Privacy op internet

Wat is privacy?	2
Wat is privacygevoelige informatie?	3
Cookies	8
Privé / incognito surfen	11
Instellingen van online accounts	12
VPN	16
Browserextensies	18
Alternatieve browsers en zoekmachines	24
Wachtwoordmanagers	28

Privacy, wat is dat?

Het is wettelijk vastgelegd, we hebben recht op privacy. Maar wat is dat eigenlijk? Privacy is best een lastig te omschrijven en breed begrip. Het heeft te maken met de bescherming van uw identiteit, met informatie die persoonlijk en vertrouwelijk is, maar het heeft ook te maken met autonomie en met recht op vrijheid en vrije meningsuiting. Het is een zeer waardevol iets, dat we graag willen beschermen!

In het dagelijks leven hebben we er wel een gevoel bij als het om onze privacy gaat. We houden onbekenden graag een beetje op afstand, we geven ze niet in blind vertrouwen onze kostbare bezittingen in handen, en we vertrouwen ze ook niet allerlei intieme informatie toe. Dat deel je uitsluitend met je geliefde, familie of goede vrienden. Of met betrouwbare en integere professionele personen, zoals de huisarts. Kortom, in het dagelijks leven onderscheiden we makkelijk wat vertrouwelijk is en wat niet.

Als het om onze identiteit op internet gaat, hebben we onze privacy veel minder scherp in beeld. En dat is niet zo gek! Want er zijn heel veel verschillende manieren waarop onze privé gegevens op internet terecht komen. Vaak hebben we het niet eens in de gaten. Daarbij is het helemaal onduidelijk wat er vervolgens met die informatie gebeurt. Waar gaat het heen, wordt het ergens bewaard en hoe lang dan? Kunnen andere mensen of instanties daar bij, hoe worden de gegevens dan verwerkt?

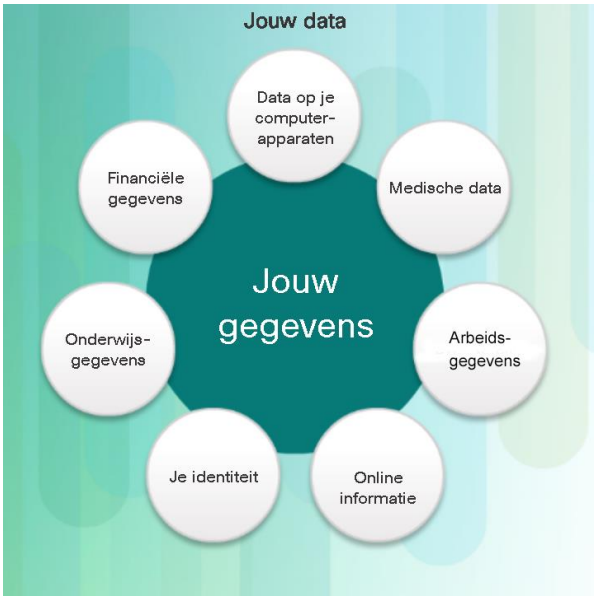
In deze cursus gaan we onderzoeken, waar onze online identiteit uit bestaat. Welke gegevens vallen daaronder en hoe kunnen we die gegevens beschermen. Veel risico's zijn te verkleinen door ons eigen gedrag een beetje aan te passen, en bewuster en kritischer om te gaan met internet.

Wat is privacygevoelige informatie?

Persoonlijke informatie, privacy gevoelige informatie, wordt in technische termen ook wel personal data genoemd. Wist u, dat zoiets onschuldigs als uw geboortedatum gevoelige informatie is? Wat is eigenlijk precies vertrouwelijke informatie, en hoe komt dat op internet terecht?
Van sommige informatie weten we het ongeveer, een profiel en/of status in sociale media maak je zelf aan.

Andere gegevens zijn in beheer van officiële instanties, te denken valt aan uw Digid (overheid) financiële gegevens (bank), medische gegevens (huisarts, ziekenhuis, verzekering) gegevens over uw opleiding (scholen en opleidingsinstituten) en gegevens over uw werk en functioneren (werkgever). Allemaal instanties die u over het algemeen uw gegevens kunt toevertrouwen.

Deze instanties moeten verantwoording afleggen voor de manier waarop ze uw gegevens bewaren en verwerken. Hier is het vooral van belang dat u er zelf ook alles aan doet om te zorgen dat derden hier geen toegang toe hebben.



Bron: CISCO online course Cyber security. Informeer naar deze cursus in uw bibliotheek!

Persoonlijke gegevens, data, zijn onder andere...:

- voorletter(s) en achternaam
- geboortedatum en geboorteplaats
- adressen (huisadres, e-mailadres)
- pasfoto
- handtekening

...maar ook:

- geslacht
- ras
- godsdienst
- gezondheid/medische gegevens
- seksuele geaardheid
- politieke voorkeur

Het lastige is, dat steeds meer organisaties en bedrijven onze gegevens online verzamelen en bewaren. Meer en meer verloopt dienstverlening online. Dat maakt het gevaar op het uitlekken van onze gegevens steeds groter.

NIEUWS & ACHTERGROND 4 juli 2018

Hackers stelen e-mailadressen en rekeningnummers bij de Persgroep

NIEUWS & ACHTERGROND 14 mei 2018

Ernstig datalek bij vereniging voor stamboomonderzoek

NIEUWS & ACHTERGROND 12 december 2017

Uber: Hackers maakten vorig jaar 174.000 accounts in Nederland buit

De gemeente Den Haag en bibliotheek Den Haag

Ook de bibliotheek heeft persoonlijke gegevens van haar leden in beheer. Natuurlijk zijn naam, adres, telefoonnummer en e-mailadres bij ons geregistreerd.
Maar misschien nóg gevoeliger is de informatie over het leengedrag van mensen. Welke boeken lees je, welke informatie zoek je? Als organisatie gaan we daar strikt vertrouwelijk mee om, dat zijn we ook wettelijk verplicht. Want hier gaat het om meer dan persoonsgegevens. Hier gaat het om de vrijheid van personen, om zich te informeren en een mening te vormen. De leengeschiedenis van klanten wordt momenteel om privacy-redenen niet bewaard, en terecht!

De bibliotheek valt onder de gemeentelijke dienst Publiekszaken. Lees hier de verklaring inzake gegevensbescherming van de Gemeente Den Haag:

https://www.denhaag.nl/nl/verklaring-inzake-gegevensbescherming.htm

Hoe komen anderen aan uw gegevens?

Het hacken van databestanden van organisaties is slechts één van de vele manieren waarop privégegevens worden verkregen. Er zijn er meer, en ze zijn niet eens allemaal illegaal!

Tracken
Persoonlijke informatie kan ook worden verzameld door middel van tracking. Tracken, of volgen, gebeurt met gebruikmaking van technologie. Er zijn verschillende methoden voor, begrippen als cookies en fingerprinting worden verderop in dit boekje nader besproken.

Heb je wel eens gemerkt dat als je iets hebt gezocht op internet - een bepaald product, of een vakantiebestemming - dat daarna ineens alle reclames die je in je scherm ziet over dat specifieke product of over die bestemming gaan? Dat komt door tracking!
Bedrijven, reclamenetwerken en andere belangengroepen kijken dus over je schouder mee.

Er kan worden vastgesteld waar je computer zich bevindt, welke browser je gebruikt, welke zoekopdrachten je intypt en welke sites je bezoekt. Aan de hand hiervan kan een profiel van je worden opgemaakt dat schrikbarend persoonlijk is. Of je homo- of heteroseksueel bent bijvoorbeeld, kan worden vastgesteld naar aanleiding van je surfgedrag. Of wat je politieke voorkeur is, en hoe het met je gezondheid gesteld is.

Gebruik je een mobiel apparaat, zoals een tablet of een smartphone, dan heb je te maken met vele verschillende apps (programma's), die informatie over je verzamelen.
Die apps vragen soms toegang tot je contactenlijst, of willen bijhouden waar je je bevindt. Soms verschaffen ze zich toegang tot je foto's, microfoon of je camera! Veel mensen realiseren zich niet dat ook de informatie hiervan via internet door bedrijven wordt binnengehaald!

Beeld: https://www.mediawijsheid.nl/privacy/

Wat zijn de gevaren van tracking?
Tracking kan om vele redenen en met verschillende doeleinden worden ingezet. Over het algemeen is het een onschuldig fenomeen, en gebruikt een bedrijf de informatie uitsluitend om je als klant beter te leren kennen en om je beter en sneller van dienst te kunnen zijn. Tracking is niet persé slecht! Maar het kán worden ingezet met minder goede bedoelingen.

Diefstal van gegevens
In sommige gevallen kan tracking leiden tot veiligheidslekken, en kan informatie gestolen worden, zoals e-mailadressen, wachtwoorden, of zelfs credit card gegevens.

Identiteitsfraude
De gevolgen van diefstal van gegevens kunnen enorm groot zijn.
Zo kan er gefraudeerd worden met identiteit. Als jouw identiteit door iemand anders wordt overgenomen en vals wordt gebruikt, kan dat heel nare gevolgen voor je hebben. Mensen kunnen zich voor jou uitgeven, en op die manier aankopen doen, reizen boeken, zich op een adres in- of uitschrijven, delicten begaan enz... Het duurt gemiddeld vijf jaar om alle schade te herstellen als je identiteit gestolen is.

