Mein Browser - wie bringe ich die Plaudertasche zum Schwweigen?

Michael Georg Schmidt

Jahreskonferenz nr 2023 - 16./17. Juni 2023

Kontakt

E-Mail: info@its-explained.com | Threema-ID: WYH86UFA

Zusammenfassung

Dieses Skript erläutert, welche Daten, welche Browser ausplaudern. Einige sind sehr geschwätzig und neugierig, andere wahren den Datenschutz besser. Sie erfahren, was Sie tun können, um möglichst wenig von Ihren Daten zu verraten.
Zusätzlich stellt dieses Skript Anwendungen vor, bei denen Sie die Herrschaft über Ihre Daten vollständig aufgeben - dennoch nutzen viele sie.

Inhaltsverzeichnis

1 Tests zum Datenschutz

Browser verraten den Websitebetreibern von sich aus eine Menge an Daten. Welche das sind, können Sie mit Hilfe der folgenden Websites selber ausprobieren – und sich wundern, wie viele Daten von Ihnen in die Welt gehen.
Die ***EFF (Electronic Frontier Foundation)*** ist eine amerikanische Bürgerrechtsorganisation, die eine Website zur Verfügung stellt, die bewertet, wie einzigartig der Browsers von Nutzer:innen ist. Die Site trägt den Namen ***amiunique.org***. Sie finden sie hier: Am I unique?.
Auch von der EFF stammt die Seite ***coveryourtracks***. Hier sehen Sie, wer Sie womit verfolgt. Testen können Sie das hier: Cover Your Tracks. Mit Hilfe der Site ***browserleaks.com*** können Sie hier Browserleaks nachvollziehen, was Ihr Browser alles ausplaudert. Gegen die Werkzeuge von ***fingerprintJS***, die einen Fingerprint erstellen, ist noch kein Kraut gewachsen. Sie können es hier: FingerprintJS selbst ausprobieren.

2 Brave/Chrome/Edge/Firefox/ Opera/Safari/Vivaldi

Welchen Einfluss Cookies auf unsere Privatsphäre haben hängt auch vom benutzten Browser ab, denn die gehen ganz unterschiedlich mit Cookies und Datenschutz um.
Die Websitebetreiber und Werbetreibenden setzen vielfältige Methoden ein, um die Daten der Nutzer:innen zu erlangen. Ein Erfolg versprechendes Verfahren ist dabei das

3 Browser Fingerprinting

Dabei werten die Websites neben gesetzten Cookies auch Daten aus, wie die Konfiguration des Browsers, des genutzten Systems, installierter Programme, installierter Schriften und vielem mehr. Wer darüber mehr erfahren möchte, kann selbst Tests dazu durchführen.
Die ***EFF*** bietet dafür Websites an.
Die Site ***amiunique*** zeigt, wie ***einzigartig*** das eigene System ist. Während wir als Menschen stolz darauf sind, wenn wir einzigartig sind, ist dies bei Browsern weniger gut, denn so ist es deutlich leichter, uns wiederzuerkennen.
Zusätzlich bietet die EFF eine Website an, die anzeigt, mit welchen Daten wir verfolgt werden. Diese Site heißt ***coveryourtracks***.
Bereits ***vier der hier aufgeführten (Meta)Daten*** reichen nachweislich aus, um Sie zu identifizieren. Wissenschaftlich nachgewiesen haben das ***Yves-Alexandre de Monjoye et all***. In den ***Quellen*** finden sie noch einige weitere Hinweise auf Informationen zu Metadaten.
Vor allem lästig sind ***Consent Banner***, die fragen die Nutzer:innen beim Aufruf einer Website immer, ob diese mit diversen Cookies einverstanden sind. Man sollte sich die Mühe machen, die ***Optionen*** oder ***Einstellungen*** anzusehen, denn hier kann man einiges an Spionageteilchen abschalten.
Eher unerwartet können auch ***Favicons*** zu den Bösewichten gehören, die Daten sammeln. Favicons sind die kleinen Bildchen, die Sie links neben der Adresse der aktuell aufgerufenen Website sehen. Sie können Daten speichern, obwohl ***AntiTracking Maßnahmen*** ergriffen wurden, der ***Browserverlauf*** gelöscht oder der ***Incognito Mode*** aktiviert ist. Dies gilt zum Glück nur für Ausnahmen und ist nicht der Regelfall.
Um einen ***Browser Fingerprint*** zu erzeugen sind ***Audio APIs*** sehr gut geeignet, um Nutzer zu identifizieren. Hierbei handelt es sich um Schnittstellen des Browsers für Audioausgaben.
Neben dem „normalen Browser Fingerprinting“ unterscheidet man auch zwischen ***Canvas Fingerprinting*** und dem Fingerprint der Firma ***FingerprintJS***.
Canvas Fingerprints sind Codeschnipsel, die Bilder und Text für den Nutzer unsichtbar rendern, also so etwas ähnliches tun, wie eine Formatierung vorzunehmen. Je nachdem wie sich die betroffenen Inhalte verhalten, kann der Anwender feststellen, welchen Browser die Nutzer:innen einsetzen.
FingerprintJS ist eine Firma, die eine Schnittstelle für Websites anbietet, die mit Java Script Code herausfindet, um welchen Browser es sich handelt,

den die Nutzer:innen gerade benutzen. Dies erkennt die Software mit einer Genauigkeit von 99,5 %, so der Hersteller.

4 Browser

Ein Browser ist das Programm mit dem Sie ins Internet gehen. ***Brave*** ist hier der Musterknabe, während ***Edge (von Microsoft)*** ein Browser ist, dem man lieber aus dem Weg gehen sollte, wenngleich er auf ***Chromium***, also dem Unterbau von ***Googles Chrome*** basiert. Im Einzelnen

4.1 Brave

Brave ***basiert auf Chromium*** und aktualisiert beim Aufruf des Browsers die Daten für ***AddBlocker*** und unsichere Seiten. Dafür ruft er die Daten von ***EasyList / Easy Privacy*** und ***uBlockOrigin*** ab. Weitere Listen mit entsprechenden Daten können Nutzer:innen nachträglich selbst ergänzen. Zusätzlich überträgt Brave jedoch auch Diagnosedaten an die URL ***b3a.brave.com***. Diese Daten sind vollständig anonymisiert. Sobald es mehr als vier Daten sind, die Brave hier überträgt, ist jedoch eine Deanonymisierung möglich. Sie können und sollten, diese Funktion daher deaktivieren.
Suchanfragen können über ***DoH (DNS over HTTPS)*** gesandt werden. Somit senden die Nutzer:innen ihre Anfragen verschlüsselt und es kann nicht jeder mitlesen, welche Anfragen die Nutzer:innen stellen.
Als ***Standardsuchmaschine*** ist ***DuckDuckGo*** voreingestellt. Dabei handelt es sich zwar um eine amerikanische Suchmaschine, jedoch verspricht sie, keine Daten der Nutzer zu speichern und keine Profile anzulegen. Allgemein gilt DuckDuckGo als Suchmaschine die vertrauenswürdig ist.
Brave ist Werbung gegenüber nicht ganz abgeneigt, wenn die Nutzer:innen damit einverstanden sind. Dieser zurückhaltenden Werbung mit dem Namen ***Brave Rewards*** müssen die Nutzer:innen explizit zustimmen. Der Sinn dahinter ist, dass Brave mit dieser Werbung Geld verdient. Die Nutzer:innen haben auch etwas davon, denn wenn sie zustimmen, sammelt Brave für sie Kryptogeld in einem integrierten ***Wallet (digitale Geldbörse)***. Die „Einnahmen“ zahlt Brave monatlich in die Wallet ein. Um zu überprüfen, ob Werbung am Brave Rewards Programm teilnimmt, sendet Brave an sein Mutterhaus gelegentlich einen vierstelligen Hash.
Für privates Surfen bietet Brave als einziger Browser einen integrierten

TOR Client an, der es möglich macht das ***Onion-Netzwerk*** ohne weitere Installationen zu nutzen. TOR ist ein Browser, der ein weitestgehend anonymes Surfen ermöglicht ***(TOR = Tor Onion Router)***.
Bereits im Auslieferungszustand hat Brave eine Konfiguration, die gut vor Datenmissbrauch schützt. Sogar vor dem ***Canvas Fingerprinting*** bietet Brave einen Schutz. Gegen ***FingerPrintJS ist leider auch Brave machtlos***.

4.2 Chrome

Chrome ist der Browser von ***Google*** dem ***Chromium*** zu Grunde liegt. Chrome ist nicht schlecht, aber sendet jede Eingabe in Echtzeit an Google, um den Nutzer:innen Vorschläge für ihre Suche zu unterbreiten. Das ist nicht so schön, weil Google damit umgehend die Eingaben speichert und dem Profil der Nutzer:innen zuordnen kann, auch wenn eine Eingabe wieder gelöscht wurde. Chrome lädt Daten für ***Add-Blocker*** und ***maliziöse Websites*** nach. Im Browser ist ***DoH*** konfigurierbar. Die Funktion ***Do not Track*** ist ebenfalls aktivierbar, jedoch gilt dieses Projekt als gescheitert und wirkungslos. Die ***Standardsuchmaschine*** von Chrome ist ***Google***, das als Datenkrake bekannt ist.

4.3 Edge

Edge ist der schlechteste Kandidat dieser Reihe. Der Browser stammt von ***Microsoft***. Mit dem ***Internet Explorer*** und eine ganze Zeit lang auch mit Edge hat Microsoft einen selbst entwickelten Browser betrieben. Seit einiger Zeit jedoch basiert Edge auf ***Chromium*** und ist damit performanter und weniger störanfällig als es die alten Versionen waren. Zusätzlich hat Edge damit die Möglichkeit alle Add-ons von Chrome zu nutzen.
Die ***Standardsuchmaschine*** von Edge ist ***Bing***, die Microsoft eigene Suchmaschine. Bing überträgt in Echtzeit alle Eingaben an Microsoft. Das führt zur Vervollständigung von Profilen. Bedauerlich ist, dass diese Funktion sogar im privaten Modus, der sich hier ***inPrivate*** nennt, aktiv ist. Sie ist nicht abschaltbar. Nicht nur bei den Eingaben ist Microsoft so neugierig, sondern auch bei den aufgerufenen URLs. Das heißt, dass Microsoft ganz genau wis-

sen will, welche Websites sich die Nutzer:innen angesehen haben.
Genauso ist die Funktion die erforderliche Diagnosedaten an Microsoft sendet, nicht abschaltbar. Hier stellt sich die Frage, weshalb Edge welche ***Diagnosedaten*** als erforderlich klassifiziert. Einige andere Browser nutzen ebenfalls ***Chromium*** als Basis und kommen ohne den Versand dieser Diagnosedaten zurecht.
Um dem ***Tracking*** zu entgehen müssen die Nutzer:innen den strengen Modus aktivieren, denn bei allen anderen Einstellungen ist diese Funktion recht wirkungslos. Das hat System, denn Microsoft selbst überlädt neu aufgerufene Browser Tabs mit Werbung und Trackern der Anbieter ***Tabula***, ***Zemanta***, ***ScorecardResearch***.
Erst mit ***Add-ons*** wie ***Customize your new Tab Page (Neuer Tab – Seite personalisieren)*** und ***Tabliss*** ist es möglich, dieser Unsitte Einhalt zu gebieten.

