7 privacytools die je moet hebben

Nu alles en iedereen met elkaar verbonden is, is privacy belangrijker dan ooit. Met deze tools zorg je voor een nodige privacy boost.

Op regelmatige basis hoor je zorgwekkende nieuwsberichten of ervaringen. Of het nu om een gigantisch privacy schandaal gaat bij een groot sociaal netwerk of je buurman zijn computer die gehackt werd waardoor hij al zijn bestanden kwijt is, het is duidelijk dat privacy en security een belangrijk gegeven vormen.

Niet alleen voor bedrijven, maar ook voor de thuisgebruikers. Waar een vraag is, is echter ook een aanbod. De afgelopen tijden schoten privacy tools dan ook als paddenstoelen uit de grond. VPN's, geëncrypteerde mailboxen, veilige berichtendiensten, browsers die adverteerders te slim af zijn, etc. In dit overzicht behandelen we de tools en services die je kan inzetten (zelfs vaak gratis) om je privacy te boosten.

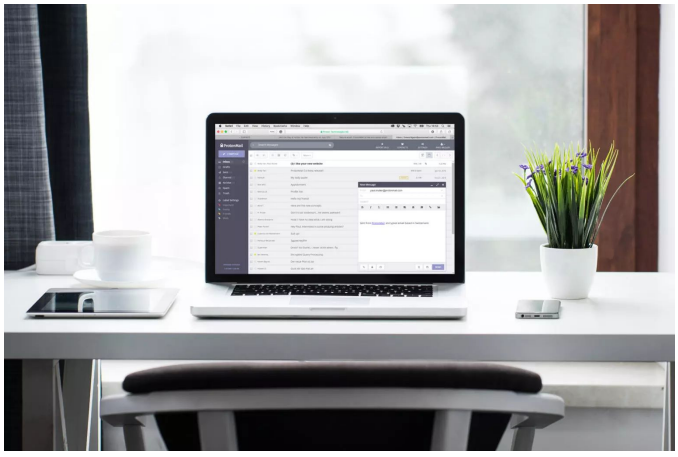
1. Geëncrypteerde mailbox

De kans is groot dat je een mailbox hebt afgesloten bij je lokale provider, maar in mijn opiniestuk kon je al lezen dat dat beslist niet de beste manier is. Een beter idee is om beroep te doen op een publieke e-maildienst, zoals Gmail of Outlook. Toch zijn er ook heel wat mensen die Microsoft en Google niet vertrouwen met hun mails. Er lopen namelijk geruchten dat Google mails kan scannen om op die manier een profiel van je op te bouwen en dat vervolgens door te verkopen aan adverteerders.

Door een geëncrypteerde mailbox te gebruiken, zorg je ervoor dat mails enkel voor jou zichtbaar zijn. De provider kan op geen enkele manier jouw mails inkijken, zelfs niet wanneer de autoriteiten hierom zouden vragen. Enkel jij (als gebruiker) hebt de encryptiesleutel.

De populairste dienst hiervoor is ongetwijfeld ProtonMail. De dienst is gevestigd in Zwitserland, waar de privacywetgeving het strengst is. Het is zelfs mogelijk om een volledig anoniem e-mailaccount aan te maken. De dienst wordt bijvoorbeeld gebruikt door bepaalde bronnen die informatie willen doorspelen aan een journalist.

Je kan de dienst gratis gebruiken, dan krijg je een mailbox van 500MB. Wordt dat te weinig, dan kan je voor 48 euro per jaar een mailbox van 5GB huren.



Bij ProtonMail blijven mails enkel voor jouw ogen.

2. Een Google-alternatief

Google is verreweg de beste zoekmachine die er bestaat (sorry, Bing), maar het is algemeen bekend dat je op de voet wordt gevolgd door Google. Op basis van je zoekgedrag, kunnen ze namelijk een persoonlijk profiel samenstellen om vervolgens te verkopen aan adverteerders. Zij kunnen je vervolgens persoonlijke advertenties sturen. Merkt Google aan je zoekopdrachten dat je wellicht binnenkort een kindje verwacht, dan krijg je binnen de kortste keren advertenties te zien van pampers.

