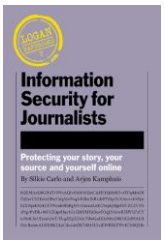

# Persoonlijke informatiebeveiliging

## Je digitale gegevens beschermen

Helma de Boer en Arjen Kamphuis

## Woord vooraf

Dit boekje is gemaakt als instructie om te leren hoe je met digitale informatiebeveiliging kunt omgaan. Het is geschreven in opdracht van het Broodfonds. Je leert hoe je je gegevens (verslag, foto's, bestanden) en je communicatie met anderen beschermt tegen ongeautoriseerde toegang. Ook leer je hoe je online minder sporen kunt achterlaten. Kortom, je leert je digitale gegevens beschermen.




De inhoud van dit boek is gebaseerd op 'Information Security for Journalists' (2014), Logan-handboek 7, geschreven door Silkie Carlo en Arjen Kamphuis. Eind 2016 maakte Helma de Boer de Nederlandse vertaling van het boek. Dit verkorte boekje is ook door haar samengesteld, in samenwerking met Arjen Kamphuis.

Het basisniveau van informatiebeveiliging wordt in dit boekje toegelicht, maar je kunt je informatie op verschillende risiconiveaus beveiligen. Afhankelijk van de dreiging neem je bijpassende maatregelen. Heb je te maken met een hoger risiconiveau (ben je bijvoorbeeld journalist, arts, advocaat, politicus of psychotherapeut/coach), overweeg dan om het uitgebreide boek 'Informatiebeveiliging voor (o.a.) journalisten' (PDF-download website NVJ) te lezen. In dit boek wordt meerdere malen verwezen naar die uitgebreide uitgave. Je herkent de verwijzing aan het logo van de Logan-uitgave met daarin het bijbehorende paginanummer:


## Introductie

Er is sprake van ongeautoriseerde toegang als jouw data wordt misbruikt, onthuld, verstoord, aangepast, geïnspecteerd, opgenomen of vernietigd. Bedreiging komt uit verschillende hoeken en niet alleen van criminelen (hacking, phishing), maar ook van concurrenten, overheden en inlichtingendiensten (sleepnet, massasurveillance, industriële spionage). Dreiging komt zelfs van datahandelaren die profielen van ieder individu willen samenstellen. Bescherming is dus belangrijk. Maar hoe moet dat?

De tips in dit boek moet je makkelijk in je dagelijkse bezigheden kunnen toepassen. Wees dus niet bang; je hoeft geen IT-expert te zijn om iets met de informatie uit dit boek te kunnen. Desondanks als tip: doe het vooral samen en vraag hulp bij het implementeren van de tips en trucs. Samen is leuker en samen weet je meer.

Blijf steeds op de hoogte van actuele veranderingen en nieuwe technologieën, zodat je je kunt blijven beschermen ook als de tijd voortschrijdt. Welke maatregelen neem jij?

NB De suggesties die in dit boek worden gedaan voor productmerken (hardware en software), zijn geen aanbevelingen voor de genoemde merken of hun producten. De besproken flexibiliteit is ook beschikbaar van andere merken.

# Inhoudsopgave

**Hoofdstuk 1: je computersysteem ..... 4**

De hardware ..... 4
Risiconiveaus ..... 5
Kwetsbaarheden van een laptop ..... 6

**Hoofdstuk 2: veilig browsen ..... 7**

Keuze webbrowser ..... 7
Extensies voor verhoging privacy ..... 8
Privacy tijdens het surfen ..... 8

**Hoofdstuk 3: veilig omgaan met data ..... 9**

Data versleutelen met VeraCrypt ..... 9
Harde schijf versleutelen ..... 11
Bestanden veilig online opslaan en delen ..... 11
Bestanden veilig verwijderen ..... 11

**Hoofdstuk 4: onlinecommunicatie ..... 13**

Metadata ..... 13
E-mail ..... 13
Chat/instant-messaging ..... 15
Bellen (telefoon, voice, video) via internet ..... 15
Overige risico's ..... 16

**Hoofdstuk 5: veilig wachtwoordengebruik ..... 18**

**Over de auteurs ..... 20**

# Hoofdstuk 1: je computersysteem

Draagbare hardware-apparaten (laptop, tablet, externe harde schijf of USB-stick) vormen het grootste probleem op het gebied van informatiebeveiliging. Je gaat er immers mee op pad. Als de gegevens op zo'n drager, bijvoorbeeld de laptop of een USB-stick, niet zijn beveiligd met een wachtwoord of als ze niet zijn versleuteld, is het niet veilig om ze mee te nemen als er gevoelige informatie op staat.