4.4 Firefox

Auch ***Firefox*** ist beim Start nicht stumm. Er nimmt Kontakt zur Adresse ***detectportal.firefox.com/success.txt*** auf. Diese Aktion kann man dem Browser allerdings leicht verzeihen, denn er überprüft auf diese Weise lediglich, ob eine Verbindung zum Internet besteht. Auch zu ***Google*** unterhält Firefox Beziehungen. Hier lädt er Bibliotheken von ***Widevine*** herunter. Widevine ist ein Tool, um angebotene Inhalte zu schützen. Insofern ist dieses Vorhaben durchaus lobenswert. Zusätzlich kontaktiert Firefox die Site ***openh264.org***. Hier lädt Firefox Videocodecs herunter um möglichst viele Videoformate darstellen zu können. Nachteil hieran ist, dass Websitebetreiber dies zum ***Browser Fingerprinting*** missbrauchen können.
Um aufgerufene Seiten auf mögliche Schädlichkeit überprüfen zu können, lädt Firefox auch entsprechende Dateien von Google herunter. Die Überprüfung findet offline statt. Somit ist Google von der Information, welche Sites die Nuterz:innen aufgerufen haben, abgeschnitten. Firefox bietet als einer von

zwei Browsern (Opera hat dies auch) ein eingebautes ***VPN (Virtual Private Network)*** an. Da der gesamte Datenverkehr der Nutzer:innen über den Anbieter eines VPNs fließt, ist zwingende Voraussetzung für einen sinnvollen Einsatz dieses VPNs, dass man dem Anbieter trauen kann. Firefox bedient sich hierfür des Anbieters ***Mullvad VPN*** – Mullvad VPN. Mullvad bietet seine VPN-Dienste zu günstigeren Preisen als Firefox an.

4.5 Opera

Opera scheint für und vermutlich von Werbung zu leben. Neben vielfältigen Links zu Onlineshops, die auf neu aufgerufenen Tabs erscheinen, lädt der Browser heimlich im Hintergrund die ***Add-ons Rich Hint Agent*** – ein Add-on, das zum ***Cashbackdienst Dify*** gehört und den ***Aliexpress Observer*** nach. Letzterer gehört zum ***Onlinehändler Ali Express***, dem chinesischen Pendant von Amazon. ***Amazon*** ist aber auch vertreten, denn Opera bringt den ***Amazon Assistent*** von Haus aus mit.
Die heimlich nachgeladenen Add-ons bleiben für den Nutzer unsichtbar. Die ***voreingestellte Suchmaschine ist Google***. ***Google*** erhält auch ***in Echtzeit sämtliche Eingaben der Nutzer:innen***, um Suchvorschläge zu generieren.
Angeblich macht sich Opera Sorgen um die Sicherheit der Nutzer:innen. Daher sendet der Browser ***sämtliche aufgerufenen URLs an sitecheck.opera.com***. Damit hat Opera die Möglichkeit viele Daten für umfangreiche Nutzerprofile zu sammeln.
Zumindest gibt sich Opera noch den Schein die Nutzer zu schützen, denn es verwendet eingebaute ***Add Blocker*** mit den Listen von ***EasyList*** und ***NoCoin***.
Positiv zu vermerken ist, dass Opera ein ***integriertes VPN (Virtual Private Network)*** anbietet.
Im Hinblick auf die anderen Besonderheiten von Opera ist jedoch Vorsicht in Bezug auf die Qualität dieses VPNs angeraten, denn der Anbieter eines VPNs „sieht“ den gesamten Netzwerkverkehr ins Internet und zurück.

4.6 Safari

Der Apple-Browser bewegt sich im Mittelfeld. Er verfügt über einen ***eingebauten Trackingschutz***. Besonders ist hier, dass der Trackingschutz „lernt“ und seine Ergebnisse so im Laufe der Zeit immer besser werden.
Ruft man einen neuen Tab auf, begrüßen einen Unmengen an Werbelinks, die jedoch abschaltbar sind. Als ***Suchmaschine*** hat Safari ***Google*** voreingestellt. Damit ist ein großer Datenkrake gleich mit an Bord. Sämtliche ***Sucheingaben gehen in Echtzeit an Google***, um von dort Vorschläge für die Suche zu erhalten. Gleichzeitig schickt Safari diese ***Anfragen auch an api-glb-eucla.snoot.apple.com***.
Somit ist auch Apple gut darüber informiert, was seine Kunden interessiert. ***Die Weitergabe an Apple ist abschaltbar***. Ist eine alternative Suchmaschine als Standard eingerichtet, wie beispielsweise Startpage.com oder DuckDuckGo.com erhält auch Google keine zusätzlichen Profilinformationen.

4.7 Vivaldi

Vivaldi erhält auch ***keine Empfehlung***, denn seine Voreinstellungen sind zu werbelastig. Sie sind zwar abschaltbar, aber der Trackinkgschutz enthält eine Liste mit etlichen Werbepartnern von Vivaldi, denen Tracking damit automatisch erlaubt ist. Die Möglichkeit Domains automatisch über HTTPS ***(DoH)*** abzurufen ***bietet Vivaldi nicht*** an. Dieses Kennzeichen sollte inzwischen jedoch Standard sein.

5 (Nicht) empfehlenswerte Browser

Auf Grund dieser Eigenschaften sieht die Liste für Browserempfehlungen wie folgt aus:

1. Brave
2. Firefox
3. Safari
4. Chrome
5. Vivaldi
6. Edge und Opera

Passt man Firefox mit den erwähnten Add-ons an, könnte er sogar Brave an der ersten Stelle ablösen.

6 Am I unique?

textbfamiunique.org ist eine Website, welche die EFF (Electronic Frontier Foundation), eine amerikanische Bürgerrechtsorganisation, zur Verfügung stellt. Sie finden Sie hier Am I unique.

Abbildung 1: Der Browser ist bereits hier sehr gesprächig.

7 Cover Your Tracks

Auch die Website ***coveryourtacks.eff.com*** stellt die EFF zur Verfügung. Sie finden sie hier - `https://coveryourtracks.eff.org/results?&aat=1&fpi_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.7383402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D`Cover Your Tracks.

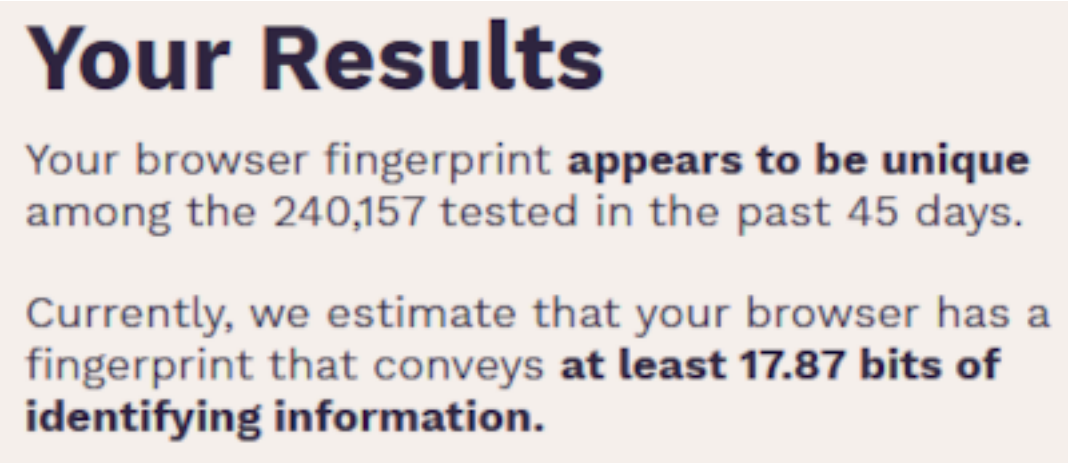


Abbildung 2: 17,87 bits of information sind viel zu viele Informationen

8 browserleaks

Die Website ***browserleaks.com*** finden Sie hier `https://browserleaks.com` /. Browserleaks verrät eindeutige und wichtige Informationen, die Sie identifizieren können. Einige Beispiele sind