Prijsaanpassingen
Een gevaar van tracking is dat belanghebbenden kunnen nagaan waar uw interesse naar uit gaat. Dat reikt verder dan de reclames op uw interesses aanpassen. Als u meerdere keren een boeking site bezoekt en steeds op hetzelfde hotel of dezelfde reis klikt, kan het goed zijn dat u ziet dat de prijs bij ieder bezoek hoger wordt. Want kennelijk bent u serieus geïnteresseerd, en dan bent u 'dus' bereid geld uit te geven!
Er zijn webshops die nagaan of u in een 'welgestelde buurt' woont, en aan de hand daarvan andere (hogere) prijzen hanteren voor hetzelfde product.

Beïnvloeding
Subtieler, maar niet minder gevaarlijk, is dat u beïnvloed wordt, zonder dat u dat in de gaten hebt. Door uw surfgedrag is na te gaan waar u in geïnteresseerd bent of waar u gevoelig voor bent. Belangengroepen kunnen u bepaalde informatie of reclames aanbieden bijvoorbeeld, Informatie die is aangepast aan uw voorkeur of overtuiging. Zo wordt u, zonder dat u het merkt, steeds bevestigd in bepaalde overtuigingen die u hebt. Dit heet de 'filterbubbel'. Het gevaar hiervan is, dat we niet meer in staat zijn onafhankelijk, objectief en kritisch onze mening te vormen.

Sociale media en privacy
Wie gebruik maakt van sociale media zet zelf informatie online. De één is daar makkelijker in dan de ander, maar zelfs wie heel voorzichtig te werk gaat, geeft veel van zijn identiteit prijs. Te denken valt aan onze geboortedatum, opleiding of baan en onze sociale status. Ook laten we daar graag weten hoe het met ons gaat, waar we mee bezig zijn, wat we wel en niet leuk vinden, en met wie we bevriend zijn. We geven er onze mening, we delen er foto's en filmpjes. Zonder dat we het in de gaten hebben, geven we heel veel van onszelf prijs. Aan vrienden, aan vrienden van vrienden... vaak ook aan volslagen onbekenden. Want ook al is uw profiel voor onbekenden afgeschermd, iemand kán een beeldscherm kopiëren of fotograferen en de inhoud doorsturen of alsnog openbaar maken.

Het lijkt onschuldig, wat geeft het nou dat je foto's of filmpjes deelt. Of persoonlijke informatie op facebook zet. "Ik heb niets te verbergen", wordt vaak gezegd. Maar dat is niet waar. Los van elkaar lijken de stukjes en beetje informatie die u over uzelf prijs geeft inderdaad niet belangrijk. Maar als iemand ze bewust verzamelt, kan hij of zij een heel 'profiel' van u maken. Via onderstaande link komen we bij een filmpje waarin duidelijk wordt, wat slimme speurders kunnen vinden van iemand die actief is op internet.

Filmpje: *https://youtu.be/YNPI6B-BUW4*

NB: Verderop in dit boekje gaan we in op accountinstellingen. Ook sociale media komen hier weer aan de orde.

Eigen 'slordigheid'

Het grootste gevaar voor onze online privacy zijn we meestal zelf. Vrijwel iedereen maakt zich er wel schuldig aan: Te vaak en te lang dezelfde (makkelijke) wachtwoorden gebruiken. Op 'Akkoord', 'Accepteer' of 'OK' klikken zonder voorwaarden echt goed door te lezen. Ingelogd blijven op gevoelige accounts. Of browsers onze wachtwoorden laten onthouden.

Over het algemeen gaat het goed, laten we dat voorop stellen! Maar probeer op de volgende punten te letten:

1) Wijzig regelmatig uw wachtwoorden (zie ook het hoofdstuk wachtwoord managers)
2) Denk na over de veiligheid van uw verbinding. WIFI in een openbare of publieke gelegenheid is niet veilig genoeg om gevoelige informatie te raadplegen. Gebruik dan liever uw mobiele data!
3) Hebt u ergens op moeten inloggen? Dat betekent dat u óók weer moet uitloggen! Zéker wanneer u dit hebt gedaan op een mobiel apparaat, óf in een publieke omgeving!
4) Let op als u gevoelige bestanden download. Ze worden daarmee opgeslagen op het apparaat dat u op dat moment gebruikt. Wees u daarvan bewust als u apparatuur gebruikt dat niet van u is (bijvoorbeeld in de bibliotheek of in een internetcafé). Of als u een mobiel apparaat gebruikt, dat is immers gevoeliger voor diefstal of verlies.
5) Gebruikt u sociale media? Check dan af en toe de instellingen van uw account. (Zie het hoofdstuk 'Instellingen van online accounts').
6) Vul niet zomaar overal uw gegevens in. (Ook niet als daar een aantrekkelijk voordeeltje tegenover staat!)
7) Wees alert op phishing mails! Ze zien er steeds professioneler uit!

Cookies

Ze hebben door alle berichtgeving een twijfelachtige reputatie. Cookies! Zodra u een website bezoekt krijgt u allereerst de vraag of je cookies accepteert.
Maar wat zijn cookies eigenlijk?

Cookies zijn kleine tekstbestandjes (de tekst is meestal een code en niet leesbaar.) Wanneer u een website bezoekt, wordt dat tekstbestandje automatisch op het apparaat gezet waarmee u op dat moment online bent. Er zijn verschillende soorten cookies. Sommige cookies zijn noodzakelijk om het bezoek aan de website mogelijk te maken. Voor het plaatsten van deze cookies hoeft geen toestemming te worden gevraagd. Dit zijn de zogeheten functionele cookies.

Er zijn ook cookies die de dienstverlening beter, makkelijker of sneller maken. Zolang uw gegevens privé blijven en niet gedeeld worden, mag een website ook deze cookies zonder toestemming op uw toestel plaatsen.

Voor andere cookies dient wel toestemming te worden gevraagd. Zodra u toestemming hebt gegeven voor het plaatsen van cookies, wordt die toestemming opgeslagen in… jawel, een cookie op uw apparaat! Dat is handig, zo hoeft u op dezelfde website niet steeds weer akkoord te geven.

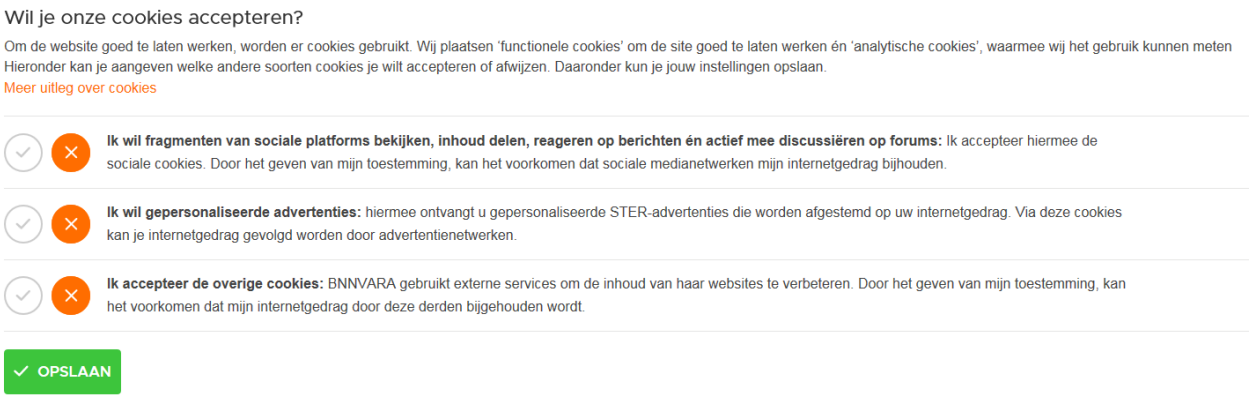
Tracking cookies

Er zijn ook cookies die u surfgedrag bijhouden, en die informatie doorsluizen naar derden, bijvoorbeeld (commerciële) organisaties. Dit zijn tracking cookies, en deze zijn niet gewenst als het om onze privacy gaat. Vaak is moeilijk na te gaan waar deze informatie terecht komt en wat daarmee gedaan wordt.

Cookies tegenhouden

Er zijn verschillende manieren om te zorgen dat cookies niet op uw apparatuur terecht komen. Als er toestemming wordt gevraagd om cookies te plaatsen, kunt u dit natuurlijk weigeren. U kunt aangeven dat u niet akkoord bent met het plaatsen van cookies.
Let op, dit kan gevolgen hebben voor de werking of de weergave van de website!

Sommige websites geven weer van welke cookies ze gebruik maken, en kunt u per categorie bepalen welke u wel en welke u niet accepteert. Zie het voorbeeld hieronder, van de website van BNNVARA.



Afhankelijk van de apparatuur die u gebruikt, zijn er tools, of apps, die u helpen inzicht te krijgen in de cookies die op uw apparatuur terecht komen, of die u helpen cookies tegen te houden. Een aantal handige tools bespreken we in de navolgende hoofdstukken.

