Spoorloos op internet?

Zonder sporen achter te laten en anoniem op internet, kan dat?

Kees van der Vlies

Internet behoort inmiddels tot de basisbehoeften van de moderne mens. Dit houdt ook in dat de mensen zich meer en meer zorgen (zouden moeten) gaan maken over: kwetsbaarheid van (steeds complexere) systemen en toepassingen, hacks, DDoS-aanvallen, privacy, identiteitsfraude, spam, oplichting, chantage, hoaxen, phishing, nepnieuws, (on)betrouwbaarheid van sites, virussen, big data, censuur, trojaanse paarden, phishing, dark web, ingewikkelde toegangsprocedures (DigiD, ING, andere internetbanken) en wat er verder nog meer aan onheil en ongemak op de gebruiker afkomt. Je zou er mismoedig of paranoïde van kunnen worden. En het erge is: het gevoel van machteloosheid neemt daarbij ook toe.

Oplossingen zijn al even verstrekkend als de bovenvermelde bedreigingen. Veel van de mogelijke beschermings- en beveiligingsmaatregelen gaan de modale internetgebruiker boven de pet.

Wat kunnen wij dan doen?

Een korte opsomming:

1. wees altijd op uw hoede, dus argwanend, doe geen ondoordachte dingen.
2. gebruik op de computer een firewall (vaak standaard al aanwezig) en een antivirusprogramma.
3. wees nóg voorzichtiger op plaatsen met ‘openbaar’ internet; bekabelde verbindingen zijn veiliger dan wifi.
4. gebruik sterke wachtwoorden en verander die periodiek.
5. gebruik VPN (Virtual Private Network).
6. reageer nooit op berichten van onbekende of onduidelijke afzenders, ook niet om iets ‘af te zeggen’ of u te laten ‘uitschrijven’.
7. wis of accepteer cookies met mate; wis ook de browsegeschiedenis (meestal met Ctrl+H op te roepen; let op: de zoekgeschiedenis wordt daarbij niet altijd ook gewist).
8. bij ‘verplichte registratie’ met e-mail of (gevaarlijker nog) met Facebook of Google, kunt u een fake-account opgeven dat u zelf daartoe hebt aangemaakt.
9. of een tijdelijk e-mailadres aanmaken; daarvoor zijn verschillende sites (zie lijstje).
10. Google, Bing, Yahoo (nu onderdeel van het Oath-concern, maar zoekfunctie: ‘powered by Bing’) en veel andere zoekmachines analyseren uw zoekopdrachten om er ‘bijpassende’ reclame aan toe te voegen, er zijn ook zoekmachines die dit niet doen: DuckDuckGo, StartPage, Qwant (van oorsprong Frans) en enkele andere.

11. beperk het gebruik of zie af van sociale media en YouTube.
12. een browser met encryptie- of anonimiteitsfunctie gebruiken, ‘HTTPS Everywhere’.

Over deze laatste gaat dit artikel.

Anoniem browsen

Sommige browsers hebben een functie waarmee u minder ‘zichtbaar’ bent op internet. Soms zit die functie verscholen of soms moet u er een plug-in of add-on voor binnenhalen. Alle belangrijke browsers hebben een functie die een grotere mate van privacybescherming zou bieden. Vaak is dat niet veel meer dan: cookies, browsegeschiedenis en tijdelijke internetbestanden wissen bij het sluiten van de browser, zoals u dat ook handmatig kunt doen. Of dat veel bedreigingen 'van buiten’ verhindert, is te betwijfelen. Wat het wél doet is: voorkomen dat iemand die na u de pc gebruikt, kan zien welke sites u bezocht hebt. Alle cookies altijd wissen is wel een erg radicale methode, die u ook hinder en ongemak kan opleveren. U moet de privéfunctie (incognito, privé, privacy of InPrivate) in de browser altijd zelf opzoeken en activeren. Of de zoek- en downloadgeschiedenis ook gewist wordt bij het sluiten van de browser, dient u zelf te achterhalen.
In dit artikel de mogelijkheden van verschillende browsers, en ook TOR en VPN komen aan de orde.