8.1 IP-Adresse

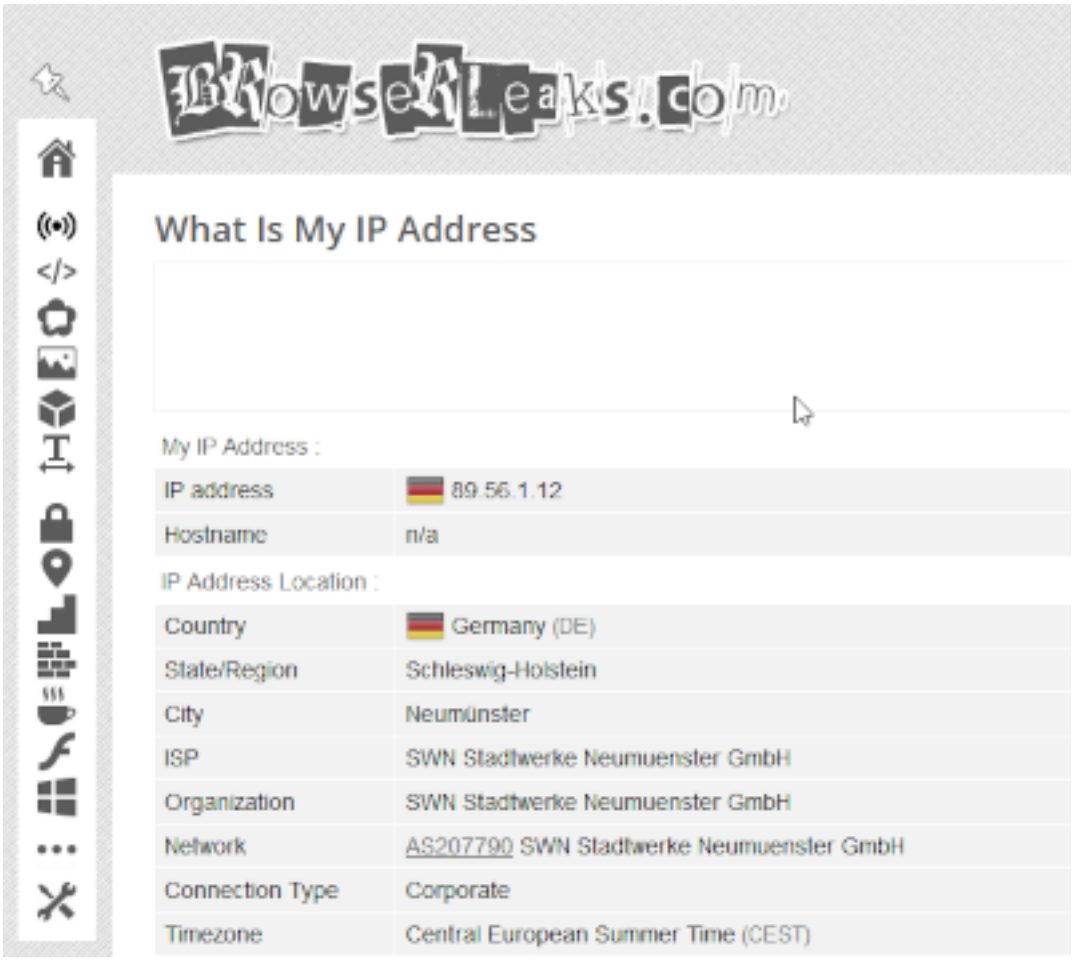


Abbildung 3: Die Site lässt keinen Zweifel daran, wo ich mich befinde.

8.2 Canvas Fingerprint

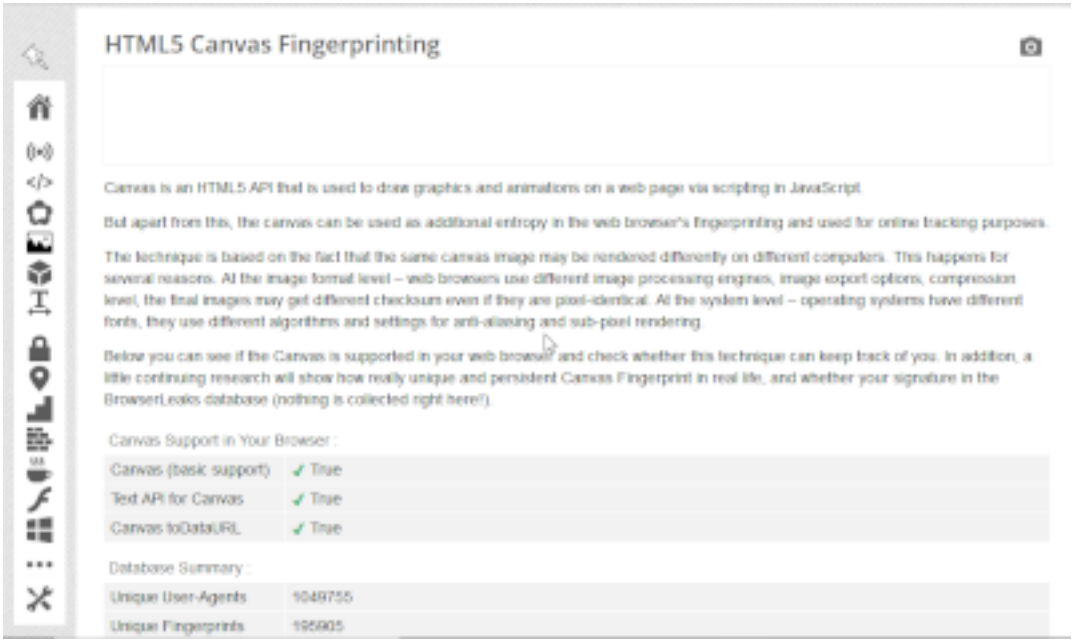


Abbildung 4: Mein Browser liefert viele Informationen in Bezug auf Canvas Fingerprinting

8.3 Font Fingerprint

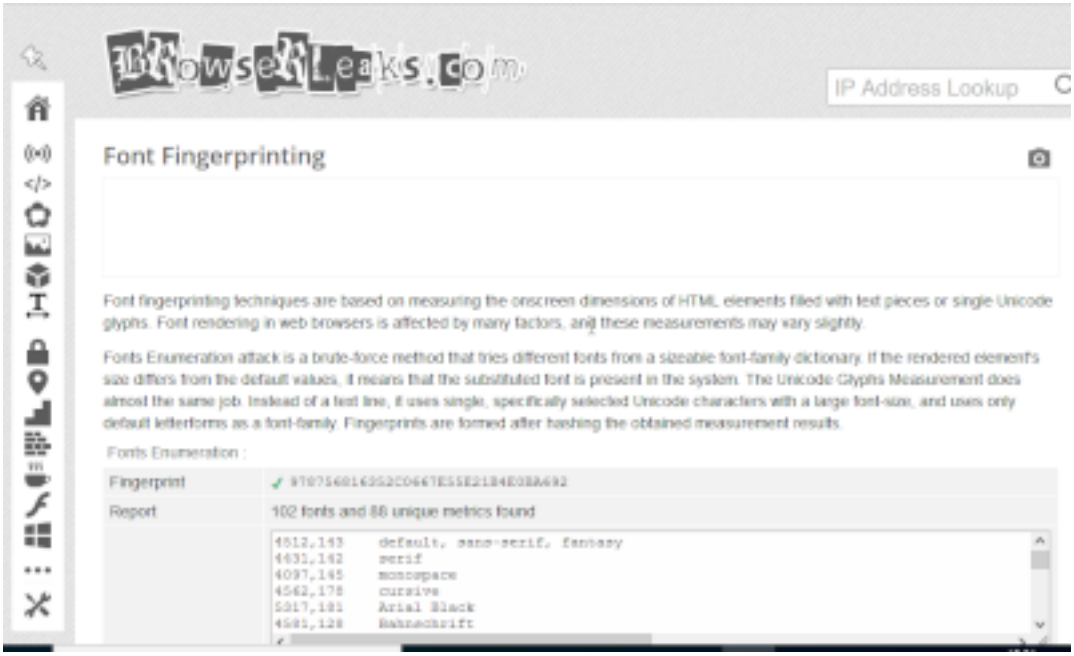


Abbildung 5: Auch die Schriften die mein Browser verwendet, helfen, mich zu identifizieren.

8.4 Social Media

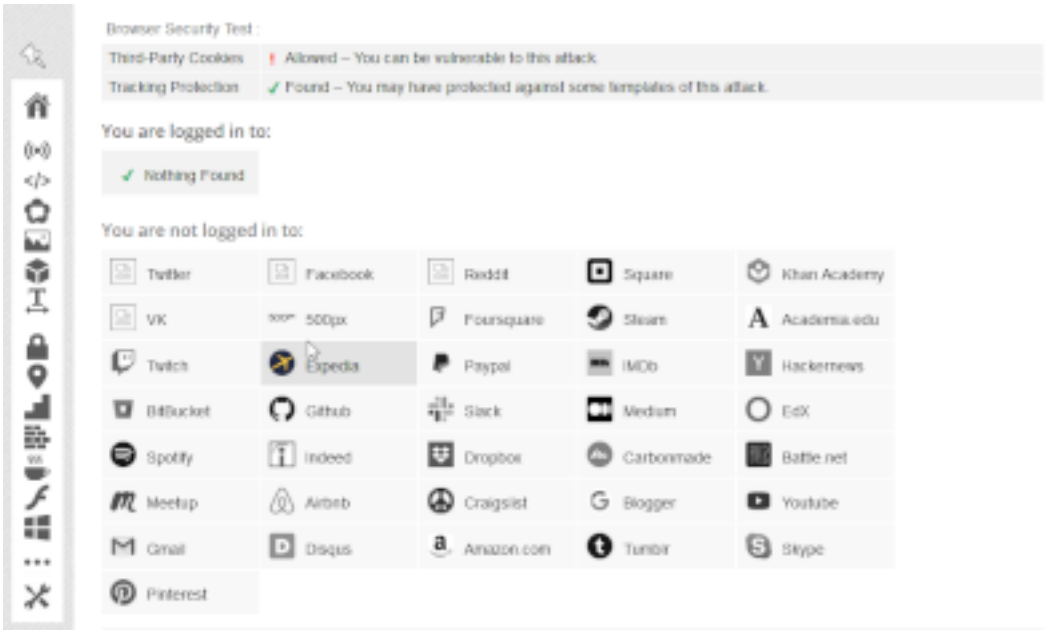


Abbildung 6: Auch ***nicht*** eigeloggte Social Media Accounts helfen Angreifern. Dort muss mich niemand suchen.

9 Sicherheitseinstellungen im Browser

Alle Angaben beziehen sich auf das Einstellungsmenü, das Sie über Extras → Einstellungen erreichen. Unter Linux ist dieses Menü oft über Bearbeiten → Einstellungen erreichbar.

9.1 Datenschutz und Sicherheit

Gehen Sie dafür auf den Punkt ***Extras → Einstellungen → Datenschutz & Sicherheit***. Wählen Sie hier unter dem Punkt Verbesserter Schutz vor Aktivitätsverfolgung die Option ***Strong*** aus. Anschließend klicken Sie auf den Button Alle Tabs neu laden. Die Warnung die Firefox ausgibt können Sie ignorieren, da in den meisten Fällen keine Einschränkungen entstehen. Sollte dies doch einmal geschehen, wählen Sie an dieser Stelle den Button ***Ausnahmen verwalten*** und fügen die betreffende Website als Ausnahme hinzu.

9.2 Do not track

Bei ***Do not track*** handelt es sich um eine Aufforderung an die Betreiber:innen von Websites, deren Befolgung freiwillig ist. Dieses Projekt gilt als gescheitert.

9.3 Datenerhebung durch Firefox und deren Verwendung

Nehmen Sie unter der Überschrift ***Datenerhebung durch Firefox und deren Verwendung*** alle Häkchen heraus. Ihre Daten gehen nur Sie selbst etwas an.

9.4 Sicherheit → Schutz vor gefährlichen Inhalten und betrügerischer Software

Setzen Sie hier bei ***allen Punkten*** einen Haken.

9.5 Zertifikate

Setzen Sie den Punkt bei ***Automatisch eins wählen*** und einen Haken bei ***Aktuelle Gültigkeit von Zertifikaten durch Anfrage bei OCSP-Server bestätigen lassen***.