Cookies zijn ook handmatig te verwijderen van uw apparaat. Zo'n schoonmaakactie kan goed zijn, omdat er soms veel (onnodige) cookies op uw apparaat terecht komen. Zie hiervoor de de stappenplannen op de navolgende pagina's.

Fingerprinting

Fingerprinting is een overkoepelende term voor verschillende methodes die specifieke elementen opsporen die een browser uniek maken. Uw browser als digitale vingerafdruk dus. De combinatie van gebruikte plug-ins, updates, schermresolutie, onderliggende software en andere elementen maken uw browser uniek, en daardoor herkenbaar tussen miljoenen andere browsers.

In praktijk betekent dit bijvoorbeeld: Uw browser vertelt websites dat u in Nederland bent (en in welke plaats) en dat u geen cookies accepteert. Dat u een aantal uitbreidingen (extensies) heeft geïnstalleerd, zoals HTTPS Everywhere en AdBlock Plus. Ook is te zien welke lettertypes u gebruikt, hoe groot uw scherm is en welk besturingssysteem u gebruikt.

Bij browser-fingerprinting wordt meestal meteen gedacht aan advertentietracking, maar het is voor sommige toepassingen ook voor de internetgebruiker erg nuttig. Banken gebruiken het bijvoorbeeld om te controleren of een gebruiker plotseling vanaf een andere locatie inlogt of dat hij dat met een onbekend apparaat doet, en kunnen zo een extra beveiligingscheck sturen
Op de website https://panopticlick.eff.org/ kunt u uw eigen browser testen op kenmerken die uw browser uniek maken.

Cookies wissen

In Chrome

1: Open Google Chrome.

2: Klik op het pictogram ‘Google Chrome aanpassen en beheren'. Dit is het pictogram met drie puntjes.

3: Klik op Meer hulpprogramma's > Browsegegevens wissen.

4: Er opent een nieuw venster. Zet een vinkje voor Cookies en andere sitegegevens, als dat vinkje er nog niet staat.

5: Selecteer achter 'Periode' vanaf welk moment de cookies verwijderd moeten worden.

6: Klik op Gegevens wissen.

In Firefox

1: Open Firefox.

2: Klik rechtsboven op de menuknop.

3: Klik nu op Opties.

4: Er opent een nieuw tabblad in Firefox. Klik links op Privacy & Beveiliging.

5: Klik bij Geschiedenis op ‘alle huidige geschiedenis wissen’.

6: Selecteer ‘Cookies’.

7: Klik op ‘Wissen’.

In Edge

1: Klik rechtsboven op het pictogram met de drie punten...

2: Klik op Instellingen en in het nieuwe menu op Kies wat u wilt wissen.

3: In het menu 'Browsegegevens wissen' staan standaard enkele opties aangevinkt. Laat het vinkje voor 'Cookies en opgeslagen websitegegevens' staan. Klik op de hokjes voor de andere aangevinkte opties om de vinkjes te verwijderen.

4: Klik op Wissen.

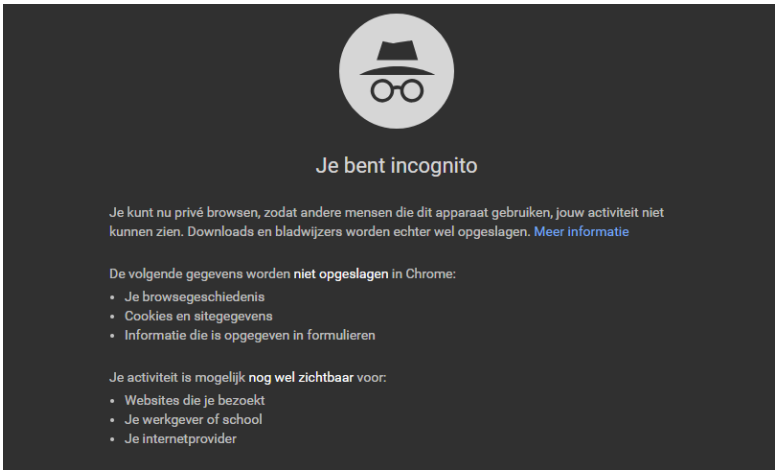
5: De gegevens worden gewist. Klik buiten het instellingenmenu op een leeg plekje om de instellingen te verlaten.

Privé / incognito surfen

Browsers slaan informatie op in de vorm van cookies, onthouden uw zoekgeschiedenis… Als u dat niet wilt, kunt u surfen op internet in 'privé modus'. Elke browser heeft zo'n instelling, die erop neerkomt dat uw surfgedrag van die sessie niet op uw computer wordt opgeslagen. Geen zoekgeschiedenis of cookies dus. Het is niet hetzelfde als anoniem surfen, want de bezochte websites zijn voor uw provider wel te achterhalen.
U kunt de prive / incognito modus inschakelen via de menubalk, of via een toetsencombinatie.

Firefox noemt de modus Privénavigatie.
In te schakelen met toetsencombinatie Ctrl + Shift + P

Chrome noemt het een incognito-venster.
In te schakelen met toetsencombinatie Ctrl + Shift + N



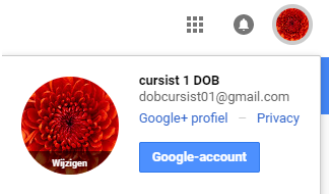
Bij **Edge** heet het InPrivate.
In te schakelen met toetsencombinatie Ctrl + Shift + P

Instellingen van online accounts

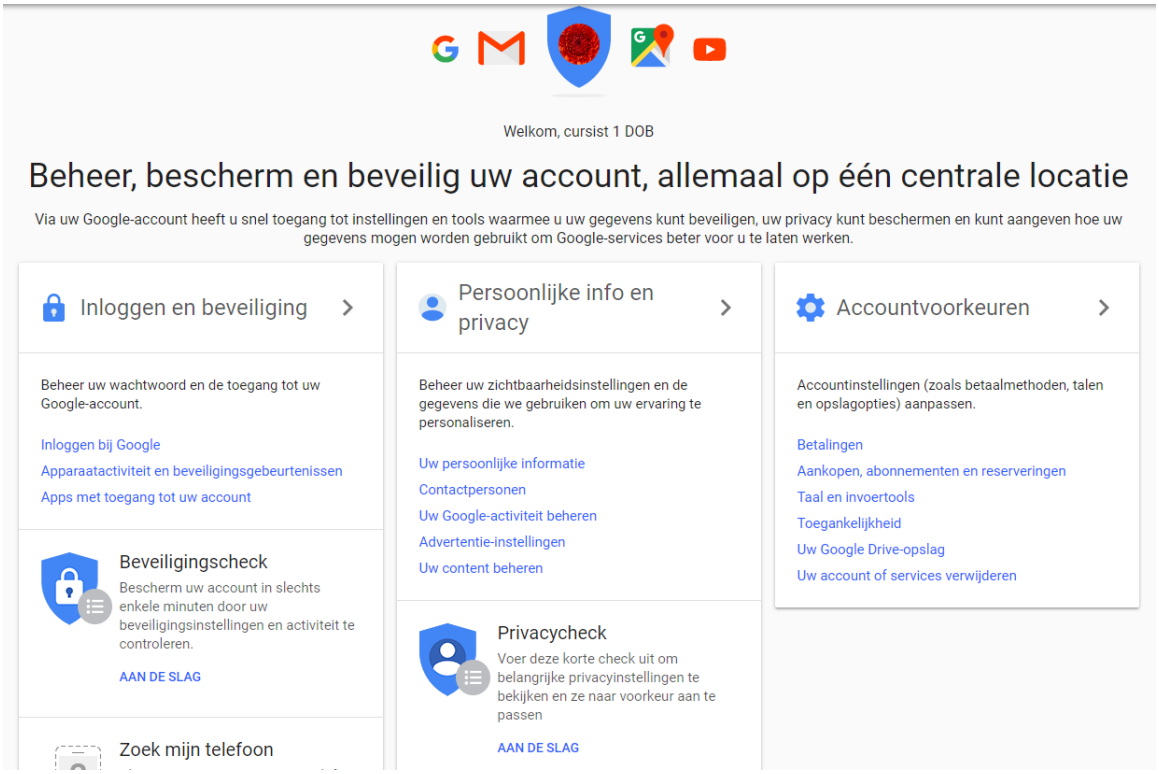
Veel zaken worden tegenwoordig online gedaan. Mail afhandelen, social media gebruiken, muziek beluisteren, bestellingen plaatsen enzovoorts. Voor al die dingen heeft u een account nodig bij desbetreffende dienst.
Soms wordt het u makkelijk gemaakt. Dan ziet u bij een dienst, bij Spotify kan dat bijvoorbeeld, een knop 'log in met Facebook' staan. Vooropgesteld dat u een Facebook account heeft, dan is dat wel handig, want ja, dan hoeft u geen nieuwe account aan te maken, geen nieuw wachtwoord te onthouden... Maar besef dat u alles wat u op Spotify doet, dan gekoppeld is aan uw Facebook profiel. Dus misschien dan toch maar een nieuwe account aanmaken?
In dit hoofdstuk kijken we naar een aantal online diensten en welke privacy aspecten daaraan verbonden zijn.

