

# Mein Browser - wie bringe ich die Plaudertasche zum Schweigen? Zum Schutz Ihrer Grundrechte

Michael Georg Schmidt  
ITS Explained

16./17. Juni 2023



# Michael Georg Schmidt

Der Referent

***Michael Georg Schmidt***

# Michael Georg Schmidt



Figure: Michael Georg Schmidt

- Beauftragter für Datenschutz und IT Sicherheit

# Michael Georg Schmidt



Figure: Michael Georg Schmidt

- Beauftragter für Datenschutz und IT Sicherheit
- Studium IT Sicherheit an TH Lübeck



# Michael Georg Schmidt



Figure: Michael Georg Schmidt

- Beauftragter für Datenschutz und IT Sicherheit
- Studium IT Sicherheit an TH Lübeck
- mit ITS Us. - Vorträge zu IT Sicherheit und Datenschutz

# Michael Georg Schmidt



Figure: Michael Georg Schmidt

- Beauftragter für Datenschutz und IT Sicherheit
- Studium IT Sicherheit an TH Lübeck
- mit ITS Us. - Vorträge zu IT Sicherheit und Datenschutz
- ITS Consultant - ITS Explained

# Michael Georg Schmidt



Figure: Michael Georg Schmidt

- Beauftragter für Datenschutz und IT Sicherheit
- Studium IT Sicherheit an TH Lübeck
- mit ITS Us. - Vorträge zu IT Sicherheit und Datenschutz
- ITS Consultant - ITS Explained
- freiberuflich Journalist

# Agenda

Heutige

***Agenda***

# Agenda

- Daten die der Browser ausplaudert

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann



# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media
- VPN - Virtual Private Network

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media
- VPN - Virtual Private Network
- Passwort Tresor

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media
- VPN - Virtual Private Network
- Passwort Tresor
- Online Speicher

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media
- VPN - Virtual Private Network
- Passwort Tresor
- Online Speicher
- Office online

# Agenda

- Daten die der Browser ausplaudert
- Entscheidend - der richtige Browser
- Warum sollte das wichtig sein?
- Was man dagegen tun kann
- Datenklau bei Nutzung von Webmailern
- Einsatz von Social Media
- VPN - Virtual Private Network
- Passwort Tresor
- Online Speicher
- Office online
- Fragen?

# Browserleaks

Plaudertasche

## ***Browserleaks***



# Browserleaks

**Browserleaks.com**

IP Address Lookup

It has long been believed that IP addresses and Cookies are the only reliable fingerprints used to track people online. But after a while, things got out of hand when modern web technologies allowed interested organizations to use new ways to identify and track users without their knowledge and with no way to avoid it.

Browserleaks is all about browsing privacy and web browser fingerprinting. Here you will find a gallery of web technologies security testing tools that will show you what kind of personal identity data can be leaked, and how to protect yourself from this.

### 📍 IP Address

The primary tool that Browserleaks uses to reveal the user's identity is its basic features, such as showing Your IP Address and HTTP Headers. IP-based geolocation (GeoIP) identifies your Country, State, City, ZIP/Postal Code, Timezone, also TCP/IP OS Fingerprinting, WABRTC Leak Tests, DNS Leak Test, IPv6 Leak Test.

### 🔍 WABRTC Leak Test

IP address detection using JavaScript. Starting with a WABRTC API, the web browser communicates with the STUN server and shares information about local and public IP addresses even if you are behind NAT and use a VPN or Proxy. This tool will show if your real public IP is leaking out.

### 📶 WebGL Report

WebGL Browser Report checks WebGL support in your browser, and offers WebGL and GPU capabilities more or less related with browser identity. Also, the page contains the How To enable or disable WebGL in your web browser.

### 📍 Geolocation API

HTML5 Geolocation API testing tool. Checks browser permissions for geolocation. Based on the latitude/longitude and accuracy returned from the browser, it shows the values of your location on the interactive map.

### 📄 Content Filters

The set of domains that try to determine Content Filters usage, in the applications that operate between the browser and the web page and manipulate the presentation and content of a visited web page. Always there are The Browser, Privacy Addback Detection.

### 🖱️ Flash Player

Describes the Flash Player Runtime properties such as: Flash Version, Plug-In, Operating System, Manufacturer, System Language, Web Browser Architecture, Screen Resolution, and other properties that describe the hardware and multimedia capabilities.

### More Tools

Here is a list of new, experimental, controversial, broken, and deprecated tools:

- [DNS Leak Test](#) - Standalone page for DNS Leak Test.
- [TCP/IP OS Fingerprinting](#) - Shows the TCP, TLS capabilities, TLS Fingerprint, Mixed Content Test.
- [GeoIP Geolocation](#) - HTTP and User Agent Client Hints Test Page.
- [Font-Face-List](#) - Font-Face-List (Google Fonts) Test Page.
- [Canvas Fingerprinting](#) - Displays the exact pixel position and size of the rectangle of HTML5 canvas.
- [Canvas Fingerprinting](#) - Checks single page identifier for most major social networks.
- [IPv6 Leak Test](#) - Checks DNS support in your web browser.
- [Privacy Protection](#) - Firefox - resource URI - fingerprinting, algorithm and locale detection.