9.6 Updates

Sie sollten dafür sorgen, dass Ihr Browser immer auf dem aktuellsten Stand ist. Deshalb setzen Sie bei ***Allgemein → Firefox Updates → Firefox erlauben → Updates automatisch zu installieren (empfohlen)*** ein.

9.7 Standardsuchmaschine

Standardmäßig ist bei Firefox ***Google*** als Suchmaschine eingestellt. Das ist ***nicht empfehlenswert***, da Google massiv Daten sammelt. Gehen Sie auf ***Suche → Standardsuchmaschine*** und ändern sie diese am besten auf ***DuckDuckGo***. Wenn Sie mit DuckDuckGo nicht so ganz glücklich sind, können Sie unter dem Punkt ***Startseite*** auch jede beliebige andere Suchmaschine, wie vielleicht ***startpage.com*** eintragen.

9.8 Sicherer Abruf von Websites

Damit niemand mitlesen kann, welche Site Sie gerade anfragen, sollten Sie auf den Punkt ***Allgemein → Verbindungseinstellungen (Einstellungen)*** gehen und hier einen Haken bei ***DNS über HTTPS*** setzen. Dann sendet Firefox Ihre Anfragen ausschließlich über Leitungen, die mit ***TLS (Transport Layer Security)*** verschlüsselt sind.

Optional

9.9 Cookies und Websitedaten

Wenn Sie die folgende Funktion wählen, löschen Sie sämtliche Daten, die Ihr Browser gespeichert hat. Auch Cookies, die dafür sorgen, dass Sie sich bei einigen Websites nicht mehr manuell anmelden müssen. Daher überlegen Sie, ob Sie das wollen.
Datenschutz & Sicherheit → Cookies und Websitedaten → Daten entfernen.

9.10 Chronik

Wenn Sie die Chronik auf ***niemals anlegen*** stellen, entspricht das dem Aufruf des privaten Modus. In diesem Modus zeigt Firefox die Icons der hier erwähnten Add-ons nicht an. Sie können diese anzeigen lassen, indem Sie unter ***Extras*** → ***Add-ons*** alle Add-ons einzeln anklicken und unter dem ***Reiter Details*** bis nach unten scrollen und dort den Button ***Im privaten Fenster ausführen – erlauben*** anklicken. Diesen Vorgang müssen Sie für alle Add-ons einzeln durchführen. Um die Container Add-ons ***Firefox Multi Container*** und ***Temporary Container*** nutzen zu können, müssen Sie unter ***Extras*** → ***Optionen*** → ***Datenschutz & Sicherheit*** → ***Chronik*** das Häkchen bei ***Immer den privaten Modus verwenden*** entfernen. Nehmen Sie auch beim ***Menüpunkt Adressleiste*** alle Häkchen heraus.
Datenschutz & Sicherheit → ***Chronik***
Hier gibt es zwei wichtige Funktionen. Die erste betrifft das Anlegen einer Chronik. Standardmäßig geschieht dies. Um zu vermeiden, dass Unbefugte sehen, wo Sie gesurft haben, sollten Sie bei ***Firefox wird eine Chronik anlegen*** niemals auswählen.
Wenn Sie diese Funktion wählen, löschen Sie Ihre gesamte Browser / Surf-Historie. ***Datenschutz & Sicherheit*** → ***Chronik löschen***.

10 Add-ons die helfen, die Privatsphäre zu schützen

10.1 uBlock Origin

Ublock Origin ist eine Browser Erweiterung, die es seit 2015 als uBlock Origin für mehrere Browser gibt. Ihre Geschichte hat 2014 als uBlock begonnen und startete mit den Browsern Chrome und Opera. Das Add-on verwaltet Blocklisten mit Informationen über Seiten, Skripte, Anbieter und ähnliches, welche die Privatsphäre der Internetnutzer bedrohen. Es ist eine Open Source Software, die der Gründer und Entwickler Raymond Hill von Anfang an betreut.

10.2 I don't care about cookies

I don't care about cookies ist ein Add-on, das sich um so genannte ***Consent Banner*** kümmert. Consent Banner sind die Pop-up Fenster die beim Aufruf vieler Webseiten erscheinen, um einen aufzufordern, doch alle Cookies anzunehmen. Alternativ kann man auch oft die Einstellungen selber anpassen. Das lohnt sich in der Regel, da man so auf viele Schnüffler verzichten kann. Lästig ist es dennoch. I don't care about cookies wählt die nutzerfreundlichsten Einstellungen automatisch und verhindert so, dass das Consent Banner überhaupt erst erscheint.

Im Vergleich

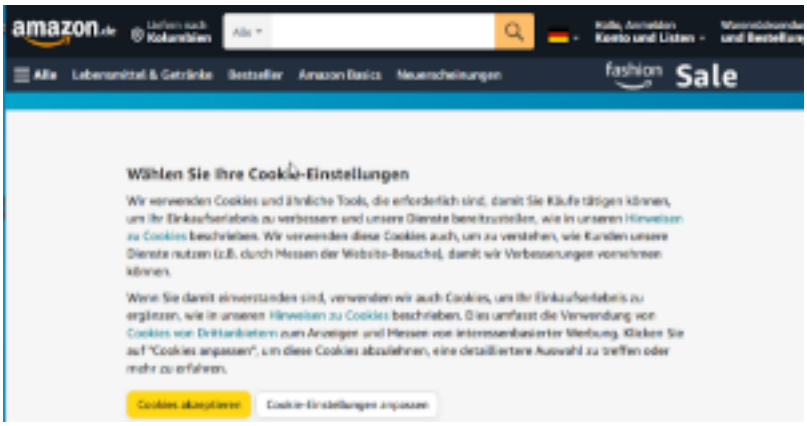


Abbildung 7: Der Aufruf von Amazon ohne ***I don't care about cookies***

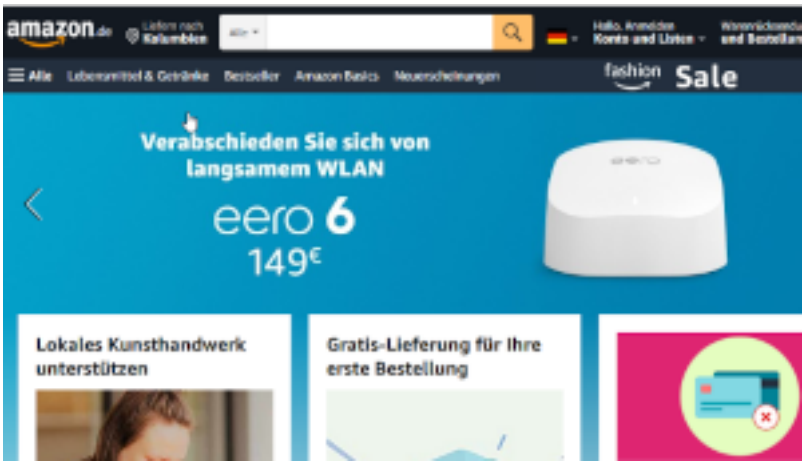
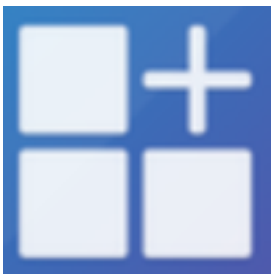


Abbildung 8: Der Aufruf von Amazon mit ***I don't care about cookies***

10.3 Multi Account Containers



Multi Account Containers ist ein Add-on, das Mozilla selbst entwickelt. Es stellt Firefox so genannte Container zur Verfügung, in denen die Nutzer:innen Websites zusammenfassen können, um sie in den entsprechenden Containern zu öffnen. Das Add-on bringt von sich aus einige ***Container wie Arbeit, Banking, Shopping und Freizeit*** mit. Jedoch kann man beliebig viele eigene Container erstellen, um häufig genutzte Sites darin zusammenzufassen. Dafür gibt es den ***Button Manage Containers***.
Das hat den Vorteil, dass die Websites die man für die Arbeit braucht, nicht „sehen können“ welche Websites man in der Freizeit aufruft und welche Cookies diese speichern. Oder, dass der Sportverein nicht weiß, nach welchen Krankheiten man gesucht hat.
Es könnte sinnvoll sein, alle Sites zum Thema IT Security in einen Container zu packen.

Abbildung 9: Eine ***IT Security Site*** im ***IT Security Container.*** zu erkennen in der URL Zeile oben rechts, links des blauen Punkts

Temporary Containers

Temporary Containers ist ein Add-on, das alle aufgerufenen Websites in Container packt, sofern sie nicht von Firefox Multi Account Containers bereits kategorisiert wurden. Das hat den Vorteil, dass die aufgerufenen Websites den geringstmöglichen Zugriff auf Ihre Daten erlangen. 15 Minuten nachdem die Nutzer:innen eine Site verlassen haben, löscht Temporary Containers alle Daten, die damit in Zusammenhang stehen von sich aus.
Es geht niemanden etwas an, wann ich wohin mit der Bahn fahren will.
Daher ist ***Temporary Containers*** für den Aufruf von ***bahn.de*** eine gute Idee.

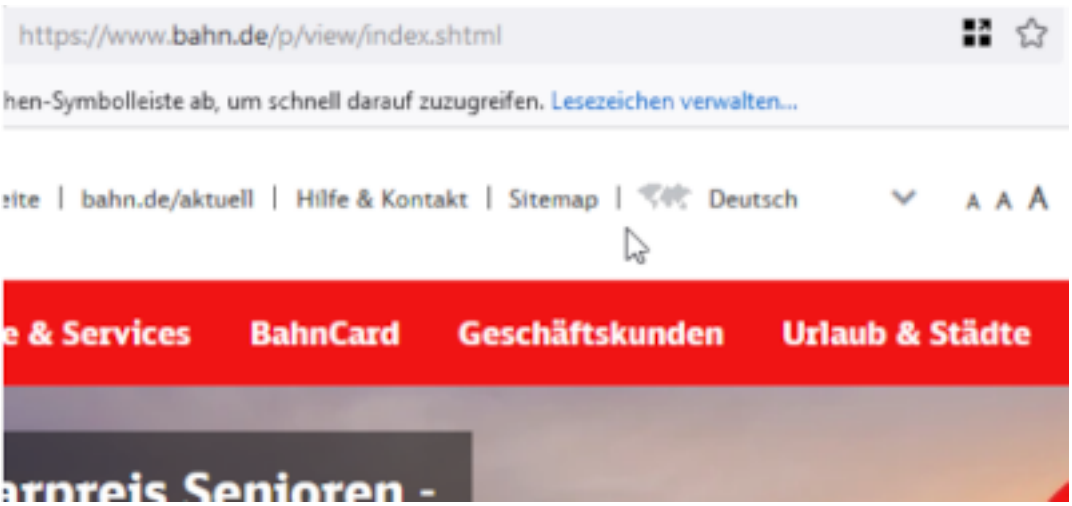


Abbildung 10: Buchungsportal der deutschen Bahn. Oben rechts an den vier Quadraten ist zu erkennen, dass die Site in einem ***Temporary Container*** geöffnet wurde.

