Laat Je Niet Hack Maken

Bang dat je computer wordt gegijzeld door ransomware? Je ex in je Facebook zit? Of dat criminele hackers jouw bankrekening plunderen?

Auteur
Daniël Verlaan is een Nederlandse journalist, werkzaam bij RTL Nieuws. Hij maakt verhalen over hackers, cybercrime en de duistere kant van het internet. Ook is hij regelmatig te gast bij de talkshow Pauw en andere televisieprogramma's.

INHOUD

Inleiding	**3**
Wat zijn hackers?	**4**
Hoe komen hackers meestal binnen?	**5**
De basis	**6**
Computer	**19**
Telefoon en tablet	**26**
Sociale media	**30**
Chatten en bellen	**34**
Geavanceerd	**38**

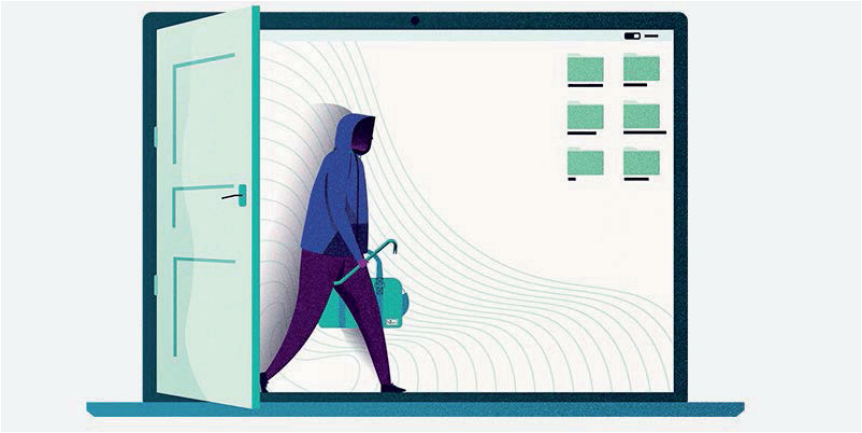
INLEIDING

Deze handleiding legt op een begrijpelijke manier uit hoe je jezelf **beschermt tegen hackers**. Aan de handleiding hebben zes professionele hackers 🦹💻 meegewerkt.

Laat Je Niet Hack Maken garandeert geen honderd procent veiligheid. Dat bestaat niet op het internet. Wel kun je het hackers en hun virussen zo lastig mogelijk maken door deze tips te volgen.

Voordat we beginnen: ga niet doodsbang achter je computer zitten. De kans dat een hacker alleen jou als doelwit heeft, is heel klein. Het meeste gevaar ontstaat doordat veel mensen een gebrekkige kennis van computers en het internet hebben. Laten we dat dit jaar eens verbeteren 👍.

WAT ZIJN HACKERS?



Hackers maken gebruik van kwetsbaarheden op het internet of in apparaten. Er zijn grofweg twee soorten: white hat hackers en black hat hackers. De zogeheten **white hat hackers** speuren naar de kwetsbaarheden om ervoor te zorgen dat ze gedicht worden. Dat maakt het internet weer een stukje veiliger.

In de media gaat het in het gros van de gevallen over **black hat hackers** 😈. Dit zijn hackers met kwade bedoelingen die bijvoorbeeld geld willen stelen of bij je inbreken om je in de gaten te houden. Of ze zijn op zoek naar gevoelige gegevens, zoals naaktfoto's of een kopie van jouw paspoort.

Er is ook een groep criminele hackers die voor de lol bij mensen inbreekt. Deze groep bestaat voornamelijk uit jongeren die hacken als een soort online kattenkwaad zien. Ondanks hun mogelijk onschuldige motief moet je nog steeds oppassen voor deze hackers.

Er bestaan ook hackers die namens een overheid bij doelwitten inbreken. Hackers in dienst van de geheime dienst of politie 👮 zijn het gevaarlijkst, maar vormen voor veel mensen geen directe dreiging. Ze hacken terroristen, criminelen en vijandige regimes, niet de normale internetgebruiker.

HOE KOMEN HACKERS MEESTAL BINNEN?

Hackers beginnen vaak met het stelen van jouw wachtwoord. Soms kun je daar niets aan doen, bijvoorbeeld als een website waar jij een profiel hebt wordt gehackt. Hackers maken dan ook **jouw wachtwoord** buit en proberen vervolgens met dat wachtwoord bij andere accounts in te breken, bijvoorbeeld je Gmail.

Het gebeurt ook dat je zelf per ongeluk je wachtwoord aan hackers geeft. Dit gebeurt bij **phishing**, een vorm van internetfraude waarbij criminelen je inloggegevens proberen te ontfutselen. Je zal vast wel eens een phishing-mail hebben ontvangen, zoals een nepbericht dat je bankrekening is geblokkeerd of een incasso niet is betaald.

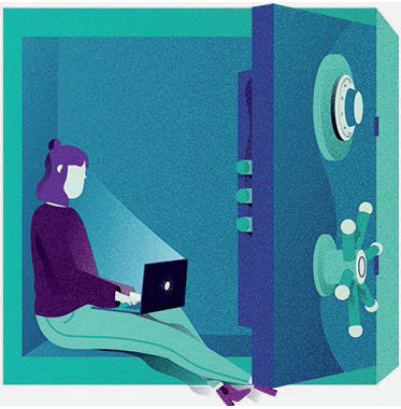
Ook breken hackers in via **bijlagen in e-mails**. Als je zo'n bijlage opent, wordt jouw computer overgenomen. Deze methode wordt vaak gebruikt voor het verspreiden van ransomware, een virus dat je computer onbruikbaar maakt door je bestanden achter slot en grendel te zetten. Hackers eisen dan losgeld om je computer weer toegankelijk te maken.

Virussen, ook wel malware genoemd, worden ook regelmatig verspreid via **downloads**, bijvoorbeeld torrents of installatiebestanden voor een programma dat je wilt gebruiken. Je denkt dat je een film of programma op je computer downloadt, maar in werkelijkheid haal je een virus binnen.

Een virus kan ook op jouw computer belanden door **online advertenties** en **overgenomen websites**. Zelfs Nederlandse websites verspreiden soms nog onbedoeld virussen. Als je jouw computer en software niet update, dan loop je een risico op dit soort infecties.

Een minder groot maar nog steeds aanwezig risico is dat een hacker met een **usb-stick** de volledige controle over jouw computer krijgt. Dat kan een usb-stick zijn die je 'toevallig' op straat vindt of van iemand krijgt, maar een kwaadwillende kan het apparaatje ook in je laptop steken als je even naar de wc bent.

DE BASIS



Nu je weet wat hackers zijn en hoe ze meestal proberen binnen te komen, kun je de eerste tips 💡 toepassen. Het gaat hierbij om de basis, een simpele lijst met maatregelen die iedereen zou moeten nemen.

UPDATEN

Veel mensen vinden updaten een vervelend en tijdrovend proces. In sommige gevallen is dat ook zo, maar het is ook de **belangrijkste bescherming !** tegen hackers. Veel hacks zijn succesvol omdat het slachtoffer verouderde software gebruikt. Daar zitten nog kwetsbaarheden in die met beveiligingsupdates worden gedicht.

Hoe ouder je software, hoe makkelijker hackers toegang krijgen

Software draait op allerlei apparaten. Denk aan Windows of MacOS op je computer of laptop, Android of iOS op je mobiele apparaten maar ook je router en slimme apparaten in huis. Bekijk regelmatig - één keer per week - of er updates voor jouw apparaten beschikbaar zijn en installeer ze zo snel mogelijk ⏰. Je kunt in sommige gevallen ook de updates automatisch laten installeren, onder andere bij Windows, MacOS en de Chrome-browser.

Daarnaast is het belangrijk om je apps en computerprogramma's te updaten, zoals je browser, PDF-lezer en Microsoft Office. Vaak krijg je **een melding** als er een nieuwe versie beschikbaar is.

WACHTWOORDEN

Tegenwoordig heb je voor praktisch elke website of app wel een account nodig, en dus ook een wachtwoord. Omdat we als mensen nooit tientallen verschillende wachtwoorden kunnen onthouden, zijn we geneigd om hetzelfde wachtwoord op meerdere plekken te gebruiken.

Dat is lekker makkelijk, maar ook **heel gevaarlijk** ⚠. Als een hacker achter jouw Spotify-wachtwoord komt, dan wil je niet dat dit wachtwoord ook toegang geeft tot je internetbankieren. En als je jouw Netflix-wachtwoord met een vriend deelt, wil je niet dat diegene op je Gmail of Facebook kan inloggen.

Daarom is het belangrijk om voor elke website of app een uniek wachtwoord te gebruiken. Enkel een cijfer 1 ☐ of letter 🅰 aanpassen, zoals veel mensen doen, is niet voldoende. Deze variaties zijn makkelijk te raden. Gelukkig bestaat hier een handige oplossing voor: wachtwoordbeheerders, beter bekend als **password managers**.

PASSWORD MANAGERS

Een password manager stopt al jouw wachtwoorden in een **digitale kluis** 🔐 en beveiligt ze met een overkoepelend wachtwoord. Je hoeft dan voortaan maar één wachtwoord te onthouden om toegang te krijgen tot al je accounts. Ook kunnen deze apps automatisch heel ingewikkelde wachtwoorden maken, zoals `6ur7qvsZpb0ZkcuSW1u!V8ng!L^lb`, en die vervolgens opslaan. Zulke wachtwoorden zijn vrijwel niet te kraken of raden.

Password managers hebben de mogelijkheid om jouw inloggegevens **in te voeren** bij websites. Dit beschermt je al tegen veel phishing-aanvallen. Als een website-adres niet correct is, zoals `ing.mijnbanklogin.nl`, zal een password manager jouw ING-inloggegevens daar niet invoeren. Ook kun je een password manager gebruiken om **notities op te slaan** 📝, zoals inlogcodes, geheime sleutels en antwoorden op geheime vragen.

Goede wachtwoordbeheerders zijn LastPass, 1Password, Bitwarden en KeePass. Als je nog nooit een wachtwoordbeheerder hebt gebruikt, kun je het beste de gratis variant van LastPass proberen.

LASTPASS (GRATIS)

LastPass is een overzichtelijke wachtwoordbeheerder met veel functies, waaronder een browser-extensie om wachtwoorden te genereren en in te voeren. LastPass heeft goede apps voor vrijwel alle besturingssystemen en kan prima gratis worden gebruikt. De betaalde variant geeft je 1 gigabyte opslagruimte voor gevoelige documenten en de mogelijkheid om wachtwoorden met anderen te delen.

1PASSWORD (3 EURO P/M)

1Password staat bekend om zijn mooie design en is geoptimaliseerd voor gebruik op Apple-apparaten, zoals je iPhone en Macbook. De app heeft sinds kort ook een handige browser-extensie (1Password X) die wachtwoorden voor je genereert en invult. 1Password-accounts werken met een speciale beveiliging in de vorm van een lange reeks tekens en cijfers die je moet invoeren om toegang te krijgen tot jouw account.

