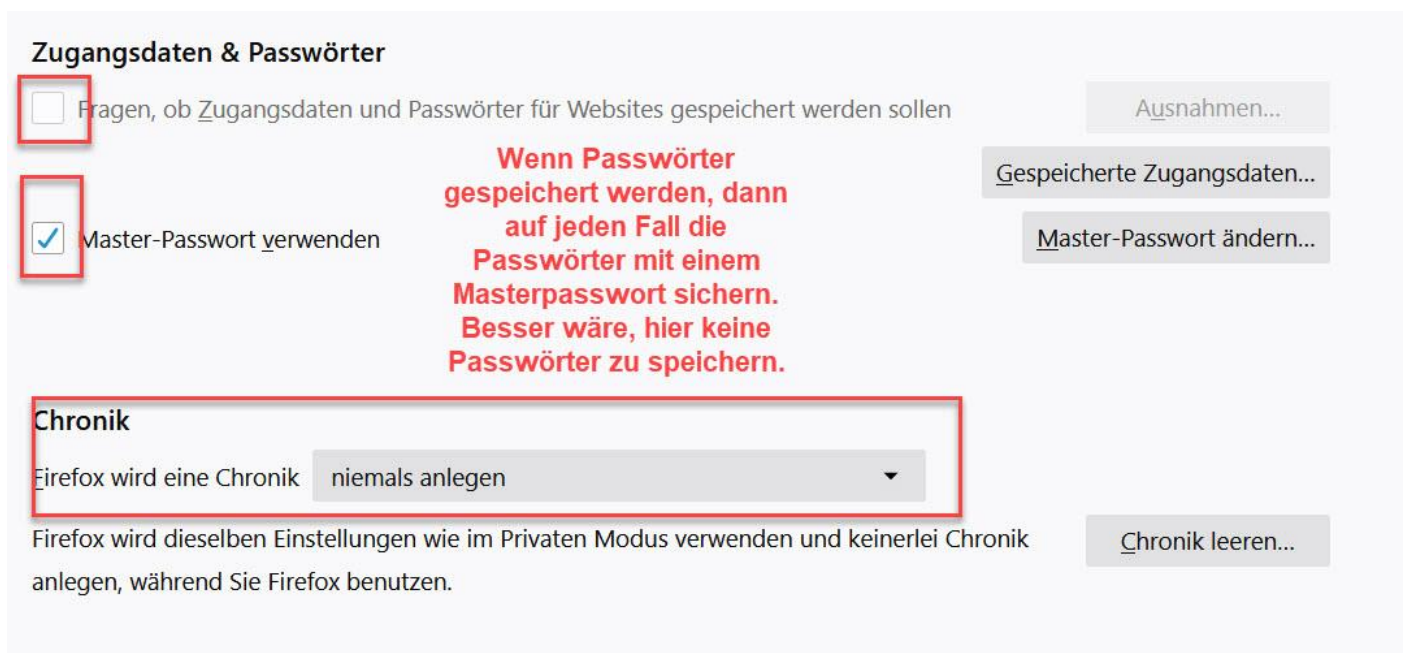
Cookies und Website-Daten
Die gespeicherten Cookies, Website-Daten und der Cache belegen derzeit 7,0 MB Speicherplatz. [Weitere Informationen](#)

ⓘ Wenn der Private Modus immer verwendet wird, löscht Firefox Cookies und Website-Daten beim Beenden.

Cookies und Website-Daten beim Beenden von Firefox löschen

Daten entfernen...
Daten verwalten...
Berechtigungen verwalten...

Zugangsdaten – Passwörter – Chronik wie im Bild



Zugangsdaten & Passwörter

Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen

Master-Passwort verwenden

Wenn Passwörter gespeichert werden, dann auf jeden Fall die Passwörter mit einem Masterpasswort sichern. Besser wäre, hier keine Passwörter zu speichern.

Ausnahmen...
Gespeicherte Zugangsdaten...
Master-Passwort ändern...

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 leeren...

