de Correspondent

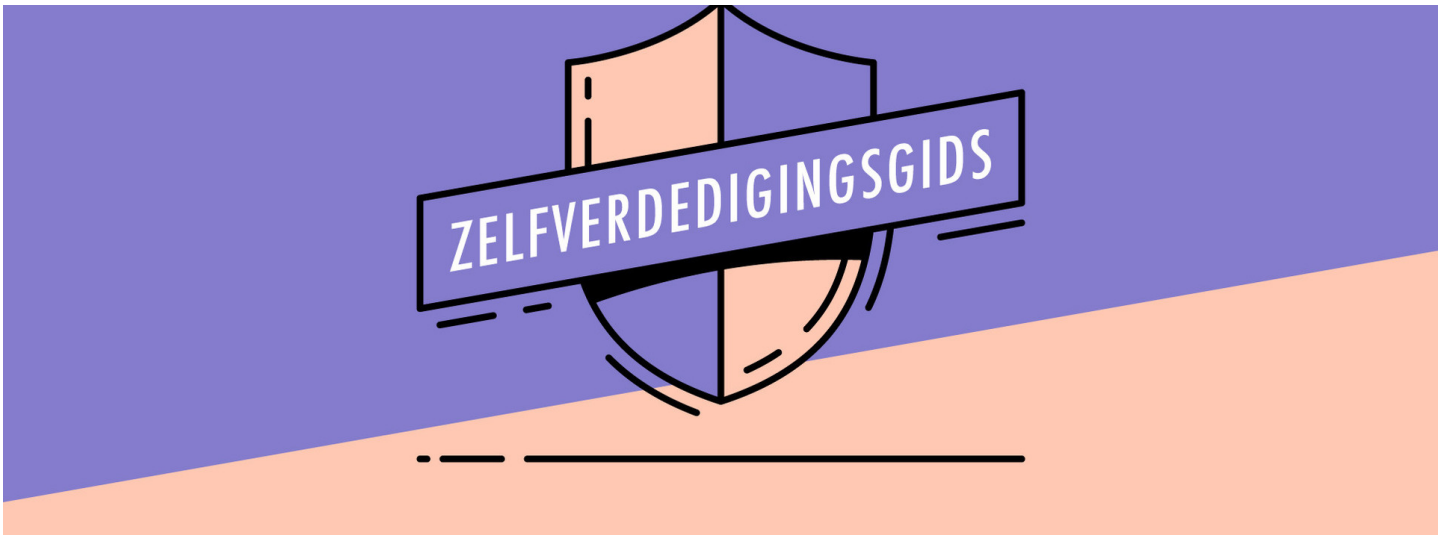
Analyse

12.09.2016 • Leestijd 10 - 14 minuten

Met deze praktische gids leer je jezelf online te beschermen tegen nieuwsgierige advertentiebedrijven en kwaadwillende hackers. We laten stap voor stap, in tekst en video, zien welke eenvoudige maatregelen je kunt nemen om in dertig minuten een acceptabel niveau van privacy en veiligheid te bereiken.

De digitale zelfverdedigings gids: bescherm jezelf op het web

Dimitri **TOKMETZIS** *Maurits* **MARTIJN**



Illustratie: Leon Postma (redactioneel ontwerper voor De Correspondent)

In ons boek *Je hebt wél iets te verbergen* laten we zien waarom het belangrijk is om grip te krijgen op je persoonlijke gegevens. Maar hoe doe je dat?

Er zijn online uitstekende gidsen te vinden die je verder kunnen helpen. Het probleem met deze gidsen is vaak de overdaad aan tips, zodat je nog steeds niet weet waar je het beste kunt beginnen. Daarnaast is het voor de meeste mensen helemaal niet nodig om al die tips op te volgen.

Deze zelfverdedigingsgids is bedoeld voor iedereen die het internet gebruikt. Met onze tips kun je in een halfuur een acceptabel niveau van privacy en veiligheid krijgen. We doen concrete aanbevelingen voor apps, plug-ins en aan te leren gewoontes die volgens ons een goede balans geven tussen privacy, veiligheid, gebruiksgemak en kosten.