BITWARDEN (GRATIS)

Bitwarden is de afgelopen jaren erg populair geworden. De dienst is volledig open, heeft voor vrijwel elk platform een goede app en is gratis te gebruiken. Zelfs het delen van wachtwoorden met een ander, veelal een betaalde optie bij password managers, is gratis. Zodra je met meer dan één persoon wachtwoorden wil delen betaal je 1 dollar per maand, waarmee je ook 1 gigabyte opslagruimte voor jouw bestanden krijgt. Technisch onderlegde gebruikers kunnen hun eigen Bitwarden-cloud beheren, om zo alles in eigen beheer te houden.

KEEPASS (GRATIS)

KeePass wordt door experts gezien als de veiligste wachtwoordbeheerder, mede doordat veel beveiligingsonderzoekers de app gebruiken en constant veiliger maken. Het nadeel van KeePass is dat de app er vrij ouderwets uitziet, alsof je een Windows XP-programma gebruikt. Gelukkig bestaat de KeePass-community uit enthousiaste ontwikkelaars die fraaie apps voor KeePass ontwikkelen, zoals MacPass voor MacOS. Ook KeePassXC valt aan te raden, in veel opzichten een betere en completere versie van KeePass, die wordt onderhouden door een enthousiaste groep ontwikkelaars.

Je denkt misschien: *is dat wel veilig, zo'n digitale kluis?* Die zorgen zijn begrijpelijk: LastPass is bijvoorbeeld twee keer gehackt. Desondanks zijn er nooit wachtwoorden gestolen, want die worden zeer veilig in de digitale kluis opgeslagen.

EEN GOED WACHTWOORD

Vaak vragen websites en apps om een goed wachtwoord te gebruiken met speciale tekens en cijfers. Maar wat is precies een goed wachtwoord? w@chtwoord007 wordt door veel mensen als een goed wachtwoord gezien, maar stiekem is het voor hackers makkelijk te kraken ⛏. Daarom kun je beter niet meer denken in termen van wachtwoorden, maar **wachtzinnen**.

Zinnen zijn lang én makkelijk te onthouden, twee vereisten voor een goed en sterk wachtwoord. Een wachtzin als elke week eet ik 2 borden boerenkool is goed te onthouden en toch lastig te kraken. Gebruik ook vooral **spaties** in je wachtwoorden; die mogelijkheid wordt vaak vergeten.

Ook is het mogelijk om als wachtwoord **verschillende woorden** achter elkaar te plakken. Gebruik hiervoor Diceware: dat is op dit moment de veiligste manier om een wachtwoord te maken dat je ook daadwerkelijk kunt onthouden.

SAMENGEVAT: DE BESTE MANIER OM JE WACHTWOORDEN TE BEWAREN

- Neem een password manager, liefst één van de vier bovenstaande.
- Gebruik als wachtwoord een wachtzin of Diceware.
- Schrijf dit wachtwoord op en bewaar het op een veilige plek, zodat je nooit de toegang tot je password manager verliest.
- Laat de password manager willekeurige wachtwoorden met minimaal 20 tekens genereren en opslaan.

ANDERE MANIEREN OM JE WACHTWOORDEN TE BEWAREN

ICLOUD SLEUTELHANGER

Voor mensen die alleen maar Apple-producten gebruiken is de iCloud Sleutelhanger een handige keuze om wachtwoorden te bewaren. De Sleutelhanger, ook wel **Keychain** genoemd, kan wachtwoorden genereren en ze automatisch invullen wanneer je ze nodig hebt. De mogelijkheden zijn wat beperkt vergeleken met andere password managers, maar de Sleutelhanger is verder een veilige keuze, mits je iCloud-account beveiligd is met een sterk wachtwoord en tweestapsverificatie.

IN DE BROWSER

Browsers als **Chrome** en **Firefox** bieden aan om je wachtwoorden op te slaan. Dat is op zich een goede manier om gemakkelijk in te loggen bij vaak gebruikte websites. Het nadeel van wachtwoorden opslaan in de browser is dat ze vaak zwak zijn: veel browsers genereren geen sterke wachtwoorden en als ze het al doen, zoals Chrome, weten veel mensen niet van deze functionaliteit. Een betere keuze is dan ook om een password manager te gebruiken.

EEN WACHTWOORDENBOEKJE

Ook **pen en papier** kan worden gebruikt als een password manager. Zorg ervoor dat je unieke wachtwoorden kiest en het boekje goed opbergt. Maak ook een kopie en bewaar die in een kluis, zodat je altijd een back-up hebt. En berg je boekje met wachtwoorden op wanneer familie, vrienden of de klusjesman langskomen.

Een handige tip is om alle wachtwoorden die in het boekje staan te laten beginnen met **hetzelfde woord**. Dat woord schrijf je dan niet op, maar onthoud je. Als iemand toch jouw wachtwoordenboekje in handen krijgt, kan deze persoon nog steeds niet inloggen op je accounts.

HOUD GESTOLEN WACHTWOORDEN IN DE GATEN

Het blijft daarnaast belangrijk om te controleren of één van je wachtwoorden door hackers is gestolen. De website Have I Been Pwned houdt gehackte websites in de gaten en waarschuwt je zodra jouw gegevens zijn gevonden. Je kunt op deze site met één druk op de knop zien of je gevaar loopt.

Als je je aanmeldt, krijg je zelfs **een melding** zodra blijkt dat jouw e-mailadres in gestolen bestanden voorkomt. Zo weet je precies bij welke dienst welk wachtwoord is gestolen en kun je het meteen aanpassen. Daarna is het grootste gevaar - dat een hacker met jouw wachtwoord inlogt - geweken.

TWEESTAPSVERIFICATIE

Hoe goed je wachtwoord ook is, het kan altijd worden gestolen. Om de gevolgen daarvan te beperken, kun je gebruikmaken van de relatief nieuwe beveiligingsmethode tweestapsverificatie, ook wel **two factor authentication (2fa)** genoemd.

Je activeert tweestapsverificatie per dienst waar je gebruik van maakt. Na het inloggen met je gebruikersnaam en wachtwoord moet je voortaan nog een tweede stap voltooien. Meestal wordt er om een code gevraagd die op je smartphone (via een sms of zogeheten authenticator-app) verschijnt.

Stel dat een hacker jouw gebruikersnaam en wachtwoord heeft, dan zou diegene ook nog toegang moeten hebben tot de code op jouw telefoon. Dat is bijna nooit het geval ⛔. Op deze website zie je bij welke online profielen en diensten je tweestapsverificatie kunt inschakelen. Denk aan Google, Apple, Facebook, Instagram, WhatsApp en Dropbox. Maar vergeet ook zeker niet DigiD, waar je kunt instellen dat je na het inloggen standaard een verificatiecode moet invoeren.

CODE VIA SMS

Inlogcodes via sms ontvang je door je mobiele telefoonnummer aan een online dienst te koppelen. De werking spreekt voor zich: na het ontvangen van de sms 💬 voer je de code die je in het bericht ziet staan in op de website of app waar je wilt inloggen. Hackers kunnen deze sms-codes via een zeer gerichte aanval onderscheppen, maar voor het gros van de mensen **is deze beveiliging voldoende**.

CODE VIA AUTHENTICATOR-APP

Een andere, veiligere manier van tweestapsverificatie is het gebruik van een authenticator-app. Met deze app scan je een QR-code (een soort barcode) van de dienst waarvoor je de beveiliging wilt activeren. Na het scannen verschijnt er een **inlogcode in de app** die iedere dertig seconden wordt ververst. Onder andere 1Password, LastPass Authenticator, Authy en Google Authenticator kunnen deze QR-codes scannen en inlogcodes genereren.

Kijk wel uit met Google Authenticator, want als je de telefoon waarop je die app hebt geïnstalleerd kwijtraakt of reset, ben je al je inlogcodes kwijt. Bij de andere apps worden de inlogcodes gesynchroniseerd op alle apparaten waarmee je ze genereert.

LET OP HET SLOTJE (MAAR VERTROUW ER NIET OP)

Het slotje 🔒 in de webadresbalk van je internetbrowser betekent dat je gebruikmaakt van een versleutelde verbinding. Hierdoor zijn de gegevens die jij verstuurt, zoals je wachtwoord of creditcardgegevens, beveiligd en kan een hacker ze niet zomaar onderscheppen. Houd er dus rekening mee dat je gevoelige informatie alleen invult op websites met zo'n slotje, ook te herkennen aan **https://** voor het webadres.

Wees er ook bewust van dat een slotje niet meteen wil zeggen dat je de website kunt vertrouwen ⃠. Veel phishing-websites die jouw inloggegevens proberen te stelen maken inmiddels ook gebruik van zo'n slotje om je vertrouwen te winnen. Blijf daarom kijken naar het webadres en of dit goed is opgebouwd.

- **Correct**: https://www.facebook.com *(facebook.com is het hoofddomein)*
- **Fout**: https://www.facebook.tech *(.tech is niet de juiste domeinextensie)*
- **Fout**: https://facebook.inlog.net *(inlog.net is hier het hoofddomein)*
- **Fout**: https://www.faceb00k.com *(er staan twee nullen in plaats van twee keer de letter o)*

MAAK BACK-UPS

Een back-up, de algemeen geaccepteerde term voor een **reservekopie**, geeft je toegang tot je bestanden als er iets fout gaat. Stel: je computer gaat plotseling kapot. Om welke verloren foto's, video's en documenten zou je verdrietig zijn, en welke bestanden heb je nodig voor je administratie? Dat zijn de bestanden om een back-up van te maken.

Een back-up zorgt ervoor dat je belangrijke bestanden veilig zijn, ook als je computer kapotgaat, je telefoon wordt gestolen of een gijzelvirus je computer ontoegankelijk maakt. Met een back-up kun je weer snel aan de slag.

Het valt aan te raden om zowel een **online als offline back-up** te maken. Een online back-up maak je met een clouddienst als Dropbox of Stack, een offline back-up via een externe harde schijf. Controleer regelmatig of alle bewaarde bestanden er nog zonder fouten in staan.

HERKEN PHISHING

Phishing-aanvallen zijn in de meeste gevallen makkelijk te herkennen. Neem bijvoorbeeld een nepmail die ogenschijnlijk van ABN Amro afkomstig is waarin staat dat jouw bankpas is geblokkeerd, terwijl je bij een andere bank zit. **Logisch nadenken** is dan al genoeg om jezelf te beschermen.

Maar een phishingmail kan heel echt lijken. Het is daarom slim om altijd goed naar de afzender van een e-mail te kijken. Als de afzender het adres @abnamro.incasso55.nl gebruikt, weet je dat de mail niet door ABN Amro is verstuurd. Dan zou er nl.abnamro.com staan.