Google

Gmail, Google Docs/Drive, Google Maps. YouTube, het zijn allemaal diensten van Google. Heeft u een account voor het een (bijvoorbeeld Gmail) dan kunt u daarmee inloggen bij het ander (bijvoorbeeld YouTube).
Als u bent ingelogd, kunt u rechtsboven in het scherm op het icoontje van uw account klikken en vervolgens op de knop 'Google account' klikken.

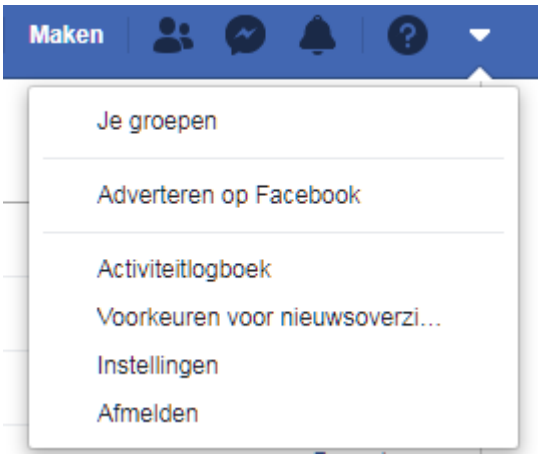


U komt dan op een scherm waar u allerlei informatie over uw account kunt vinden, en kunt aanpassen.

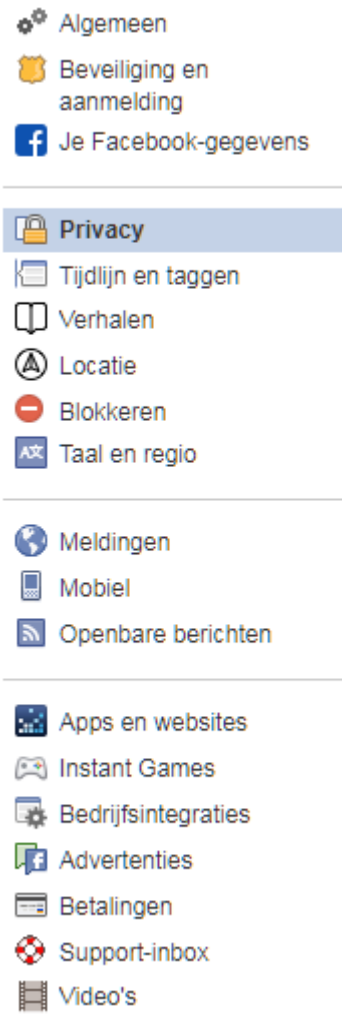


Facebook

Facebook en privacy, het lijkt geen goede match. Waar moet u zijn als u een account heeft om uw instellingen te beheren en waar moet u op letten?



Via het pulldown menuutje rechtsboven kunt u de optie 'Instellingen' selecteren. We lopen een aantal onderdelen na.



In het kopje *Privacy* kunt u aangeven voor wie berichten die u op Facebook plaatst zichtbaar zijn en hoeveel van uw gegevens te zien is.

Bij *Tijdlijn en taggen* kunt u aangeven wie berichten op uw tijdlijn kan plaatsen en of berichten waarin u getagd bent meteen zichtbaar worden.

Bij *Locatie* kunt u aangeven of de locatiegegevens (als u Facebook via uw telefoon of tablet gebruikt) worden bijgehouden.

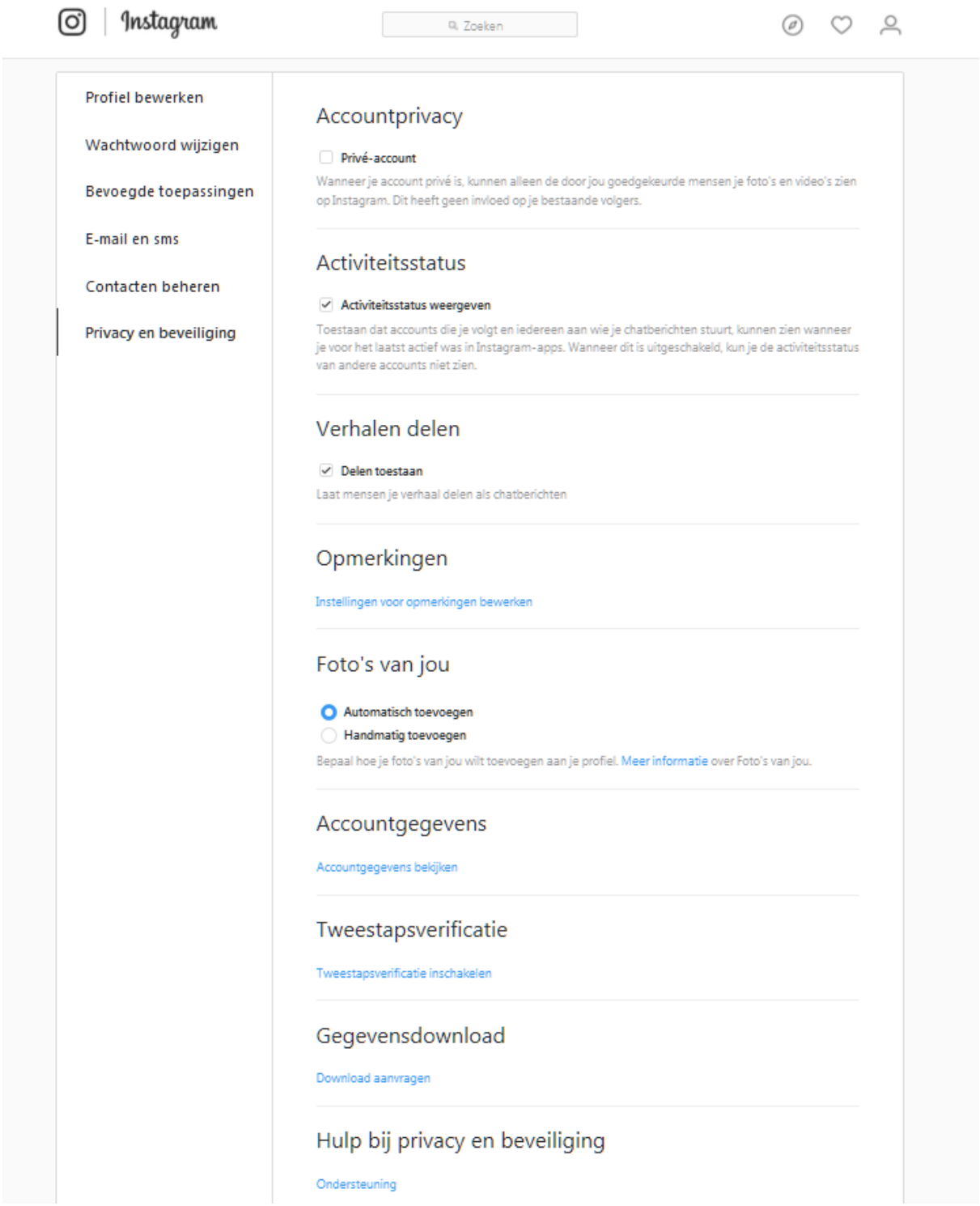
Bij *Apps en websites* kunt u zien of Facebook gekoppeld is aan andere apps of sites (bijvoorbeeld omdat u daarop inlogt met uw Facebook account). U kunt hier ook deze koppelingen uitzetten.

Bij *Advertenties* ziet u welke Facebook pagina's u advertenties voorschotelen. Dan kunnen er meer zijn dan u denkt! Heeft u eens geklikt op informatie van een schoenenfabrikant, dan is de kans groot dat u meer informatie over schoenen te zien krijgt. Het loont de moeite om de verschillende onderdelen die onder dit kopje te vinden zijn eens goed door te kijken en te verwijderen waar u geen berichten van wil ontvangen.

Filmpje (Consumentenbond):
https://www.youtube.com/watch?v=OK2q2mhb50E

Instagram

Instagram is een veelgebruikt platform om foto's te delen. Bij het aanmaken van een account zijn de foto's die u deelt standaard voor iedereen zichtbaar. U kunt echter ook instellen dat u mensen eerst moet toelaten tot uw account voordat ze iets kunnen zien (privé-account). Dat doet u via Instellingen -> Privacy en beveiliging. Hier kunt u diverse onderdelen van uw account inzien en aanpassen.



Tweestapsverificatie

Wilt u van een online account gebruik maken, dan moet u gebruikersnaam en wachtwoord opgeven. Pas dan krijgt u toegang. Maar wat nou als uw wachtwoord ontvreemd wordt? Dan kan degene die het in handen heeft bij alle gegevens van dat account. Om het bij even bij Google te houden: alle mails en bijvoorbeeld alle documenten en foto's die u bij Google Docs en Google Photos hebt opgeslagen.