Zoek je een privacy gerichte zoekmachine die je niet volgt, dan zijn DuckDuckGo en Startpage de bekendste opties. Bij die diensten worden je zoekgegevens niet opgeslagen, gedeeld of verkocht. Dit vermijdt ook dat je terechtkomt in een ‘filterbubbel’.

DuckDuckGo

Stel dat je ervan overtuigd bent dat corona een samenzwering is om 5G-chips in mensen te injecteren en hier zoek je dan ook geregeld informatie over op. Google zal merken dat deze insteek je interesseert, en zal zoekopdrachten die gaan over deze samenzwering hoger zetten in de zoekresultaten. Het resultaat: je eigen mening wordt steeds bevestigd. Leuk, maar niet objectief.

DuckDuckGo bouwt zijn eigen zoekresultaten op (via eigen crawlers) terwijl Startpage gebruikmaakt van de zoekresultaten van Google. Dat laatste heeft mijn persoonlijke voorkeur, omdat je gebruikmaakt van de kwalitatieve zoekresultaten van Google zonder te moeten inleveren op privacy.

Op deze manier blijf je wel Google steunen, en wanneer je anti-Google bent wil je dat misschien liever niet. Hoe dan ook, bij beide zoekmachines ben je zeker van een privacybewuste zoekervaring.

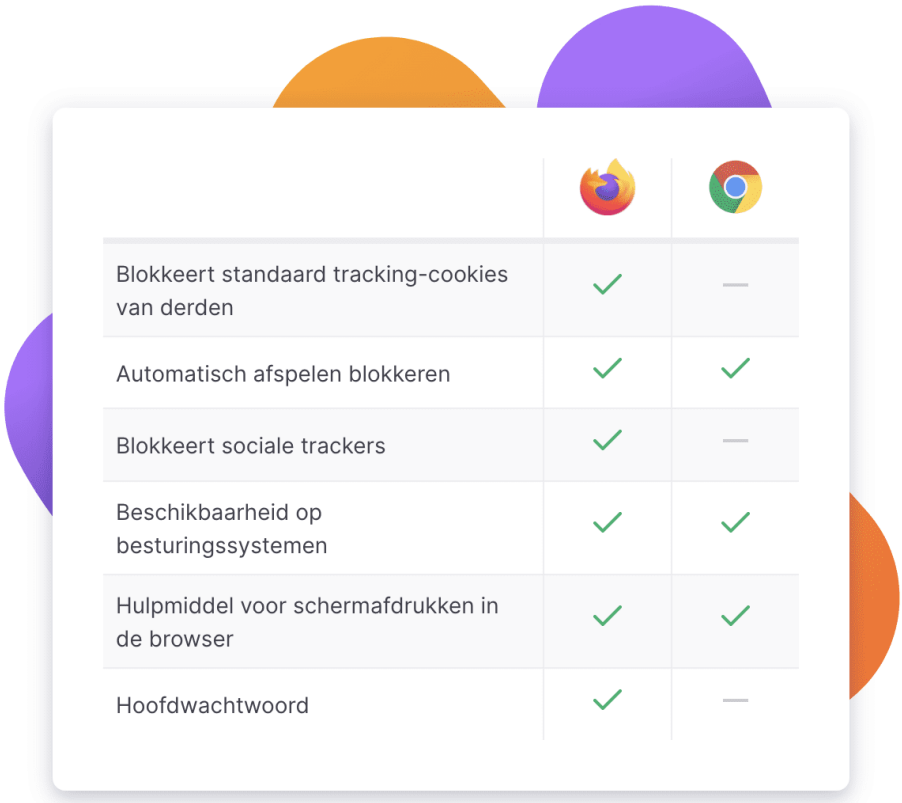
Gebruik een zoekmachine die geen profiel van je opbouwt.