Dat betekent dat we harde keuzes hebben gemaakt. Zijn er andere apps, plug-ins en gewoontes die ook de moeite waard zijn? Zeker. We moedigen je vooral aan om je daar na het lezen van deze gids verder in te verdiepen. Maar tijd is

kostbaar, de mogelijkheden zijn eindeloos en niet iedereen is even technisch onderlegd.

Voordat je begint nog een algemeen advies: wees niet bang om fouten te maken. Het beschermen van je data is niet iets dat je altijd heel consistent kunt doen. Iedereen doet weleens wat doms, of maakt het zich makkelijk door toch maar even dat onbeschermde netwerk op te gaan, toch meer data achter te laten dan hij eigenlijk had gewild.

We hopen dat je met deze gids die situaties in ieder geval herkent en stukje bij beetje je eigen privacy en veiligheid onder controle krijgt.

Eerst even dit. Als op internet iets gratis is, ben jij waarschijnlijk het product. We doen daarom in deze gids een aantal aanbevelingen voor betaalde diensten. We worden door geen van deze diensten gesponsord, maar bevelen ze aan omdat we er goede ervaringen mee hebben en omdat de prijzen in onze ogen redelijk zijn. Als je alle adviezen van ons opvolgt, kost dat je 50 tot 80 euro per jaar.

1. Windows

Windows... tja. Windows is toch een beetje een probleemgeval. Vergis je niet, Microsoft heeft de laatste jaren veel gedaan om het besturingssysteem veiliger en stabieler te maken. Maar toen kwam de laatste versie, Windows 10, een ware privacyramp. Microsoft zuigt bakken data van je computer en de standaardinstellingen zijn ronduit nadelig voor wie zijn privacy wil beschermen. Kortom: veel werk aan de winkel.

1. **Stel een goed wachtwoord in.** En zorg er, zoals bij al je apparaten, voor dat je dat ook moet intypen als je computer uit de slaapstand ontwaakt.
2. **Ga naar Privacyinstellingen.** Zet onder het kopje Algemeen allereerst je reclame-id uit. Deze unieke code gebruiken adverteerders om je te kunnen volgen. Het is belachelijk dat zo'n code in je besturingssysteem zit. De overige opties kun je naar wens uitzetten. Ons advies, en dat geldt voor eigenlijk alle opties die hierna komen: de meeste heb je gewoon niet nodig. Als je ze wel nodig hebt, dan word je er wel om gevraagd en kun je ze alsnog aanzetten. Zet ze dus gewoon standaard uit.
3. **Ga vervolgens naar Locatie.** Zet daar alles uit en wis je geschiedenis.
4. **Ga daarna naar Camera en microfoon.** Zet bijna alles uit. Je kunt overwegen om ze aan te laten voor Skype of een andere communicatie-app.
5. **Loop ook de rest van de instellingen door.** Pas die aan naar je eigen wensen.
6. **Ga terug naar de algemene instellingen.** Kijk onder Systeem bij het kopje Info, helemaal onderaan. Druk daar op BitLocker en zet de versleuteling van je harde schijf aan. Als je je laptop verliest, dan kan niemand bij je data komen.
7. **Kijk ook nog even online bij je Microsoft-account.** Controleer of daar alles ingesteld staat zoals je het hebben wilt.
8. **En, heel belangrijk, installeer altijd zo snel mogelijk de beveiligingsupdates.** Er worden zeer vaak lekken gevonden in de software. Als je de updates uitstelt, blijven die lekken bestaan, en loop je dus meer risico om gehackt te worden.

2. Mac

Sinds de onthullingen van Edward Snowden profileert Apple zich als een privacyvriendelijk en veilig alternatief voor Windows en Android. De standaardinstellingen van Mac OS, het besturingssysteem, zijn gericht op het beperken van het weglekken van data en het beveiligen van de computer. En Apple slaagt daar redelijk goed in.