Bij veel accounts is het mogelijk een extra controle in te bouwen. Dat heet tweestapsverificatie, soms ook wel tweestapsauthenticatie genoemd. Na het invoeren van uw wachtwoord, krijgt u een sms met een code op uw telefoon. Pas na het invullen van die code krijgt u toegang tot de account. U kunt de code ook via een app laten lopen, bijvoorbeeld Google Authenticator of Authy. De codes worden dan door de app gemaakt.

Tweestapsverificatie instellen

Op https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/ vindt u een overzicht voor veelgebruikte accounts om tweestapsverificatie in te stellen.

Hieronder een overzicht van de diensten die tweestapsverificatie aanbieden. Door op de naam van de dienst te klikken verlaat je Veiliginternetten.nl en ga je naar de site van de aanbieder van de dienst. Je komt op de specifieke pagina uit van de dienst waar je de tweestapsverificatie kunt instellen.

- Apple*
- Dropbox*
- Facebook*
- Google*
- LinkedIn*
- Microsoft*
- Twitter*
- WhatsApp*
- Yahoo*

Door op de links te klikken, word je naar de website in de link gestuurd. De link opent automatisch in een nieuw tabblad

Risico's

U krijgt uw code via uw telefoon binnen. Raakt u de telefoon kwijt, dan kunt u geen codes meer ontvangen en niet meer in uw account. Het is vaak wel mogelijk om een tweede telefoon op te geven. Bijvoorbeeld een oude telefoon die het nog doet en die u nog in bezit heeft. Of het toestel van een familielid. Mocht u er dan iets met uw eigen telefoon gebeuren, dan bent u niet meteen uw toegang tot al uw accounts kwijt.

Filmpje: (Veiliginternetten.nl): https://www.youtube.com/watch?v=zNdMqFpqz90

VPN

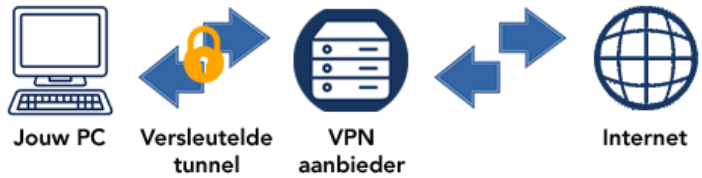
Als u van internet gebruik maakt, dan loopt het internetverkeer via de provider waarbij u een abonnement heeft afgesloten. Wanneer u een website opzoekt, dan stuurt uw provider u door naar deze website. Vervolgens krijgt u de website op uw scherm te zien.
Dat kan omdat elke website een eigen code heeft: een ip-adres. Omdat die nummers voor mensen niet te onthouden zijn, is die code omgezet naar een begrijpelijke url. Bijvoorbeeld www.nu.nl. Ook uw computer heeft een ip-adres. Zo weet de website dat u het bent die de informatie heeft opgevraagd. Uw provider verbindt als het ware de ip-adressen met elkaar.

Waarom VPN gebruiken

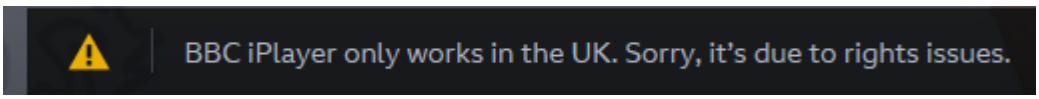
Wilt u niet dat uw provider en de bezochte websites weten welke sites / pagina's u bezoekt? Dan kunt u gebruik maken van een VPN verbinding. VPN staat voor Virtual Private Network. Dit is eigenlijk een tussenschakel. Het internetverkeer loopt dan niet rechtstreeks tussen u, uw provider en de websites. Een VPN server kan overal ter wereld staan en versleutelt ook het internetverkeer. Daardoor is het verband tussen de opvragende computer en bezochte website niet meer te maken. De bezochte website ziet het ip-adres van de VPN server en niet dat van u.

Directe internetverbinding:

Internetverbinding via VPN:



Er zijn diverse redenen om van VPN gebruik te maken. De eerste is anonimiteit, uw ip-adres is immers niet meer te herleiden. Ten tweede zorgt de versleuteling van het internetverkeer ervoor dat een eventuele hacker alleen maar willekeurige tekens te zien krijgt in plaats van uw gegevens. En hoewel er nog meer redenen te bedenken zijn, willen we als derde noemen dat VPN veel gebruikt wordt om landenblokkades te omzeilen. Sommige websites zijn namelijk alleen maar in het land van herkomst (onbeperkt) te gebruiken. De BBC is hier een bekend voorbeeld van.



Door een VPN server te kiezen die in het betreffende land staat, omzeilt u de blokkade. Er wordt immers een ip-adres uit dat land weergegeven en niet uw eigen Nederlandse ip.

VPN diensten

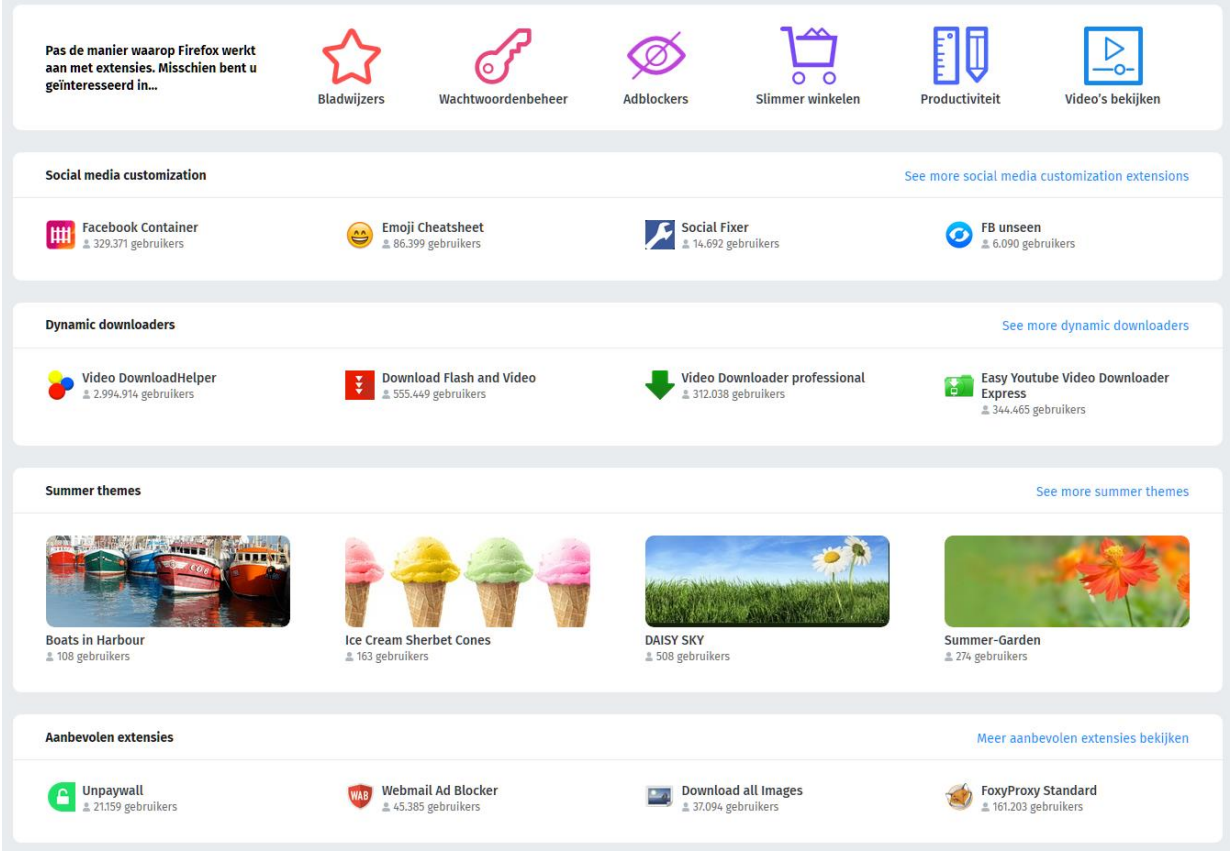
Om met VPN te werken moet u een account afsluiten bij een VPN aanbieder. Dat kost gemiddeld tussen de 5 en 10 euro per maand. Er zijn ook enkele gratis aanbieders. Daar gelden echter wel beperkingen, bijvoorbeeld in het aantal serverlocaties waarmee u verbinding kunt zoeken, of de hoeveelheid dataverkeer die u per maand kunt gebruiken. Na het afsluiten van een account en het installeren van de benodigde software krijgt u vaak een icoontje in uw browser te zien, zodat u snel de verbinding kunt in- en uitschakelen. Anders kunt u de verbinding via het Startmenu regelen.

Meer informatie over VPN vindt u onder meer op https://www.vpngids.nl/. Hier vindt u onder meer een overzicht van diverse aanbieders.

Filmpje (Consumentenbond): https://www.youtube.com/watch?v=kopUhOAK-to

Wat zijn browser extensies

Browser extensies zijn uitbreidingen voor een browser, die een extra functie toevoegen. Er zijn duizenden verkrijgbaar, op allerlei gebied. U kunt bijvoorbeeld uw browser een geheel nieuw uiterlijk geven, de werking van tabbladen aanpassen, het downloaden makkelijker maken enzovoorts. In deze module laten we enkele extensies zien op het gebied van privacy.