3. Een privacybewuste browser

De meest gebruikte applicatie op je computer en smartphone, is wellicht je browser. Het is dan ook belangrijk om een browser te kiezen die op een gezonde manier omgaat met je privacy. Een browser zoals Chrome volgt al je handelingen namelijk nauwgezet. Op mobiele apparaten wordt je locatie zelfs gevolgd. Heel wat overbodige (en eigenlijk schadelijke) cookies worden door Chrome gebruikt om een profiel op te bouwen van gebruikers en om de prestaties van advertenties te monitoren.

Een browser zoals Firefox of Safari (en al helemaal sinds macOS Big Sur) countert dit probleem door dergelijke trackers te gaan blokkeren. Deze browsers zorgen er dus voor dat adverteerders je niet kunnen volgen. Mozilla, het bedrijf achter Firefox, is een non-profitorganisatie.

In tegenstelling tot Google (dat in feite een advertentiebedrijf is), hebben ze dus geen winstbelang. De browser bevat ook tal van andere handige functies ter bescherming van je persoonlijke gegevens. Zo word je bijvoorbeeld gewaarschuwd wanneer je een website bezoekt die recent het slachtoffer is geweest van een data lek. Firefox is bovendien beschikbaar op alle platformen en met een Firefox-account kan je alles netjes synchroniseren, dus er is weinig reden om de browser niet te gebruiken.



Firefox is een browser die respect heeft voor je privacy.

4. Privacy in je cloudopslag

De tijd waarin we onze bestanden simpelweg op onze eigen computer bewaarden, ligt achter ons. Tegenwoordig wordt er volop gebruikgemaakt van cloudopslag zoals OneDrive, Google Drive of Dropbox. Handig, want zo heb je overal toegang tot je bestanden. Bovendien heb je zo ook steeds een back-up van je bestanden.

Uiteraard houdt het wel een risico in om al je bestanden te bewaren op de server van iemand anders (ook al gaat het hier om gigantische bedrijven zoals Google of Microsoft).

In de vorige editie van Clickx leerde je hiervoor alvast een oplossing kennen in de vorm van Cryptomator. Zo kan je namelijk eerst je bestanden encrypteren, alvorens ze naar de cloud worden gestuurd. Dat is een ideale oplossing, want zelfs wanneer de servers van Google gehackt worden en iemand jouw bestanden in bezit krijgt, kunnen die alsnog niet worden ingekeken.

Er zijn ook Cloud providers die een dergelijke encryptie “out-of-the-box” voorzien. Sync bijvoorbeeld, waarvan je in dit nummer ook een review kan vinden. Of je nu een veilige Cloud provider gebruikt of een eigen encryptietool maakt in feite niet veel uit. Het gebruiksgemak bij een tool zoals Sync ligt in ieder geval wel hoger.

Gebruik een veilige Cloud provider of encrypteer je bestanden vooraleer ze naar de Cloud worden gestuurd.