Google Chrome

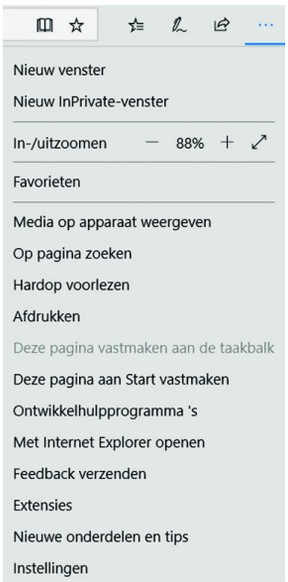
Rechtboven op de drie stippen klikken en kiezen (Ctrl+Shift+N) en een *Nieuw incognito-venster* opent zich. Daaronder ziet u trouwens ook de handmatige methode om de Geschiedenis te bekijken en te wissen.

Do not track
Bijna alle moderne browsers hebben de mogelijkheid ‘Do not track’ in te schakelen, of ‘Bescherming tegen volgen’ zoals Firefox het noemt. Vivaldi heeft het over ‘Niet traceren’. SeaMonkey over ‘Volgactiviteiten’. Brave over: ‘Volg mij niet’. Lees, waar mogelijk, de uitleg door op de desbetreffende link te klikken.

De geschiedenis van de sites die u bezoekt en de links die u daarvoor gebruikt, schijnen waardevol te zijn. Althans voor commerciële doeleinden van bedrijven, meestal niet voor uzelf. Kijk of u de mogelijkheid krijgt de volgbescherming per site of onderdeel uit te schakelen. Zie bv. Firefox.
Hecht overigens niet te veel waarde aan deze ‘beveiliging’. Het zijn de andere partijen in het grote internetcarroussel die uw verzoek al dan niet (geheel) honoreren.
Over ad-blockers, die verschillende browsers tegenwoordig ook als extra functie aanbieden, is het laatste woord nog niet gesproken. Adverteerders en websitebeheerders zijn er niet gelukkig mee en er zijn al technieken ontwikkeld om ad-blockers te omzeilen, die dan weer tegen-technieken oproepen. En zo is het een soort kat- en muisspel geworden. Zie ook onder ***Meer dan IP-adres***. Het moge duidelijk zijn dat het om grote (financiële) belangen gaat.

Apple heeft het in de browser Safari voor adverteerders veel moeilijker gemaakt gebruikers te volgen. Ook andere browserontwikkelaars zitten klem tussen (advertentie)inkomsten en privacy.
En daarnaast gaan er waarschuwingen rond dat zelfs https niet meer volledig garandeert dat de gebruiker met een authentieke (dus niet vervalste) website communiceert. Deze zaken vallen buiten het kader van dit artikel.

Microsoft Edge



Als u InPrivate-tabbladen of vensters gebruikt, worden uw browsegegevens (zoals geschiedenis, tijdelijke internetbestanden en cookies) niet op uw pc opgeslagen bij het sluiten van Edge.
Selecteer in Microsoft Edge het pictogram *Meer*, de drie stippen in de rechterbovenhoek (of Alt X) en kies vervolgens *Nieuw InPrivate-venster*.

Edge direct in de InPrivate-functie starten kan ook.
Als u Edge in de taakbalk (meestal onderaan het Bureaublad-scherm) hebt opgenomen, kunt u door rechtsklikken op het e-pictogram een keuzelijstje zien, waarin *Nieuw InPrivate-venster* gekozen kan worden.

Defender en de grote spelers

De real-time browse-bescherming in Windows (Defender) werkt goed, maar alleen doordat de sites bij gebruikersbezoeken ‘gescreend’ worden door... inderdaad: Microsoft. Als u dus bij het browsen stuit op zo’n gesignaleerde website (bv. met phishing), heeft Microsoft uw verzoek (en IP-adres en alle andere gegevens die al eerder verzameld waren) eerst bekeken en gefilterd.
Dat geldt ook voor sommige andere browser-beveiligers, die vaak verbonden zijn aan antivirusprogramma’s.