Extensies zijn specifiek voor een browser gemaakt. Een extensie voor Chrome werkt dus niet in bijvoorbeeld Firefox. Maar van veel extensies zijn varianten voor meerdere browsers beschikbaar. In Firefox worden extensies ook wel add-ons genoemd.

In het menu van uw browser zit een functie om naar extensies te zoeken. Als u een geschikte extensie heeft gevonden kunt u die simpel toevoegen. Soms is het nodig de browser opnieuw op te starten om de extensie in te schakelen. U kunt extensies ook rechtstreeks downloaden van de websites van de makers (als u die weet).

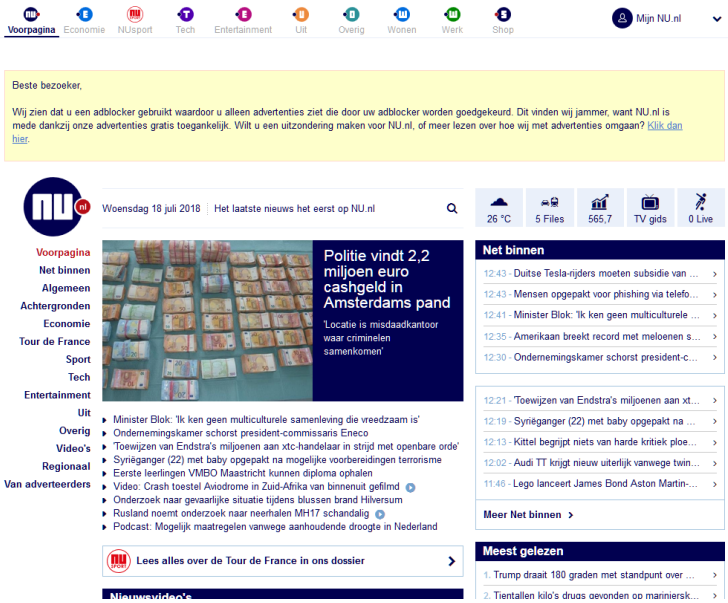
Als een extensie niet werkt in (de versie van) uw browser, kunt u deze ook niet installeren. De optie om hem toe te voegen zal dan inactief blijven.

Extensies die u heeft geïnstalleerd zijn soms zichtbaar met een icoontje in de browser, soms werken ze op de achtergrond.

AdBlock / Adblock Plus

Een webpagina wordt soms overspoeld met reclames. Die leiden ontzettend af van de eigenlijke inhoud van de pagina. Met een adblocker, zoals de hier genoemde extensies, kunt u het overgrote deel van de advertenties blokkeren. Dat geeft meteen een rustiger beeld.

Nu.nl in standaard weergave



Nu.nl met adblocker

Het is wel zo dat websites die gratis diensten aanbieden hiervoor afhankelijk zijn van inkomsten uit advertenties. Door het blokkeren van de advertenties benadeelt u dus een beetje de site. Het is aan ieder voor zich om daar een afweging in te maken.
AdBlock en Adblock Plus zijn twee verschillende producten, hoewel ze elkaar nauwelijks ontlopen. Meer informatie over de verschillen kunt u met een zoekopdracht op internet vinden. Bijvoorbeeld op https://simpler.nl/magazine/adblock-vs-adblock-plus/

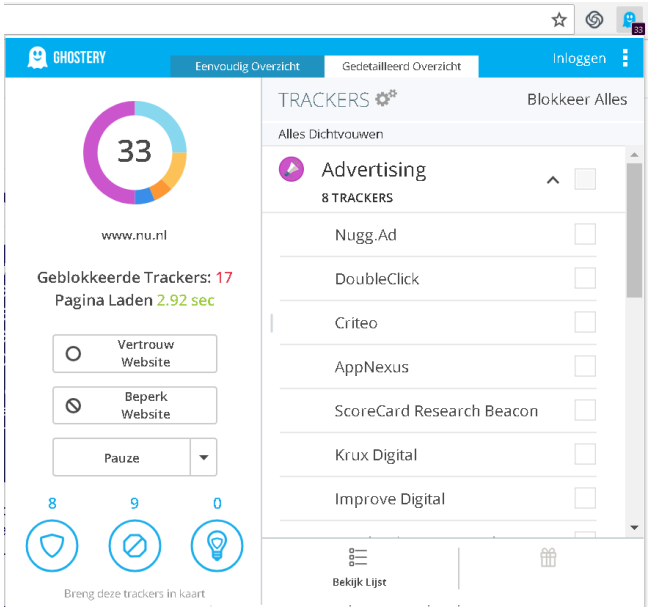
Filmpje adblockers (Consumentenbond):
https://www.youtube.com/watch?v=waXQU52gjPc

HTTPS Everywhere *(https://www.eff.org/https-everywhere)*

Verbindingen met websites zijn veiliger als ze via een versleuteling tot stand worden gebracht. De verbinding loopt dan niet via http maar via https. U ziet dat terug in de url, waar dan ook een slotje te zien is.
De extensie HTTPS Everywhere geeft meer privacy bij het surfen op het internet: indien een website een versleutelde verbinding toestaat, zorgt deze extensie er voor dat die wordt afgedwongen.
Betreffende website moet dan wel in de door HTTPS Everywhere standaardlijst van websites zijn opgenomen (hoewel het ook mogelijk is zelf websites toe te voegen).

Ghostery *(https://www.ghostery.com)*

De extensie Ghostery blokkeert ook advertenties maar doet nog meer. Op veel websites zijn trackers geplaatst (door bijvoorbeeld de maker van de site of adverteerders) die informatie doorsturen over wat u op de site doet, hoe lang u er op verblijft enzovoorts. Ghostery geeft een overzicht van deze trackers, die u vervolgens kunt blokkeren. Rechtsboven in de knoppenbalk van uw browser ziet u het icoontje van Ghostery, met daarin een getal als de extensie iets vindt. Klik op het icoontje voor meer details.



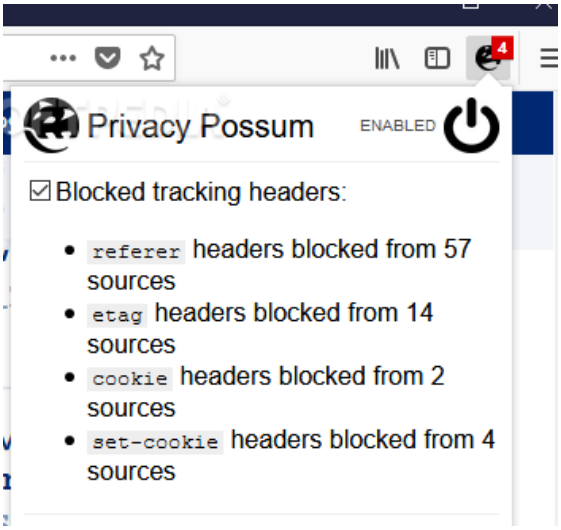
De extensie Privacy Badger *(https://www.eff.org/privacybadger)* biedt soortgelijke functionaliteit en is van dezelfde organisatie als HTTPS Everywhere.

Privacy Possum (*https://github.com/cowlicks/privacypossum*)

Privacy Possum is een voortzetting op Privacy Badger. Deze extensie waakt over uw privacy op een aantal manieren:

- Tracking cookies worden geblokkeerd
- Zogeheten 'referer headers' worden geblokkeerd. Dit is een stukje code waarmee de website die u opvraagt kan zien wat de locatie van de gebruikte computer / browser is.
- Etags worden geblokkeerd. Dit is een tracking methode waarmee gebruikers toch kunnen worden gevolgd als ze in de browser met een privé / incognito sessie werken.
- Fingerprinting wordt geblokkeerd

Na installatie ziet u bovenin de browser het icoontje van Privacy Possum staan. Met een getalletje wordt ook hier aangegeven wat er geblokkeerd wordt op de pagina.

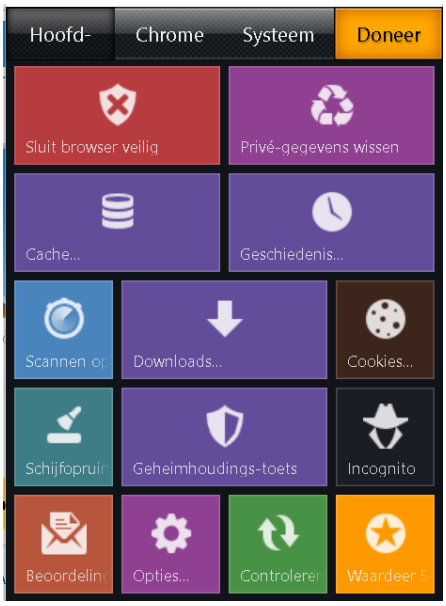


Ook op bekende websites (zoals nu.nl) gaat de teller lopen, bijvoorbeeld door advertenties die erop te vinden zijn.

Er is geen doorklikmogelijkheid om te kijken wat er precies geblokkeerd is.