Dat merk je ook als je je Mac wilt beveiligen: je hoeft eigenlijk niet zoveel te doen. Ga naar de instellingen, ga naar Security & Privacy onder instellingen. Daar:

1. **Stel een wachtwoord in.** Ook voor als het scherm in slaap valt.
2. **Schakel je FileVault in.** Dat is de versleuteling van je harde schijf, en voorkomt dat vreemden bij je data kunnen als je je computer verliest.
3. **Schakel je Firewall in.** Die waakt erover dat programma's niet zomaar contact kunnen leggen met andere computers.
4. **Geef onder het tabje Privacy aan welke programma's je locatiegegevens en contacten mogen inzien.** Ons advies: geen. Als een programma die nodig heeft, dan vraagt het er wel om en kun je alsnog toestemming geven.
5. **Van groot belang, en dat geldt voor alle apparaten, is dat je beveiligingsupdates meteen installeert.** Er worden soms veiligheidslekken gevonden. Apple verhelpt die doorgaans snel, maar als je die updates niet installeert,

blijft het lek gewoon bestaan. Apple geeft gebruikers zelf een seintje als er een nieuwe update is.

6 **Tot slot, als iemand anders op je computer werkt, geef hem of haar dan een gastaccount.** Dat kun je instellen onder Users & Groups.

In de video hierboven lopen we nog even langs een aantal tips.

3. Android

Android is het besturingssyteem van Google voor smartphones (en tablets, maar hier gaat het over smartphones). Androidtelefoons komen in alle soorten en maten, dus het is lastig om heel specifieke tips te geven. Wel zijn er een aantal algemene tips te geven die de meeste typen smartphones delen.

1 **Gebruik een vergrendelingsscherm met een wachtwoord of pincode.** Je smartphone is de toegangspoort tot je privéleven, eentje die je ook nog eens makkelijk kunt kwijtraken. Er zijn apps beschikbaar (zoek op 'smart unlock' in de Play Store) waarin je kunt aangeven wat veilige netwerken zijn (zoals thuis of op het werk). Als je op die plekken bent, hoef je je wachtwoord niet in te voeren. Als je een pin gebruikt, kies dan niet je pincode die je bijvoorbeeld voor je bankpas gebruikt: je toetst deze code immers vaak in het openbaar in.

2 **Loop goed je Google-instellingen door.** Google geeft je automatisch een reclame-id, die apps kunnen gebruiken om je te volgen. Deze kun je uitzetten in je

Google-instellingen op je telefoon. Zet je locatie standaard uit: als apps die nodig hebben, dan vragen ze er wel om.

3. **Ga nooit onbeschermd een openbaar wifinetwerk op.** Doe dat via een virtual private network, een VPN. Een VPN zorgt voor een private en versleutelde verbinding, zodat anderen op het netwerk niet kunnen zien wat je aan het doen bent. Private Internet Access en Freedome van F-Secure zijn goede VPN-diensten.
4. **Installeer altijd direct beveiligingsupdates.** Android is niet het meest veilige besturingssysteem en het is daarom zaak om de software zo up-to-date mogelijk te houden.
5. **Download geen apps buiten de officiële Google Play Store.** Behalve als je goed weet wat je doet.
6. **Vraagt een app veel toestemmingen?** Kijk dan of er wat meer privacyvriendelijke alternatieven zijn.
7. **Ga bij de instellingen naar het het kopje 'beveiliging' en klik op 'versleutelen.'** Doe dat écht. Als je je telefoon verliest, kunnen anderen niet zomaar bij de inhoud van je smartphone komen. Ze hebben dan je wachtwoord nodig om de versleuteling ongedaan te maken.

4. iPhone

Apple maakt het betrekkelijk makkelijk om je privacy en veiligheid op de iPhone te regelen. Apple houdt nauw toezicht op welke apps er in de App Store terechtkomen en het gebeurt niet vaak dat daar malware tussen sluipt.

Daarnaast is Apple, in tegenstelling tot Google die Android beheert, niet afhankelijk van advertentieinkomsten. Het beveiligen van een iPhone is dan ook vrij simpel:

1. **Gebruik een wachtwoord.**
2. **Zet het delen van locatie en contacten standaard uit.** Als apps ze echt nodig hebben, dan vragen ze er wel om.
3. **Ga nooit onbeschermd een openbaar wifinetwerk op.** Doe dat alleen via een virtual private network, een VPN. Een VPN zorgt voor een private en versleutelde verbinding, zodat anderen op het netwerk niet kunnen zien wat je aan het doen bent. Private Internet Access en Freedome van F-Secure zijn goede VPN-diensten.
4. **Installeer altijd direct beveiligingsupdates.** Apple maakt relatief veilige software, maar je moet wel de beveilingsupdates installeren.