Het is algemeen bekend dat veel persoonlijke gegevens, zoals van sociale media, gedeeld en te gelde gemaakt worden. Vergemakkelijkt doordat verschillende services onder één concern vallen van Microsoft, Google of Facebook.

Of doordat juist bepaalde taken uitbesteed worden aan speciale bedrijven, zoals het in opspraak geraakte en op 1 mei 2018 failliet verklaarde Cambridge Analytica. De relatie met Facebook had beide partijen uiteindelijk geen goed gedaan. Inmiddels lijkt Cambridge Analytica onder een nieuwe naam (Emerdata) vrolijk verder te gaan.

De informatie dient dan niet alleen Het Goede Doel (beveiliging), maar kan op allerlei manieren (commercieel, politiek, staatsveiligheid, wetenschappelijk) ingezet worden.
‘Big data, you know.’

Naast phishing krijgen nepnieuws en haat- of discriminerende berichten de laatste tijd meer aandacht. Voorheen waren het vooral ‘aanstootgevende’ teksten en afbeeldingen die, soms tot het ridicule toe, geweerd werden, of ging het juist om een lakse houding bij wraakvideo’s e.d.

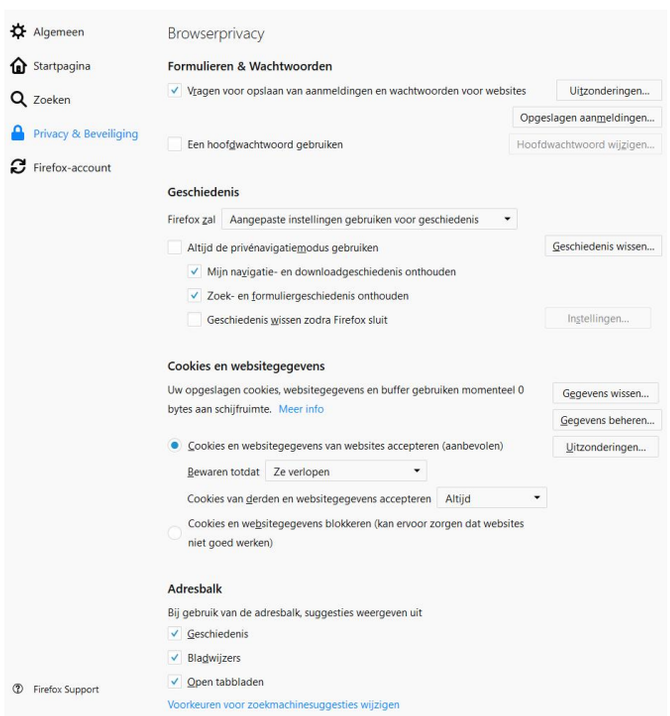
Mozilla Firefox

Hier zijn het de drie lijntjes rechtsboven (ook wel de 'hamburger' genoemd) die u moet aanklikken en in het menuutje vervolgens op *Nieuw privévenster* klikken. Of direct in de open browser Ctrl+Shift+P intoetsen.

Het uiterlijk en de bediening van Firefox kunnen onder Android een beetje anders zijn. Firefox verschaft ook meer informatie en keurig in het Nederlands! Voor Firefox en Chrome bestaan ook VPN-extensies of add-ons, die apart opgehaald en geïnstalleerd moeten worden. Meer over VPN bij Opera.

Onder *Voorkeuren* (Preferences) zijn veel zaken in te stellen, ook op het gebied van *Privacy en beveiliging*. *Bescherming tegen volgen* is iets uitgebreider dan bij andere browsers.

Scroll daartoe naar beneden op de Browserprivacy-pagina.