Let ook goed op het **taalgebruik**. In veel phishingmails staan taalfouten of word je aangesproken met Geachte heer / mevrouw. De meeste organisaties weten heus wel wie jij bent en hoe ze je moeten aanspreken.

Vaak proberen phishingmails je **te laten schrikken** 😟, bijvoorbeeld door te beweren dat je bankrekening is geblokkeerd of dat je een incasso moet betalen. Of de e-mails stellen dat je iets hebt gewonnen . Als je het niet zeker weet, bel dan de betreffende organisatie. Gebruik daarbij niet het telefoonnummer uit de e-mail, maar zoek het op via de officiële website.

Inspecteer ook altijd de **linkjes** in een e-mail. Dat doe je door met je muiswijzer op de link te staan zonder erop te klikken. Zo zie je het adres waar de link je naar toe wil sturen. Hieruit is meestal op te maken of het om phishing gaat of niet. Bij mobiele apparaten druk je lang op de link om deze te kopiëren. Vervolgens kun je deze in een nieuwe e-mail plakken om het volledige webadres te zien.

Als je een e-mail of de linkjes erin niet vertrouwt, surf dan via de browser naar de website van de betreffende organisatie en **log daar in**. Daar vind je vaak ook alle ontvangen berichten en facturen. Je kunt de organisatie ook **altijd bellen** 📞 om te vragen of een ontvangen e-mail echt van dat bedrijf afkomstig is. Nog een belangrijke stelregel:

> *Als het te mooi lijkt om waar te zijn, dan is het dat waarschijnlijk ook.*

Als je een Google-account hebt, helpt deze browser-plugin je tegen phishing-aanvallen: Password Alert. De plugin **stuurt je een waarschuwing** zodra je jouw Google-wachtwoord invoert op een valse inlogpagina. Voor veel mensen is Google en het daarbij horende Gmail hun belangrijkste online account, en daarom kan het lonen om deze officiële Google-plugin te installeren.

KLIK NIET ZOMAAR OP LINKJES

Niet alleen bij phishing geldt dat je niet zomaar op linkjes moet klikken. Het is sowieso goed advies, of je de link nu via e-mail, social media of in een sms-bericht krijgt. Een smartphone kan bijvoorbeeld worden gehackt doordat je op een verkeerd linkje drukt.

Dit gebeurt lang niet bij iedereen en je hoeft ook niet bang te worden van ieder linkje. Maar als je het niet vertrouwt, **inspecteer de link** 🔍 dan eerst op de manier zoals hierboven staat beschreven.

PAS OP MET BIJLAGEN EN CHECK BESTANDEN DIE JE NIET VERTROUWT

Net als bij linkjes moet je ook oppassen met **bijlagen in e-mails**. Via deze weg worden vaak virussen verspreid, waarmee hackers toegang kunnen krijgen tot jouw apparaat. Dat doen ze door in een ogenschijnlijk ongevaarlijk bestand, zoals een Word-document, een virus te verstoppen.

Naast Word-documenten stoppen hackers hun virussen ook in Excel-, PDF-, ZIP- en EXE-bestanden. Het beste is om Word- en Excel-documenten niet op de computer te openen, maar in de website Google Docs. Als er een virus in zit, dan raakt jouw computer niet geïnfecteerd. PDF-bestanden kun je het beste in de browser openen, door het bestand in een browsertabblad te slepen. Of klik met de rechtermuisknop op het PDF-bestand en kies openen met > browser.

Als je een bestand niet vertrouwt, kun je het downloaden ⬇ naar je computer (**niet openen!**) en vervolgens uploaden naar VirusTotal. Deze website analyseert het bestand en vertelt je of het een virus bevat. Houd er rekening mee dat zowel Google als VirusTotal na het uploaden de beschikking hebben over het bestand.

Schakel ook de optie verberg extensies uit voor zowel Windows als MacOS, waardoor je altijd ziet welke extensie een bestand heeft.

KIJK UIT MET OPENBARE WIFI

Openbare wifi-netwerken, zoals Wifi in de Trein, zijn niet veilig. Hackers kunnen meegluren met wat jij online doet en zo proberen om inloggegevens te stelen. Maak gebruik van je **4G-verbinding** of creëer een **met wachtwoord beveiligde hotspot** op je telefoon. Met zo'n hotspot (Android, iPhone) maakt je laptop gebruik van de mobiele verbinding van jouw telefoon om te internetten.

Als je toch van een openbaar wifi-netwerk gebruik wilt maken, zorg er dan voor dat je alleen inlogt bij websites met **een slotje**. Deze gegevens worden versleuteld en zijn voor anderen niet zomaar in te zien. Dit advies geldt ook voor wifi-netwerken van restaurants en hotels : die zijn dan wel met een wachtwoord beveiligd, maar worden nog steeds door veel mensen gebruikt.

Let ook goed op bij het welkomstscherm dat je soms te zien krijgt. Soms wordt er gevraagd om een app, softwareprogramma of certificaat te installeren. Dat is **absoluut niet nodig** om verbinding met het internet te maken, en mogelijk een teken dat een hacker toegang tot jouw smartphone of laptop wil. Vraag het desnoods na bij de aanbieder van het wifi-netwerk.

Tot slot is het belangrijk om te beseffen dat een wifi-netwerk met een wachtwoord niet per se veilig is. Ook deze wifi-netwerken kunnen in handen zijn van een criminele hacker.

GEBRUIK EEN VPN

Het valt ook sterk aan te raden om een **virtueel particulier netwerk (VPN)** te gebruiken zodra je met een openbaar wifi-netwerk verbindt. Een VPN bouwt een digitale tunnel waar jouw dataverkeer doorheen gaat. Hierdoor zien anderen niet wat jij op het internet doet. Op die manier bescherm je jezelf tegen digitale inbrekers.

De meeste mensen hebben dankzij Netflix wel eens van een VPN gehoord. Met zo'n VPN kun je doen alsof je **uit een ander land** komt, door bijvoorbeeld met een Amerikaanse server te verbinden. Op die manier is het met sommige VPN-diensten mogelijk om het uitgebreide Amerikaanse aanbod van Netflix te zien.

Een VPN is ook handig als je niet wilt dat jouw internetprovider weet wat jij allemaal op het internet uitspookt. Je kunt een VPN-verbinding altijd aan laten staan op je computer. Het nadeel van een VPN is dat je internetverbinding er **iets langzamer** van wordt.

Van de betaalde VPN-diensten zijn de gemakkelijkste Private Internet Access, NordVPN en Freedome, die respectievelijk 3, 5 en 6 euro per maand kosten. AirVPN en Mullvad zijn voor de gevorderde gebruiker.

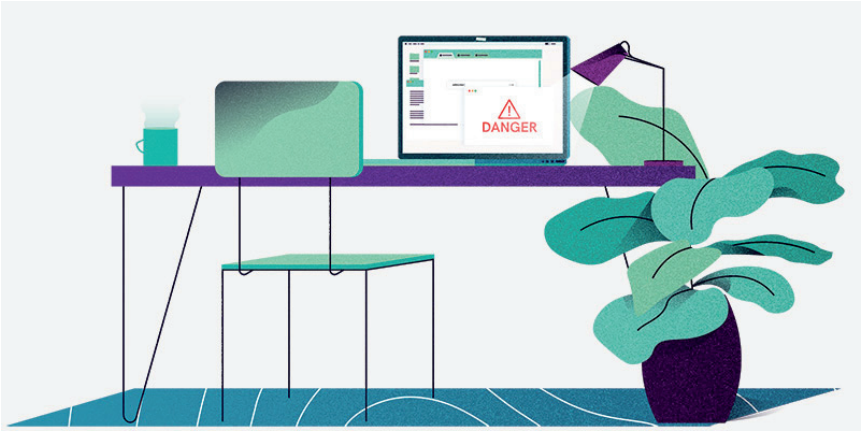
Gebruik geen gratis VPN-dienst. Deze diensten blijken veelal jouw privé-informatie te verkopen, bijvoorbeeld welke websites je bezoekt. Mocht je krap bij kas zitten en geen VPN kunnen veroorloven, dan kun je altijd een gratis account van TunnelBear of WindScribe gebruiken. Met zo'n gratis account krijg je elke maand respectievelijk 500 megabyte of 10 gigabyte dataverkeer, genoeg voor die paar keer dat je met een openbaar wifi-netwerk wilt verbinden.

LAAT JE SPULLEN NIET ONBEHEERD ACHTER

Deze tip lijkt misschien voor de hand liggend, maar je ziet nog vaak genoeg laptops op tafels staan van mensen die even naar de wc 🚽 zijn. Naast het risico dat je eigendom kan worden gestolen, dreigt ook het gevaar dat iemand met kwade bedoelingen jouw apparaat gebruikt. Dat kan gebeuren als de laptop niet is vergrendeld of dichtgeklapt.

Stel daarom altijd een korte tijd (1 minuut) in waarna je laptop zich **automatisch vergrendelt**. Als je dan plotseling weg moet van je computer en je vergeet hem mee te nemen, dan is het apparaat binnen een minuut niet meer toegankelijk voor anderen. In het algemeen geldt: neem je laptop mee als je van je plek gaat.

COMPUTER



We gaan als eerste aan de slag met de computer 💻, het apparaat dat het gemakkelijkst te hacken is. De meeste virusinfecties komen voor op Windows-computers.

VIRUSSCANNERS HEBBEN NOG STEEDS NUT

Windows-computers zijn standaard voorzien van een virusscanner, genaamd Defender. Dat is een goed programma, maar ook Kaspersky Anti-virus en BitDefender (beide 30 euro per jaar) scoren de afgelopen jaren goed.

In Defender zit een functie die je belangrijkste mappen beschermt tegen ransomware of andere schadelijke software die met je bestanden knoeit. Deze optie schakel je in bij Defender via Virus- en bedreigingsbeveiliging > Instellingen voor virus- en bedreigingsbeveiliging > Controlled Folder Access. Daar kun je ook extra mappen toevoegen, zoals een map met zakelijke documenten of familiefoto's 👨‍👩‍👧.

Een tweede tip is het Nederlandse Hitman Pro.Alert (30 euro per jaar). Dit programma gebruik je naast een virusscanner en beschermt tegen malware die kwetsbaarheden in je computer misbruikt om bijvoorbeeld mee te kijken met wat je typt ⌨.

Voor Mac-computers is een virusscanner niet per se nodig: het besturingssysteem maakt het voor malware moeilijker om je computer te infecteren. Daardoor zijn er weinig virussen in omloop voor Apples besturingssysteem. Mocht je er toch één willen, dan zijn Kaspersky Anti-virus (37 euro per jaar), BitDefender (39 euro per jaar) en ESET Security (30 euro per jaar) goede keuzes.

Het loont om voor een virusscanner te betalen: deze software is vaak beter en uitgebreider. Als je niet in staat bent om ervoor te betalen, kun je het beste het gratis Avast of AVG downloaden en installeren.