10.4 No Script

NoScript ist ein Klassiker. Das Programm verhindert die Ausführung von Skripten auf Websites. Das erhöht die Sicherheit beim Surfen erheblich, ist jedoch zunächst äußerst lästig, denn ständig laden Inhalte oder ganze Seiten nicht. Dann ist die Nutzer:in gefragt, von Hand Skripte freizugeben. Das kann einmalig aber auch dauerhaft geschehen. So lernt No Script mit der Zeit, was „gut“ ist und verhindert irgendwann nur noch Skripte, die für die Nutzer:innen nicht von Vorteil sind.

Abbildung 11: ***No Script*** hindert Amazon daran, einige Skripte auszuführen

10.5 Referer Modifier

Referer Modifier ist ein Add-on, das dafür sorgt, dass die aktuell aufgerufene Website nicht erfährt, auf welcher Website die Nutzer:in vorher war. Standardmäßig überträgt der Browser diese Information an die aktuell aufgerufene Website. Referer Modifier fälscht diese Informationen.

10.6 User Agent Switcher

User Agent Switcher ist ein Add-on, das die Möglichkeit bietet, sowohl die Angaben über das Betriebssystem – Windows, Mac, Linux oder andere – als auch den verwendeten Browser zu fälschen. Es steht jeweils eine Vielzahl von Alternativen zur Verfügung.

10.7 Privacy Badger

Privacy Badger ist ein Add-on, dass sich ausgeklügelt um die Privatsphäre der Nutzer:innen kümmert. Privacy Badger blockiert keine Websites an Hand von Listen, sondern lernt selbstständig. Taucht ein Tracker zum dritten mal beim Einsatz des Privacy Badgers auf, blockiert er automatisch Websites, die diesen Tracker einbinden. Zusätzlich teilt das Add-on allen Websites von sich aus mit, dass die Nutzer:innen nicht – in keiner Form – getrackt werden wollen. Es ist ein Klassiker der EFF (Electronic Frontier Foundation – eine amerikanische Bürgerrechtsorganisation), die bekannt für ihre wirksamen und ausgeklügelten Tools ist.

11 Einsatz von VPN

VPN steht für ***Virtual Private Network***. Dabei handelt es sich um eine Technik, die es möglich macht, sichere, ***verschlüsselte Ende zu Ende (E2EE - End-to-End-Encryption)*** Verbindungen über unsichere Netzwerke wie das Internet herzustellen. Wenn Sie im Internet surfen, können ***bis zu 40 Hops (Zwischenstationen)*** zwischen Ihnen und dem aufgerufenen Ziel liegen. Das sind alles potentielle Angreifer. Ein VPN schließt das aus, indem es Direktverbindungen herstellt, die besonders gut gesichert sind. ***Der Schwachpunkt eines VPN ist immer der Anbieter, denn dem muss die Nutzer:in vertrauen. Der Anbieter könnte nämlich sämtlichen Datenverkehr mitschneiden.***
Es gibt viele VPN-Anbieter. Sicherlich auch einige, denen man vertrauen kann. Der Autor dieses Skripts vertraut auf ***Proton-VPN -*** `https://proton.me/` ***- inklusive seiner anderen Angebote***

11.1 Proton-VPN

Proton-VPN gibt es sowohl in einer kostenlosen als auch in kostenpflichtigen Versionen, die mehr Möglichkeiten bieten. Hier erfahren Sie mehr darüber - ProtonVPN

12 Browser, die ein VPN anbieten

Mozilla bietet mit seinem ***Firefox*** einen Browser an, der ein VPN mitbringt. Sie finden den Zugang hier - Firefox.

Abbildung 12: Auch das Mozilla VPN gibt es in kostenpflichtigen Versionen. Es lohnt sich, stattdessen das Angebot von ***Mullvad VPN*** anzusehen - Mozilla VPN, denn das ist das VPN, das hinter Mozilla steckt.

13 Bevorzugte Sprachen für die Darstellung von Websites wählen

Wie Sie bereits gesehen haben, werten Skripte auch aus, welche Sprache Sie für Ihren Browser bevorzugen. Dies ist eine wichtige Information, weil damit in den meisten Fällen ein Rückschluss auf das Herkunftsland der Nuter:innen möglich ist. Deshalb empfiehlt es sich, auch diese Information zu verfälschen. Gehen Sie dafür auf ***Extras*** → ***Einstellungen*** → ***Allgemein*** → ***Sprache*** → ***Bevorzugte Sprache für die Darstellung von Websites wählen***

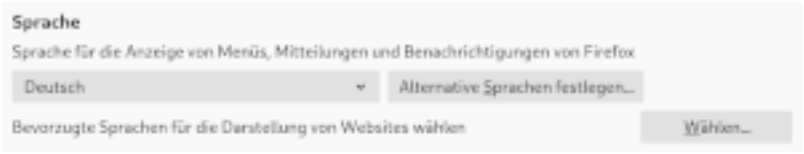


Abbildung 13: Hier stellen Sie die bevorzugte Sprache ein. Wählen Sie aber eine, deren Schriftzeichen Sie auch lesen können.

Klicken Sie auf den Button ***wählen*** und suchen Sie sich eine Sprache aus, die nicht der Sprache des Landes entspricht in dem Sie sich hauptsächlich aufhalten. Achten Sie jedoch darauf, dass Sie eine Sprache wählen, deren Buchstaben Sie kennen, nicht dass Sie, wenn etwas schief geht, nicht einmal die Zeichen lesen können. In der Regel dürfte diese Einstellung für Sie keine Rolle spielen, da Sie vermutlich vor allem Websites aufrufen, die originär die von Ihnen bevorzugte Sprache verwenden.

14 Am I unique - nach den Erweiterungen

Nachdem wir einige Add-ons installiert und Einstellungen vorgenommen haben, ist der Browser zwar immer noch „einzigartig“, aber er erzählt ganz andere Dinge als vorher.

Im Vergleich:

Abbildung 14: Die ***echten*** Angaben

Abbildung 15: Das was ein Schnüffler sieht

15 Cover your tracks - nach den Erweiterungen

Auch ***Cover your tracks*** kommt nach den Erweiterungen zu ganz anderen Ergebnissen.
Im Vergleich:

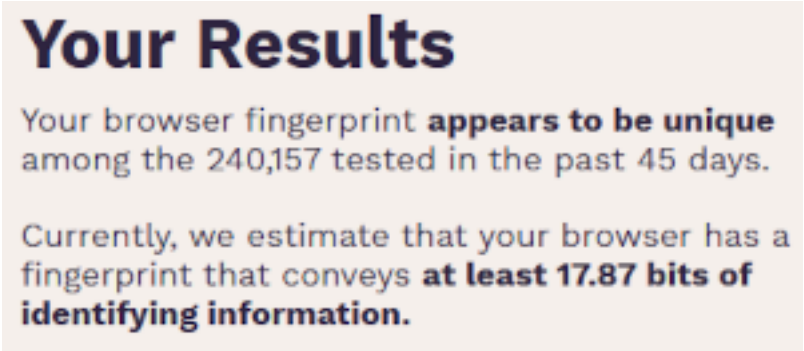


Abbildung 16: Die Realität

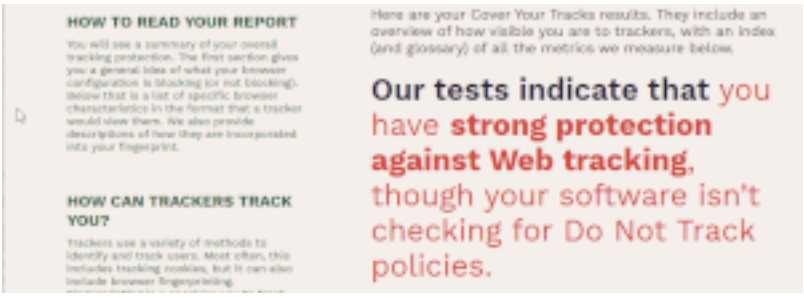


Abbildung 17: Das, was ein Schnüffler sieht

16 Browserleaks

Browserleaks verrät wesentlich weniger Informationen nach den Umstellungen.

16.1 IP-Adresse mit VPN

Ursprünglich war ich ohne VPN im Internet unterwegs. Der Test gab den genauen Standort preis.
Im Vergleich:

16.2 Ohne VPN

Abbildung 18: Die echte IP-Adresse

16.3 Mit VPN

Abbildung 19: Das, was ein Schnüffler sieht

17 Canvas Fingerprint ohne und mit Add-on

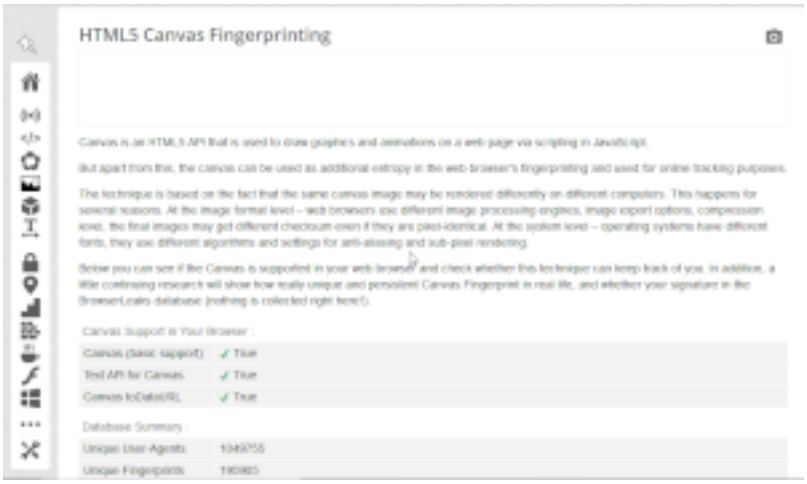


Abbildung 20: Canvas Fingerprint im Auslieferungszustand

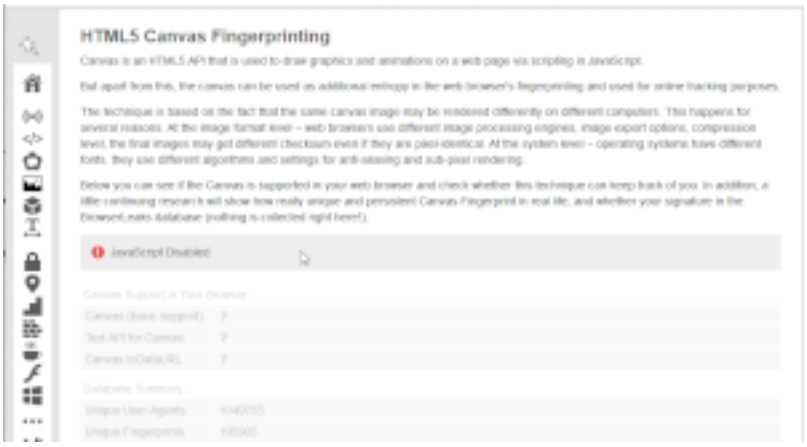


Abbildung 21: Mit Add-on ist das Canvas Fingerprinting sehr viel schweigsamer

18 Font Fingerprint ohne und mit Add-on

Auch installierte Schriften können jemanden identifizieren.