Privacy Policy

The site does not collect any data, does not have or process any fingerprint records. All information shown is read-only. Some third-party services (Google, Disqus) may collect anonymized data and set unimportant cookies. You can control everything on the [Data Settings](#) page.

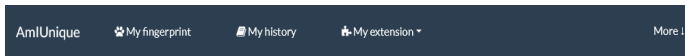
Browserleaks © 2011-2021. All Rights Reserved.  
mailto:admin@browserleaks.com

Die Site **Browserleaks**  
<https://browserleaks.com/>  
zeigt, welche Daten Ihr  
Browser leakt.

# Am I Unique

Einzigartig

***Am I unique***



## My browser fingerprint

Are you unique?

Yes! You are unique among the 3961309 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.



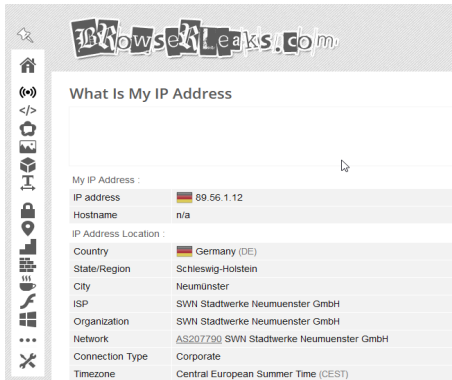
Figure: Einzigartigkeit ist schön, aber nicht im Netz.

# IP-Adresse und Standort

Standort


## ***IP-Adresse und Standort***

# IP-Adresse und Standort



The screenshot shows the website 'ipwhois.com' with the title 'What Is My IP Address'. Below the title is a search bar. The main content area displays the following information:

My IP Address :

IP address	 89.56.1.12
Hostname	n/a

IP Address Location :


Country	 Germany (DE)
State/Region	Schleswig-Holstein
City	Neumünster
ISP	SWN Stadtwerke Neumuenster GmbH
Organization	SWN Stadtwerke Neumuenster GmbH
Network	AS207790 SWN Stadtwerke Neumuenster GmbH
Connection Type	Corporate
Timezone	Central European Summer Time (CEST)

Figure: Sogar der Standort ist erkennbar.

# Der richtige Browser

Petze oder nicht

***Entscheidend -  
der richtige Browser***

# Entscheidend - der richtige Browser



Figure: Der falsche Browser - und Sie haben verloren.



Figure: **Brave** ist aktuell einer der sichersten Browser.





Figure: **Brave** ist aktuell einer der sichersten Browser.



Figure: Anfangs ist Safari zu neugierig - lässt sich aber trainieren.

Petzen

***Ab jetzt - Finger weg!***



Figure: Der IE verschiebt Massen an Daten zu Microsoft.



Figure: Edge ist in dieser Hinsicht nicht besser als der IE.



**Figure:** Opera hatte mal einen guten Ruf - jetzt klaut er Daten.



**Figure:** Auch Vivaldi bedient sich skrupellos an Ihren Daten.

# Warum sollte das wichtig sein?

Unbequem

***Warum sollte das wichtig sein?***



# Browser Fingerprinting



Figure: Browser hinterlassen Fingerabdrücke.

# Browser Fingerprint

AmlUnique

My fingerprint

My history

My extension

More

## My browser fingerprint

### Are you unique ?

Yes! You are unique among the 3961309 fingerprints in our entire dataset.

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

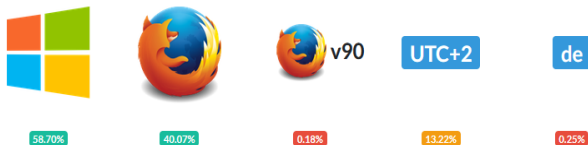


Figure: Beispiel für einen Browser Fingerprint.

# Was man dagegen tun kann

Abhilfe

***Was man dagegen tun kann***

# Richtiger Browser mit Add-ons



Figure: Firefox(ESR).

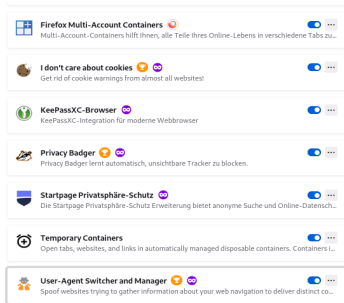


Figure: Die richtigen Add-ons.

# Hilfreiche Add-ons

Helferlein

## ***Hilfreiche Add-ons***

# I don't care about cookies



Figure: I don't care about cookies kümmert sich um Consent Banner.

# Ohne und mit I don't care about cookies

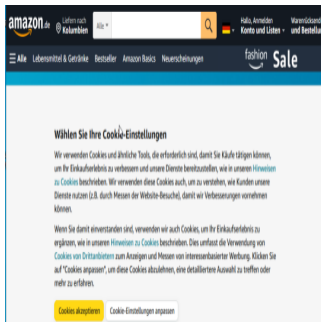


Figure: Ohne I don't care about cookies.



Figure: Mit I don't care about cookies.

# Multi Account Containers



Figure: Für jedes Thema ein Container.