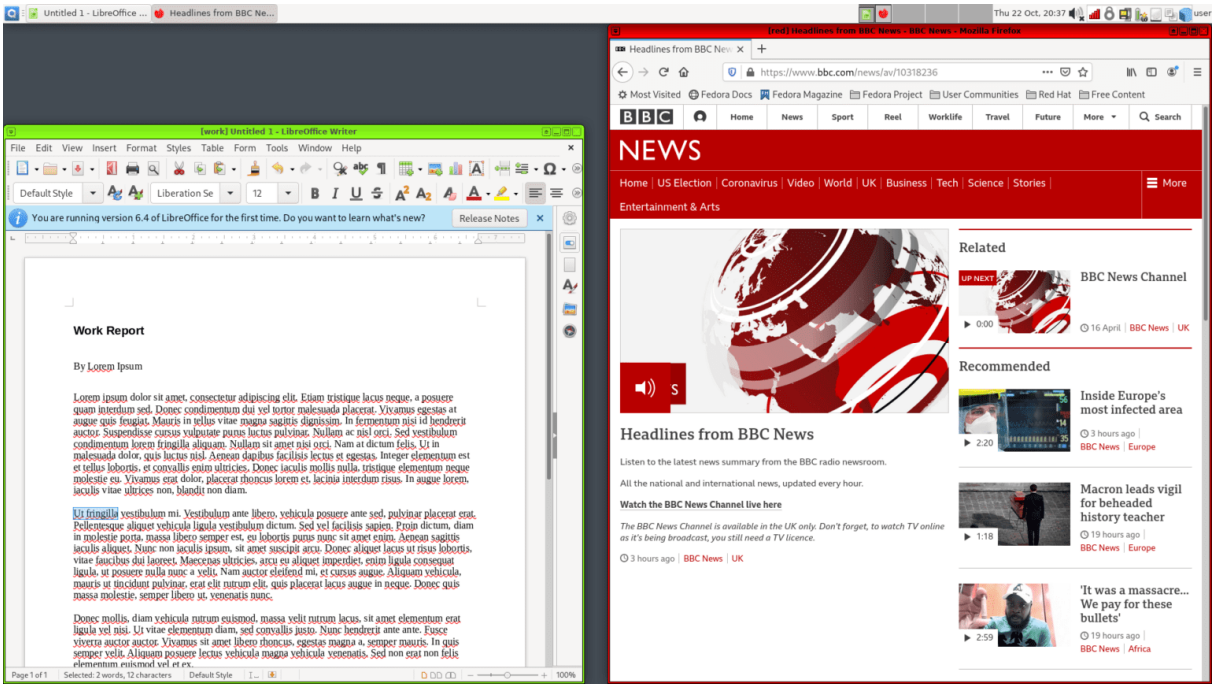
5. Besturingssysteem

Het is voor de hand liggend om een privacy bewuste browser en goede VPN te gebruiken, maar wie écht geeft om privacy, kiest ook voor een beter besturingssysteem.

De meeste computers draaien op Windows 10, maar dat platform verzamelt heel wat persoonlijke gegevens, zoals je locatie en spraakopdrachten die je geeft aan Cortana. Die gegevens worden gebruikt om de software beter te maken en om gepersonaliseerde advertenties te kunnen tonen.

Ook in dit geval zijn er echter alternatieven, en dan gaat het in eerste instantie om Linux. Zoals je eerder in onze koopgids van Linux distributies hebt kunnen lezen, zijn er heel wat verschillende varianten. Linux Mint is niet dé meest privacy bewuste variant van Linux, maar wel een stuk meer privacy gericht dan Windows.

Bovendien is de software ook ideaal voor beginners. Meer geavanceerde gebruikers kunnen Qubes uitproberen, het besturingssysteem dat bijvoorbeeld ook door privacy-goeroe Edward Snowden wordt gebruikt.