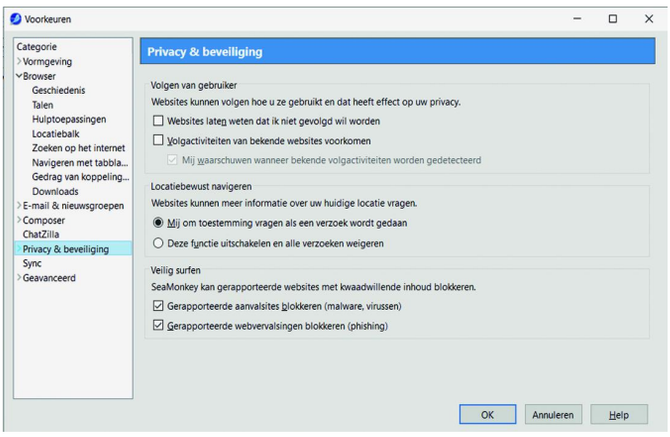


SeaMonkey

De privacy- en beveiligingsmaatregelen in SeaMonkey vindt u onder *Bewerken* > *Voorkeuren...* > *Privacy & beveiliging*. Zie ook de andere Voorkeuren en hun mogelijkheden.
Een nieuwe privévenster openen kan met Ctrl+Shift+B, of via *Bestand* > *Nieuw* > *Privévenster*. Zoals al uitgelegd: dan wordt geen geschiedenis bewaard.

Bij SeaMonkey kunt u andere gebruikersprofielen aanmaken, waarin u andere voorkeuren, bladwijzers, opgeslagen berichten e.d. kunt opslaan dan in het standaardprofiel.

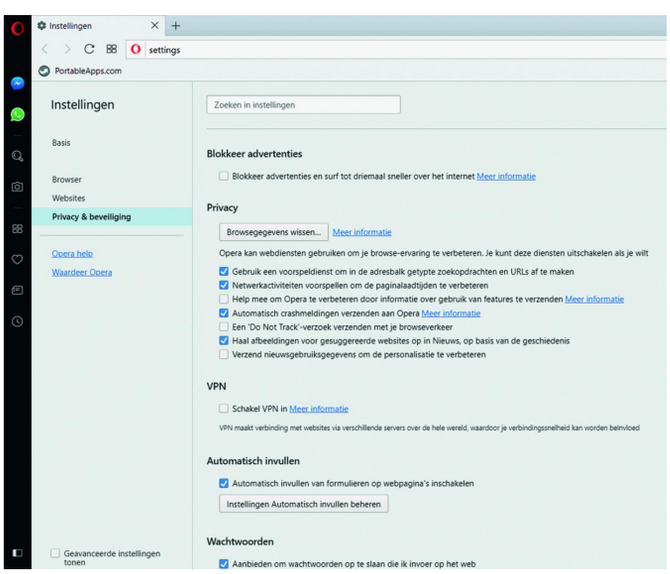
Dit kun je nauwelijks een veiligheidsmaatregel noemen, maar kan wel handig zijn bij meerdere gebruikers van de browser of als je de browser in een andere ‘hoedanigheid’



wilt gebruiken. Let wel: het IP-adres blijft gelijk en de trackingmogelijkheden worden niet automatisch anders.

Opera

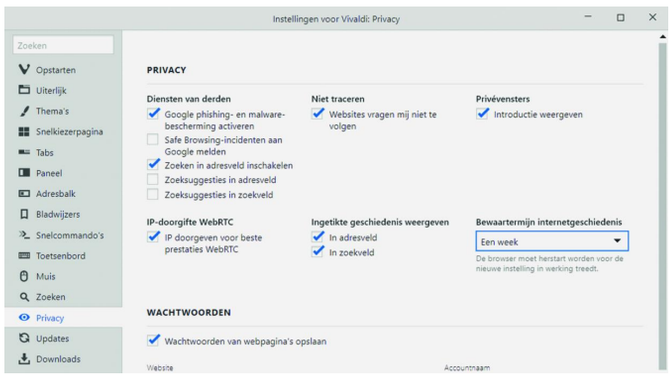
Een te weinig gewaardeerde browser, die zich kan meten met de groten. Het bedrijf Opera bestaat al meer dan twintig jaar en heeft flink wat innovaties op zijn naam staan. Opera-technologie is o.a. toegepast door Adobe en Nintendo. In de browser: Klik op de rode O (van Opera) in de linkerbovenhoek. Kies uit het menu: *Instellingen* (Alt+P) en vervolgens *Privacy & beveiliging*. Bestudeer de mogelijkheden en scroll (daartoe) door naar beneden.