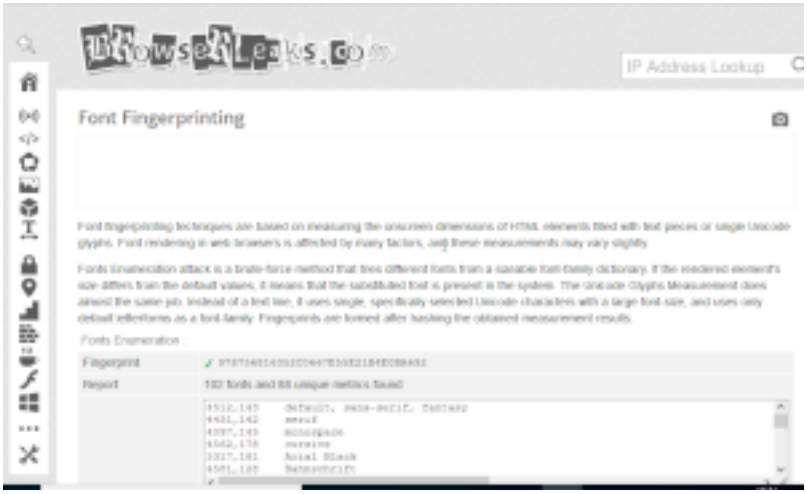


Abbildung 22: Ohne Add-on verrät der Browser viel über installierte Schriften

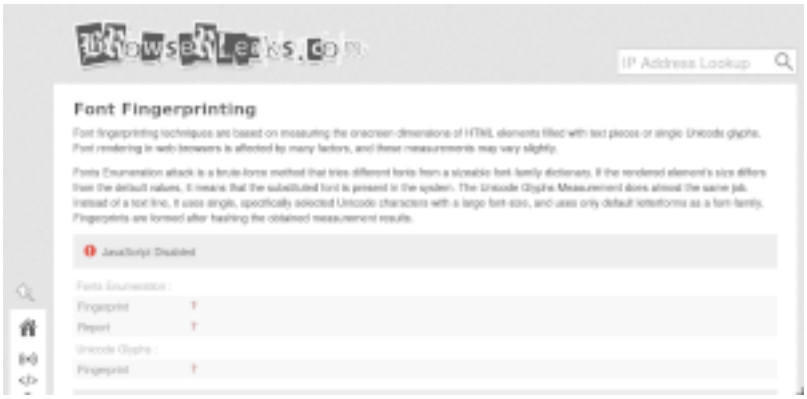
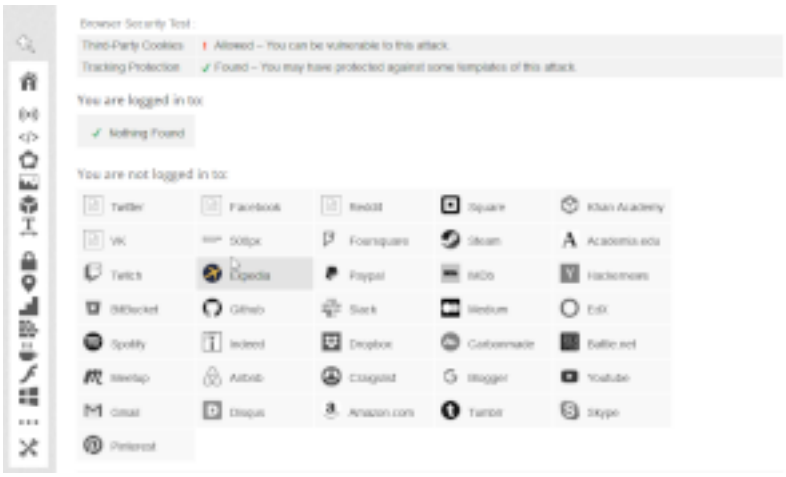


Abbildung 23: Das Add-on verbirgt die installierten Schriften

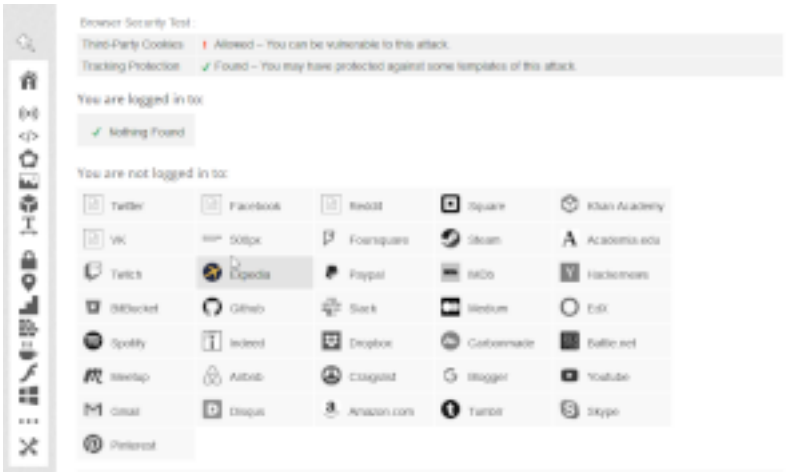
19 Social Media Login Detection

Bei den ***Social Media Logins*** ist kein Unterschied zu erkennen, da dieser Rechner nie in ein Social Media Tool eingeloggt war. Wäre er das gewesen, würde ein Angreifer dies nach der Aktivierung des Tools nicht mehr sehen. Interessant für Angreifer ist hier der Umkehrschluss, denn das Tool zeigt an, in welchen Social Media die Nutzer:in nicht eingeloggt ist. Dort muss er Angriffe also gar nicht erst nach ihr suchen. Da die meisten Menschen in Social Media aktiv sind, lässt sich so schnell klären, wer welches Medium nutzt.



20 Social Media Login Detection

Bei den ***Social Media Logins*** ist kein Unterschied zu erkennen, da dieser Rechner nie in ein Social Media Tool eingeloggt war. Wäre er das gewesen, würde ein Angreifer dies nach der Aktivierung des Tools nicht mehr sehen. Interessant für Angreifer ist hier der Umkehrschluss, denn das Tool zeigt an, in welchen Social Media die Nutzer:in nicht eingeloggt ist. Dort muss er Angriffe also gar nicht erst nach ihr suchen. Da die meisten Menschen in Social Media aktiv sind, lässt sich so schnell klären, wer welches Medium nutzt.



21 Nutzung von Social Media

Social Media verraten viel über ihre Nutzer. Damit Sie diese Informationen nicht automatisch mit ihrem digitalen ***Fingerprint*** verknüpfen, könnten Sie für die Nutzung von Social Media eine ***Virtuelle Maschine*** einsetzen, die dann nur die Standardinformationen enthält. Somit ist es schwieriger diese Daten genau Ihnen zuzuordnen.

Abbildung 24: Social Media

21.1 Software zur Virtualisierung von Computern

Eine Software zur Virtualisierung von Computern ist VirtualBox. Die Einrichtung und Nutzung von VirtualBox ist einfach. Dies Software gilt als recht sicher.

Abbildung 25: VirtualBox

21.2 Vorgefertigte Images für virtuelle Maschinen

Fertige „Virtuelle Maschinen“finden Sie kostenlos bei osboxes.orgzum Download. Das erleichtert die Installation einer virtuellen Maschine noch weiter.

22 Passwort Tresore

22.1 Lokaler Passwort Tresor

Passwort Tresore sind sind Programme, die Ihre Passwörter sicher verschlüsselt speichern - im Idealfall. Nicht alle sind zuverlässig.

Abbildung 26: KeePassXC

Empfehlenswert ist ***KeePassXC***. KeePassXC ist open Source Software und Sie können es ***lokal*** verwenden.

22.2 Online Passwort Tresor

Eine Alternative sind ***online Passworttresore***. Damit hat man von überall, wo man eine Internetverbindung hat, auch Zugriff auf seine Passwörter.
Problematisch ist jedoch, dass damit Ihre Passwörter zum einen

- dem Anbieter
- Angreifern die sich online befinden

ausgeliefert sind. Für Angreifer lohnen sich online Passwort Tresore besonders, weil bei relativ geringem Aufwand - sie haben online Zugang und müssen sich nicht auf ihren lokalen Rechner hacken - viele Passwörter unterschiedlicher Nutzer zu erbeuten sind.
Handelt es sich um einen amerikanischen Anbieter, sind sie der Gefahr ausgeliefert, dass amerikanische Behörden die Herausgabe Ihrer Daten - somit auch Passwörter - vom Anbieter verlangen können, ohne, dass Sie davon Kenntnis erlangen.

23 Onlinespeicher

Auch hier gibt es viele bekannte Angebote, die von amerikanischen Anbietern stammen. Sie sollten Sie meiden, denn auch hier gilt, dass amerikanische Behörden die Herausgabe Ihrer Daten verlangen können.
Besser ist es, Sie nutzen ***Anbieter aus Europa***, denn die unterliegen der DSGVO oder dem Datenschutzrecht der Schweiz, das ähnlich streng ist.
Wichtig für die Wahl des Onlinespeichers sind folgende Aspekte

- Anbieter in Europa
- E2EE - Ende-zu-Ende-Verschlüsselung bei der Datenübertragung.
  Eine Transportwegverschlüsselung mit TLS reicht ***nicht*** aus.
- Die Daten müssen verschlüsselt gespeichert werden

24 Anbieter von Onlinespeicher denen ich vertraue

Ich vertraue den Anbietern Proton und
Tresorit. Beide Anbieter stammen aus der Schweiz.