Berechtigungen wie im Bild

Berechtigungen

- Standort [Einstellungen...](#)
- Kamera [Einstellungen...](#)
- Mikrofon [Einstellungen...](#)
- Benachrichtigungen [Weitere Informationen](#) [Einstellungen...](#)
 - Benachrichtigungen bis zum Neustart von Firefox deaktivieren
- Automatische Wiedergabe von Audio-Inhalten verhindern [Ausnahmen...](#)
- Pop-up-Fenster blockieren [Ausnahmen...](#)
- Warnen, wenn Websites versuchen, Add-ons zu installieren [Ausnahmen...](#)
- Externen Anwendungen den Zugriff auf den Dienst für Barrierefreiheit in Firefox verweigern [Weitere Informationen](#)

Datenerhebung und Sicherheit wie im Bild

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](#)

- Firefox erlauben, Daten zu technischen Details und Interaktionen an Mozilla zu senden [Weitere Informationen](#)
 - Firefox das Installieren und Durchführen von Studien erlauben [Firefox-Studien ansehen](#)
 - Personalisierte Erweiterungsempfehlungen durch Firefox [Weitere Informationen](#)
- Nicht gesendete Absturzberichte automatisch von Firefox senden lassen [Weitere Informationen](#)

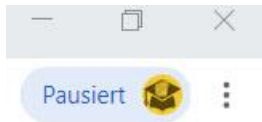
Sicherheit

Schutz vor betrügerischen Inhalten und gefährlicher Software

- Gefährliche und betrügerische Inhalte blockieren [Weitere Informationen](#)
 - Gefährliche Downloads blockieren
 - Vor unerwünschter und ungewöhnlicher Software warnen

Chrome-Einstellungen für sicheres Surfen.