5. Firefox en Chrome

Veilig surfen begint bij een goede browser. Gebruik Firefox of Chrome. Maak optimaal gebruik van de vele privacyinstellingen die deze browsers hebben:

1. **Blokkeer cookies waar mogelijk.**
2. **Sla wachtwoorden niet op in je browser.**
3. **Wis geregeld je cookies.**
4. **Daarnaast is er een aantal plug-ins,** extra software, om je privacy en veiligheid tijdens het surfen te verbeteren.

5. **Gebruik in ieder geval Privacybadger.** Dat is een plug-in die onnodige cookies blokkeert en dus ook advertenties tegenhoudt. Deze plug-in wordt onderhouden door de burgerrechtenorganisatie Electronic Frontier Foundation (EFF). In tegenstelling tot enkele andere plug-ins (Adblock Plus en Ghostery bijvoorbeeld) zit er dus geen commercieel bedrijf achter. Jouw belangen staan voorop.
6. **Download ook HTTPS Everywhere.** Eveneens van de EFF. Sommige websites hebben een beveiligde verbinding, maar bieden die niet standaard aan. HTTPS Everywhere dwingt zo'n beveiligde verbinding af.
7. **Log nooit in op een openbaar netwerk zonder VPN.** VPN staat voor Virtual Private Network. Je kunt een programma downloaden dat ervoor zorgt dat al je verkeer door een beveiligde tunnel gaat, zodat anderen op jouw netwerk jouw verkeer niet kunnen onderscheppen. Maak liever geen gebruik van een gratis VPN-dienst; die zijn niet altijd te vertrouwen. Twee goede en gebruiksvriendelijke VPN's zijn Private Internet Access en F-secure. Deze geven je beide meerdere accounts, zodat je ook een VPN op je smartphone kan zetten of je account kunt delen met je geliefde. Een bijkomend voordeel is dat je je internetverkeer via servers in andere landen kunt laten lopen, zodat je landblokkades - bijvoorbeeld van Netflix, of de BBC - kunt omzeilen.
8. **Een van de zwakke schakels in alle beveiliging zijn wachtwoorden.** Idealiter heb je voor iedere website een uniek, sterk wachtwoord. Er zijn trucjes waarmee je dat kunt doen, maar een makkelijke en veilige manier is het gebruik van een

wachtwoordmanager zoals LastPass.
Met LastPass heb je maar één wachtwoord nodig. Zorg ervoor dat dat een lang wachtwoord is dat alleen jij kunt onthouden, bijvoorbeeld iets als maArt.1s:een.maAnd.waArin.het.w33r.n0g.r0t.kAn.zijn!%.
Je kunt een plug-in downloaden (en een app op je smartphone) die op alle sites (en apps) herkent als om een wachtwoord wordt gevraagd. Als je ingelogd bent bij LastPass, wordt je gebruikersnaam en wachtwoord automatisch ingevuld. Je hoeft dus geen andere wachtwoorden meer te onthouden en je kunt ze op verschillende apparaten gebruiken.
Is dat onveilig? Ja en nee. Ja, LastPass is in 2015 gehackt. Nee, want LastPass slaat de wachtwoorden goed op (versleuteld). En als je tweefactorauthenticatie instelt, is het nagenoeg onmogelijk om vanaf een andere computer toegang te krijgen tot je LastPass-account. Tweefactorauthenticatie is een vorm van controle waarbij je niet alleen toegang krijgt met iets wat je weet (een wachtwoord), maar ook moet aantonen dat je iets hebt (een telefoonnummer waarop je een sms krijgt bijvoorbeeld). Je hoeft dat maar één keer op ieder apparaat dat je gebruikt in te stellen en dat voorkomt dat anderen, vanaf een andere computer, op je account kunnen inloggen - ook al hebben ze je wachtwoord. Je krijgt bij het inloggen op LastPass een code via je telefoon toegestuurd. Tweefactorauthenticatie is een simpele, maar doeltreffende manier om je gegevens te beveiligen en alle grote mailaanbieders ondersteunen dit tegenwoordig.

9 Het systeem is niet onfeilbaar, maar wel een stuk veiliger dan het gebruiken van een beperkt aantal

wachtwoorden, die ook nog eens makkelijk te raden zijn.