# Multi Account Containers - Beispiel

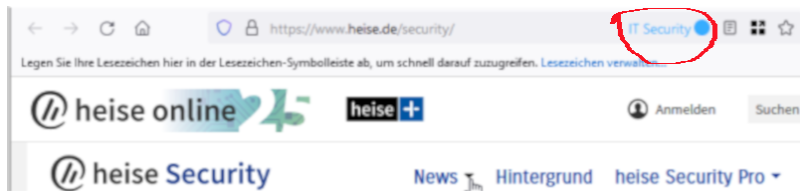


Figure: Für jedes Thema ein Container.

# Temporary Containers



Figure: Für jede Site ein Container.

# Temporary Containers - Beispiel

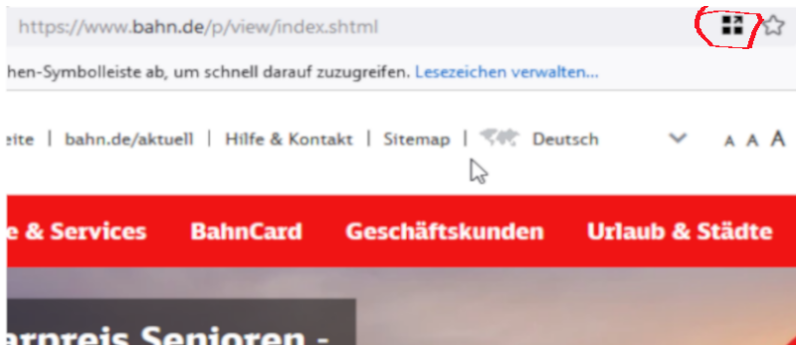


Figure: Für jede Site ein Container.

# User Agent Switcher



Figure: Schnüffler täuschen.

# User Agent Switcher - Beispiel

The screenshot shows a web browser window with a User Agent Switcher extension. The main interface displays a list of browser profiles:

Profile	Browser	OS	User Agent
1	Chrome 99.0.7113.93	Windows 10	Mozilla/5.0 (Windows NT 10.0; AppleWebKit/5...
2	Chrome 92.0.4495.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...
3	Chrome 92.0.4476.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...
4	Chrome 91.0.4433.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) A...
5	Chrome 90.0.4430.85	Windows 8	Mozilla/5.0 (Windows NT 6.2; Win64; x64) Ap...
6	Chrome 90.0.4430.93	Windows 8.1	Mozilla/5.0 (Windows NT 6.3) AppleWebKit/53...

Below the list, the details for the selected profile (Profile 6) are shown:

- userAgent:** Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0
- appVersion:** 5.0 (X11)
- platform:** Linux
- product:** Gecko
- vendor:** oscpu
- oscpu:** Linux x86\_64

At the bottom, there are four buttons: "Options", "Restart", "Refresh Tab", and "Reset". Below these are four colored buttons: "Test UA" (blue), "Consider Containers" (brown), "Apply (active window)" (green), and "Apply (all windows)" (green).

Figure: Möglichst viel gefaked.

# Referer Modifier



Figure: Ich komme von ganz wo anders.

# Privacy Badger



Figure: Blockt viele Schädlinge.

# Firefox richtig konfigurieren

Richtige Konfiguration

## ***Einstellungssache***



# Browser-Datenschutz

**Extras** → **Einstellungen** → **Datenschutz & Sicherheit** → **Browser-Datenschutz** → **Streng**

**Streng**

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

Firefox blockiert Folgendes:

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

ⓘ Um die Änderungen anzuwenden, müssen alle Tabs neu geladen werden.

[Alle Tabs neu laden](#)

**⚠ 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](#)

**Figure:** Wählen Sie die strengsten Voraussetzungen.

# Do not track

## **Extras** → **Einstellungen** → **Datenschutz & Sicherheit** → **Do not track**

Websites eine "Do Not Track"-Information senden, dass die eigenen Aktivitäten nicht verfolgt werden sollen

### Weitere Informationen

- Immer
- Nur wenn Firefox bekannte Elemente zur Aktivitätenverfolgung blockieren soll

Figure: Gute gemeint, aber wirkungslos.

# Betrügerische Software

***Extras*** → ***Einstellungen*** → ***Datenschutz & Sicherheit*** → ***Schutz vor betrügerischen Inhalten und gefährlicher Software***

Sicherheit

## Schutz vor betrügerischen Inhalten und gefährlicher Software

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

Figure: Alle Punkte bestätigen.

# Firefox Updates

**Extras** → **Einstellungen** → **Allgemein** → **Firefox Updates**

## Firefox-Updates

Firefox aktuell halten, um höchste Leistung, Stabilität und Sicherheit zu erfahren.

Version 102.11.0esr (64-Bit) [Neue Funktionen und Änderungen](#)

**Figure:** Aktuelle Software schließt Sicherheitslücken.

# Standardsuchmaschine

**Extras** → **Suche** → **Standardsuchmaschine**

## Standardsuchmaschine

Das ist Ihre Standardsuchmaschine in der Adress- und Suchleiste. Sie können diese jederzeit ändern.