Merk op dat Opera ook (sinds ruim twee jaar; nadat SurfEasy overgenomen werd) de functie *VPN inschakele*n heeft. Klik aldaar ook op *Meer informatie*. Op de website waarnaar deze link doorschakelt, staat een prima uitleg (in het Engels) over VPN en de andere beveiligings- en privacyvoorzieningen zoals 'Ad-blocker', 'Private browsing', 'Cookies' en 'Security badges'. VPN in Opera gebruiken is vrijwel onmerkbaar: alleen in de adresbalk verschijnt links een groen blokje met VPN, zoals ook https met een slotje wordt aangeduid.

Vivaldi

De nog jonge browser Vivaldi heeft standaard, linksbeneden in de zijbalk, het instellingenpictogram staan. U kent het wel: het tandwieltje. Daarop klikken geeft u toegang tot veel instellingen, waaronder *Privacy*. Daar ziet u dan dit: Dus veel mogelijkheden, ook bijv. het beheer van wachtwoorden voor sites, de bewaartermijn van de geschiedenis en de talrijke vormgevingsfuncties van de browser.
Scroll bij de *Instellingen* ook door naar beneden.



Vivaldi, ontworpen door ex-Opera-ontwikkelaars, kan tot de beste browsers gerekend worden.

VPN is niet altijd VPN

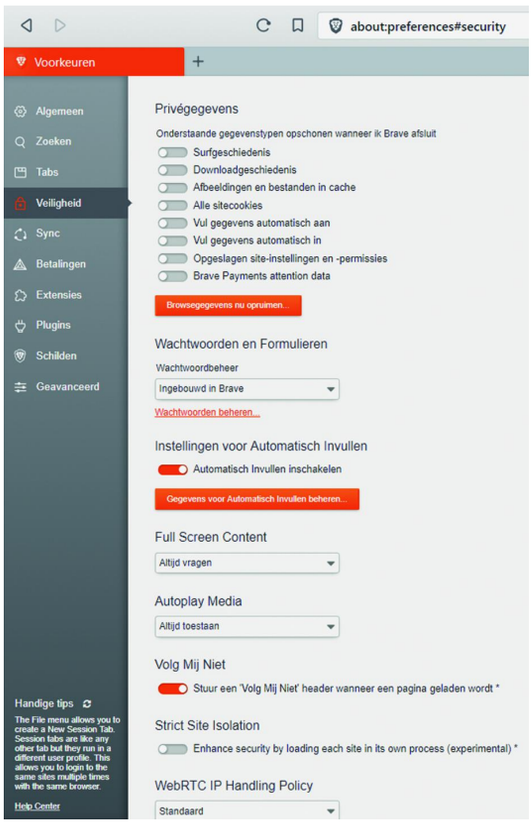
Het beginsel van versleuteling van het internetverkeer wordt o.a. bij VPN-technologie toegepast. Belangrijk is natuurlijk dat de ver- en ontsleuteling al aan het begin van de verbinding (dus op de pc of smartphone) plaatsvindt; dat is wat VPN doet: tunneling: de T in de protocolnamen van PPTP (en L2TP). Er zijn nog een paar andere VPN (de)coderingsprotocollen (IPSec, SSL VPN) die nog verder gaan of die vooral voor mobiel gebruik bestemd zijn.
Tegen de VPN-veiligheid die Opera biedt, zijn bedenkingen geuit; het zou om nauwelijks meer gaan dan een 'proxy', dus een serverfunctie tussen de gebruiker en internet in, al wordt er wel een versleutelingslaag overheen gelegd. (Alle VPN-add-ons voor browsers zijn overigens proxyfuncties!). Maar elke vorm van beveiliging is een verbetering t.o.v. niks doen.