ZET AUTOMATISCHE UPDATES AAN

Zoals je hierboven al las: updaten is belangrijk. Daarom is het aan te raden om updates **automatisch** te laten installeren. Dit kun je doen voor Windows en MacOS, maar sinds kort ook voor software als de Chrome-browser.

Het is daarbij verstandig om te controleren of een melding om je software te updaten legitiem ✓ is. Veel virussen worden verspreid via een nepmelding, zoals een update voor Adobe Flash Player. Deze meldingen verschijnen meestal via een website. Als je er zeker van wilt zijn, open dan het betreffende programma en kijk handmatig of er een update beschikbaar is.

GEBRUIK CHROME EN DEZE DRIE EXTENSIES

Chrome is op dit moment de veiligste en meest gebruiksvriendelijke browser die je kunt gebruiken. Ook Firefox, Safari en Edge zijn goede keuzes, zolang je Internet Explorer maar mijdt. Installeer sowieso deze drie extensies:

UBLOCK ORIGIN

Adblocker uBlock Origin is een gratis extensie die reclame en trackers op het internet blokkeert. Het beschermt tegen zogeheten malvertising: virussen die via online advertenties worden verspreid. Daarnaast houd je spionerende bedrijven buiten. In tegenstelling tot bekendere namen als Adblock en Adblock Plus heeft uBlock Origin geen discutabel verdienmodel.

Wees er wel bewust van dat je met een adblocker broodnodige inkomsten van websites ontneemt. Door je favoriete websites op de whitelist te zetten, kun je een bedrijf of persoon toch aan jouw bezoek laten verdienen.

HTTPS EVERYWHERE

HTTPS Everywhere forceert wanneer het kan een beveiligde https-verbinding. Als een aanvaller probeert jouw verbinding te onderscheppen om je vervolgens naar een website met een onbeveiligde (en dus af te luisteren) verbinding te sturen, wordt deze poging door HTTPS Everywhere geblokkeerd. De extensie is gratis te downloaden.

PDF VIEWER

Criminelen verstoppen regelmatig malware in PDF-bestanden, omdat de software waarmee deze wordt geopend (Adobe Reader) vaak beveiligingslekken bevat. Je kunt PDF-bestanden daarom beter openen in de browser: dat doet PDF Viewer, een gratis extensie voor Chrome. De browser opent standaard al PDF-documenten, maar met deze extensie krijg je meer functies, zoals een document doorzoeken. Firefox heeft ook een optie om PDF-bestanden in de browser te openen.

Let wel goed op welke extensies je installeert en installeer er niet te veel. Extensies kunnen verregaande rechten hebben en in sommige gevallen zien wat je allemaal in de browser typt. Je kunt per extensie zien welke permissies het heeft.

SCHAKEL JAVASCRIPT EN MACRO'S UIT EN ZET JE FIREWALL AAN

Hackers maken vaak gebruik van specifieke opties in populaire programma's om je computer met malware te infecteren. Door deze opties uit te schakelen, maak je het aanvallers lastiger. Het gaat om Javascript in Adobe Reader en de macro's in Microsoft Office. Schakel ze **beide uit**.

Een firewall moet je juist inschakelen, omdat dit systeem je tegen aanvallen van buitenaf beschermt. Doe dit bij MacOS en het liefst ook op jouw router; bij Windows staat de firewall standaard al ingeschakeld. Mocht je nog een extra beveiliging naast je firewall willen hebben, dan kun je kijken naar Little Snitch voor MacOS of GlassWire voor Windows. Deze apps houden in de gaten 🔎 welke apps met het internet verbinden.

VERMIJD FLASH

Ooit was Flash een belangrijke technologie voor het kijken van filmpjes en spelen van spelletjes 🎮, maar de software is inmiddels zwaar verouderd en daardoor **gevaarlijk**. Het beste is om Flash te mijden. In veel browsers staat Flash al standaard uitgeschakeld en moet je het speciaal inschakelen. Doe dit alleen als je de website die gebruik wil maken van Flash vertrouwt.

In het gros van de gevallen maken websites gebruik van betere technologieën, zoals HTML5, om interactieve elementen als video's en spelletjes te tonen. Flash-maker Adobe trekt in 2020 definitief de stekker uit de software en raadt iedereen al een tijd aan om geen gebruik meer te maken van Flash.

BEVEILIG JE ROUTER

Veel mensen vinden het lastig om hun router, het apparaat dat toegang tot het internet biedt, goed te configureren. Dat is begrijpelijk: routers zijn **zeer lastige apparaten** . Omdat elke router anders werkt, zul je zelf in de (online) handleiding moeten opzoeken hoe je deze tips doorvoert.

- Beveilig je wifi-netwerk met de optie WPA2-AES en een lang wachtwoord en schakel Wifi Protected Setup (WPS) uit
- Schakel UPNP uit. Deze technologie is **onveilig** en geeft gemakkelijker toegang tot jouw netwerk en apparaten
- **Update** je router-software
- Maak een **gastnetwerk** aan met wachtwoord om je gasten en slimme apparaten als beveiligingscamera mee te laten verbinden

- Zorg ervoor dat je wifi-netwerk niet naar jou **te herleiden** valt. Noem het dus niet Familie Jansen
- **Kijk uit** met port forwarding: zet alleen poorten open die je echt nodig hebt

USB-STICKS EN SLIMME APPARATEN

Een bekende truc van hackers is om het slachtoffer een **geïnfecteerde usb-stick** in zijn of haar computer te laten steken, waarna het apparaat wordt overgenomen. Kijk daarom altijd goed uit met usb-sticks, of je ze nou op straat vindt of van iemand krijgt . Als je een usb-stick niet vertrouwt, laat er dan een professional naar kijken of gooi het stickje weg.

Ook kun je jezelf afvragen of je al die slimme internet-of-things-apparaten nodig hebt. Is het echt essentieel dat de waterkoker met je wifi kan verbinden? Is het belangrijk dat de Barbie van je zoon of dochter een camera heeft die met het internet is verbonden? Al deze slimme apparaten zijn **toegangspunten** waarmee hackers jouw netwerk kunnen binnendringen.

Daarnaast kunnen hackers deze apparaten overnemen. Dit gebeurde bij de slimme beveiligingscamera van de Action. Hackers konden meegluren en via de microfoon mensen laten schrikken . Koop daarom alleen slimme apparaten die je écht nodig hebt en het liefst van betrouwbare merken.

VEILIG INTERNETBANKIEREN

Sommige mensen zijn bang om hun bankzaken online te regelen. Dat hoeft niet: internetbankieren is de laatste jaren **erg veilig** geworden. Je kunt de website of mobiele app van jouw bank gebruiken om betalingen over te maken. In de meeste gevallen is de app de veiligste keuze: op een recente versie van Android en iOS is het voor criminelen lastig om dit soort apps over te nemen.

CHECK KORTE LINKJES

Korte linkjes worden ontzettend veel gebruikt op het internet: ze maken simpel gezegd een lange link korter. Eén van de bekendste diensten daarvoor is Bit.ly. Maar korte linkjes worden ook vaak gebruikt om **gevaarlijke websites te verhullen**. Daarom is het verstandig om korte linkjes te checken, zodat je weet waar je uit komt. Dat kan met het Nederlandse Check Je Linkje, dat heel simpel laat zien waar je uitkomt en of die website mogelijk gevaarlijk is. Voor de meer geavanceerde gebruikers is er Urlscan.io.

BESTANDEN VERWIJDEREN

Bestanden die je verwijdert kunnen vaak nog met speciale programma's worden hersteld . Om je daartegen te beschermen, gebruik je Eraser. Met dit programma voor Windows verwijder je de bestanden volledig van je harde schijf. Voor MacOS is de gratis app Permanent Eraser een goede keuze.

PLAK JE WEBCAM AF EN KIJK OM JE HEEN

Criminele hackers kunnen meegluren met je webcam. Het Openbaar Ministerie raadt zelfs aan om daarom je webcam standaard af te plakken. Op die manier kan een aanvaller jou niet chanteren met foto's en video's van privémomenten, zoals tijdens omkleden, zelfbevrediging of seks . Door een stukje tape over je webcam te plakken, maak je dit onmogelijk. Er zijn ook elegantere opties zoals het Nederlandse CamHatch (10 euro) of het Zwitserse Soomz (9 euro voor drie stuks). Op de Chinese webwinkel AliExpress vind je veel goedkope webcamcovers.

Als je veel onderweg bent en vaak met je laptop in de trein of een koffietentje zit, **kijk dan regelmatig om je heen**. Zijn er mensen die mee kunnen lezen met wat je typt? Zien ze geen gevoelige informatie op je beeldscherm, zoals een wachtwoord, telefoonnummer of je huisadres? Wees er bewust van dat je in een openbare ruimte werkt.

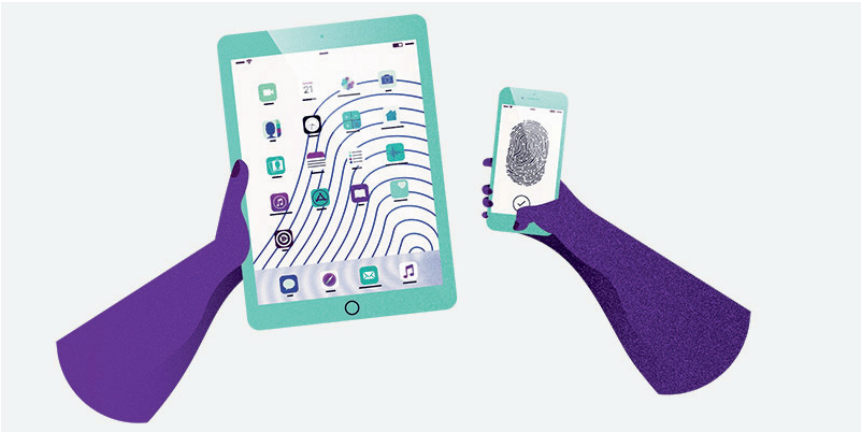
KIES EEN CHROMEBOOK

Heb je niet zo veel technische kennis maar wil je wel graag browsen, e-mailen en video's kijken? Dan is een Chromebook een **slimme keuze**. Deze laptop is goedkoop en zeer veilig, omdat er alleen Googles Chrome-browser op draait. Hackers en hun virussen maken hierdoor minder kans om jouw computer te infecteren. Met de laptop kun je verder alles wat je normaal ook in de browser doet. Heb je iets meer geld te besteden? Dan is een **iPad met toetsenbord** ook een goede keuze om je online zaken te regelen.

AF EN TOE EEN HERINSTALLATIE KAN GEEN KWAAD

Probeer eens in de drie jaar je computer opnieuw te installeren. Dat houdt in: een backup maken, vervolgens de harde schijf wissen en daarna het besturingssysteem (Windows, MacOS) opnieuw installeren. Je computer wordt er niet alleen sneller van, alle overbodige en mogelijk schadelijke programma's en bestanden 🗃 worden tevens gewist.