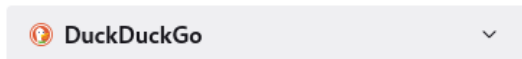


Figure: DuckDuckGo oder Startpage.

# Sicherer Abruf von Websites

**Extras** → **Allgemein** → **Verbindungs-Einstellungen** → **Einstellungen** → **am Ende der Maske**

Verbindungen mit localhost, 127.0.0.1/8 und ::1 werden nie über einen Proxy geleitet.

- Keine Authentifizierungsanfrage bei gespeichertem Passwort
- Bei Verwendung von SOCKS v5 den Proxy für DNS-Anfragen verwenden
- DNS über HTTPS aktivieren

Anbieter yerwenden **Cloudflare (Standard)** ▾

Hilfe

Abbrechen

OK

Figure: Sicherer Abruf von Websites.

# Cookies und Website-Daten

Bequemlichkeit versus Sicherheit

## ***Cookies und Website-Daten***

# Mit Bedacht anwenden

## **Extras** → **Datenschutz & Sicherheit** → **Cookies & Websitedaten**

### Cookies und Website-Daten

Die gespeicherten Cookies, Website-Daten und der Cache belegen derzeit 135 MB Speicherplatz. [Weitere Informationen](#)

Cookies und Website-Daten beim Benden von Firefox löschen

Daten entfernen...

Daten verwalten...

Ausnahmen verwalten...

**Figure:** Verräterische Daten, die das Leben bequemer machen.



# Chronik

## **Extras** → **Datenschutz & Sicherheit** → **Chronik**

### Chronik

Firefox wird eine Chronik **nach benutzerdefinierten Einstellungen anlegen** ▾

- Immer den Privaten Modus verwenden
- Besuchte Seiten und Download-Chronik speichern
- Eingegebene Suchbegriffe und Formulardaten speichern
- Die Chronik löschen, wenn Firefox geschlossen wird

**Chronik löschen...**

**Einstellungen...**

**Figure:** Entscheiden Sie, wie wichtig Ihnen die Chronik ist.

## Ein Wort zur Chronik

Bei den Einstellungen zur Chronik gibt es folgende wichtige Aspekte

- Chronik anlegen / niemals anlegen / nach Benutzer ...
- immer den privaten Modus verwenden
- die Chronik löschen, wenn Firefox geschlossen wird
- Chronik (manuell) löschen

# Bevorzugte Sprache

***Extras → Allgemein → Bevorzugte Sprache für die Darstellung von Websites wählen***

Bevorzugte Sprachen für die Darstellung von Websites wählen

Wählen...

**Figure:** Eine andere als die Muttersprache, wenn möglich.


# Webmailer

Sicher oder bequem

***Webmailer***

# Webmailer

*E-Mail-Adresse*

| 

*Passwort*

Passwort speichern  
Wähle diese Option nur bei der Verwendung eines privaten Geräts.

Anmelden

Registrieren

Farben wechseln

Zugangsdaten verloren

Figure: Bequem, aber auch vom Datenklau betroffen.

# Webmailer

## Ein Wort zu Webmailern

Bei den Webmailern gibt es folgende wichtige Aspekte

- sie sind bequem

## Ein Wort zu Webmailern

Bei den Webmailern gibt es folgende wichtige Aspekte

- sie sind bequem
- auch hier fallen Daten an, die der Browser weiterleiten kann

## Ein Wort zu Webmailern

Bei den Webmailern gibt es folgende wichtige Aspekte

- sie sind bequem
- auch hier fallen Daten an, die der Browser weiterleiten kann
- ein potentieller Angreifer hat direkten Zugriff auf Ihren Account



## Ein Wort zu Webmailern

Bei den Webmailern gibt es folgende wichtige Aspekte

- sie sind bequem
- auch hier fallen Daten an, die der Browser weiterleiten kann
- ein potentieller Angreifer hat direkten Zugriff auf Ihren Account
- ist eine E-Mail mit Trackern versehen, erhält der Absender Ihre Daten - mehr als bei einem Mailclient

# Mailclient statt Webmailer



Figure: Sicherer als ein Webmailer.

# Mail-App

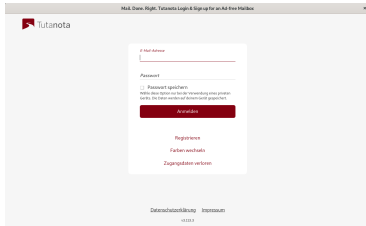


Figure: Die Tutanota App.

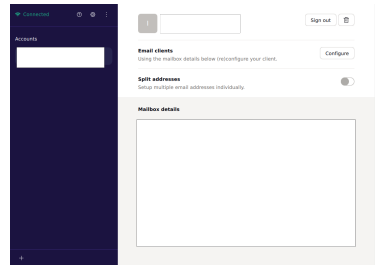


Figure: Die Proton Bridge - mit einem Mail-Client zu nutzen.