Het is niet duidelijk óf, hoelang en wélke logbestanden van de VPN-gebruiker op de Opera-servers bewaard worden; om over uitwisseling daarvan nog maar niet te spreken. Er klinkt af en toe een 'lasterlijk' bericht dat Opera, van oorsprong Noors, maar sinds 2016 in handen van een Chinees consortium, gewantrouwd zou moeten worden.

Opera heeft de VPN-service (app) voor iOS en Android begin dit jaar gestaakt. De Aloha-browser (voor iOS en Android) zou die leemte kunnen opvullen:
https://alohabrowser.com/ (gevestigd op Cyprus?)
In alle browsers kunt u gebruikmaken van de vele gratis en betaalde VPN-aanbieders. Daar heeft CompuLinks in het verleden (2016-3 en 2017-3, met ook een recensie van Opera) al aandacht aan besteed. Kijk ook op de volgende sites:
https://vpndiensten.nl/
https://www.want.nl/waarom-vpn-gebruiken/
https://nl.wikipedia.org/wiki/Virtueel_Particulier_Netwerk https://www.strato.nl/server/wat-is-vpn-virtual-private-network/

Brave

De jongste browser, Brave (2016), heeft natuurlijk veel geleerd van bestaande browsers (is op Chromium gebaseerd) en heeft tal van functies overgenomen en uitgebreid. Klik op de drie streepjes rechtsboven in de balk en dan op *Instellingen* (Ctrl+,). U krijgt dan de tab Voorkeuren (?). Klik daar op *Veiligheid*; dan krijgt u de mogelijkheden: bij browser afsluiten Surf-/browse-geschiedenis, Downloadgeschiedenis, cache, cookies opschonen bij afsluiten, Wachtwoordbeheer, Volg mij niet, e.a. Kijk ook nog even naar wat de andere items onder 'Voorkeuren' u te bieden hebben.



Bovendien kunt u meteen Tor inschakelen (Ctrl+Alt+N), zodat uw IP-adres niet achterhaald kan worden op de sites die u bezoekt. Zie de kadertekst over Tor. Een prima toevoeging, net zoals VPN bij Opera. Brave is gebouwd op 'open software-bronnen' en voor iedereen 'transparant', als je tenminste weet hoe je software moet ontleden. Interessant aan Brave is dat ze ad-blockers combineren met 'n advertentiebetaaldienst. Iedereen weet dat 'gratis' op internet betekent dat er altijd ergens een geldstroom richting website-exploitanten gaat.

De internetgebruikers zijn niet de doelgroep van websites, maar het product waar geld aan verdiend wordt door advertenties en soms andere gegevens. Daarom moeten we als gebruikers ons niet in slaap laten wiegen door de schijnbare vrijheid van gratis internet.

Brave heeft hier het volgende op gevonden: de browsergebruiker kan kiezen voor 'geen (of alleen bepaalde) advertenties ('Brave advertenties' genoemd ;-) en 'trackers', maar toch het verdienmodel van website-beheerdeers niet in de war schoppen. De gebruiker kan opgeven naar welke adverteerders 'zijn bijdrage' mag gaan, alleen 'zijn naam' (lees: IP-adres) komt er niet bij te staan, dus trackers krijgen die nooit. Brave zelf (contactadres in San Francisco) handelt de geldstroom af. Het is net als de anonimiteit van de uitgebrachte stemmen bij Nederlandse verkiezingen. Er wordt nagegaan wie er gestemd heeft, maar niet op welke partij of kandidaat hij of zij gestemd heeft: het stemgeheim. Wel wordt de uitslag na telling zorgvuldig vastgesteld. Zo wordt bezoek aan een gesponsorde site (anoniem) geregistreerd en gehonoreerd.
Over het concept en de browser zijn gemengde oordelen verschenen. Ik werk er al enige tijd probleemloos mee.