Beginnen Sie mit Klick auf das 3-Punkte Menü und wählen Einstellungen

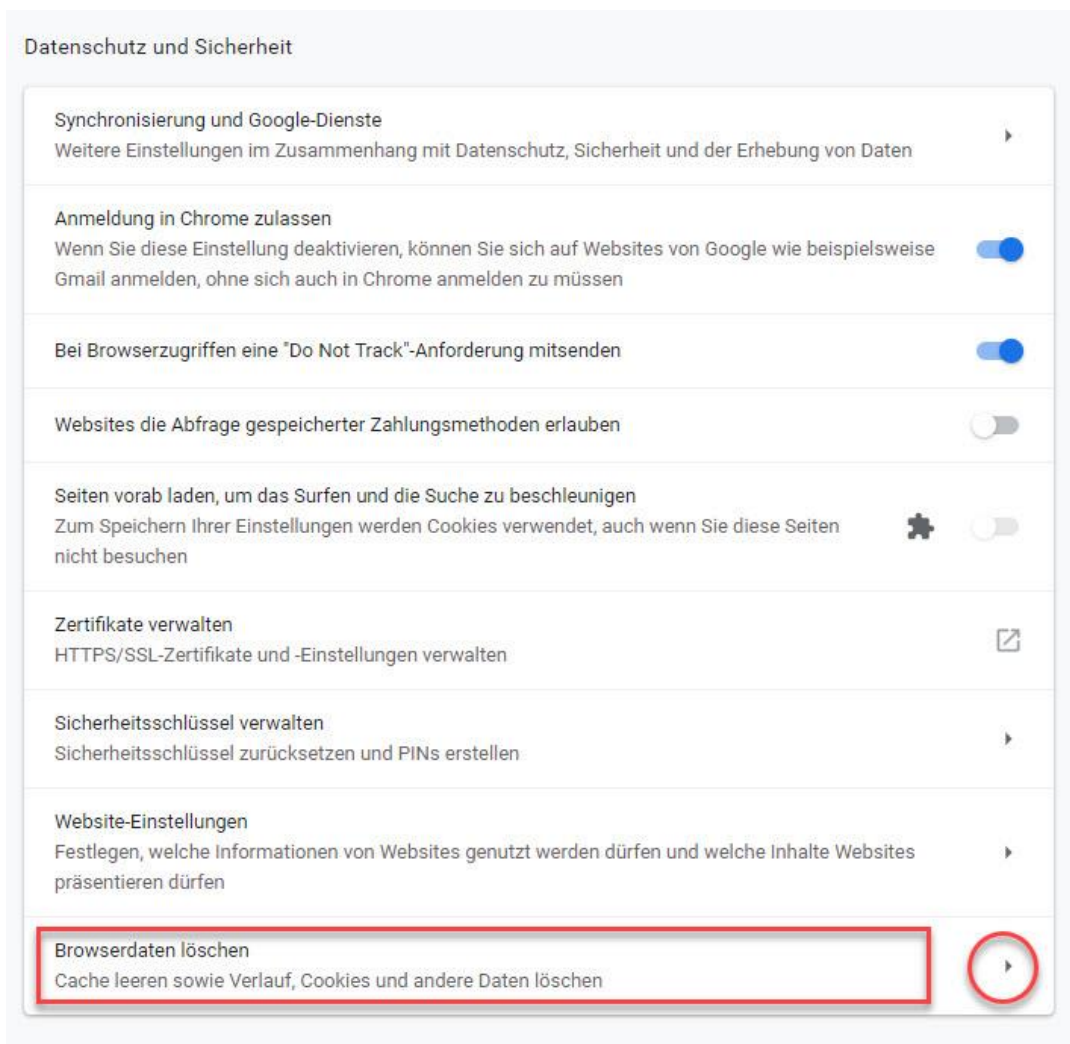


Autofill

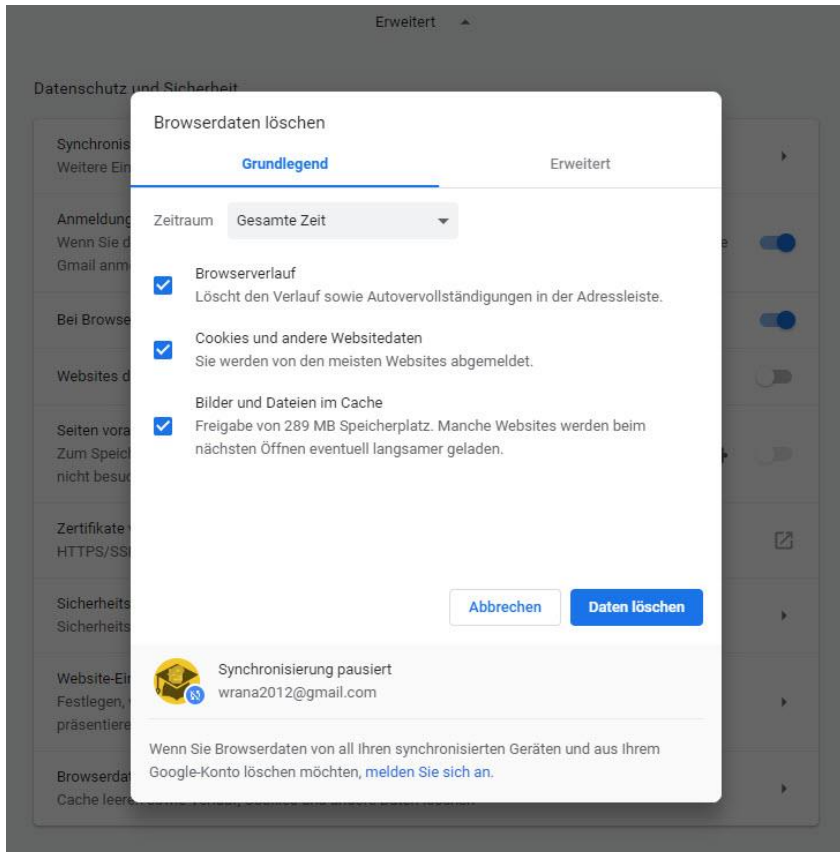
Alle Schalter für Passwörter – Zahlungsmethoden – AntiFill-Einstellungen sollten hier links stehen, d.h. deaktiviert sein