# Social Media

Beziehungssache

## ***Social Media***

# Social Media



Figure: Social Media verraten viel

- Social Media verraten viel

# Social Media



Figure: Social Media verraten viel

- Social Media verraten viel
- Besser separat nutzen

# Social Media



Figure: Social Media verraten viel

- Social Media verraten viel
- Besser separat nutzen
- Wenn im Browser, dann in virtueller Maschine

# Virutelle Maschinen

Nichts zum anfassen

***Virtual Box***



# Eine Software zur Virtualisierung - Virtual Box



- kostenlos

Figure: Kostenlos und recht sicher - [Virtual Box](#).

# Eine Software zur Virtualisierung - Virtual Box



- kostenlos
- einfach zu bedienen

Figure: Kostenlos und recht sicher - [Virtual Box](#).

# Eine Software zur Virtualisierung - Virtual Box



- kostenlos
- einfach zu bedienen
- hohes Maß an Sicherheit

Figure: Kostenlos und recht sicher - [Virtual Box](#).

# Eine Software zur Virtualisierung - Virtual Box



Figure: Kostenlos und recht sicher - [Virtual Box](#).

- kostenlos
- einfach zu bedienen
- hohes Maß an Sicherheit
- fertige Images stehen bei [osboxes](#) zur Verfügung



**Figure:** osboxes.org bietet eine Vielzahl an fertigen Images.

# TOR

Zwiebelringe

**TOR**

# Ein ganz besonderer Browser - TOR

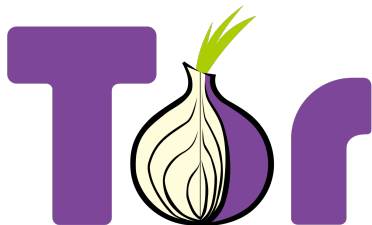
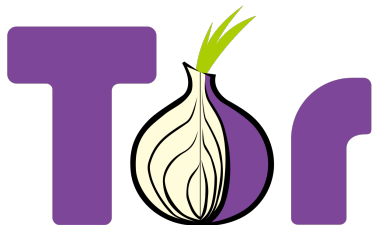


Figure: **Ausschliesslich unverändert** nutzen.

- TOR bietet hohes Maß an Anonymität

# Ein ganz besonderer Browser - TOR



**Figure:** Ausschliesslich  
unverändert nutzen.

- TOR bietet hohes Maß an Anonymität
- TOR ist das Tor zum Darknet



# Ein ganz besonderer Browser - TOR

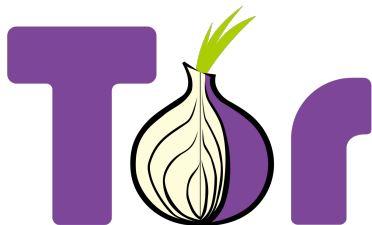


Figure: **Ausschliesslich unverändert** nutzen.

- TOR bietet hohes Maß an Anonymität
- TOR ist das Tor zum Darknet
- TOR **muss** mit **VPN - Virtual Private Network** genutzt werden.

# VPN - Virtual Private Network

Versteckspiel

## VPN - Virtual Private Network

# VPN - Virtual Private Network

- E2EE verschlüsselt



Figure: Virtual Private Network.

# VPN - Virtual Private Network



Figure: Virtual Private Network.

- E2EE verschlüsselt
- *Normale* Anfragen passieren bis zu 40 Hops

# VPN - Virtual Private Network



Figure: Virtual Private Network.

- E2EE verschlüsselt
- *Normale* Anfragen passieren bis zu 40 Hops
- Server sammelt Anfragen sehr vieler Nutzer

# VPN - Virtual Private Network



Figure: Virtual Private Network.

- E2EE verschlüsselt
- *Normale* Anfragen passieren bis zu 40 Hops
- Server sammelt Anfragen sehr vieler Nutzer
- Anfragende nicht erkennbar

# VPN - Virtual Private Network



Figure: Virtual Private Network.

- E2EE verschlüsselt
- *Normale* Anfragen passieren bis zu 40 Hops
- Server sammelt Anfragen sehr vieler Nutzer
- Anfragende nicht erkennbar
- **Schwachstelle:** Anbieter kann alle Daten mitlesen

# VPN-Anbieter denen ich vertraue

Vertrauenssache

# VPN-Anbieter denen ich vertraue



# VPN-Anbieter denen ich vertraue



Figure: ProtonVPN.



Figure: Mullvad VPN.



Figure: Mozilla VPN.



# Was bringt das?

Wozu der Aufwand?

# Was bringt das?

# Browser Fingerprint - angepasst



Figure: Ohne Anpassungen.

### My browser fingerprint

Are you unique ?

**Yes! You are unique among the 3960187 fingerprints in our entire dataset.**

The following informations reveal your OS, browser, browser version as well as your timezone and preferred language. Moreover, we show the proportion of users sharing the same elements.

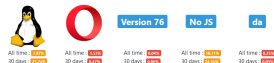
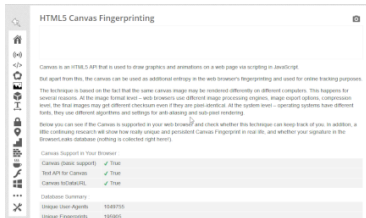


Figure: Mit Anpassungen.