25 Online Office Anbieter

Die bekanntesten online Office Anbieter sind ***Google docs*** und ***M 365 - früher Office 365***.
Bei beiden Anbietern haben Sie wieder das Problem, dass die Anbieter aus Amerika stammen und somit dem Zugriff durch amerikanische Behörden unterliegen.
Beide sind nicht eben für Vertraulichkeit bekannt. Microsoft bietet nicht einmal eine E2EE bei der Datenübertragung an.
Möchten Sie Ihre Daten bei M365 verschlüsselt speichern, muss der Schlüssel bei Microsoft gespeichert sein. Somit haben hierauf wiederum amerikanische Behörden Zugriff.
Wenn Sie eine teurere Lizenz kaufen, können Sie Ihre Passwörter lokal speichern - aber nur auf Hard- oder Software von Microsoft.
Eine E2EE beim E-Mailing bietet Microsoft nicht an. Obwohl diese in der DSGVO vorgeschrieben ist - nach dem Stand der Technik.
Außerdem verarbeitet Microsoft Nutzerdaten zu eigenen Zwecken. Allerdings gibt Microsoft weder preis, welche Daten das sind, noch zu welchen Zwecken dies geschieht.
Wenn Sie Personen bezogene Daten speichern, dürfen Sie diese ohnehin nicht auf Speichern amerikanischer Unternehmen speichern, weil - wie schon mehrfach erwähnt - die Daten dem Zugriff amerikanischer Behörden unterliegen.

26 Eine Alternative

Eine sichere Alternative für all das bietet Tresorit an. Ein Blick darauf lohnt sich, denn Tresorit verschlüsselt sogar die ***Betreffzeilen*** von E-Mails. Außerdem arbeitet Tresorit auch mit Gmail und Outlook - aber dann sicher.
Als Office Programm kann LibreOffice kostenlos genutzt werden.

27 Quellen

1. Add-on Canvas Blocker – Programmerweiterung für Firefox, um Canvas Fingerprinting zu vermeiden.
   https://addons.mozilla.org/de/firefox/addon/canvasblocker/

2. Add-on Fake Filler – ein Add-on, das in Formularen automatisch frei erfundene Daten einträgt
   https://addons.mozilla.org/de/firefox/addon/fake-filler/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

3. Add-on Firefox Multi Account Containers – Programmerweiterung für Firefox, um Websites einzelnen Containern zuzuordnen
   https://addons.mozilla.org/de/firefox/addon/multi-account-containers/

4. Add-on I don‘t care about cookies – Programmerweiterung für Firefox, um lästige Consent Banner weitgehend automatisch zu handhaben.
   https://addons.mozilla.org/de/firefox/addon/i-dont-care-about-cookies/

5. Add-on Custom Tab Title and Favicon – ein Add-on, das den Namen geöffneter Tabs und das dazugehörige Favicon ändert
   https://addons.mozilla.org/de/firefox/addon/custom-tab-title-and-favicon/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

6. Add-on Firefox Multi Account Containers – Programmerweiterung für Firefox, die es den Nutzer:innen möglich macht, für unterschiedliche Anwendungsbereiche wie Privat, Arbeit, Banking und beliebiges mehr, Container anzulegen, so dass die Sites sich untereinander nicht mehr „sehen“ können.
   https://addons.mozilla.org/de/firefox/addon/multi-account-containers/

7. Add-on NoScript – Programmerweiterung für Firefox, die die Ausführung von Skripten verhindert. Ausnahmen sind konfigurierbar.
   https://addons.mozilla.org/de/firefox/addon/noscript/

8. Add-on Privacy Badger – ein Add-on der EFF (Electronic Frontier Foundation – eine amerikanische Bürgerrechtsorganistion) zum Schutz der Privatsphäre

https://addons.mozilla.org/de/firefox/addon/privacy-badger17/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

9. Add-on Referer Modifier – ein Add-on, das die Webadresse, die man vor der aktuellen aufgerufen hat, fälscht
   https://addons.mozilla.org/de/firefox/addon/referer-modifier/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

10. Add-on für Chrome und Edge – Tabliss – entfernt Werbung
    https://tabliss.io/

11. Add-on Tab ReTitle – ein Add-on, das geöffneten Tabs andere Namen gibt. Aus Amazon wird Wikipedia oder ähnliches. Dieses Add-on verändert jedoch nicht das Favicon
    https://addons.mozilla.org/de/firefox/addon/tab-retitle/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search

12. Add-on Temporary Containers – Programmerweiterung für Firefox, die alle Websites, die die Nutzer:innen keinem Container zugeordnet haben, in einen vorübergehenden Container legen. Die dort abgelegten Daten löscht das Add-on nach 15 Minuten automatisch.
    https://addons.mozilla.org/de/firefox/addon/temporary-containers/

13. Add-on uBlockOrigin – Programmerweiterung für Firefox, ein ausgefeilter Blocker für Werbung.
    https://addons.mozilla.org/de/firefox/addon/ublock-origin/

14. Am i unique – Website der amerikanischen Bürgerrechtsorganistaion EFF (Electronic Frontier Foundation), um festzustellen, wie leicht man über den eigenen Browser identifizierbar ist.
    https://amiunique.org/

15. Apple – Verwalten von Cookies und Websitedaten mit Safari auf dem Mac
    https://support.apple.com/de-de/guide/safari/sfri11471/mac

16. Browser Leaks – Website, die zeigt, welche Daten der eigene Browser automatisch überträgt.
    https://browserleaks.com/

17. Browser Fingerprinting – eine Erkllärung, was Browser Fingerprinting ist.
https://browser-fingerprint.cs.fau.de/

18. Browser Fingerprinting API – eine Erklärung wie Browser Fingerprinting über Schnittstellen funktioniert.
https://fingerprintjs.com/

19. Building a privacy – first future for web advertising – Goolge erklärt Werbeverfahren, die vermeintlich Datenschutz konform sind
https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

20. Canvas Fingerprinting – Erklärung dieser besonderen Form des Fingerprintings
https://de.wikipedia.org/wiki/Canvas_Fingerprinting

21. Chip - Cookies akzeptieren oder nicht? Das sollten Sie tun – ein Artikel zu Cookies aus der Zeitschrift Chip
https://praxistipps.chip.de/cookies-akzeptieren-oder-nicht-das-sollten-sie-tun_42136

22. Codingkids.de - History Check: Was sind denn Magic Cookies? - Eine Erklärung zu Magic Cookies
https://www.codingkids.de/wissen/history-check-was-bitteschoen-sind-magic-cookies

23. Cookies – RFC 6265 – RFC = Request for Comments. Der Beginn eines Versuchs, Internettechniken zu standardisiern. Inzwischen ist RFC genau das.
https://datatracker.ietf.org/doc/html/rfc6265

24. Cookiebot.com – Cookie-Checker | Ist Ihre Webseite DSGVO- und CCPA-konform? - Test für Websitebetreiber:innen, auf Datenschutzkonformität https://www.cookiebot.com/de/cookie-checker/?gclid=EAIaIQobChMI-9X6oMz88QIVFNayCh2FqAltEAAYAyAAEgKKqvD_BwE

25. Cortina-consult.com – Was sind Cookies? - Eine Erklärung, was Cookies sind
https://cortina-consult.com/was-sind-cookies/

26. c‘t 14/21 Surfen ohne Nerverei und Tracking (Artikelserie) – Grundlage dieses Skripts
https://www.heise.de/ct/artikel/c-t-14-2021-Der-Blick-ins-Heft-mit-Surfen-ohne-Nerverei-und-Tracking-6070723.html

27. coveryourtracks – Website der EFF (Electronic Frontierfoundation), die Tracking von Websites aufzeigt
https://coveryourtracks.eff.org/results?&aat=1&fpi_whorls=%7B%22v2%22%3A%7B%22plugins%22%3A%22permission+denied%22%2C%22hardware_concurrency%22%3A8%2C%22audio%22%3A%2235.73833402246237%22%2C%22canvas_hash_v2%22%3A%22f139fb61b2b20249d81082f9012141dc%22%2C%22webgl_hash_v2%22%3A%2233dbdb28a8e5050332bc8f7473462c56%22%7D%7D

28. de Montjoye, Y.-A., Radaelli, L., Singh, V. K. & Pentland, A.. Science . Unique in the shopping mall:On the reidentifiability ofcredit card metadata. Ausführliche Informationen zu Metadaten.
https://science.sciencemag.org/content/sci/347/6221/536.full.pdf

29. Developer.mozilla.org – Set-Cookie – Informationen für Entwickler, zum Setzen von Cookies
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

30. Die 6 gängigen Cookie Consent Tools im Vergleich – Vergleich von Tools, die Cookies auf Websites setzen
https://www.e-recht24.de/artikel/datenschutz/12495-cookie-consent-tools.html

31. DNS over HTTPS – Erklärung wie sichere Domainanfragen funktionieren
https://de.wikipedia.org/wiki/DNS_over_HTTPS

32. External Protocol Flooding Vulnerability – Erläuterung von Angriffsmöglichkeiten
https://schemeflood.com/

33. FingerprintJS – Anbieter ausgesprochen ausgeklügelten Fingerprintings
https://fingerprintjs.com/demo/

34. Fingerprinting the Fingerprinters: Learning to detect Browser Fingerprinting Behaviors – ein Versuch den Fingerprintern auf die Spur zu kommen
https://arxiv.org/abs/2008.04480

35. Firefox 85 cracks down on supercookies – Firefox wehrt sich ab Version 85 gegen Supercookies

https://blog.mozilla.org/security/2021/01/26/supercookie-protections/

36. Firefox 85 knackt Supercookies – Firefox wehrt sich ab Version 85 gegen Supercookies https://blog.mozilla.org/press-de/2021/01/26/firefox-85-knackt-supercookies/

37. Firefox 86 introduces total cookie protection – Firefox 86 führt den "totalen" Cookieschutz ein
https://blog.mozilla.org/security/2021/02/23/total-cookie-protection/

38. Firefox Download – hier kann Firefox herunter geladen werden
https://www.mozilla.org/de/firefox/new/

39. Firefox Sicherheitskompendium – Anleitung um Firefox sicherer zu machen
https://www.heise.de/ct/entdecken/?volltext=sicherheitskompendium&sort=datum_auf&redautor=Mike+Kuketz

40. Flashcookies and privacy – Flashcookies und Privatsphäre
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862

41. Flashcookies and privacy II: Now with HTML5 and Etag – Flashcookies und Privatsphäre im Zusammenspiel mit HTML5 und Etags
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390