TELEFOON EN TABLET



De smartphone 📱 is voor velen het belangrijkste apparaat in hun leven. Daarom is het extra belangrijk om dit apparaat, of je nu een Android of iPhone hebt, goed te beveiligen.

NEEM EEN IPHONE

Oké, dit is een beetje kort door de bocht, maar in het algemeen geldt: iPhones zijn **beter beveiligd** dan Android-telefoons. Daarom hebben mensen die meer risico lopen om gehackt te worden, zoals advocaten 👩‍⚖️ en politici 🤴, meestal een iPhone. Daarnaast worden iPhones vijf jaar lang van updates voorzien.

De best beveiligde Android-telefoons komen van Google en worden uitgebracht onder de naam **Pixel** (voorheen Nexus). Google werkt er hard aan om Android zodanig aan te passen dat fabrikanten als Samsung, Huawei en OnePlus gemakkelijker updates kunnen uitbrengen.

SNEL UPDATEN

Deze tip staat weer hoog in het lijstje: update altijd **zo snel mogelijk** ⏰ jouw mobiele apparaten. Updates dichten beveiligingslekken waarmee je smartphone of tablet door een hacker kan worden overgenomen.

Daarnaast is het belangrijk om regelmatig je apps te updaten. Ook apps kunnen lek zijn, waardoor een aanvaller toegang krijgt tot jouw privégegevens.

SCHAKEL ENCRYPTIE IN

Encryptie zorgt ervoor dat jouw gegevens, zoals je berichtjes en foto's, in een **digitale kluis** worden bewaard. Bij alle iPhones en de meeste Android-telefoons staat encryptie standaard ingeschakeld, maar bij sommige Android-toestellen moet je dit handmatig doen. De optie voor encryptie vind je via Instellingen > Beveiliging.

Stel: iemand vindt jouw telefoon en koppelt hem aan een computer. Encryptie zorgt er dan voor dat diegene niet al jouw chatgesprekken en foto's kan zien. Dat is alleen mogelijk als de pincode wordt ingevoerd, de sleutel tot jouw digitale kluis. Daarom is het gebruik van **een pincode** ook belangrijk.

GEBRUIK EEN ZESCIJFERIGE PINCODE EN DE VINGERAFDRUKSCANNER

Door een pincode te gebruiken, kunnen anderen niet zomaar in jouw telefoon of tablet komen. Kies een **zescijferige** pincode die alleen jij weet en geen standaardcode, zoals 0-0-0-0-0-0, 1-2-3-4-5-6 of 1-1-2-2-3-3. Ook het gebruik van je geboortedatum is af te raden, net als alle andere cijfercombinaties die zijn gebaseerd op privégegevens. Je kunt bij iPhones en sommige Androids inschakelen dat je telefoon na tien keer een verkeerde pincode invoeren **wordt gewist**. Dat is een extra beveiligingsmethode, maar kan - als je geen backup hebt gemaakt - ook gevaarlijk zijn.

Het gebruik van de **vingerafdrukscanner** is in veel gevallen nog makkelijker. Het werkt snel en is vaak nog veiliger ook, want mensen kunnen je vingerafdruk niet afkijken. Wil je de vingerafdrukscanner tijdelijk uitschakelen? Start dan je toestel opnieuw op. Je moet dan weer de pincode invoeren om toegang tot het apparaat te krijgen. Als je geen vingerafdrukscanner op je Android-telefoon hebt, kun je eventueel ook vergrendeling met **een patroon** gebruiken.

Ook je simkaart is voorzien van een pincode. Deze pas je in je smartphone aan, bijvoorbeeld naar een zescijferige pincode in plaats van de standaardcode 0-0-0-0. Zet ook alle **contactpersonen** die op je simkaart staan over naar je telefoon en verwijder ze dan van je simkaart. Op die manier lek je geen privégegevens van anderen als jij je telefoon verliest of deze wordt gestolen.

INSTALLEER ALLEEN APPS UIT DE APP STORE OF GOOGLE PLAY

Het gros van de malware op smartphones en tablets wordt binnengehaald doordat mensen apps **buiten de officiële app-winkels** om installeren. Dit gebeurt meestal omdat mensen een betaalde app of game gratis willen downloaden. In die 'gratis' app zit dan malware verstopt die bijvoorbeeld je creditcardgegevens steelt. Dit risico geldt voor zowel Android als iOS.

Bij Android is er nog een tweede gevaar: er zijn genoeg apps in Google Play die legitiem lijken maar alsnog malware bevatten. Doe daarom **onderzoek**. Googel de naam van de app, lees reviews en kijk hoeveel installaties er zijn geweest. Installeer dus niet zomaar apps op je Android-telefoon of -tablet.

Het is ook belangrijk om de **rechten** van een app te controleren. Een zaklamp-app heeft natuurlijk geen toegang nodig tot jouw adresboek. Bij zowel Android als iOS kun je per app de rechten controleren en aanpassen. Bij Android ga je naar Instellingen > Apps, bij iOS naar Instellingen > Privacy.

SCHAKEL WIFI EN BLUETOOTH UIT ALS JE HET NIET NODIG HEBT

Via wifi en bluetooth kunnen derden **jou volgen**, bijvoorbeeld de route die je door het station neemt. Als je onderweg geen wifi of bluetooth nodig hebt, is het verstandig om deze opties tijdelijk uit te schakelen via de instellingen van jouw apparaat. Daarnaast bescherm je jezelf zo tegen aanvallen via wifi of bluetooth.

Als je ooit met een wifi-netwerk verbonden bent geweest, maakt je mobiele apparaat daar automatisch weer verbinding mee. Dat is een stukje gemak, maar het brengt ook risico's met zich mee. Een veelgebruikte aanvalsmethode van hackers is om een **nep-wifi-netwerk** aan te maken, zoals Wifi in de trein of McDonald's Free Wifi, waarmee mensen dan automatisch verbinden. Op die manier proberen ze mee te gluren met wat jij op het internet doet en wachtwoorden te onderscheppen.

Het is verstandig om regelmatig je lijst met vertrouwde wifi-netwerken **op te schonen**. Als je verbinding maakt met het wifi-netwerk van een hotel 🛏, verwijder het dan na je verblijf weer uit het geheugen van je telefoon. Dit doe je door via de instellingen naar het wifi-netwerk te gaan en daar op vergeten te drukken. Ook kun je in Android en iOS per wifi-netwerk instellen dat je er niet automatisch mee verbindt.

TOON GEEN NOTIFICATIE-INHOUD

De inhoud van notificaties kan **gevoelig** 🙈 zijn. Misschien stuurt iemand wel zijn of haar wachtwoord via WhatsApp, of ontvang je inlogcodes via sms. Door de inhoud van notificaties te verbergen (Android, iOS) zorg je ervoor dat anderen deze gegevens niet zien. Pas als jij je telefoon ontgrendelt, wordt de inhoud zichtbaar.

MAAK EEN BACKUP VAN JE APPARAAT

Backups zijn **enorm belangrijk**. Mocht je telefoon worden gestolen, dan kun je met een backup altijd weer opnieuw beginnen. Google en Apple bieden opties aan om een volledige backup van je telefoon te maken. Kijk ook naar een backup voor je foto's en video's, voor velen het belangrijkste op hun telefoon. Onder andere iCloud, Google Foto's en Dropbox zijn goede keuzes om je foto's te backuppen. Vergeet geen tweestapsverificatie voor deze diensten in te schakelen.

SOCIALE MEDIA

We delen enorm veel op sociale media . Soms iets te veel en daar maken hackers misbruik van. Deze vorm van data verzamelen wordt Open Source Intelligence (OSINT) genoemd en kan worden ingezet bij een hackaanval.

KIJK UIT MET WAT JE DEELT

Mensen plaatsen geregeld foto's van hun **paspoort, rijbewijs en concertkaartjes** op sociale media. Misschien denk je: *dat is dom*. Dat is het ook, maar het gebeurt nog steeds massaal . De barcode op je concertkaartje kan door een ander worden gebruikt, met een foto van een paspoort en rijbewijs kun je een lening op naam van iemand anders afsluiten.

Kijk dus goed uit met wat je deelt op sociale media. Heb je een vervelende ex die je in de gaten houdt? Plaats dan niet op sociale media waar je op dat moment bent. Wacht je op een pakketje van een webwinkel? Een hacker kan zich voordoen als een medewerker van de webwinkel om vervolgens 'gegevens te controleren'. Het is vooral een kwestie van beseffen **wat voor jou de risico's** zijn.

LET OP JE PRIVÉGEGEVENS

Bij veel bedrijven hoef je enkel je naam, geboortedatum en woonadres op te geven om te verifiëren dat jij het écht bent. Deze gegevens zijn **erg gemakkelijk** online te vinden: mensen vieren hun verjaardag 🎈 op sociale media en vertellen (indirect) waar ze wonen, bijvoorbeeld door een Instagram-foto te plaatsen van hun nieuwe huis 🏠.

Het lukte een hacker om op deze manier een medewerker van een telecomprovider om de tuin te leiden en een telefoonnummer van iemand anders op zijn naam te zetten. Daardoor kreeg hij de controle over de WhatsApp van het slachtoffer. Deze manier van hacken wordt ook wel **social engineering** genoemd, een aanvalstechniek waarbij mensen worden gemanipuleerd.

Daarnaast zijn vaak onbedoeld je antwoorden op **geheime vragen** online te vinden, zoals de naam van je eerste huisdier 🐱 of de geboorteplaats van je moeder. Let hier op.

GOOGLE JEZELF

Wat doet een hacker die informatie over een doelwit wil verzamelen? Juist: de naam van het doelwit **googelen**. Doe dit ook regelmatig bij jezelf, zodat je weet wat er allemaal online over jou te vinden is. Je kunt bijvoorbeeld een melding instellen, zodat je een e-mail krijgt wanneer jouw naam wordt gevonden in de zoekmachine. Ook is het mogelijk om in sommige gevallen gevoelige informatie uit de zoekmachine te laten verwijderen.

ZET JE BERICHTEN OP PRIVÉ EN LOG JEZELF UIT

We plaatsen ontzettend veel berichten op sociale media. Het is daarom goed om per sociaal netwerk te kijken of jouw profiel **op privé** moet worden gezet. Deel je veel over jouw privéleven op Facebook en Instagram? Zet je Facebook-profiel dan op privé en je Instagram-account achter een slotje 🔒. Hetzelfde geldt voor Snapchat.

Twitter is een iets ander verhaal, omdat velen er juist zitten om gehoord te worden. Mocht je een openbaar Twitter-profiel hebben, let dan extra goed op **wat je deelt**: van je locatie- tot privégegevens. Log jezelf ook uit als je geen gebruik meer maakt van het apparaat waarmee je op Twitter bent ingelogd, bijvoorbeeld een openbare computer of de laptop van een vriend.