# Canvas Fingerprint



**HTML5 Canvas Fingerprinting**

Canvas is an HTML5 API that is used to draw graphics and animations on a web page via scripting in JavaScript.

But apart from this, the canvas can be used as additional entropy in the web browser's fingerprinting and used for online tracking purposes.

The technique is based on the fact that the same canvas image may be rendered differently on different computers. This happens for several reasons. At the image format level – web browsers use different image processing engines, image export options, compression level, the final images may get different checksums even if they are pixel-identical. At the system level – operating systems have different fonts, they use different algorithms and settings for anti-aliasing and sub-pixel rendering.

Below you can see if the Canvas is supported in your web browser and check whether this technique can keep track of you. In addition, a 4tho continuing research will show how really unique and persistent Canvas Fingerprint in real life, and whether your signature in the BrowserLeaks database (profiling is collected right here).

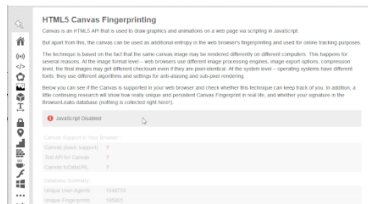
Canvas Support in Your Browser

Canvas (basic support)	✓ True
Test API for Canvas	✓ True
Canvas is/has/hasn't	✓ True

Database Summary

Unique User Agents	108876
Unique Fingerprints	108865

Figure: Ohne Anpassung.



**HTML5 Canvas Fingerprinting**

Canvas is an HTML5 API that is used to draw graphics and animations on a web page via scripting in JavaScript.

But apart from this, the canvas can be used as additional entropy in the web browser's fingerprinting and used for online tracking purposes.

The technique is based on the fact that the same canvas image may be rendered differently on different computers. This happens for several reasons. At the image format level – web browsers use different image processing engines, image export options, compression level, the final images may get different checksums even if they are pixel-identical. At the system level – operating systems have different fonts, they use different algorithms and settings for anti-aliasing and sub-pixel rendering.

Below you can see if the Canvas is supported in your web browser and check whether this technique can keep track of you. In addition, a 4tho continuing research will show how really unique and persistent Canvas Fingerprint in real life, and whether your signature in the BrowserLeaks database (profiling is collected right here).

JavaScript Disabled

Canvas Support in Your Browser

Canvas (basic support)	✓ True
Test API for Canvas	✓ True
Canvas is/has/hasn't	✓ True

Database Summary

Unique User Agents	108876
Unique Fingerprints	108865

Figure: Mit Anpassung.

# Browserleaks

## Your Results

Your browser fingerprint **appears to be unique** among the 240,157 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.87 bits of identifying information.**

Figure: Ohne Anpassungen.

The screenshot shows a report interface with two main sections. The left section, titled 'HOW TO READ YOUR REPORT', explains that the user will see a summary of their overall tracking protection, with the first section providing a general idea of what is blocked or not blocked, and the second section listing specific browser characteristics that a tracker would see. The right section, titled 'Here are your Cover Your Tracks results', states that the user's tests indicate they have strong protection against web tracking, but that their software is not checking for Do Not Track policies.

**HOW TO READ YOUR REPORT**

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would see them. We also provide descriptions of how they are incorporated into your fingerprint.

**HOW CAN TRACKERS TRACK YOU?**

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting.

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

**Our tests indicate that you have strong protection against Web tracking, though your software isn't checking for Do Not Track policies.**

Figure: Mit Anpassungen.

# VPN im Vergleich

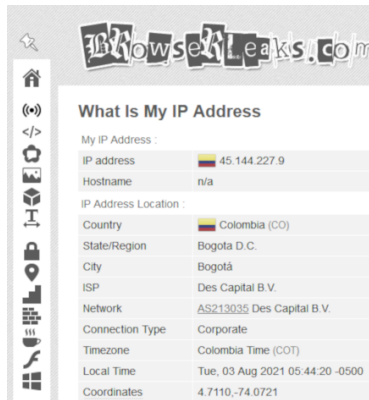


What Is My IP Address

My IP Address :

IP address	89.56.1.12
Hostname	n/a
IP Address Location :	
Country	Germany (DE)
State/Region	Schleswig-Holstein
City	Neumünster
ISP	SWN Stadwerke Neumuenster GmbH
Organization	SWN Stadwerke Neumuenster GmbH
Network	AS207790 SWN Stadwerke Neumuenster GmbH
Connection Type	Corporate
Timezone	Central European Summer Time (CEST)

Figure: Ohne VPN.



What Is My IP Address

My IP Address :

IP address	45.144.227.9
Hostname	n/a
IP Address Location :	
Country	Colombia (CO)
State/Region	Bogota D.C.
City	Bogotá
ISP	Des Capital B.V.
Network	AS213035 Des Capital B.V.
Connection Type	Corporate
Timezone	Colombia Time (COT)
Local Time	Tue, 03 Aug 2021 05:44:20 -0500
Coordinates	4.7110,-74.0721

Figure: Mit VPN.

