Zo beveilig en bescherm je jezelf online

© Getty

28 maart 2016 09:50

Het is je recht om jezelf online te beschermen tegen inbrekers en pottenkijkers. Maar hoe doe je dat eigenlijk? We geven je tien tips om online, privé te houden - wat privé is.

Dit artikel verscheen eerder in Bright Ideas, het tweewekelijkse webmagazine van Bright met verdieping over vernieuwing. Een jaar lang toegang tot alle artikelen kost 24 euro.

1. Gebruik je gezonde verstand

Denk even rustig na voordat je ergens klakkeloos op klikt. Als je een e-mailtje krijgt van jouw bank dat je een nieuwe contactloze betaalpas kunt aanvragen door op een linkje te drukken, ga even met je muis op het linkje staan zodat je de url weet. Als deze leidt naar x.co/betaalpas, weet je dat het foute boel is.

Je loopt niet constant het risico dat je wordt gehackt, maar wel dat je een vervelende mail krijgt met een phishing- of malware-link. Oh, en houd je software up-to-date, vooral Flash en Silverlight.

2. Neem een VPN

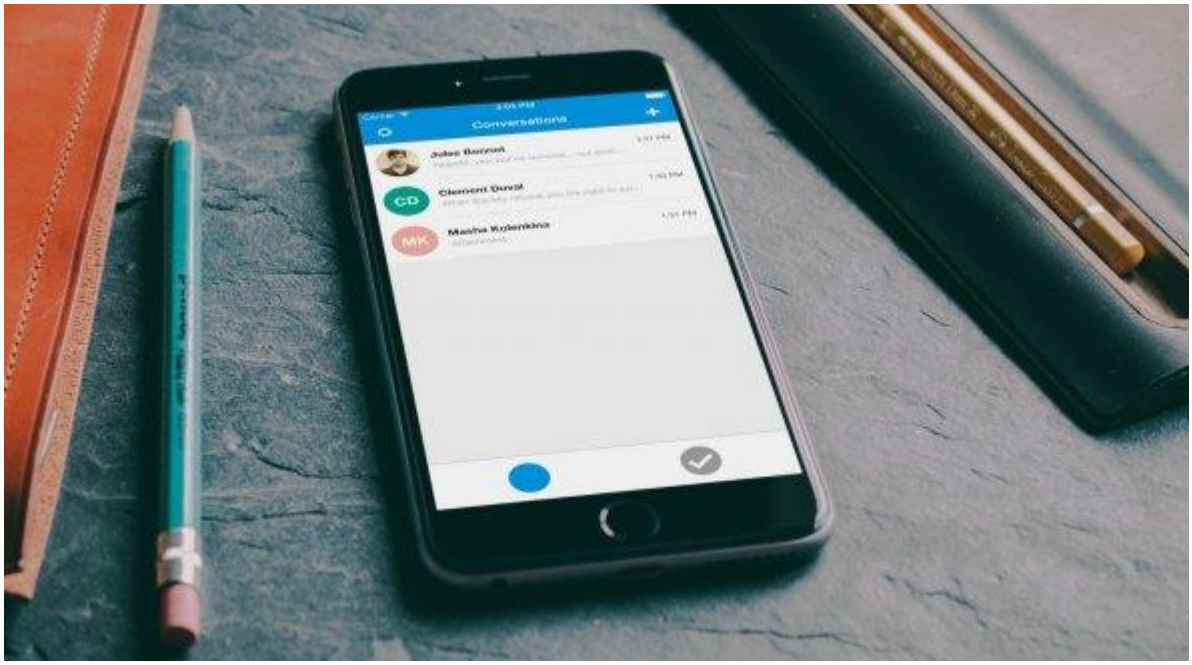
Een VPN-verbinding beschermt je tegen pottenkijkers. Je activeert een versleutelde verbinding waardoor je internetprovider of de inlichtingendiensten een stuk lastiger mee kunnen kijken

met wat jij precies uitspookt. Dat komt omdat je voor derden verbergt wie je bent en wat je precies doet.
Daarnaast is een VPN een belangrijk middel op jezelf te beschermen als je verbindt met een openbaar wifi-netwerk, waar het vrij gemakkelijk is om te zien wat andere gebruikers van hetzelfde netwerk uitspoken. Goede opties voor een VPN zijn AirVPN, iVPN en Mullvad. Als je goedkoop een VPN wilt proberen, is Private Internet Access een interessante optie.

3. We Signallen!

Een stap die we allemaal zonder te veel moeite kunnen nemen, is het installeren van Signal. De app is beschikbaar voor Android en iOS en laat gebruikers veilig met elkaar communiceren. Dat kan via chatberichten, maar ook middels VoIP-gesprekken (bellen via een internetverbinding).