Werken met tijdelijk e-mailadres

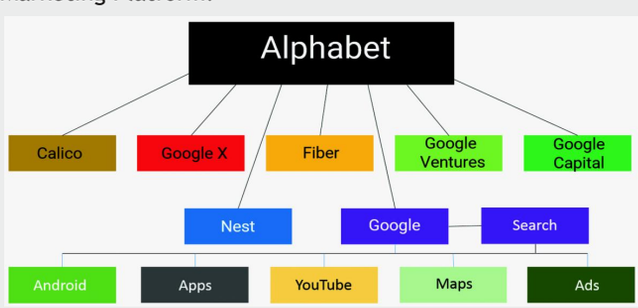
Hoe vaak wordt u niet gevraagd uw e-mailadres op te geven? Wie een beetje actief is op internet en op onderzoek uitgaat, komt ze al gauw tegen: sites waarvoor u zich moet aanmelden of laten registreren. Dat is o-zo-gemakkelijk en vlot. Maar wat er met uw persoonlijke gegevens gebeurt, is nooit duidelijk.

En u weet - even een zijstapje - dat internet een bijzonder goed geheugen heeft. Teksten, foto's, video's, muziek, die (met uw naam erbij) op internet gezet zijn, blijven daar 'eeuwig' staan. En het kost veel (niet zelden vergeefse) moeite om die gegevens van internet te laten verwijderen. Maar overal waar die gegevens inmiddels gedowload, gekopieerd of verspreid zijn, blijven ze een niet te achterhalen eigen leven leiden. Daar hebben de zoekmachines meestal geen vat op. Dus maak een tijdelijk e-mailadres aan, bv. via een van de volgende sites:
https://en.getairmail.com
https://www.tempmailaddress.com
https://www.guerrillamail.com
https://temp-mail.org/nl/
https://www.mailinator.com
https://temp-mail.org
https://www.emailondeck.com
http://www.fakemailgenerator.com/#/
https://10minutemail.com/10MinuteMail/
https://getnada.com
https://mailto.space
https://tempail.com
https://www.throwawaymail.com

Lees voor een beoordeling:
https://www.lifewire.com/best-disposable-email-address-services-1171097

Meer dan IP-adres

Adverteerders zijn overigens al enige tijd bezig andere gebruikerskenmerken te inventariseren en voor hun doelen te gebruiken. Als opslaan en gebruiken van IP-adressen en 'gewone' cookies niet meer (helemaal) lukt, worden er meer 'forensische' gegevens verzameld en geanaliseeerd, zoals: welke browser wordt gebruikt, welke hardware, welke lettertypen, welke schermresolutie, welke tijdzone, patroon van inlogtijden, opgeslagen historische en sociale media-data en nog veel meer gegevens die bij elkaar een profilering of 'vingerafdruk' kunnen opleveren en dus tot gerichtere advertenties leiden. De grote speler op het gebied van internetgebruikersanalyse, DoubleClick, is al tien jaar in handen van (Alphabet/)Google, dat met de grootste zoekmachine, met YouTube, met de browser Chrome en met het besturingssysteem Android al vele netten heeft uithangen. Double Click is sinds kort werkzaam onder de naam Google Marketing Platform.



U weet dat adverteerders het nagaan van het gebruikersgedrag vooral in uw belang wensen uit te leggen. Er wordt gesproken over 'verbeterde gebruikservaring', 'afgestemd op uw interesses', 'optimale personalisering', 'snelheid', 'het belang van uw privacy' (ja, ja!).
En naarmate de commerciële belangen met meer hindernissen geconfronteerd worden, komen er waarschuwingen: internet kan niet langer 'gratis' diensten aanbieden, internet moet toch voor iedereen toegankelijk blijven, wij houden ons aan de regels, maar er zullen door criminelen nog meer illegale praktijken gebruikt worden, er zijn toch al afspraken gemaakt, er is al toezicht, de Europese privacy-regels (GDPR, in Nederland de AVG) zijn te streng, dit belemmert de ontwikkeling van de techniek, wereldwijde vrije informatie-uitwisseling komt in het gedrang.
Vooral in de VS zoekt men naarstig naar nieuwe 'slimme' technologieën (en argumenten) om prospectgegevens uit het internetverkeer te peuren en obstakels te omzeilen.