Passwörter

**Passwörter nicht  
im Browser speichern**

# Passwörter nicht im Browser speichern

## Zugangsdaten und Passwörter

- Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen [Ausnahmen...](#)  
[Gespeicherte Zugangsdaten...](#)
- Zugangsdaten und Passwörter automatisch ausfüllen
- Starke Passwörter erzeugen und vorschlagen
- Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren [Weitere Informationen](#)
- Hauptpasswort verwenden [Weitere Informationen](#) [Hauptpasswort ändern...](#)  
Früher bekannt als Master-Passwort

Figure: *Hauptpasswort* →  
früher *Masterpasswort*

- Ohne *Hauptpasswort.png*  
Passwörter im Klartext



# Passwörter nicht im Browser speichern

## Zugangsdaten und Passwörter

Fragen, ob Zugangsdaten und Passwörter für Websites gespeichert werden sollen [Ausnahmen...](#) [Gespeicherte Zugangsdaten...](#)

Zugangsdaten und Passwörter automatisch ausfüllen

Starke Passwörter erzeugen und vorschlagen

Alarme für Passwörter, deren Websites von einem Datenleck betroffen waren [Weitere Informationen](#)

Hauptpasswort verwenden [Weitere Informationen](#) [Hauptpasswort ändern...](#)

Früher bekannt als Master-Passwort

Figure: **Hauptpasswort** →  
früher **Masterpasswort**

- Ohne **Hauptpasswort.png** Passwörter im Klartext
- Angreifer kann Passwörter auslesen

# Passwörter nicht im Browser speichern

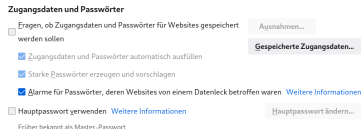


Figure: **Hauptpasswort** →  
früher **Masterpasswort**

- Ohne **Hauptpasswort.png** Passwörter im Klartext
- Angreifer kann Passwörter auslesen
- Personen mit physischem Zugriff können Passwörter auslesen

# Passwort Tresor

Sicher im Tresor

***Lokaler Passwort  
Tresor KeePassXC***

# KeePassXC

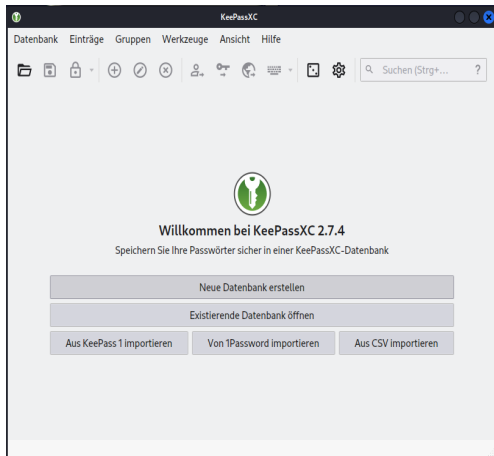


Figure: Ein **lokaler** Open Source Passwort Tresor.

# KeePassXC im Betrieb

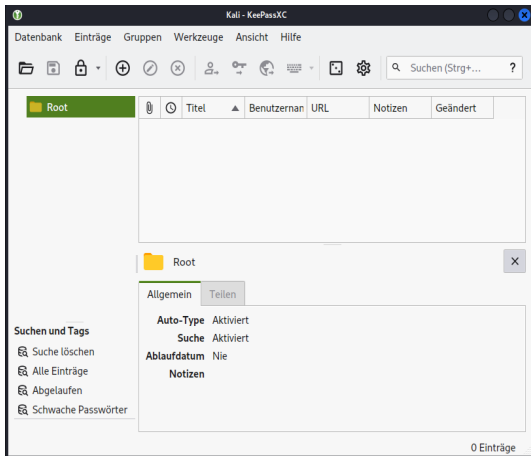


Figure: Hier legen Sie Ordner an.

# KeePassXC ist vielfältig verwendbar



Figure: KeePassXC

- Sicherer Passwort Tresor

# KeePassXC ist vielfältig verwendbar



Figure: KeePassXC

- Sicherer Passwort Tresor
- Fügt Passwörter automatisch ein

# KeePassXC ist vielfältig verwendbar



Figure: KeePassXC

- Sicherer Passwort Tresor
- Fügt Passwörter automatisch ein
- Speichert auch andere Geheimnisse



# KeePassXC trägt Passwörter ein

E-Mail-Adresse oder Benutzername



**Figure:** Auf Wunsch setzt KeePassXC Passwörter ein.

# Online Passwort Tresor

Unsicher im Tresor

## ***Online Passwort Tresore***

# Passwörter unsicher speichern

## *Argumente gegen Onlinetresor*

- Anbieter muss vertrauenswürdig sein

# Passwörter unsicher speichern

## *Argumente gegen Onlinetresor*

- Anbieter muss vertrauenswürdig sein
- amerikanische Anbieter sind verpflichtet Daten herauszugeben

# Passwörter unsicher speichern

## *Argumente gegen Onlinetresor*

- Anbieter muss vertrauenswürdig sein
- amerikanische Anbieter sind verpflichtet Daten herauszugeben
- Angriff lohnt sich, wegen der Menge an Passwörtern