KIJK UIT VOOR DE KAMER VAN KOOPHANDEL

Veel zzp'ers schrijven zich bij de Kamer van Koophandel (KvK) in met hun **woonadres en privénummer**. Dat is lekker makkelijk en je kunt zo direct met je eigen bedrijfje 💪🔧 aan de slag. Hierdoor duiken helaas ook overal op het internet privégegevens op die aan je bedrijf gekoppeld zijn. Deze gegevens kunnen door hackers worden misbruikt.

Als je jezelf wilt inschrijven bij de KvK, gebruik dan een **werkadres** in plaats van je woonadres. Daarvoor moet je wel een werkruimte hebben. Er zijn ook organisaties waarbij je voor enkele tientjes per maand een inschrijflocatie voor de KvK kunt huren. Gebruik voor de inschrijving ook een ander telefoonnummer, bijvoorbeeld een **prepaid 06-nummer**. Verwerk bovendien **niet je eigen naam** in de naam van je bedrijf. Door geen verwijzing naar je naam te gebruiken, ben je minder goed vindbaar in het handelsregister.

BLIJF ALERT MET GOOGLE ALERTS

Met Google Alerts houd je nieuwe online content in de gaten 👀. Vul als trefwoord je eigen naam in en je weet precies wanneer jouw naam op een website wordt genoemd. Veel interessanter is het om gevoelige gegevens in de gaten te houden, zoals **je e-mailadres, woonadres of telefoonnummer**. Zo weet je precies wanneer een website deze gegevens publiceert en kun je daarna eventueel actie ondernemen.

MAAK EEN VEILIGE KOPIE VAN JE ID

Het is wel degelijk mogelijk om een **veilige digitale kopie** van jouw paspoort, identiteitskaart of rijbewijs 🚗 te maken. De overheid heeft daarvoor een handige app uitgebracht: KopieID. Met de app streep je gevoelige informatie weg, zoals een burgerservicenummer.

Ook kun je met een watermerk het doel van de kopie aangeven, zoals kopie voor hotelovernachting op datum.

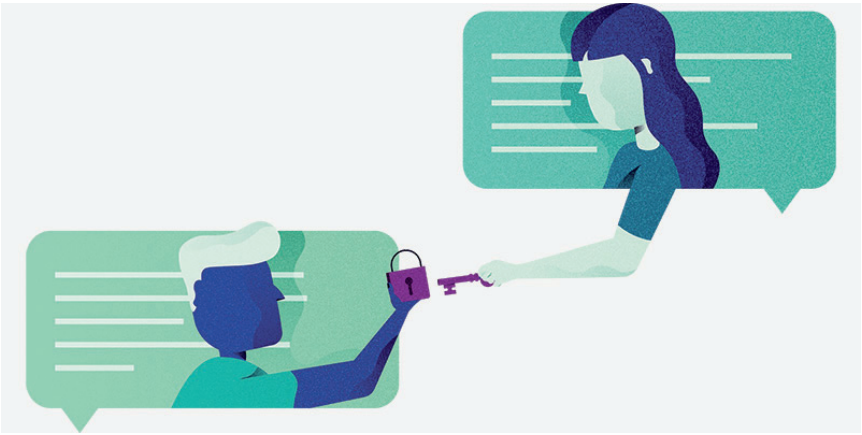
CONTROLEER WELKE APPARATEN ZIJN INGELOGD

Waar ben je eigenlijk allemaal ingelogd? Zit er niet iemand stiekem mee te loeren met je e-mails of WhatsApp'jes? Dat wordt getoond in het overzicht met **actieve sessies** dat je onder andere bij Google, Facebook en WhatsApp in kunt zien. Verwijder alle aangemelde sessies die je niet herkent.

DOE DE SECURITY CHECKUPS

Veel bedrijven bieden de mogelijkheid om je beveiligingsinstellingen na te lopen, waaronder Google, Facebook en Twitter. Je ziet op die manier onder meer wanneer je voor het laatst je wachtwoord hebt gewijzigd en welke apps en diensten allemaal toegang hebben tot jouw account. Als je periodiek deze controles uitvoert, vind je altijd wel een app of dienst die geen toegang meer hoeft te hebben tot jouw account.

CHATTEN EN BELLEN



We chatten 💬 en bellen ☎ wat af. Laten we dat in de toekomst ook zo veilig mogelijk doen. Kortom: hoe communiceer je zonder dat anderen mee kunnen lezen of luisteren?

END-TO-END-ENCRYPTIE

Sinds april 2016 is Nederland **veel veiliger gaan communiceren**. Die maand werd WhatsApp voorzien van end-to-end-encryptie. Dit zorgt ervoor dat alleen de zender en ontvanger een bericht kunnen lezen. Als iemand anders het bericht onderschept, ziet diegene een brij van onleesbare tekens.

Je kunt het vergelijken met het versturen van een ansichtkaart. Je schrijft wat op de achterkant en plakt er een postzegel op. Bij normale encryptie kan de postbode (in dit geval WhatsApp) lezen wat op de ansichtkaart staat. Bij end-to-end-encryptie stop je de ansichtkaart in een **verzegelde envelop** ✉, waardoor alleen de ontvanger het bericht op de kaart kan lezen.

End-to-end-encryptie werkt niet alleen met berichtjes, maar ook bij het versturen en ontvangen van foto's, video's, documenten en locatiegegevens. Daarnaast kun je ook telefoon- en videogesprekken met end-to-end-encryptie beveiligen.

WHATSAPP EN FACEBOOK

WhatsApp is eigendom van Facebook, een bedrijf dat geld verdient met het verzamelen van zo veel mogelijk informatie over zijn gebruikers. Door end-to-end-encryptie weet Facebook niet wat voor berichtjes of foto's jij stuurt. Facebook kan wel zien met wie je contact hebt en wanneer, ook wel **metadata** genoemd. Wees daar dus bewust van.

ALTERNATIEVEN VOOR WHATSAPP

De keuze voor een chat-app is heel persoonlijk. Sommigen houden van gemak, anderen willen hun privacy zo veel mogelijk beschermen. Hieronder vind je vijf alternatieven voor WhatsApp.

SIGNAL

Signal is de veiligste en meest privacyvriendelijke chat-app. Net als WhatsApp kun je de app ook op een computer gebruiken en is het mogelijk om berichtjes na een bepaalde tijd (van enkele seconden tot een week) automatisch te laten verwijderen. Daarnaast slaat Signal nauwelijks gegevens op over zijn gebruikers. De app ziet er alleen niet zo mooi uit en heeft ook minder functies dan de concurrentie.

TELEGRAM

Telegram is geen veilige keuze omdat berichten standaard in de cloud worden opgeslagen. Dit vinden sommigen fijn: als je van telefoon wisselt kun je direct beginnen waar je was gebleven. Tegelijkertijd is het opslaan van al je berichten, foto's en video's in de cloud een groot risico. Mocht je toch voor Telegram kiezen, wees daar dan bewust van. De reden dat mensen toch voor Telegram gaan is dat het één van de meest gebruiksvriendelijke chat-apps is.

IMESSAGE

Apples chat-app werkt alleen met iPhones en iPads. Berichten worden versleuteld met end-to-end-encryptie en je kunt ook je Macbook of iMac gebruiken om berichtjes te sturen.

iMessage ondersteunt allerlei andere apps, waardoor je bijvoorbeeld gemakkelijk in een chatgesprek geld terugvraagt, een Uber boekt of je navigatieroute deelt. Apple bewaart wel metadata voor maximaal een maand, dus houd daar rekening mee.

THREEMA

Het Zwitserse Threema is een geliefde chat-app onder journalisten, omdat je alleen een gebruikersnaam deelt om met elkaar te communiceren. Op die manier hoeft een journalist zijn of haar telefoonnummer niet openbaar op het internet te zetten. De app heeft een fraai design en veel functies, maar ook één nadeel: Threema kost 2,99 euro, waardoor het aantal gebruikers veel lager ligt dan bij gratis chat-apps.

WICKR ME

Wickr Me is vergelijkbaar met Threema: ook bij deze app heb je geen telefoonnummer of e-mailadres nodig om een account te creëren. Je kunt automatisch verdwijnende berichten instellen, de app op meerdere apparaten gebruiken en groepen creëren. In tegenstelling tot Threema is Wickr Me gratis.

WIRE

Het Zwitserse Wire heeft in korte tijd een grote groep fans gekregen. Dat is niet heel vreemd: de app baseert zijn encryptie op die van Signal en combineert een fraai design met de flexibiliteit van Telegram. Zo kun je Wire overal tegelijkertijd gebruiken, of je nu op je smartphone, computer of via de browser wil chatten. Naast berichten sturen kun je ook (video)bellen, bestanden delen en gifjes versturen - en dat allemaal versleuteld met end-to-end-encryptie.

BERICHTEN AUTOMATISCH LATEN VERWIJDEREN

Wat je niet hebt, kan ook niet worden gestolen. Dat geldt ook voor chatberichten. Voer je gevoelige gesprekken met iemand en wil je dat niemand ze leest? Schakel dan automatisch verdwijnende berichten □□ in. Onder andere Signal, Telegram, Wickr Me en Wire ondersteunen deze functie.

BELLEN EN VIDEOBELLEN

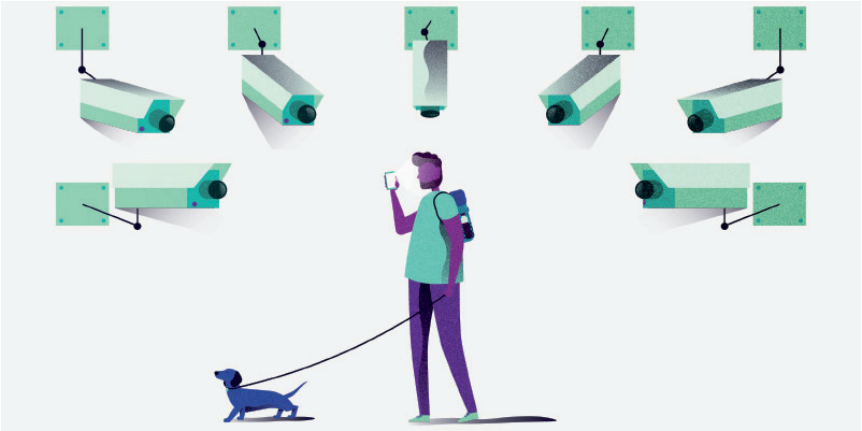
Met onder andere WhatsApp, Signal en FaceTime kun je **bellen met end-to-end-encryptie**. Dit houdt in dat de dienst die je gebruikt je niet kan horen of zien. Deze apps zijn ook aan te raden als je gevoelige gesprekken wilt voeren. Als je een keer met je neef uit Australië wilt videobellen, is Skype - dat niet van end-to-end-encryptie is voorzien - geen probleem.