Weiterscrollen auf ERWEITERT und dort mit Klick diese Rubrik öffnen

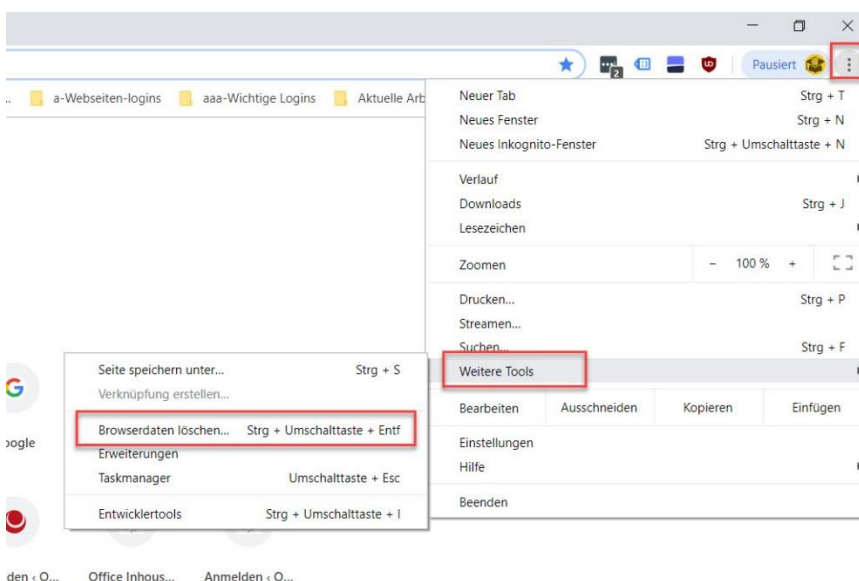
Datenschutz und Sicherheit wie im Bild



Klicken Sie zum Schluss auf den Pfeil von Browserdaten löschen und wählen Sie den Zeitraum und die Datenarten, die Sie löschen möchten. Im Tab "Erweitert" sind die Daten genauer beschrieben. Anschließend klicken Sie auf DATEN LÖSCHEN.



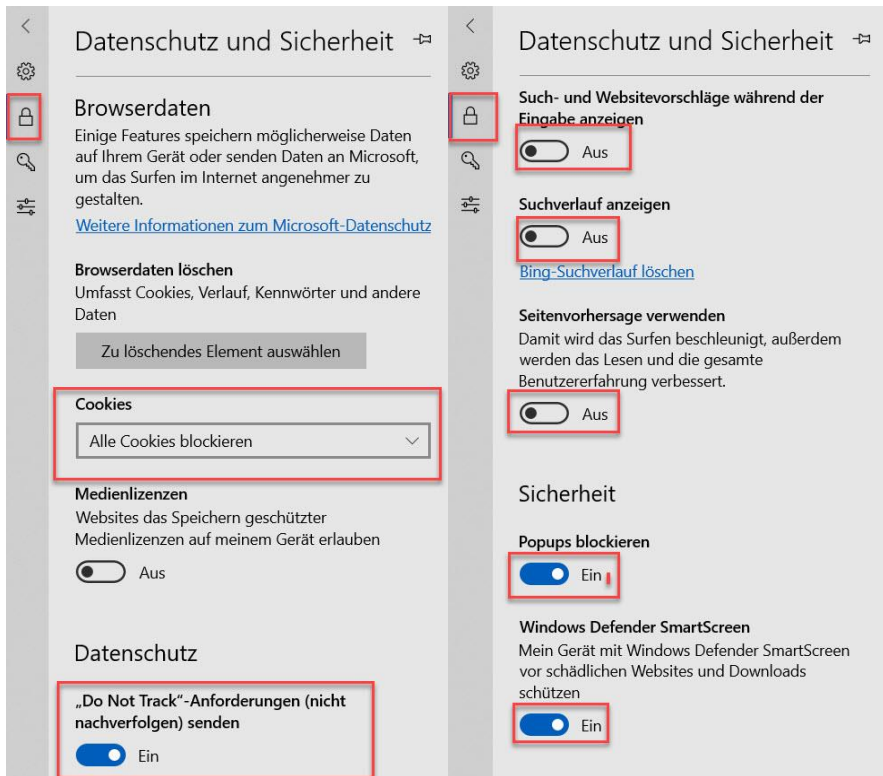
Kurzer Weg, damit man nicht immer durch alle Einstellungen muss.



Edge Einstellungen für sicheres Surfen im Internet

Öffnen Sie die Einstellungen: 3 Punkte Menü oben rechts und anschließend EINSTELLUNGEN anklicken

Nehmen Sie Einstellungen vor wie in den Bildern



Kennwörter und AutoAusfüllen



Im letzten Befehl **ERWEITERT**



Stellen Sie bitte ein:



Das waren die notwendigsten Einstellungen.

NOTIZEN

Impressum

Othmar Wrana

PCA Wrana

Hunsrückstr. 68

65205 Wiesbaden

☎ **0151-252 362 83**

✉ wrana@inhouseschulung.com

Präsenzschulung in Firmen (**Inhouse-Schulungen**)

und alle Videobeiträge in meinem BLOG

<https://office-inhouse-schulung.de>

Office Online Coaching bei akuten Fragen

und **persönliche Hilfestellung** per Fernwartung:

<https://inhouseschulung.com>

E-Learning Office-Kurse finden Sie im Member-Bereich Gratis und kostenpflichtige Videoschulungen
(noch im Aufbau: bitte schauen – kann sich schon geändert haben):

<https://digitale-office-uni.de>

YouTube Kanal:

<https://www.youtube.com/c/OthmarWrana>