# Passwörter unsicher speichern

## *Argumente gegen Onlinetresor*

- Anbieter muss vertrauenswürdig sein
- amerikanische Anbieter sind verpflichtet Daten herauszugeben
- Angriff lohnt sich, wegen der Menge an Passwörtern
- Risiko erheblich höher als bei lokalem Tresor

# Sicherer Onlinespeicher

Daten immer zugreifbar

## Onlinespeicher

## ***Sicherer Onlinespeicher sollte folgende Merkmale haben***

- E2EE - End-to-End-Encryption



## ***Sicherer Onlinespeicher sollte folgende Merkmale haben***

- E2EE - End-to-End-Encryption
- verschlüsselte Speicherung

## ***Sicherer Onlinespeicher sollte folgende Merkmale haben***

- E2EE - End-to-End-Encryption
- verschlüsselte Speicherung
- Speicherort in Europa

# Onlinespeicher denen ich vertraue



Figure: Tresorit.

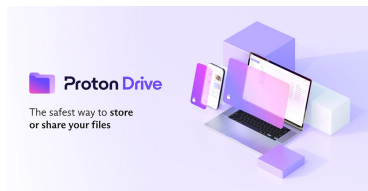


Figure: ProtonDrive.

Daten außer Kontrolle durch online Arbeit

***Online Office -  
achtung Anbieter!***

Wenn Sie online zusammenarbeiten wollen oder müssen, achten Sie darauf, den richtigen Anbieter zu nutzen. Sonst sind Ihre Daten ganz schnell außer *Ihrer* Kontrolle.

Online arbeiten

***Herrschaft über die eigenen  
Daten aufgeben***

# Die beiden größten Anbieter



Figure: Google docs.



Figure: M 365.

# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich



# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich
- Microsoft verarbeitet Nutzerdaten zu eigenen Zwecken
  - gibt nicht preis welche das sind

# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich
- Microsoft verarbeitet Nutzerdaten zu eigenen Zwecken
  - gibt nicht preis welche das sind
- Verschlüsselung der gespeicherten Daten bei Microsoft nur möglich mit Schlüssel bei Microsoft
  - Microsoft und Behörden haben Zugriff, also wirkungslos

# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich
- Microsoft verarbeitet Nutzerdaten zu eigenen Zwecken
  - gibt nicht preis welche das sind
- Verschlüsselung der gespeicherten Daten bei Microsoft nur möglich mit Schlüssel bei Microsoft
  - Microsoft und Behörden haben Zugriff, also wirkungslos
- Schlüssel at home
  - nur in teurerer Version
    - nur in Hard- oder Software von Microsoft
      - somit unwirksam

# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich
- Microsoft verarbeitet Nutzerdaten zu eigenen Zwecken
  - gibt nicht preis welche das sind
- Verschlüsselung der gespeicherten Daten bei Microsoft nur möglich mit Schlüssel bei Microsoft
  - Microsoft und Behörden haben Zugriff, also wirkungslos
- Schlüssel at home
  - nur in teurerer Version
    - nur in Hard- oder Software von Microsoft
      - somit unwirksam

# Problematisch weil ...

- amerikanische Anbieter
  - Zugriff amerikanischer Behörden jederzeit möglich
- Microsoft verarbeitet Nutzerdaten zu eigenen Zwecken
  - gibt nicht preis welche das sind
- Verschlüsselung der gespeicherten Daten bei Microsoft nur möglich mit Schlüssel bei Microsoft
  - Microsoft und Behörden haben Zugriff, also wirkungslos
- Schlüssel at home
  - nur in teurerer Version
  
- verschlüsseltes E-Mailing ausgeschlossen
  - aber gesetzlich gefordert

# Eine Alternative

Bleiben Sie in Europa

# Tresorit

- Anbieter in Europa



Figure: Tresorit für online  
Zusammenarbeit.

- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt



**Figure: Tresorit für online Zusammenarbeit.**





- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt
- Verschlüsselt auch E-Mail Betreffzeilen

**Figure: Tresorit für online Zusammenarbeit.**



**Figure: Tresorit für online Zusammenarbeit.**

- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt
- Verschlüsselt auch E-Mail Betreffzeilen
- Nutzbar mit Gmail und Outlook



**Figure: Tresorit für online Zusammenarbeit.**

- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt
- Verschlüsselt auch E-Mail Betreffzeilen
- Nutzbar mit Gmail und Outlook
- bietet elektronische Signatur



**Figure: Tresorit für online Zusammenarbeit.**

- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt
- Verschlüsselt auch E-Mail Betreffzeilen
- Nutzbar mit Gmail und Outlook
- bietet elektronische Signatur
- sicherer Onlinespeicher



**Figure: Tresorit für online Zusammenarbeit.**

- Anbieter in Europa
- Ende-zu-Ende-verschlüsselt
- Verschlüsselt auch E-Mail Betreffzeilen
- Nutzbar mit Gmail und Outlook
- bietet elektronische Signatur
- sicherer Onlinespeicher
- ... einiges mehr

# Fragen

Alles klar?

# Fragen

# Fragen?



**Gerne jetzt!**

Oder später:

[info@its-explained.com](mailto:info@its-explained.com)

Threema-ID: WYH86UFA