Het normale bellen is voor het gros van de mensen ook een veilige manier om te communiceren. Een hacker kan niet zomaar jouw telefoonverbinding overnemen. Dat moet dan echt een gerichte aanval zijn van bijvoorbeeld een opsporingsdienst. Daarover later meer.

E-MAIL

In tegenstelling tot veel chat-apps is e-mail juist **niet veilig**. E-mail bestaat anno 2018 uit een stel aan elkaar geknoopte technologieën die zorgen dat het werkt, maar niet dat het veilig of betrouwbaar is. We gebruiken e-mail omdat het zakelijk en algemeen geaccepteerd is, maar verstuur er zo min mogelijk gevoelige informatie mee.

GEAVANCEERD



Allereerst complimenten dat je al zo ver bent gekomen 🖐. Je kennis van online veiligheid is al flink toegenomen. Hieronder vind je verschillende geavanceerde tips 🔧 om je beter tegen online surveillance of vastberaden hackers te weren.

DENK NA OVER WAT VOOR JOU DE GEVAREN ZIJN

Het is belangrijk om na te denken over jouw threat model, oftewel wat **voor jou de gevaren zijn**. Ben je een vrouw 💁 op het internet? Dan kan het zijn dat je vervelende mannen achter je aan krijgt. Ben je een journalist? Dan is het mogelijk dat de overheid je in de gaten houdt. En ben je iemand met een computer en bankrekening? Je snapt hem al: iedereen kan een doelwit zijn.

Neem gepaste maatregelen met betrekking tot jouw threat model. Er zijn heel veel maatregelen in deze handleiding die iedereen zou moeten nemen, omdat veel gevaren voor iedereen gelden. Maar als activistische feminist 💪 met een Twitter-account is het waarschijnlijk stukken belangrijker dat je jouw huisadres en mobiele telefoonnummer afschermt dan voor het gros van de mensen op Twitter.

Elke situatie is anders en vergt een andere aanpak. Er is dan ook **geen gouden regel die je tegen alles beschermt**. Stel: je denkt dat je gewelddadige partner jou in de gaten houdt, bijvoorbeeld door in te loggen op je e-mail of via WhatsApp Web mee te lezen met jouw berichtjes. Dan kun je beter de chatfunctie van het spelletje Wordfeud gebruiken om een vriend te informeren over jouw situatie, een communicatiemiddel dat je partner hoogstwaarschijnlijk niet in de gaten houdt.

HERKEN SPEAR PHISHING

Laten we dan beginnen met de moeilijkste tip, want **spear phishing** is ontzettend lastig te herkennen. Spear phishing is een variant van phishing waarbij de aanvaller een bericht opstelt dat speciaal is gemaakt om jou in de val te lokken. De hacker gebruikt bijvoorbeeld informatie van jouw socialemediaprofielen om zijn spear phishing-bericht van geloofwaardige informatie te voorzien.

Een voorbeeld: je schrijft op Facebook dat je trein een uur vertraging had. De aanvaller kan een nepmail van de NS opstellen waarin je compensatie aangeboden krijgt. Je hoeft alleen even in te loggen waarna je wachtwoord wordt buitgemaakt of een formulier in te vullen na het openen van het formulier leest de hacker mee met wat jij typt.

Gelukkig krijgt het gros van de mensen niet met spear phishing te maken. Spear phishing komt meestal voor bij mensen die **een groot risico lopen** om gehackt te worden, zoals politici, journalisten en advocaten. Desondanks is het altijd goed om op je hoede te zijn. Als je iets niet vertrouwt, zoek dan het bedrijf of de organisatie op via Google en bel het telefoonnummer om te vragen of het bericht daadwerkelijk van de juiste afzender is.

VERSLEUTEL JE HARDE SCHIJF EN BACKUPS

Je kunt Macbooks en iMacs met één druk op de knop versleutelen door FileVault in te schakelen. Het is enorm simpel en zorgt ervoor dat iemand die jouw laptop vindt of steelt niet bij je privébestanden kan. **Schakel deze functie dus direct in**.

Bij Windows is het een ander verhaal. Al jaren maakt Microsoft zijn versleutelingsdienst Bitlocker alleen in de Pro-versie van Windows beschikbaar. Dat is precies de versie die consumenten nauwelijks gebruiken .

Er zijn gelukkig **goede alternatieven**, waarvan Veracrypt de veiligste en betrouwbaarste optie is. Zorg ervoor dat je een backup maakt voordat je begint met het versleutelen van je harde schijf. Het soms urenlang durende versleutelingsproces kan fout gaan en met een backup heb je dan altijd je bestanden nog.

Over backups gesproken: ook die kun je versleutelen. Denk bijvoorbeeld aan een externe harde schijf die je met Veracrypt versleutelt. Een goede app is Cryptomator dat bestanden direct versleutelt en naar de cloud uploadt. Op die manier staan al jouw belangrijke bestanden veilig versleuteld in de cloud. **Bewaar je wachtwoord van de backup goed**: als je deze kwijtraakt heb je geen toegang meer tot jouw bestanden.

MAAK EEN ZEER STERK WACHTWOORD MET DICEWARE

De Diceware-methode wordt door experts gebruikt om een zeer sterk wachtwoord te maken. Diceware maakt gebruik van de willekeurigheid van het gooien van dobbelstenen en een lange lijst met woorden.

Je begint door met de dobbelsteen te rollen. Doe dit vijf keer achter elkaar en noteer bij iedere worp het getal dat je gooit. Je krijgt dan een vijfcijferige reeks die correspondeert met een woord op de hierboven genoemde lijst. Stel, je gooit 3-5-5-5-4, dan is je woord kwibus.

Dit proces herhaal je zeven keer om écht veilig te zijn. Je krijgt dan een reeks met zeven compleet willekeurige Nederlandse woorden, zoals kwibus teugel flits augurk bagger zondag nylon. Wiskundig gezien is de Diceware-methode op dit moment de veiligste manier om een wachtwoord te maken dat je ook kan onthouden.

TWEESTAPSVERIFICATIE MET EEN SECURITY KEY

Het gebruik van een fysieke usb-sleutel, ook wel een security key of beveiligingssleutel genoemd, is volgens experts de **veiligste vorm van tweestapsverificatie**. Je registreert de security key bij diensten als Google, Facebook, Twitter en Dropbox, en vervolgens wordt bij het inloggen om de usb-sleutel gevraagd.

Je steekt de usb-sleutel in de computer of verbindt deze met je smartphone om een inlogpoging goed te keuren. De online dienst controleert of de security key bij jouw account hoort, en de usb-sleutel ziet of jij jezelf bij de juiste website of app aanmeldt ✓. Op die manier word je beschermd tegen phishing en nepwebsites: de inlogpoging wordt alleen goedgekeurd als jouw security key met de juiste online dienst verbindt.

Het valt aan te raden om **twee security keys** aan te schaffen: één voor aan je sleutelbos (die je altijd bij hebt), en één als backup om veilig op te bergen. Beide usb-sleutels koppel je aan een online dienst. Ook is het verstandig om andere, minder veilige opties voor tweestapsverificatie **uit te schakelen**, zoals inlogcodes via sms.

De Zweedse fabrikant Yubico maakt goede beveiligingssleutels. De beste keuze is de blauwe security key, die met alle grote online diensten werkt. Twee stuks kosten 39 euro. De Yubikey 5 met nfc (49 euro) werkt met Android-smartphones, maar slechts zeer beperkt met iPhones. Er is ook een versie voor usb-c-poorten (63 euro).

SCHAKEL AUTOMATISCH INVULLEN UIT EN AUTOMATISCH VERGRENDELEN IN

Sommige wachtwoordbeheerders bieden de mogelijkheid om op websites automatisch je wachtwoord in te vullen. Dat is **niet veilig**. Een aanvaller zou een wachtwoordbeheerder kunnen foppen met een neppagina. Daarom kun je deze optie, die je onder andere in LastPass vindt, uitschakelen. Zo bepaal je zelf wanneer jouw wachtwoord bij een website wordt ingevoerd.

Ook is het verstandig om je wachtwoordbeheerder **automatisch te laten vergrendelen** nadat je de app een X aantal minuten niet hebt gebruikt. Op die manier voorkom je dat je digitale kluis met al je wachtwoorden langer open blijft dan nodig.

DE SMARTPHONE ALS SPIONAGE-APPARAAT

Smartphones zijn **ideale spionage-apparaten**. Opsporingsdiensten kunnen je telefoon tappen en de locatie ervan opvragen, hackers kunnen inbreken en naast je locatie bekijken ook de microfoon of camera inschakelen. Wees hier bewust van.

Android en iOS houden standaard bij **waar je allemaal bent geweest** en deze gevoelige data kan met derden worden gedeeld. Je kunt deze optie uitschakelen bij zowel Android als iOS, waarna je telefoon niet meer constant bijhoudt waar je bent. Dat weerhoudt een opsporingsdienst of hacker er echter niet van om achter jouw locatie te komen.

Eén van de extreme maatregelen die je kunt nemen is je telefoon uitschakelen en in een Faraday-hoesje (die kun je zelf knutselen) of magnetron (zet hem **niet** aan) stoppen. Dat is de enige manier om er zeker van te zijn dat niemand jouw locatie kan peilen of microfoon kan afluisteren.

KIJK UIT MET CHAT-BACKUPS IN DE CLOUD

Veel chat-apps bieden aan om al je chatgesprekken naar de cloud te backuppen, zoals Google Drive en iCloud. Kijk hiermee uit. Alle berichten worden onderweg naar de ontvanger versleuteld met end-to-end-encryptie, maar zodra ze op jouw telefoon staan vervalt deze versleuteling, anders kun je ze niet lezen. Als je dan een backup maakt, worden jouw chats in leesbare vorm en dus zonder versleuteling naar de cloud geüpload. Een opsporingsdienst kan jouw **chatgeschiedenis opvragen**. Houd er ook rekening mee dat jouw berichtjes in een onversleutelde chatbackup van één van jouw contacten kunnen staan.

VEILIGE GEHEIME VRAGEN

Vaak zijn antwoorden op geheime vragen onbedoeld online te vinden, zoals de naam van je eerste huisdier 🐱 of de geboorteplaats van je moeder. Als een hacker de antwoorden op jouw geheime vragen goed invult, kan hij je wachtwoord opnieuw instellen en zo toegang krijgen tot jouw online accounts. Je kunt beter **willekeurige antwoorden** op geheime vragen geven en deze **opslaan met een password manager**.

Houd er wel rekening mee dat de antwoorden in sommige gevallen **uitgesproken** moeten worden, bijvoorbeeld als je een klantenservice belt. In plaats van een ingewikkelde tekenreeks kun je dan beter vier willekeurige woorden vos-fietspad-tosti-bruidsjurk als antwoord kiezen.