Afhankelijk van de specifieke risico's die je loopt en de kennis van een eventuele kwaadwillende, varieert de beschermingsstrategie voor informatiebeveiliging. Meestal is het eenvoudigweg voldoende om je laptop of telefoon steeds bij je te houden, maar het is van belang dat je je bewust bent van de risico's die je loopt en welke kwetsbaarheden je eigen systeem heeft (zelfs als je ze niet wilt of kunt oplossen). Daarom leer je in dit hoofdstuk hoe een laptop in elkaar zit (hardware). We geven tips voor veiliger gebruik (besturingssysteem en algemeen gebruik), je leert het risiconiveau inschatten waar jij mee te maken hebt. Verder krijg je informatie over de aankoop van een veilige laptop. Als we het in dit boek over de laptop hebben, bedoelen we alle fysieke onderdelen inclusief de accu en harde schrijf. Ook kijken we naar hardware die je met je laptop kunt verbinden, zoals een willekeurig toetsenbord, muis, webcam, etc.

## De hardware

Je laptop bestaat in grote lijnen uit de volgende onderdelen:

1. Hardware – alle  fysieke onderdelen die samen een computer vormen, zoals de accu, harde schijf, moederbord en de overige onderdelen in het apparaat, plus de hardware die je met de laptop kunt verbinden (zoals muis, microfoon, en webcam).
2. Firmware – op het moederbord geprogrammeerde basissoftware die instructies geeft over hoe dat apparaat moet communiceren met de andere hardware van je laptop.
3. Het besturingssysteem – Windows, macOS, Linux, etc.
4. Applicaties – je software/programma's.

De grootste risico's voor je hardware/laptop zijn: de kans op diefstal of beschadiging, de kans dat er fysiek mee wordt gerommeld en de kans dat de laptop op afstand wordt benaderd om gegevens te stelen. Tips voor beveiliging:

- Voer steeds de beschikbare updates uit en zorg voor een virusscanner
- Overweeg het gebruik van Linux als besturingssysteem;
- gebruik een webcamcover;
- gebruik geen gratis, onbeveiligde wifi-hotspots;

**Besturingssysteem**
Het besturingssysteem is naast de firmware de belangrijkste software op een computer. Het bestuurt de computer als deze opstart en is de interface waarmee je je computer gebruikt. Bij je aankoop heb je eigenlijk alleen de keuze tussen de besturingssystemen van Microsoft (Windows) en Apple (macOS). Je kunt er ook voor kiezen een ander besturingssysteem te installeren en te gebruiken, zoals Linux (Mint of Ubuntu). Vooral de besturingssystemen Windows en macOS zijn kwetsbaar voor spyware, keyloggers, andere malware en virussen. Die kunnen op allerlei manieren binnenkomen, bijvoorbeeld via een phishing-mail met een onbetrouwbare link, gedownloade software/apps of soms via kwetsbaarheden in je systeem zelf (zogenaamde "achterdeurtjes"). De beste manieren om het

besturingssysteem daar tegen te beschermen: voer updates direct uit als ze beschikbaar zijn en zorg voor een goede virusscanner.

**Linux als besturingssysteem**

Je kunt overwegen om als alternatief het opensourcebesturingssysteem Linux te installeren. De software is niet alleen gratis, ook de broncode – de code waarmee het systeem is gemaakt – is publiek en open. Hierdoor kan een onafhankelijke expert op ieder willekeurig moment de broncode bekijken en zich ervan vergewissen dat er geen beveiligingsfouten in zitten. Opensource-besturingssystemen zijn bovendien minder kwetsbaar voor malware (kwaadaardige software, vaak spyware) en virussen. Dat komt omdat ze veel minder worden gebruikt dan de bekende besturingssystemen van Microsoft en Apple. Hierdoor loont het voor criminelen niet om iets speciaal voor die systemen te ontwikkelen. Je kunt voorgeïnstalleerde besturingssysteem vaak makkelijk verwijderen van Windows-laptops. Een alternatief is om verschillende besturingssystemen naast elkaar te gebruiken. Het is niet aan te raden een besturingssysteem van een Mac te verwijderen, omdat dit negatieve invloed kan hebben op de werking van het complete systeem.