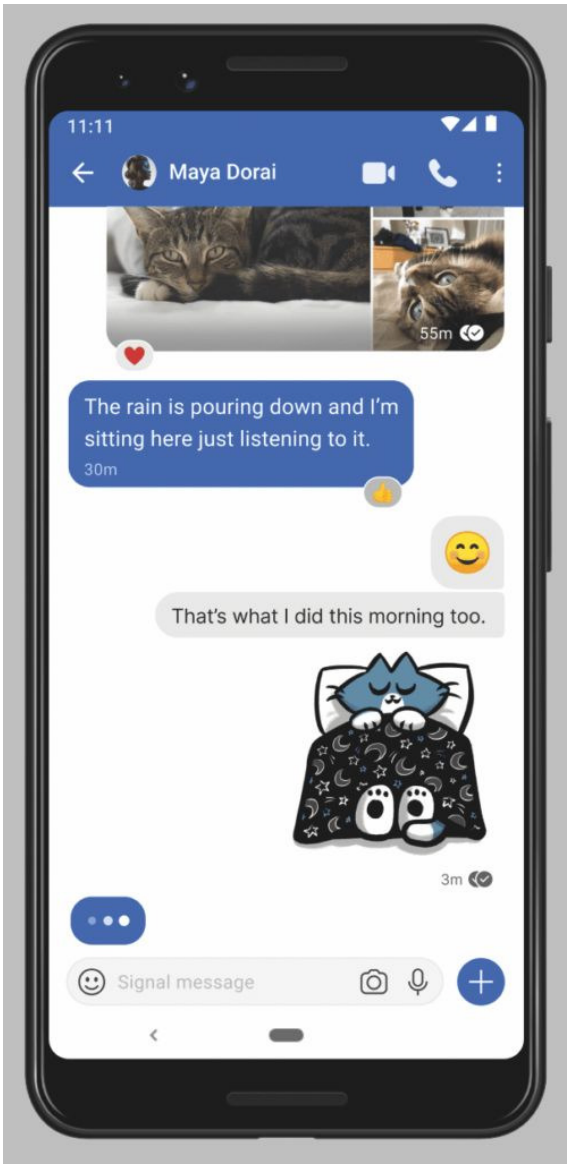
Heel gebruiksvriendelijk is Qubes niet, maar wel veilig!

6. Een betere Instant Messenger

We vallen in herhaling, maar we verwijzen opnieuw even naar een vorig nummer van Clickx waar je een keuzewijzer kon vinden van de voornaamste Instant Messengers. Het gaat hier dan bijvoorbeeld om tools zoals Telegram, WhatsApp en Facebook Messenger.

Toen kwam Signal ook uit de bus als de tool die gebruikers het meeste privacy biedt. Via E2EE wordt elke vorm van communicatie (een bericht, videogesprek of audiogesprek) geëncrypteerd alvorens deze worden verstuurd. Zo weet je zeker dat enkel jij en de ontvanger de berichten kunnen lezen en dat er niemand je conversaties afsnoept. Het is de communicatietool bij uitstek van Edward Snowden.

Het bedrijf achter Signal wordt uitsluitend gefinancierd door subsidies en donaties en dus niet door het verkopen van advertenties of gegevens. Bovendien is de tool ook open-source waardoor kritische gebruikers de hele broncode kunnen doorspitten. De tool is gratis te gebruiken op Android, iOS, Windows, Mac en Linux.



Met Signal weet je zeker dat enkel jij en de ontvanger de conversatie kan volgen.

7. Privacy met een VPN-dienst

Een VPN (Virtual Private Network) kan uiteraard niet ontbreken in ons lijstje. Het wordt wat omschreven als “de heilige graal” op privacy gebied, maar dat is het natuurlijk niet.

Wanneer je volledig anoniem wil surfen, dan biedt een VPN je niet wat je zoekt. Volledige anonimiteit kan je enkel krijgen via de beruchte Tor Browser. Een VPN geeft je wel wat meer privacy, in die zin dat je internetprovider (zoals Proximus of Telenet) niet langer je netwerkverkeer kan inkijken. Ze kunnen dus niet zien welke websites je bezoekt.

We hebben het geluk om in het vrije België of Nederland te wonen, maar in veel andere landen is het gebruik van een VPN de enige manier om geblokkeerde websites te bezoeken. Ook is een VPN een slimme zet wanneer je gebruikmaakt van publieke draadloze netwerken. Er wordt namelijk een beveiligde tunnel opgezet tussen de server en jouw apparaat, zodat je niet vatbaar bent voor man-in-the-middle-attacks. Zo vermijd je dus dat je netwerkverkeer wordt afgesnoept door een cybercrimineel.

Bij het kiezen van een VPN, dien je na te gaan of het bedrijf al dan niet logs bijhoudt van jouw netwerkverkeer. Enkele gerenommeerde VPN’s zijn: Mullvad, ProtonVPN en IVPN.

In tegenstelling tot wat de marketingpraatjes je doen geloven, is een VPN niet de heilige graal.

Bron: TechPulse van 3 februari 2021