DIGITALE ACHILLESHIEL: JE TELEFOONNUMMER

Je mobiele telefoonnummer 📱 is **één van de zwakste plekken** in je online beveiliging. Het nummer geeft namelijk in veel gevallen toegang tot het resetten van je wachtwoord. Dat weten hackers ook, waardoor ze bij een zeer gerichte aanval jouw telecomprovider kunnen opbellen en zich als jou kunnen voordoen. Deze aanval wordt ook wel **sim-swapping** genoemd. Als ze jouw 06-nummer in handen krijgen, hebben ze ook toegang tot jouw online accounts.

Vraag daarom aan je telecomprovider of je **een wachtwoord voor de klantenservice** in kunt stellen. Als je vervolgens telefonisch 📞 iets wilt wijzigen, moet je dit wachtwoord uitspreken voordat je wordt geholpen. Dit kan in Nederland bij T-Mobile en Vodafone. Om helemaal zeker te zijn dat je niet wordt gehackt via sim-swapping, kun je jouw telefoonnummer bij **al jouw online accounts verwijderen**. Het is veiliger om de combinatie van een security key en authenticator-app te gebruiken om je accounts te beveiligen.

LET OP LOCATIEGEGEVENS IN FOTO'S

Zodra je met je smartphone een foto 📷 maakt, worden er allerlei extra gegevens opgeslagen, zoals de datum en het tijdstip wanneer de foto is genomen, maar ook de exacte locatie 🌍. Deze gegevens worden ook wel **EXIF-data** genoemd.

Zodra je een foto deelt op sociale media, zoals Facebook, Twitter, Instagram of WhatsApp, wordt deze EXIF-data verwijderd. Maar in andere gevallen niet, zoals bij het e-mailen of uploaden van foto's naar je website.

Wil je er zeker van zijn dat alle EXIF-data uit de foto is gehaald? Gebruik dan het Nederlandse ImgClean.io, dat via de browser al deze gegevens uit een foto haalt.

VEILIG BELLEN

Als je veilig wilt bellen zonder via een telefoontap **afgeluisterd** te worden, dan is het aan te raden om Signal te gebruiken. Bij Signal worden telefoongesprekken versleuteld met end-to-end-encryptie. Voor veel mensen is deze maatregel overdreven, maar voor risicogroepen als journalisten en advocaten kan het soms nodig zijn.

Bellen via Signal (en eventueel WhatsApp) beschermt je ook tegen **IMSI-catchers**. Dit zijn apparaten die een telefoonmast imiteren, waarna jouw telefoongesprekken en berichtjes via dit apparaat worden afgetapt. IMSI-catchers worden meestal door opsporingsdiensten ingezet, maar zijn ook door hackers in elkaar te knutselen.

VERSLEUTELD E-MAILEN MET PROTONMAIL

ProtonMail is momenteel één van de **meest gebruiksvriendelijke diensten** om versleuteld te e-mailen. De end-to-end-encryptie geldt echter alleen wanneer ProtonMail-gebruikers met elkaar mailen. Bij andere e-mailadressen, zoals Gmail of Outlook, vraagt ProtonMail of je een wachtwoord wilt instellen. De ontvanger kan de e-mail alleen openen met dat wachtwoord. Op die manier voegt ProtonMail een extra beveiligingslaag toe. Een account met 500MB is gratis, voor meer opslagruimte en functies betaal je tussen de 5 en 20 euro per maand.

BROWSE MET TOR

De Tor-browser stuurt jouw internetverkeer langs verschillende computers. Op die manier wordt je privacy beschermd: websites weten niet waar je vandaan komt en je provider ziet niet wat jij op het internet doet. Dat is handig voor sommige Nederlanders, maar **soms levensreddend** in landen als Iran en Rusland.

Naast anonimiteit maakt Tor het ook mogelijk om geblokkeerde websites te bezoeken, wat in een land als Turkije erg belangrijk is. Tor biedt ook toegang tot het **dark web**, het gedeelte van het internet dat je met een normale browser niet kunt bezoeken. Op het dark web vind je voornamelijk marktplaatsen voor drugs en wapens, websites waar kinderporno wordt gedeeld en nazistische communities.

Dat is het nadeel van de anonimiteit die Tor biedt: het kan ook door kwaadwillenden gebruikt worden.

Bedenk goed of en wanneer je Tor nodig hebt. Ga je een misstand melden aan de media? Gebruik dan Tor via de openbare wifi in een koffietentje om er zeker van te zijn dat je jouw melding zo anoniem mogelijk doet. Het internet is met de Tor-browser wel een **heel stuk trager**, dus ga er niet Netflix mee streamen 💻. Daarnaast zien websites dat je met Tor surft, waardoor ze soms jouw **inlogpogingen blokkeren**. Het is dan ook aan te raden om niet met Tor te internetbankieren.

GEBRUIK PGP (ALLEEN ALS HET ÉCHT MOET)

PGP, dat staat voor **Pretty Good Privacy**, wordt gebruikt om de inhoud en bijlagen van e-mails te versleutelen met end-to-end-encryptie. Het is al jaren één van de sterkste vormen van encryptie, maar ook ontzettend ingewikkeld in gebruik. Denk goed na of je PGP echt nodig hebt 🤔, anders is het makkelijker om Signal te gebruiken.

Als je PGP nodig hebt maar niet weet hoe je het zelf kunt instellen, kijk dan eerst bij Keybase, een sociaal netwerk waar je relatief makkelijk teksten met PGP kunt versleutelen. Heb je meer functies nodig, zoals het versleutelen van bestanden met PGP, schakel dan de hulp in van een expert. Bij het Privacy Café van Bits of Freedom werken vrijwilligers die regelmatig PGP bij mensen installeren.

OPENWRT OP JE ROUTER

Veel fabrikanten stoppen na een tijd met het updaten van routers. Het is dan aan te raden om OpenWrt te installeren. De software is beschikbaar voor allerlei routers en wordt regelmatig geüpdatet om zo beveiligingslekken 🩹 te dichten.

OpenWrt werkt niet met wifi-modems van internetproviders, die worden door de bedrijven zelf beheerd. Je kunt wel je eigen router kopen en deze aan het wifi-modem van je internetprovider koppelen. Zet de wifi-modem wel in de modus Bridge/DMZ, zodat het apparaat enkel de internetverbinding doorstuurt.

CHAT VIA OTR

Off The Record (OTR) is net als Signal een zeer veilige manier om met anderen te chatten. OTR wordt gebruikt met een e-mailadres en een app op je desktop (Adium voor MacOS, Pidgin voor Windows en Linux) of smartphone (Conversations voor Android, ChatSecure voor iOS). De apps laten je met andere OTR-gebruikers chatten, maar voor velen zal Signal de betere keuze zijn.

DRAAI JE EIGEN VPN

Als je technisch onderlegd bent, kun je zelf de touwtjes in handen nemen en een eigen VPN draaien. De makkelijkste optie is Algo, dat je op een eigen en liefst nieuwe server installeert. Je beheert dan zelf je beveiligde internetverbinding en kunt er vervolgens via al je apparaten mee verbinden. Omdat Algo zo makkelijk op te zetten is, kun je er ook een **tijdelijke VPN** mee creëren.

MAAK JE EIGEN BEVEILIGINGSCAMERA

NSA-klokkenluider Edward Snowden heeft gewerkt aan Haven, een gratis Android-app waarmee je een oude smartphone kunt inzetten als **slimme beveiligingscamera**. Zo'n apparaat komt van pas als je denkt dat een aanvaller fysiek toegang tot jouw apparaten wil krijgen om je te hacken, bijvoorbeeld door een met malware besmette usb-stick in je laptop te steken.

Haven gebruikt de camera's, microfoons, lichtsensor en versnellingsmeter van een telefoon om bewegingen en geluid te monitoren. Leg de oude smartphone in je hotelkamer en je wordt gewaarschuwd zodra iemand de ruimte betreedt. Ook maakt Haven foto's en video's van de inbreker. Snowden noemt Haven dan ook een **digitale waakhond** die je overal mee naartoe kunt nemen.

IPOD TOUCH MET SIGNAL

Smartphones maken constant verbinding met zendmasten om onder andere telefoontjes, sms'jes en data te ontvangen. Dat laat een flink spoor aan (meta)data achter, dat door opsporingsdiensten kan worden misbruikt. Risicogroepen als journalisten, advocaten en politici moeten hier rekening mee houden. Een iPod Touch met Signal is dan een **veilige manier om te communiceren**. De muziekspeler draait op de laatste versie van iOS, heeft toegang tot de App Store en kan via wifi onder andere met Signal bellen. Om een account bij Signal aan te maken, moet je wel een (tijdelijk) telefoonnummer registreren, bijvoorbeeld een prepaid simkaart of VoIP-nummer. Deze tip geldt ook voor iPads (zonder simkaart), hoewel die wat lastiger in je broekzak passen.

NEEM EEN PRIVACYSCHERM

Een privacyscherm plaats je voor het scherm van je laptop, smartphone of tablet, waardoor **pottenkijkers** 👀 niet meer vanaf de zijkant op je scherm mee kunnen kijken. Het enige dat zij zien is een zwart scherm. Zo'n privacyscherm werkt zelfs zo goed dat je de telefoon echt recht voor je neus moet houden om ook maar iets te zien. Ligt de telefoon schuin voor je op de tafel, dan kun je niet eens je berichtjes lezen. Fellowes heeft goede privacyschermen van tussen de 10 en 50 euro.

GEBRUIK EEN 'USB-CONDOOM'

Ja, usb-condoom is een beetje een vies woord, maar het omschrijft precies wat de SyncStop doet: ervoor zorgen dat er tijdens het opladen geen malware op je smartphone of tablet wordt geïnstalleerd. SyncStop laat **alleen stroom** en geen data door. Mocht je ooit jouw smartphone of tablet via een vreemde computer of usb-ingang willen opladen, dan houdt SyncStop een eventuele malware-aanval tegen.

TAILS EN QUBES

Deze twee besturingssystemen zijn voor de experts, want ze zijn lastig in gebruik. Zowel Tails als Qubes draaien vanaf een usb-stick die je in een willekeurige computer kunt stoppen.

Trek de usb-stick eruit en de computer heeft geen idee wat jij precies hebt gedaan. Tails **beschermt je privacy** en biedt daarvoor allerlei apps aan, zoals Tor en Thunderbird met PGP. Qubes biedt de **beste beveiliging** en wordt gebruikt door mensen die het doelwit zijn van (staats)hackers.

Maar onthoud: als je weinig technische kennis hebt kan het gebruik van één van deze twee besturingssystemen juist je online veiligheid verminderen. Probeer daarom altijd apparaten en diensten te gebruiken omdat je ze **snapt en beheerst**, niet alleen omdat je denkt dat het veiliger is. Dat is ook gelijk een goede tip om deze uitgebreide handleiding mee af te sluiten.