Click & Clean (*https://www.hotcleaner.com*)

De extensie Click & Clean ruimt alle sporen van uw internetgebruik weg. Uw surf- en downloadgeschiedenis worden verwijderd, opgeslagen wachtwoorden en data voor formulieren worden geschoond, cache en cookies worden geleegd. Bekijk goed de mogelijkheden voordat u een actie onderneemt die meer weggooit dan u zou willen.



Het loont de moeite om via de knop Opties even precies de instellingen na te lopen.

Extensies zoeken en toevoegen

In Chrome
Ga naar https://chrome.google.com/webstore/category/extensions

U kunt de webstore ook vanuit de browser benaderen. Klik rechtsboven in het scherm op de 3 puntjes, kies vervolgens voor 'Meer hulpprogramma's' en dan voor 'Extensies'.
Chrome toont een pagina met geïnstalleerde extensies, met onderaan een link naar de webstore.

Zoek naar een geschikte extensie

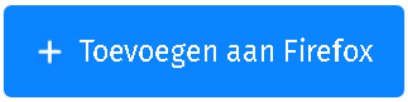
Klik op de blauwe knop 'Toev. aan Chrome'.

In Firefox
Ga naar https://addons.mozilla.org/nl/firefox/

Vanuit de browser: Klik in de menubalk op Extra en vervolgens op Add-ons.
Firefox toont de pagina om extensies te zoeken. Hierop staan enkele suggesties, met onderaan een knop 'Bekijk meer add-ons'.

Zoek naar een geschikte extensie

Klik op de blauwe knop 'Toevoegen aan Firefox'.



In Edge
Ga naar https://www.microsoft.com/nl-nl/store/collections/edgeextensions

Vanuit de browser: Klik rechtsboven op de drie puntjes ... en vervolgens op Extensies.
Klik daarna op de link 'Extensies downloaden vanuit de store'.

Zoek in het venster dat opent naar een geschikte extensie

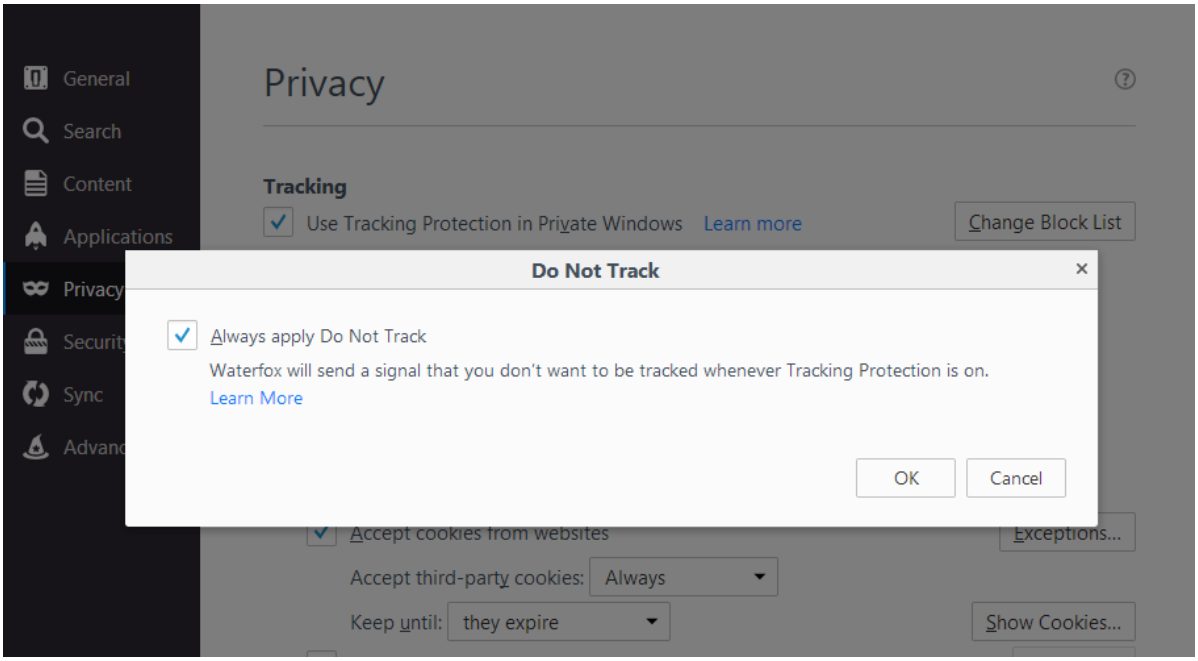
Klik op de blauwe knop 'Kopen'. Deze tekst is wat verwarrend omdat de meeste extensies gratis zijn.

Alternatieve browsers en zoekmachines

Terwijl u over internet surft, wordt er achter de schermen heel wat informatie verzamelt. Websites die u bezoekt laten hun sporen na door middel van de welbekende cookies. Uw browser houdt bij welke websites u bezoekt in de 'geschiedenis' functie. Uw zoekmachine houdt bij waar u naar heeft gezocht.

Waterfox browser

Waterfox is gebaseerd - het zal u wellicht niet verbazen - op Firefox. Beide browsers zien er vrijwel identiek uit en maken achter de schermen dan ook gebruik van dezelfde 'engine'. Waterfox is ooit gemaakt als sneller alternatief voor Firefox, maar Firefox heeft die achterstand middels een grote update (sinds versie 57) ingelopen. Wat zijn dan de verschillen?



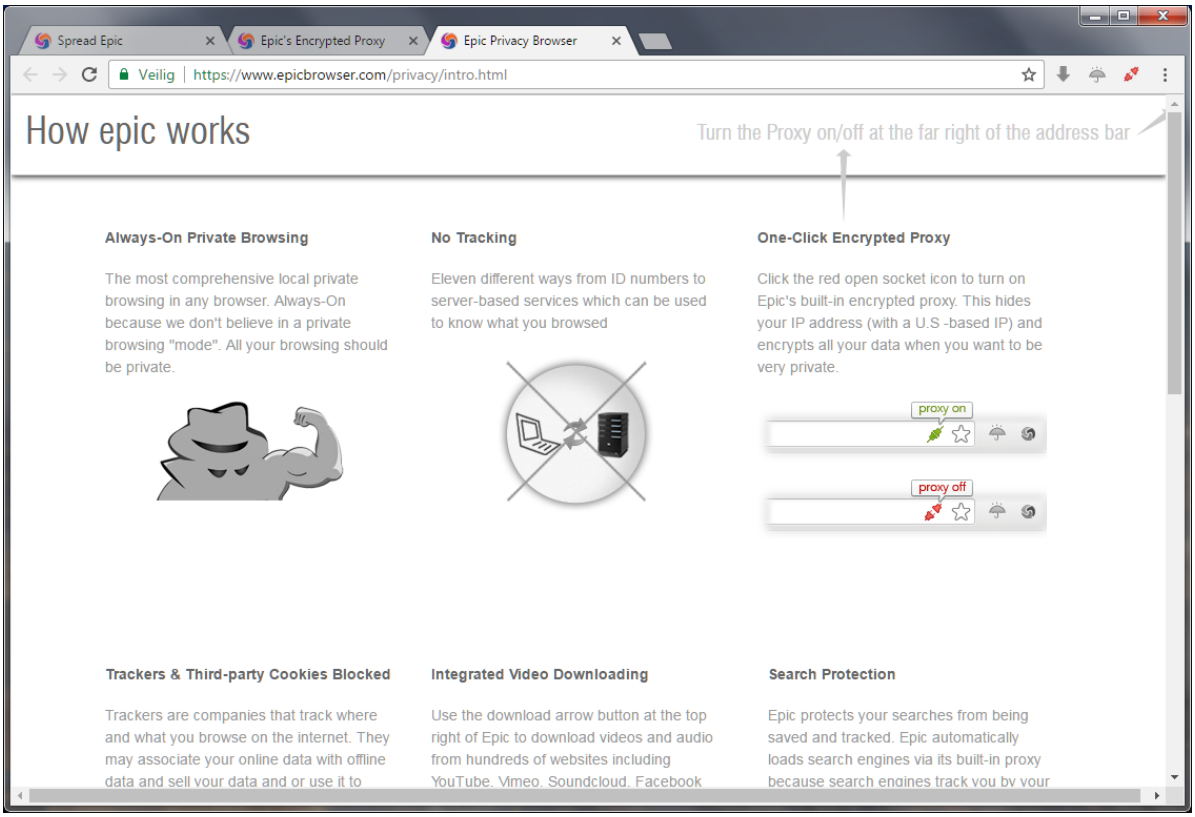
Waterfox profileert zich als veiliger op het gebied van uw privacy, door tracking cookies te blokkeren.
Een andere reden waarom een overstap van Firefox naar Waterfox handig kan zijn, is dat Firefox sinds versie 57 een groot aantal extensies niet meer ondersteund. Met Waterfox zijn deze nog wel gewoon te gebruiken.