6. Hoe mail je veilig?

Op het werk ben je iemand anders dan thuis of in de kroeg. Dat geldt ook voor e-mail. Zorg ervoor dat je communicatiestromen je verschillende rollen representeren en gebruik daarom drie mailadressen (of twee als je werk en privé erg overlappen).

1. **Adres één gebruik je voor werk of studie.** Dat adres publiceer je nergens online en geef je niet aan Jan en alleman.
2. **Adres twee gebruik je voor belangrijke privézaken.** Denk aan contacten met de overheid, nutsbedrijven en familie. Mails die je niet wilt missen. Ook dit adres bewaak je met je leven.
3. **Adres drie gebruik je voor de rest.** Als je kaartjes bestelt. Als je online winkelt. Voor abonnementen of wat voor internetdienst dan ook. Dit is het adres waar heel veel ongevraagde nieuwsbrieven en spam op gaan binnenkomen.

Het voordeel van deze opdeling is dat je phishingmails makkelijker herkent. Als je bijvoorbeeld een bankmail binnenkrijgt op je werkadres, weet je dat het zaakje stinkt.

Phishing is nog steeds de belangrijkste hackmethode. Maar hoe herken je het? Kijk altijd eerst naar de afzender, maar ga daar niet blind op af. Er zijn mails in omloop die van een betrouwbare bron lijken te komen.

Het handigst is om met je muis even boven een link te hangen die je, volgens de afzender, moet volgen. Vaak zie je dan de bestemming van het linkje verschijnen en dan zie je ook vrij snel dat er iets niet in de haak is.

Tot slot moet je natuurlijk gewoon je boerenverstand gebruiken. De meeste instanties communiceren belangrijke zaken nog steeds per post. Bij twijfel: bel of google en laat de mail ongeopend.

Schakel in je mailprogramma het laden van 'remote content' uit. Dat voorkomt dat er plaatjes en documenten worden meegeladen als je je mail bekijkt. Marketeers sturen vaak een piepklein plaatje mee. Als dat wordt geladen, dus getoond, weten ze dat de mail is geopend en dat het mailadres dus wordt gebruikt. Dat leidt alleen maar tot meer nieuwsbrieven en spam.

Tot slot, je mailbox bevat zeer gevoelige gegevens, zoals correspondentie, maar ook wachtwoorden, telefoonnummers en foto's. **Beveilig je mailaccounts daarom met tweefactorauthenticatie.**

7. Gebruik Signal

Signal is een gratis app die je kunt installeren op je smartphone. Signal is te zien als een extreem veilig alternatief voor WhatsApp.

Met Signal kun je versleuteld sms'en, chatten én bellen. Let wel: alleen met mensen die ook Signal hebben geïnstalleerd. Versleutelingsexperts zijn zeer te spreken over de

bescherming die Signal aan communicatie biedt. Wij raden het iedereen aan.

Nog niet genoeg gehad?

Goed, je hebt een aantal tips opgevolgd en een acceptabel niveau van privacy en veiligheid bereikt. Maar het kan altijd beter. Zeker als je verantwoordelijk bent voor de data van andere mensen, is het handig om je apparaten nog wat meer dicht te timmeren en je beveiligingspraktijken te oefenen.

Wil je verder, kijk dan ook eens op deze sites:

- Bits of Freedom heeft de Internetvrijheid Toolbox samengesteld.
- De Amerikaanse EFF heeft ook goede handleidingen.
- Op Deep.Dot.Web, een site over het *dark web*, staan ook goede tips.
- Er is een boek: *Fake It! Your Guide to Digital Self-Defense*.
- Als je echt diep wilt gaan, kijk dan bij Anonymous.

Meer hierover?

Lees verder:

zelfverdedigingsgids-bescherm-jezelf-op-het-web/1596273331110-ded43079

De Correspondent is een dagelijks, advertentievrij medium met als belangrijkste doelstelling om de wereld van meer context te voorzien. Door het nieuws in een breder perspectief of in een ander licht te plaatsen, willen wij het begrip 'actualiteit' herdefiniëren: niet om je aandacht te trekken, maar om je inzicht te bieden in hoe de wereld werkt.

Alle verhalen lezen? Dat kan voor €7 per maand op: decorrespondent.nl

decorrespondent.nl