Tips

Vergelijk ze goed, ze hebben allerlei services te bieden:

- keuze van de levensduur van het tijdelijke adres (meestal 10 tot 60 minuten, maar dagen lang kan ook)
- het adres kan soms ook (een beperkte tijd) als verzendadres van e-mail gebruikt worden
- ze werken met of zonder wachtwoord te gebruiken
- de keuze uit verschillende (tijdelijke) e-mailadressen die u kunt gebruiken
- de meeste zijn in het Engels, soms kunt u een andere taal kiezen; het Nederlands kan dan belachelijk slecht zijn.

Een enkele blijkt een reclame-generator. Anderen lijken qua lay-out en tekst zó op elkaar dat ze van dezelfde eigenaar moeten zijn.

Tor

Over Tor (oorspronkelijk The Onion Router) zijn honderden artikelen geschreven. Op internet kunt u daarover alles vinden. Het gaat er bij Tor om uw IP-adres, dat informatie bevat over u, uw provider en land, te 'vermommen'. Als u Tor inschakelt, wordt het internetverkeer van uw pc via een netwerk van duizenden servers (over de hele wereld) afgehandeld, die allemaal onder andere IP-adressen werken. Bovendien wordt er voortdurend geschakeld tussen die servers, zodat de route steeds verandert.

Daardoor kan de communicatie met websites iets trager verlopen, maar daar staat anonimiteit tegenover. Meer informatie:
https://nl.wikipedia.org/wiki/Tor_(netwerk)
https://www.torproject.org/ (aldaar is ook Tor als aparte browser te downloaden) en
https://www.vpngids.nl/privacy/anoniem-browsen/hoe-installeer-tor/

Tor is er voor Windows, MacOS, Linux en in 32 bits- en 64 bits-versies, ook in het Nederlands. Hoever men is voor smartphones blijft onduidelijk, Android staat wel op lijst. De basis van de Tor-browser is Firefox en kan daarom ook als een 'gewone' browser gebruikt en aangepast worden. Het moge duidelijk zijn dat Tor geen browse-of zoekgeschiedenis opslaat.

De Windows-versie van de Tor-browser kan op een USB-geheugenstick gezet worden, zodat u deze (als portable app) 'overal' kunt gebruiken, zonder installatie en zonder sporen achter te laten op de gastcomputer.

Er valt nog veel meer over te zeggen: Tor ligt niet goed bij totalitaire regimes, bij geheime diensten (al maken die er zelf gebruik van), bij misdaadbestrijders (criminelen gebruiken het en het dark web werkt met deze technologie). Maar ook mensenrechten- en persvrijheidsorganisaties, WikiLeaks, klokkenluiders en mensen die veel in crypto-currency (Bitcoin e.d.) doen, gebruiken Tor.
De browser Brave heeft Tor al 'ingebouwd'.

Er is een speciaal ontworpen (Debian Linux) besturingssysteem, TAILS, dat met de Tor-browser werkt. Tails kan op een DVD of USB-geheugenstickje geïnstalleerd worden, waarna u de computer vanaf die DVD of dat stickje moet booten. U werkt vanaf dat moment niet onder Windows, maar onder Linux. Op de computer blijven na het sluiten van Tails geen sporen achter van de activiteiten en het internetgebruik onder Tails. De hard disk wordt door Tails helemaal niet aangesproken, al is die voor de gebruiker nog wel toegankelijk. De laatste jaren wordt Tails alleen nog in een 64-bits-versie uitgebracht. Het is een volwaardig besturingssysteem, dus er kunnen ook de gebruikelijke taken in worden uitgevoerd.