Epic browser (www.epicbrowser.com)

De Epic browser is gebaseerd op Chromium, het open source (dat wil zeggen dat ontwikkelaars zelf aanpassingen kunnen doen) project van Google. Google zelf heeft de Chrome browser ook daarop gebaseerd.
Epic wist standaard na elk gebruik de zoekgeschiedenis en cookies en verstuurt zoekopdrachten via hun eigen servers (dus niet die van Google), waardoor het nauwelijks te achterhalen is vanaf welke computer de zoekopdracht is gedaan. Advertenties en trackers worden standaard geblokkeerd.

Wie nog meer privacy wil, kan gebruik maken van de proxy knop, waarbij het internetverkeer nog meer wordt omgeleid. Hierdoor wordt het surfen wel wat trager.

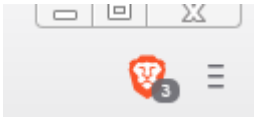
Omwille van de veiligheid en privacy is het bij deze browser standaard niet mogelijk om extensies toe te voegen. Die optie is wel in te schakelen.



Brave browser

Een browser die privacy hoog in het vaandel zet, is Brave. Brave blokkeert cookies, advertenties en heeft een ingebouwde tracking-bescherming, waardoor u niet digitaal gevolgd kunt worden. Daardoor is de browser behoorlijk snel, wat voor het surfen weer een voordeel is. Brave blokkeert ook 'fingerprinting'.

Als u met Brave een website bezoekt, ziet u rechtsboven in het scherm een schildje met een getal staan. Door hierop te klikken opent een venster waarin u kunt zien wat er allemaal voor betreffende website geblokkeerd is.

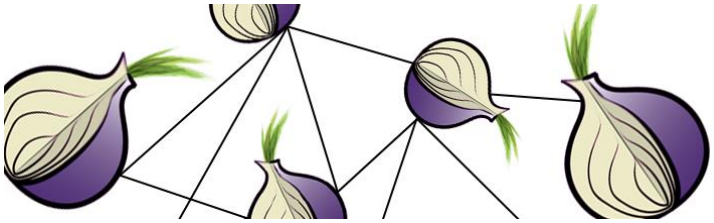


Door op het schildje te klikken, krijgt u meer informatie en kunt u de instellingen aanpassen.

Tor browser

Als we het over browsers en privacy hebben, moeten we ook het Tor project noemen. Deze browser (of eigenlijk moeten we zeggen: het hele achterliggende netwerk) biedt een grote mate van privacy en anonimiteit. Daardoor wordt Tor veel gebruikt door mensen die écht niet gevonden willen worden. Denk dan bijvoorbeeld aan journalisten in landen waar geen persvrijheid is. Maar ook aan zaken die het daglicht niet kunnen verdragen, het zogeheten 'dark web'.

U kunt de Tor browser gewoon downloaden, installeren en gebruiken zoals elke andere browser, zonder dat daar speciale truukjes voor nodig zijn.
Het Tor-netwerk vermomt uw identiteit door het omleiden het internetverkeer via verschillende Tor-servers. Dat internetverkeer is versleuteld en kan daarom niet worden herleid. Men ziet alleen verkeer afkomstig van willekeurige knooppunten op het Tor-netwerk, in plaats van uw computer.
Door al die omleidingen achter de schermen merkt u wel dat de Tor browser langzamer is dan u van andere browsers gewend bent. U kunt er wel vanuit gaan dat u voor adverteerders, trackers e.d. niet of nauwelijks te achterhalen bent.



Overigens bestaat 100% anonimiteit niet. De FBI heeft al meerdere mensen opgepakt die dachten, door het gebruik van Tor, hun duistere praktijken onvindbaar te maken.
Tor wordt veel geassocieerd met mensen 'die wel iets te verbergen zullen hebben'. Voor privacy is het beter gewoon een VPN te gebruiken.

Alternatieve zoekmachines

Wie iets op internet zoekt, doet dat meestal met Google. 'Googelen' is niet voor niets al een werkwoord geworden. Met ongeveer 6 miljard zoekopdrachten per dag is Google de zoekgigant. Andere zoekmachines als Bing, de zoekmachine van Microsoft, of het aloude Yahoo blijven ver achter, zoals onderstaand overzicht (1e kwartaal 2019) laat zien.

Nederland	Desktop	Smartphone	Tablet
Google	92,37%	98,41%	97,27%
Bing	4,63%	0,41%	0,48%
Yahoo!	1,12%	0,48%	0,54%

Even technisch: zoekresultaten komen tot stand door algoritmes waar de zoekmachines mee werken. Zoekmachines die data bijhouden over de zoekopdrachten die u doet, gebruiken die gegevens om resultaten te tonen die het best bij u passen. Maar wellicht is er nog veel meer over een onderwerp te vinden, dat niet zo snel aan u wordt getoond. Of misschien vindt u het sowieso niet prettig dat uw zoekresultaten in een profiel worden vastgelegd.

DuckDuckGo en Startpage

DuckDuckGo en Startpage zijn 2 zoekmachines die geen informatie van websites opslaan, zodat er geen cookies geïnstalleerd worden. Zoekopdrachten worden ook niet opgeslagen, dus er wordt geen profiel opgebouwd.
Zoals Startpage in hun verklaring stelt:

Privacy!

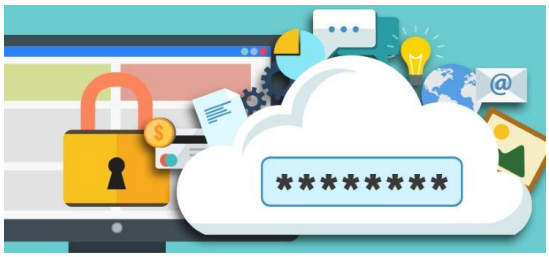
De Privacy Verklaring van StartPage geldt als één van de beste in de industrie:

- ✓ IP adressen van haar gebruikers worden niet opgeslagen.
- ✓ Identificerende cookies worden niet gebruikt.
- ✓ Persoonlijke gegevens worden niet verzameld.
- ✓ Geen uitwisseling van persoonlijke gegevens met derden-partijen.
- ✓ Biedt een beveiligde, versleutelde verbinding (HTTPS/SSL).
- ✓ En bovendien een gratis proxy service die anoniem bezoeken van websites mogelijk maakt.

In Waterfox zitten deze 2 zoekmachines al toegevoegd aan de lijst met zoekmachines die u als standaard kunt instellen. Maar natuurlijk kunt u ze bij andere browsers als standaard toevoegen.

Wachtwoordmanagers

U heeft ongetwijfeld een aantal online accounts. Elke account heeft een wachtwoord. Veiligste is als u voor elk account een apart wachtwoord heeft. Mocht er dan een account onverhoopt gehackt worden, dan kan er niet met hetzelfde wachtwoord bij andere accounts worden ingelogd. Bij voorkeur kiest u voor niet al te voor de hand liggende wachtwoorden.



Hoe meer accounts en hoe meer wachtwoorden u heeft, hoe moeilijker het wordt om alle wachtwoorden te onthouden. In een wachtwoordmanager kunt u alle wachtwoorden die u gebruikt opslaan. Bezoekt u dan een site waar u dit wachtwoord nodig heeft dan vult de wachtwoordmanager deze voor u in. Uw wachtwoordmanager is natuurlijk ook met een wachtwoord beveiligd. Dat is dan in principe het enige wachtwoord dat u nog hoeft te onthouden.

Hoe werkt het?

Een wachtwoordmanager maakt een digitale kluis aan, waarin uw wachtwoorden worden opgeslagen. Wanneer u een wachtwoordmanager voor het eerst gebruikt, wordt de kluis aangemaakt en moet u uw hoofdwachtwoord voor de kluis opgeven. Daarna kunt u wachtwoorden van uw accounts toevoegen. U kunt dat ook stapsgewijs doen, de eerstvolgende keer als u een account gebruikt. Wachtwoordmanagers kunnen uw wachtwoorden ook analyseren en verbeteren.

Lastpass en Dashlane

Lastpass en Dashlane zijn twee voorbeelden van wachtwoordmanagers die goed bekend staan. Behalve het hoofdwachtwoord kunt u ook nog kiezen voor tweestapsverificatie.

LastPass •••| dashlane

Van beiden zijn gratis en betaalde versies verkrijgbaar.
https://www.lastpass.com/nl https://www.dashlane.com/nl

Risico's

De meeste wachtwoordmanagers bewaren hun kluis in de 'cloud', en niet op uw apparaat (pc, tablet, telefoon). Dat heeft als voordeel dat u op elk apparaat/browser waarop u uw wachtwoordmanager installeert de beschikking heeft over uw opgeslagen wachtwoorden. Aan de andere kant, mocht ooit een hacker erin slagen de (zware) beveiliging van de wachtwoordmanager servers te kraken, dan heeft die in theorie toegang tot alle accounts. Een groter risico is misschien dat u zelf uw hoofdwachtwoord vergeet. Een aantal wachtwoordmanagers hebben de mogelijkheid tot noodtoegang, waarbij een ander (bijvoorbeeld een familielid) onder bepaalde voorwaarden toegang krijgt tot uw kluis. De betaalde versies van LastPass en Dashlane hebben die functie, de gratis versie van Dashlane ook. Meer informatie hierover is te lezen op hun websites.