42. Gadotti, A., Houssiau, F., Rocher, L., Livshits, B. & de Montjoye, Y.-A.. Department of Comuting and Data Science Institute, Imperial College London, ICTEAM, Université catholique de Louvin. When the Signal is in the Noise: Exploiting Diffix's Sticky Noise.
arxiv.org – Artikel über die hochgradige Anonymisierung von Datenbanken https://arxiv.org/pdf/1804.06752.pdf

43. Gieselmann, H. 36. Chaos Communication Congress (2019, 29.12.). 36C3: Wie gängige Methoden zur Anonymisierung von Daten versagen – Nachweis, dass anonymisierte Daten keinesfalls anonym bleiben
https://www.heise.de/newsticker/meldung/36C3-Wie-gaengige-Methoden-zur-Anonymisierung-von-Daten-versagen-4624450.html

44. Github – Evercookies – eine Bauanleitung
https://github.com/samyk/evercookie

45. Github – Unified ID – Erklärung einer neuen Methode zur Werbung
https://github.com/UnifiedID2/uid2docs

46. Google – Building a privacy-first future of web advertising – Google erklärt seine Vision von Werbung unter Wahrung der Privatsphäre
https://blog.google/products/ads-commerce/2021-01-privacy-sandbox/

47. Google – Cookies in Chrome löschen, aktivieren und verwalten – eine Anleitung zur Handhabung von Cookies in Chrome
https://support.google.com/chrome/answer/95647?hl=de&co=GENIE.Platform%3DAndroid

48. Gumm, D. / TH Lübeck Metadaten sind strukturierte Daten, die Inhaltsdaten beigeordnet sind und etwas über diese aussagen.

49. Hayden, M. V. - We kill based on metadata. Wikipedia, Michael V. Hayden & Holland, M. - Heise Security – ein Beitrag in dem der ehemalige Direktor der CIA, später auch der NSA, erklärt, dass Amerika Menschen allein auf Basis von Metadaten tötet
https://www.heise.de/newsticker/meldung/Ex-NSA-Chef-Wir-toeten-auf-Basis-von-Metadaten-2187510.html

50. heise security - Feature mit Bug: Microsoft Edge telefoniert besuchte Seiten nach Hause
https://www.heise.de/news/Feature-mit-Bug-Microsoft-Edge-telefoniert-besuchte-Seiten-nach-Hause-8980355.html

51. Here's how to enable DoH in each browser, ISPs be damned – Anleitung, um DoH in jedem Browser zu aktivieren
https://www.zdnet.com/article/dns-over-https-will-eventually-roll-out-in-all-major-browsers-despite-isp-opposition/

52. Hiller, A., Hakuna Metadata - Warum Metadaten und Browserverläufe mehr über uns verraten als oft vermutet. netzpolitik.org – Erläuterung, weshalb Metadaten so gefährlich für die Anwender sind
https://netzpolitik.org/2017/hakuna-metadata-warum-metadaten-und-browserverlaeufe-mehr-ueber-uns-verraten-als-oft-vermutet/

53. HSTS – HTTP Strict Transport Security – eine Transportverschlüsselung
https://de.wikipedia.org/wiki/HTTP_Strict_Transport_Security

54. HSTS – HTTP Strict Transport Security – eine Transportverschlüsselung
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

55. Human Who Codes – HTTP cookies explained – eine Erklärung von HTTP-Cookies
https://humanwhocodes.com/blog/2009/05/05/http-cookies-explained/

56. Inside digital – Cookies löschen & deaktivieren: So bleiben Deine Internet-Nutzerdaten geheim – Anleitung zum Umgang mit Cookies
https://www.inside-digital.de/ratgeber/cookies-loeschen-oder-deaktivieren-so-machst-du-es-richtig

57. Intelligent Tracking Prevention – intelligente Vermeidung von Tracking
https://webkit.org/blog/7675/intelligent-tracking-prevention/

58. IONOS – Canvas Fingerprinting – Erläuterung zum Canvas Fingerprinting
https://www.ionos.de/digitalguide/online-marketing/web-analyse/canvas-fingerprinting-webtracking-ohne-cookies/

59. IONOS – Cookies deaktivieren: Wie lassen sich Cookies deaktivieren?
https://www.ionos.de/digitalguide/websites/webseiten-erstellen/cookies-im-browser-deaktivieren/

60. Johns Hopkins University. The Price of Privacy: Re-Evaluating the NSA, A Debate – Die Podiumsdiskussion in der Michael Vincent Hayden erklärt, dass Amerika Menschen auf Grund von Metadaten tötet (ehemaliger Direktor der CIA, später NSA)
https://www.youtube.com/watch?v=kV2HDM86XgI

61. Kaspersky, How to enable Cookies – wie man Cookies aktiviert
https://support.kaspersky.com/common/windows/2843#block2

62. Kaspersky, What are Cookies – eine Erläuterung, was Cookies sind
https://www.kaspersky.com/resource-center/definitions/cookies

63. Kuksov, I. / Kaspersky. Wie flüchtige Metadaten für echte Probleme sorgen können. kaspersky.de – Erklärung wie Metadaten zu echten Problemen werden können
https://www.kaspersky.de/blog/office-documents-metadata/9915/

64. Kurz, C. & Rieger, F. / Chaos Computer Club. Stellungnahme des Chaos Computer Clubs zur Vorratsdatenspeicherung
https://www.ccc.de/system/uploads/150/original/VDSfinal18.pdf?1403228408

65. LibreOffice - https://de.libreoffice.org/

66. Marketing / Open Data Security. What is Metadata and what does it reveal. opendatasecurity.io? - Was Metadaten sind
https://opendatasecurity.io/what-is-metadata-and-what-does-it-reveal/

67. Microsoft Support – Löschen und Verwalten von Cookies
https://support.microsoft.com/de-de/windows/l%C3%B6schen-und-verwalten-von-cookies-168dab11-0753-043d-7c16-ede5947fc64d

68. Mozilla VPN – kostenloses VPN, das Mozilla anbietet
https://www.mozilla.org/de/products/vpn/

69. mozilla Support – Cookies blockieren
https://support.mozilla.org/de/kb/Cookies-blockieren

70. Neuer Tab – Seite personalisieren
https://chrome.google.com/webstore/category/collection/customize_your_new_tab_page

71. Netzpolitik.org. Fehler bei IP-Adressen: Viele Briten fälschlich wegen Kinderpornos verhaftet – Gefahren von Metadaten
https://www.derstandard.at/story/2000070834253/fehler-bei-ip-adressen-viele-briten-faelschlich-wegen-kinderpornos-verhaftet

72. openh264.org – Website, die Video Codecs anbietet
https://www.openh264.org/

73. owasp – Secure Cookie Attribute – Erläuterung, was sichere Cookies ausmacht
https://owasp.org/www-community/controls/SecureCookieAttribute

74. PC-Magazin – So werden Sie mit Cookies ausspioniert
https://www.pc-magazin.de/ratgeber/so-werden-sie-mit-cookies-ausspioniert-1048816.html

75. Privacy-Preserving Ad Click Attribution for the Web – Ergänzungen von Trackern, um die Privatsphäre zu schützen
https://webkit.org/blog/8943/privacy-preserving-ad-click-attribution-for-the-web/

76. Privacy-Preserving Product Analytics (P3A) – Privatsphäre schüztende Analyseverfahren
https://brave.com/privacy-preserving-product-analytics-p3a/

77. Protecting against HSTS abuse – Schutz gegen den Missbrauch von HTTP Strict Transport Security
https://webkit.org/blog/8146/protecting-against-hsts-abuse/

78. ProtonVPN – ein schweizer VPN Anbieter mit kostenlosen und kostenpflichtigen Angeboten
https://proton.me/

79. remind / HAW Hamburg – Informationen zu Metadaten
http://www2.bui.haw-hamburg.de/pers/ulrike.spree/remind/metadaten.htm

80. State partitioning – Verwaltung von Nutzerdaten auf Seiten des Browsers
https://developer.mozilla.org/en-US/docs/Web/Privacy/State_Partitioning

81. Tales of Favicons and Caches: Persistant Tracking in modern Browsers – Erläuterungen zu dauerhaftem Tracking durch moderne Browser
https://www.cs.uic.edu/~polakis/papers/solomos-ndss21.pdf

82. techopedia, Zombie Cookie - Kaspersky, What are Cookies – eine Erläuterung von Zombie Cookies
https://www.kaspersky.com/resource-center/definitions/cookies

83. The most popular solution to cookie laws – rechtskonforme Einbindung von Cookies
https://www.osano.com/cookieconsent

84. The Verge - Microsoft Edge is leaking the sites you visit to Bing
https://www.theverge.com/2023/4/25/23697532/microsoft-edge-browser-url-leak-bing-privacy

85. The Verge – Privacy and ads in chrome are about to become flocing complicated – Erläuterung einer neuen Trackingform durch Google. Nur für Chrome. Seit dem 14. Juli 2021 von Google eingestellt, bevor offiziell eingeführt
https://www.theverge.com/2021/3/30/22358287/privacy-ads-google-chrome-floc-cookies-cookiepocalypse-finger-printing

86. TLS (Transport Layer Security) – Verschlüsselung auf Transportwegen
https://de.wikipedia.org/wiki/TLS

87. TOR Browser Bundle – Browser für weitestgehend anonymes Surfen
https://www.torproject.org/de/download/

88. Verbesserter Schutz vor Aktivitätsverfolgung in Firefox für Desktop
https://support.mozilla.org/de/kb/verbesserter-schutz-aktivitatenverfolgung-desktop

89. Verbraucherportal-bw.de – Cookies – hilfreich oder gefährlich
https://www.verbraucherportal-bw.de/,Lde/Startseite/Verbraucherschutz/Cookies+_+hilfreich+oder+gefaehrlich_

90. Verbraucherzentrale – Cookies kontrollieren und verwalten
https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/cookies-kontrollieren-und-verwalten-11996

91. VPN (Virtual Private Network) – Erklärung, was VPN sind https://de.wikipedia.org/wiki/Virtual_Private_Network

92. What is canvas fingerprinting and how the companies use it to track you online – Erklärung der Technik Canvas Fingerprinting und wie sie eingesetzt wird https://www.andreafortuna.org/2017/11/06/what-is-canvas-fingerprinting-and-how-the-companies-use-it-to-track-you-online/

93. Widevine – Software die vor Schadcode schützen soll https://www.widevine.com/ 85 Wikipedia – Secure cookie – Erläuterung was sichere Cookies sind https://en.wikipedia.org/wiki/Secure_cookie