Signal maakt bij beide gebruik van end-to-end-encryptie, waarbij de inhoud van een bericht zodanig wordt versleuteld dat alleen de ontvanger het kan openen. De technologie achter Signal is ook geïntegreerd in WhatsApp, waardoor de chat-app van Facebook opvallend genoeg als relatief veilig wordt gezien.



4. Versleutel je bestanden met VeraCrypt

VeraCrypt is op dit moment één van de beste gratis en open source programma's om bestanden

te versleutelen. De software creëert een soort extra harde schijf op je computer, een zogeheten 'container'.

Daarin kun je bestanden versleuteld opslaan. Na het invoeren van je wachtwoord verschijnt de externe harde schijf op je computer en kun je er bestanden in slepen. Zo'n container-bestand kun je vervolgens naar de cloud uploaden.

Stack biedt gratis 1TB cloudopslag in Nederland aan, waar je jouw VeraCrypt-containers naar kunt uploaden. Als je voor jouw cloudopslag wilt betalen, dan is SpiderOak een veiligere optie.

5. Onthoud maar één wachtwoord

Hoe meer wachtwoorden je moet onthouden, hoe zwakker ze worden. Je gebruikt misschien hetzelfde wachtwoord voor al jouw sociale netwerken. Of elke keer een kleine aanpassing en dat is compleet onveilig.
Met een wachtwoordbeheerder hoef je maar één wachtwoord te onthouden om toegang te krijgen tot al je andere wachtwoorden. LastPass is het meest veelzijdig, 1Password het mooist en KeePass wordt gezien als het veiligst.

En als we dan toch bezig zijn: creëer een lastig wachtwoord. Dat hoeft niet per se met veel cijfers en hoofdletters, maar het moet wel lang zijn. Een wachtwoord als 'Deeerste3StarWarsfilmszijndebestefilms' is echt een prima wachtwoord - en je onthoudt 'm heel gemakkelijk!

6. Koop een Yubikey

De Yubikey ziet eruit als een usb-stickje, maar dient ergens anders voor: hij beveiligt al je wachtwoorden nog een extra keer. Als je de sleutel gebruikt, moet je na het inloggen met je e-mailadres en wachtwoord, nog een extra code invoeren.

Die kan je krijgen via een authenticatie-app of sms'je, maar je kunt ook je Yubikey in de usb-poort steken om aan de dienst te laten weten dat jij het écht bent. Dit werkt met onder andere Google en Dropbox.

Oke, je hoeft geen Yubikey te kopen om echt veilig te zijn. Maar het kan heel veel voordelen bieden. Allereerst zorgt het voor tweestaps-verificatie. Schakel dit altijd in, want heel veel diensten ondersteunen dit.

In de Yubikey 4 zit ook een nfc-chip, een contactloze methode om snel data uit te wisselen. Daarmee kun je gemakkelijk inloggen op je wachtwoordmanager op je telefoon, zoals de eerdergenoemde LastPass of KeePass. Houd hem even tegen je Android aan en je logt bijvoorbeeld in. En ook niet onbelangrijk: hij ziet er tof uit aan je sleutelbos.

