REFERENTIEDOCUMENT BROWSER

www.data-detox.nl

DATA DETOX KIT

Inhoud

1. Browsers vergelijken

Meer privacy in je browser kun je op verschillende niveaus verkrijgen, maar de eerste stap is om te beslissen welke browser je gebruikt als je het internet op gaat.

Chrome

Voordelen

• Beveiliging: Chrome behoort tot de beste browsers die er zijn.
• Flash is ingebouwd en wordt automatisch geüpdatet, wat betekent dat de kwetsbaarheid wordt beperkt tot een minimum (let wel, de beveiligingsonderzoeken van Chrome werden door Google gefinancierd in 2011 en er is sindsdien veel veranderd).
• "Incognitomodus": gemakkelijk te gebruiken browsemodus die voorkomt dat Chrome je browsegeschiedenis opslaat.
• Anti-volgsysteem: beste selectie advertentieblokkers van derden.

Beperkingen

• Privacy: advertenties vormen de grootste inkomstenbron van Google. Hiervoor gebruiken ze informatie die ze verzamelen via de aangeboden diensten, zoals Chrome, om uit te zoeken wat je doet, waar je bent, wat je koopt, enz.
• Standaardinstellingen: op Android kunnen gebruikers deze instellingen niet wijzigen.
• Geen open source.

Firefox

Voordelen

• Goede staat van dienst op het gebied van beveiliging, met een goed beloningssysteem voor het opsporen van bugs.
• Heeft een gemakkelijk te gebruiken privémodus en de privacyinstellingen kunnen ook worden aangepast.
• Anti-volgsysteem: goede selectie advertentieblokkers van derden (vlak achter Chrome).
• Intrekken SSL-certificaat: doet dit beter dan alle andere browsers.
• Gegevensbescherming is een kernpunt: in het manifest van het bedrijf staat, "De veiligheid en privacy van personen op het internet zijn fundamenteel en moeten niet als optioneel worden beschouwd."
• De broncode is beschikbaar (Firefox is de enige browser die volledig open source is).
• Non-profit: Firefox is ontwikkeld door Mozilla, een non-profitorganisatie die gratis kwalitatief goede software maakt. Dat betekent dat de browser niet wordt gebruikt als onderdeel van een overkoepelend programma om winst te maken.
• "Nieuw privévenster": gemakkelijk te gebruiken browsemodus die voorkomt dat Firefox je browsegeschiedenis opslaat en een zekere bescherming tegen trackers biedt.

Beperkingen

• Beveiliging nog niet zo goed als Chrome.

Safari
Voordelen
• Beveiliging: goede keuze voor OSX. Goede reputatie voor beveiliging en stapt in een vroeg stadium over op nieuwe functies.
Beperkingen
• Niet volledig open source.

Opera
Voordelen
• Beveiliging: staat erom bekend dat nieuwe beveiligingsfuncties worden toegevoegd voordat andere browsers dat doen en heeft de reputatie dat ze beveiligingsgaten sneller dichten dan andere browsers.

Beperkingen
• Volledig closed source.

Internet Explorer
Beperkingen
• Slechtste reputatie op het gebied van beveiliging. (Maar als je versie 10 of groter gebruikt, kun je de ergste problemen omzeilen.)
• Malware: heeft het hoogste ontdekkingspercentage van kwaadaardige software.
• Beveiliging: er zijn over de jaren heen veel ernstige beveiligingsgaten in de programmering geconstateerd.
• Volledig closed source (en Microsoft heeft samengewerkt met de Amerikaanse geheime dienst).

2. Zoekmachines
Privacyvriendelijke alternatieven voor Google Zoeken en Bing:
• DuckDuckGo - https://myshadow.org/duckduckgo
• Searx - https://myshadow.org/searx
• StartPage - https://myshadow.org/startpage

3. Checklist praktijk: browser
• Wijzig je standaard zoekmachine naar een zoekmachine die je privacy respecteert.
• Wijzig de taal naar Engels (meest gebruikte taal, geeft je een minder unieke browse-vingerafdruk).
• Installeer Firefox en pas de instellingen aan: automatisch alle geschiedenis wissen, cookies van derden uitschakelen en geschiedenis wissen als Firefox wordt gesloten. Hier vind je stapsgewijze instructies: https://myshadow.org/how-to-increase-your-privacy-on-firefox
• Stel buffer in op 0 MB: onder menu --> opties --> privacy en beveiliging --> cookies en websitegegevens --> gegevens wissen --> gebufferde webinhoud.
• Plug-ins en add-ons installeren. Hier vind je details: https://myshadow.org/prevent-online-tracking.
• Log uit bij alle commerciële diensten zoals Gmail, Facebook en Twitter als je ze niet gebruikt.

4. Volgfunctie in de browser: visualisatie-instrumenten
Trackography
Laat zien welke trackers van derde partijen aanwezig zijn op mediawebsites; de volgroute van de website naar de server van de tracker; en het privacybeleid van de meest dominante trackers.

Lightbeam Laat in realtime zien welke trackers van derde partijen op een website actief zijn; legt verband tussen trackers van derden op verschillende websites (bijv. Google Analytics).

5. Privacy en beveiliging door uitsplitsing

Met deze strategie vergroot je de privacy en beveiliging omdat je verschillende browsers voor verschillende dingen gebruikt. Je gebruikt in Chrome bijvoorbeeld alleen diensten van Google, gebruikt een andere browser voor Facebook en gebruikt Firefox voor de rest van het browsen.

6. Browse-vingerafdruk

Een browse-vingerafdruk bestaat uit een gedetailleerde reeks gegevens over je apparaat, lettergrootte, pixels, schermafmeting, taal, soort besturingssysteem, tijdzone, of je cookies accepteert en nog veel meer. De combinatie van deze elementen maakt dat jouw apparaat een unieke identificatie heeft.
Met Panopticlick (https://panopticlick.eff.org/) kun je testen hoe uniek je browse-vingerafdruk is.