Voor informatiebeveiliging heeft opensourcesoftware altijd de voorkeur boven software met onbekende, gesloten broncode. Wij raden daarom aan om te werken met Linux (versie Mint of Ubuntu) omdat dit veiliger is dan besturingssystemen van Microsoft (Windows) en Apple/Mac (iOS). Je moet er wel mee leren werken (niet moeilijker dan een overstap tussen Windows en Mac). Vraag hulp bij een IT-collega van het Broodfonds en doe het vooral niet alleen.

**Webcamcover**

Verschillende onderdelen van je laptop kunnen worden gebruikt om jou en je werk in de gaten te houden, bijvoorbeeld via de webcam, je microfoon en de wifi-, bluetoothkaart en het 3/4G-modem. Zo kunnen webcams in het geheim op afstand worden bediend. Ook de beelden kunnen worden opgenomen. Een eenvoudige manier om dit op te lossen: plak een sticker of webcamcover over je webcam. Dit is zeker aan te raden voor je telefoon, want via apps is het bijzonder gemakkelijk om de controle over je camera te krijgen.

**Gebruik geen gratis wifi-hotspots**

Ieder onderdeel van je laptop dat connectie met een ander apparaat kan maken (wifi- en bluetoothkaart en 3/4G-modem), kan in het geheim op afstand worden benaderd. Je kunt voorkomen dat iemand met jou meekijkt door geen gebruik te maken van gratis, onbeveiligde wifi-hotspots. Het is namelijk heel makkelijk om bijvoorbeeld in een horecagelegenheid een extra hotspot aan te maken die zich voordoet als gratis inlogpunt van die gelegenheid. Maar onderwijl log jij in via een ander persoon, die ongemerkt alles ziet wat je doet, de zogenaamde man-in-the-middle (MITM). Ook andere onderdelen, zoals de microfoon van je laptop, kunnen kan in het geheim op afstand worden geactiveerd op informatie op te vangen.


## Risiconiveaus

Het op afstand verkrijgen van toegang tot hardware, firmware en chipsets is waarschijnlijk alleen mogelijk door inlichtingendiensten of technologisch geavanceerde, rijke landen. Maar alle technologie wordt door de tijd heen gemakkelijker toegankelijk voor minder machtige groepen. Zelfs als je niet te maken hebt met een hoog risicofactor, is het verstandig om voorzorgsmaatregelen te nemen voor je veiligheid. We leggen hieronder uit welke risiconiveaus er zijn (basis, middelmatig, hoog en top). In dit boek behandelen we alleen het niveau 'basisrisico'.

- **basisrisico**: *sleepnet, ook wel dragnet, (algemene) surveillance, laag niveau individueel hacken, diefstal, datalek, privacy* | Je kunt beginnen met een willekeurige laptop. De meeste systemen zijn redelijk goed te beveiligen tegen de gewone bedreigingen op softwareniveau. Verder kun je jezelf beschermen door je laptop steeds bij je te houden, zodat er geen fysieke interventie of diefstal kan plaatsvinden. Je kunt veel andere risico's vermijden via een goede software- en applicatiekeuze en het updaten daarvan. Bijvoorbeeld een goede onderzoeksjournalist is dit niveau snel ontgroeid.
- **middelmatig risico**: *gerichte surveillance, door een kwaadwillende die voorbereid is of de mogelijkheid heeft om vrij onbeperkt middelen in te zetten* | Gebruik een laptop waarvan je het voorgeïnstalleerde besturingssysteem kunt verwijderen om je eigen systeem te installeren.
- **Hoog risico**: *gerichte surveillance door een inlichtingendienst* | Er is maar een handvol apparaten die op een betrouwbare manier te beveiligen zijn tegen het op afstand benaderen van hardware, firmware en chipset.
- **toprisico**: *gerichte, gestuurde surveillance door een inlichtingendienst* | In situaties met een zeer hoog risico moet je ervoor zorgen dat je ten minste twee laptops hebt waarop alle benodigde beveiligingsmaatregelen zijn uitgevoerd. Eén van beide moet nooit, onder geen enkel beding met het internet worden verbonden. Dat is je "airgap"-laptop: een laptop die nooit online gaat.

## Kwetsbaarheden van een laptop

De laptop die je aanschaft, bepaalt het maximaal bereikbare veiligheidsniveau. Sommige apparaten zijn beter te beveiligen dan andere. Vier punten zijn bepalend zijn voor de maximaal te bereiken mate van beveiliging van het apparaat. Het gaat om: de onderhoudsmogelijkheid van de hardware, de meegeleverde firmware, chipsets en het besturingssysteem. We gaan hier kort op in, zodat je de belangrijkste kwetsbaarheden van een laptop kent.