7. Installeer de nodige browserextensies

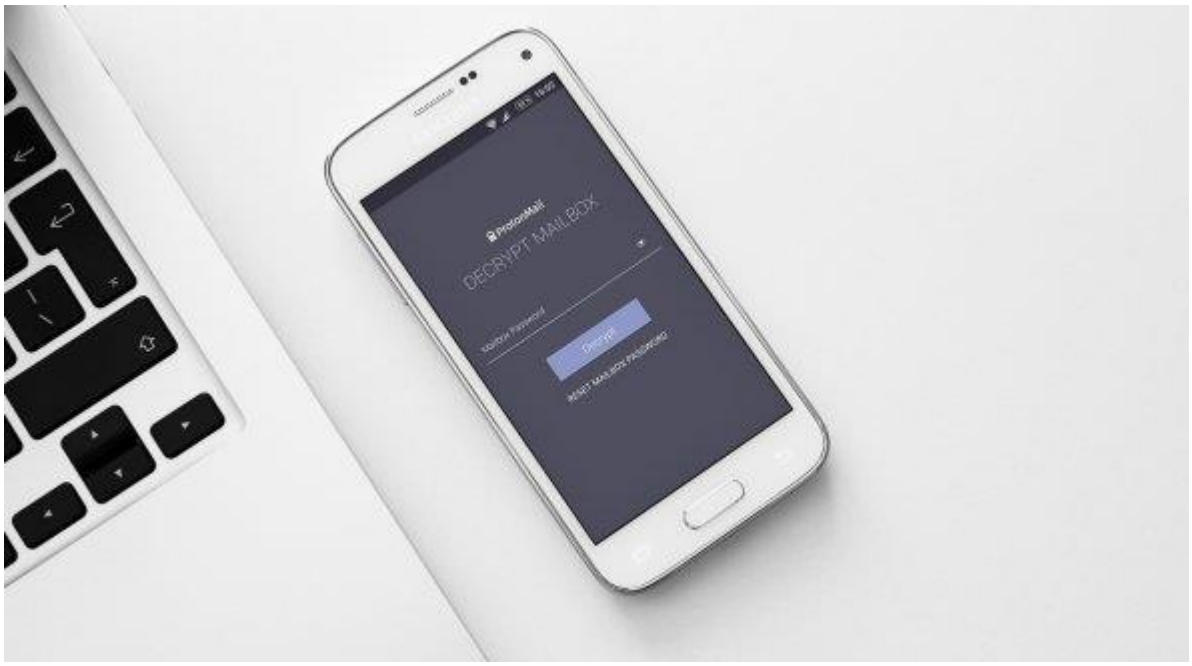
Het gaat om twee browserextensies van de Electronic Frontier Foundation (EFF), genaamd HTTPS Everywhere en Privacy Badger. HTTPS Everywhere forceert wanneer het kan een beveiligde https-verbinding, Privacy Badger blokkeert advertenties en trackers die je op het internet volgen. Beide extensies zijn eigenlijk onmisbaar als je veilig het internet op wil.

8. Tor wanneer het moet of kan

Tor is één van de weinige technologieën die heeft bewezen enorm lastig te kraken te zijn. Het netwerk van Tor zorgt ervoor dat jouw verstuurde en ontvangen data via verschillende computers wordt gestuurd, waardoor je internetgedrag wordt geanonimiseerd.
Tor wordt regelmatig door dissidenten gebruikt om anoniem kritiek te uiten op totalitaire regimes, maar ook door criminelen om bijvoorbeeld drugs en wapens te verhandelen. Dat is het nadeel wanneer software je zodanig goed anonimiseert. Je hoeft de Tor-browser niet constant te gebruiken, maar als je ooit een keer écht anoniem wilt surfen: gebruik dan Tor.

9. Neem ProtonMail

Als je veilig wilt e-mailen, is Pretty Good Privacy (PGP) een goede optie. PGP wordt gebruikt door mensen als Edward Snowden en Glenn Greenwald en maakt gebruik van krachtige end-to-end-encryptie om een bericht te versleutelen. Alleen de ontvanger heeft de sleutel om het bericht te openen. Maar hoe je het wendt of keert: PGP blijft een verdraaid lastige technologie om in je dagelijks leven efficiënt te gebruiken.



Dat vinden ook de oprichters van ProtonMail, een e-maildienst à la Gmail die standaard end-to-end-encryptie biedt, ook. ProtonMail is gratis te gebruiken en versleuteld berichten standaard tussen ProtonMail-gebruikers.

Wil je een versleuteld bericht veilig naar een ander persoon sturen, zoals een Gmail-gebruiker? Dan kun je jouw e-mail beveiligen met een wachtwoord dat je via een ander veilig kanaal aan de ontvanger geeft. Daarnaast wordt je gehele inbox versleuteld waardoor zelfs ProtonMail geen toegang heeft tot jouw e-mails.

10. Zet Tails op je oude USB

Heb je nog ergens een oude USB-stick slingeren? Steek hem in je computer en installeer het besturingsssyteem Tails, dat door onder andere Snowden wordt gebruikt. Tails is een besturingssysteem dat specifiek is gebouwd om anonimiteit te bieden en veilig te zijn. Je steekt

het apparaatje in een willekeurige computer, start hem op vanaf de usb-stick en komt in een speciaal beveiligde Linux-omgeving die geen sporen achter laat.

Tails beschikt standaard over de Tor-browser, een e-mailprogramma met ondersteuning voor PGP en een chat-programma om veilig te communiceren. Je gaat Tails niet snel dagelijks gebruiken, maar het is wel een fijn idee dat je op elke computer een veilige omgeving kunt creëren.

Dit artikel verscheen eerder in Bright Ideas, het tweewekelijkse webmagazine van Bright met verdieping over vernieuwing. Een jaar lang toegang tot alle artikelen kost 24 euro.

Bron: RTL Nieuws
URL: http://www.rtlnieuws.nl/economie/home/zo-beveilig-en-bescherm-je-jezelf-online