**Onderhoudsmogelijkheden hardware**
Kies bij voorkeur een laptop waarvan je de behuizing kunt openschroeven. Je kunt dan wat basis-hardware-onderhoud doen en kiezen welke onderdelen je wilt houden, vervangen of zelfs uitschakelen. Laptops van de merken IBM/Lenovo, HP, en Dell zijn vaak geschikt en er is uitgebreide documentatie over de hardware beschikbaar[1]. De behuizing van een MacBook is niet gemakkelijk te openen. Kun je dit wel zelf, houd er dan rekening mee dat hardware-onderhoud ertoe kan leiden dat de garantie vervalt.

**Firmware**
Firmware geeft instructies over hoe de verschillende computeronderdelen met elkaar moeten communiceren. Hackers met voldoende vaardigheden (overheidsniveau) zijn in staat om op afstand controle over je laptop te krijgen via firmware.


**Chipsets**
Sinds rond 2006 plaatst Intel speciale onderdelen in hun chipsets. Hiermee wordt een geautomatiseerd management van systemen over een netwerk mogelijk, maar de functionaliteit kan ook worden misbruikt om spyware te installeren of het systeem op andere wijze te manipuleren. Alle laptops die na 2008 zijn gemaakt, hebben zulke chipsets en zijn daarom kwetsbaar voor deze aanvalsmogelijkheden als ze in een netwerk zijn aangemeld.

---

[1] De genoemde flexibiliteit en documentatie is ook beschikbaar van andere merken – de suggesties die hierboven zijn gedaan, zijn geen aanbevelingen voor de genoemde merken of hun producten.

# Hoofdstuk 2: veilig browsen

In dit hoofdstuk worden een aantal opties aangedragen die helpen om de inbreuk op je privacy tijdens het internetsurfen te minimaliseren in verschillende situaties. Surfen doe je met een webbrowser, zoals Chrome, Internet Explorer/Edge of Firefox. Je loopt allerlei risico's tijdens het surfen, zoals:

- het verzamelen van je identiteitsgegevens (identiteitsfraude), locatie, surfgedrag (inclusief de pagina's die je bezoekt en wanneer);
- het verzamelen van je wachtwoorden en automatisch voor-ingevulde informatie;
- het verzamelen van je locatie (en vorige locaties);
- malware-injectie op je laptop via de browser (kwaadaardige software, soms spyware).

Sommige overheden brengen restricties aan in toegang tot bepaalde websites. In het westen kennen we nauwelijks internetrestricties, maar je ziet dat we wel te maken hebben met serieuze privacy-problemen. Tips voor informatiebeveiliging tijden het surfen:

1. gebruik een goede webbrowser (eventueel Tor-browser om anoniem te surfen);
2. gebruik extensies/plug-ins voor privacy en bescherming tegen trackers (dataverzamelaars);
3. webbrowserpas je privacy-instellingen aan en zoek privé;
4. gebruik een wachtwoordmanager (zie hoofdstuk 5).

## Keuze webbrowser

Van de meeste browsers kun je de functionaliteit verbeteren via uitbreidingen (het toevoegen van extensies, zogenaamde plug-ins). Wij bevelen twee opensource-browsers specifiek aan:

- Firefox als webbrowser voor algemeen gebruik op Linux- en Windows-computers;
- Chromium als webbrowser voor Mac-computers (een opensourcekloon van Google Chrome);


Wil je anoniem surfen, kies dan voor de Tor-browser. Met Tor kun je anoniem surfen en blokkades omzeilen. De browser anonimiseert je locatie en identiteit.

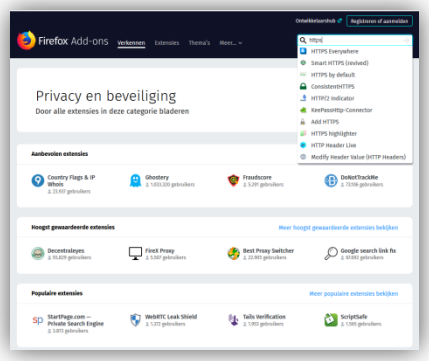
**Onveilige sites herkennen**

Een veilige site herken je aan de url: het internetadresbalkje boven in de browser. Start de url met 'https' dan verschijnt er een slotje in de adresbalk. Zo'n site is geverifieerd en heeft een beveiligde verbinding. Het beveiligingsniveau kan verschillen:

| *url-balk start met* | *status* |
|---|---|
| http://www | Geen beveiligde verbinding, geen verificatie (de site kan wel veilig zijn) |
| https:// | Beveiligde verbinding, verificatie (de site hoeft niet veilig te zijn) |
| Triodos Bank N.V. (NL) | Beveiligde verbinding, verificatie, ter herleiden naar organisatie (je kunt ervan uitgaan dat de site veilig is) |

Staat er een vreemde url die niet past bij de site die je dacht te bezoeken (bijvoorbeeld ‘gogle’ in plaats van ‘google’), dan moeten er alarmbellen gaan rinkelen. Wil je controleren of een site écht veilig is, gebruik dan de tool ‘Veilig browsen, site-status’ van Google.

## Extensies voor verhoging privacy




Als je een algemene webbrowser gebruikt, kun je er zeker van zijn dat je identiteit, locatie en surfactiviteiten worden geregistreerd. Er zijn echter verschillende plug-ins die je kunt installeren om je privacy en veiligheid iets te verbeteren. Er is een keur aan privacy-verhogende extensies te vinden die geschikt zijn voor zowel Firefox als Chromium.

We raden in het bijzonder aan om de volgende opensource-extensies te installeren:

- HTTPS Everywhere: forceert encryptie voor alle verbindingen tussen webbrowser en webserver die je bezoekt.
- NoScript: blokkeert JavaScript. JavaScript is een essentieel onderdeel op verschillende websites, maar de software kan worden misbruikt om je surfgedrag te volgen, je wachtwoorden te lekken en om malware toe te voegen. NoScript is heel effectief, maar je moet daarvoor rechten toekennen aan websites of weigeren, afhankelijk van in hoeverre je de site vertrouwt.
- Ghostery: blokkeert een flinke lijst trackers die je surfgedrag volgen. Let er wel op dat je ‘Ghostrank’ uitschakelt bij ‘Instellingen” → “Opties” omdat Ghostery zelf je data gebruikt voor marketingdoeleinden.
- KeePassX of LastPass: een wachtwoordgenerator en –manager voor Firefox. Zie hoofdstuk 5.

## Privacy tijdens het surfen

Naast het gebruik van de genoemde uitbreidingen in je browser, zijn er nog een paar dingen die je kunt doen om minder sporen online achter te laten. Door iets anders te werk te gaan, wordt het veel moeilijker om je te volgen en je surfgedrag vast te leggen.

- Allereerst zet je bij ‘privacy-instellingen’ van Windows 10 álle knoppen om informatie te delen uit.
- Gebruik startpage.com als zoekmachine. Startpage zoekt in Google, maar Google kan nu je zoektermen niet zien en opslaan.
- Zet het delen van je GPS-locatie (overal) op je telefoon standaard uit.
- Zet ‘webgeschiedenis bewaren’ uit in je Google-account en browser (accountinstellingen → services → webgeschiedenis verwijderen en onderbreken).
- Overweeg het gebruik van een VPN om je surfgedrag te beschermen en eventueel je IP-adres te maskeren. Een VPN-verbinding (Virtueel Privé Netwerk), geeft je een beveiligde (versleutelde) en soms anonieme (omgeleide) toegang tot een netwerk en maakt daarmee de internetverbinding veiliger. Lees meer in de VPN-gids en Bits of Freedom.
- Blijf niet ingelogd bij je Google-account (of andere dienst).
- Gebruik Vimeo in plaats van YouTube waar dat kan. Zo verspreid je je internetsporen.
- Koppel geen diensten (Twitter, LinkedIn, Facebook, etc.), maar log steeds (geautomatiseerd) apart in met verschillende wachtwoorden via je wachtwoordmanager, zie hoofdstuk 5.

# Hoofdstuk 3: veilig omgaan met data

Je moet met verschillende risico's rekening houden als je data opslaat of meeneemt. Risico's waar je mee te maken hebt als je gegevens digitaal opslaat:

- verlies;
- corrupt /onbetrouwbaar/defect raken;
- interceptie (merk je niet) en/of diefstal (merk je wel);
- mogelijk herstellen van 'verwijderde' data door derden;
- anonimiseren ongedaan maken/compromitteren van metadata.

Je kunt je digitale bestanden op verschillende manieren tegen deze risico's beveiligen. In dit hoofdstuk leer je hoe je dat op een veilige manier doet. We bespreken de volgende acties voor informatiebeveiliging:

1. versleutelen van data;
2. op een veilige manier online opslaan en delen van bestanden;
3. op een veilige manier bestanden/data verwijderen;
4. back-up van data;
5. metadata verwijderen.

Om je data te beschermen tegen ongeautoriseerde toegang is het belangrijk om de data te versleutelen. Dat kun je bijvoorbeeld doen met VeraCrypt. Dit is een eenvoudig programma waarmee je bestanden of volledige schijven kunt versleutelen en zelfs het bestaan ervan kunt verbergen.

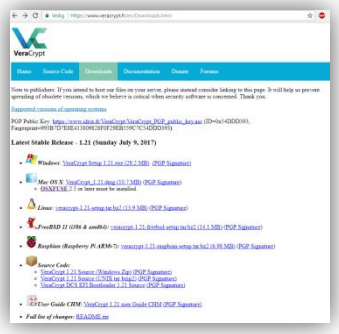
## Data versleutelen met VeraCrypt

VeraCrypt is opensource-software voor het versleutelen van bestanden. Met VeraCrypt kun je een versleutelde container maken die als een soort digitale kluis voor bestanden werkt. Zo'n kluis is beveiligd met een wachtwoord en ziet er in "rust" uit als een gewoon bestand. Als de kluis is gemaakt en er zijn bestanden in opgeslagen, kun je deze naar een extern opslagapparaat verplaatsen, bijvoorbeeld een USB-drive, of je verstuurt de kluis via het internet naar anderen. Zelfs als de kluis met de bestanden wordt onderschept, kan niemand erin kijken, zodat de inhoud ervan veilig blijft. De inhoud is alleen toegankelijk voor degenen met het wachtwoord.

**Belangrijk! Vergeet je wachtwoord niet, want er is geen enkele manier om de data terug te krijgen omdat het bestand is versleuteld. Verlies van wachtwoord betekent verlies van data.*

**Installatie van VeraCrypt**

Download VeraCrypt en installeer deze op je apparaat. De installatie werkt op dezelfde manier als die van andere programma's. VeraCrypt werkt op dezelfde manier in Windows, Mac en Linux-systemen. De versleutelde containers zijn bovendien onderling compatibel op die systemen. Dat helpt je om veilig met andere mensen samen te werken, omdat je niet hoeft te weten met welk besturingssysteem iemand werkt. Hier vind je een uitgebreide tutorial voor VeraCrypt. Mac-gebruikers moeten naast Veracrypt ook FUSE for macOS downloaden.

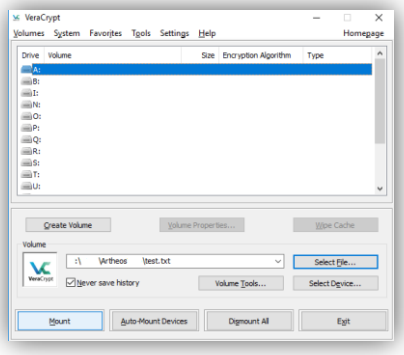


**Een bestand versleutelen met VeraCrypt**

1. Maak een versleuteld volume

Je maakt eerst een leeg bestand aan op de plek die als container gaat fungeren (bijvoorbeeld een leeg kladblok-bestand). Start VeraCrypt. Vervolgens:

- voor een versleuteld volume op:
  - de harde schijf: selecteer 'Volumes' → 'Create New Volume' (creëer nieuw volume) → 'Create an encrypted file container' (maak een versleutelde container voor bestanden) → selecteer 'Standard VeraCrypt volume'→ en selecteer het bestand waarin de container op je computer moet worden opgeslagen. Kies 'ja' als om overschrijven wordt gevraagd. Je kunt het bestand later verplaatsen. Geef de container een onopvallende naam.
  - een USB-stick of externe harde schijf: selecteer 'Volumes' → Create New Volume' → Encrypt a non-system partition/drive' (versleutel een externe partitie of drive). Bij 'Volume Location' kies je 'Select device'. Tip: om de USB-drive te ontsleutelen heb je VeraCrypt ook nodig, dus als je van plan bent om bestanden te ontsleutelen op een computer waarop VeraCrypt niet is geïnstalleerd, zet dan ook het installatiebestand van VeraCrypt op de USB-stick, naast de versleutelde container.
- Het volgende venster is getiteld 'Encryption Options' (versleutelingsopties). De standaardinstellingen voldoen.
- Daarna zie je het scherm 'Volume size'. Selecteer hier de grootte van de container. De grootte bepaalt hoeveel data je in de container kunt opslaan. Je losse bestand mag niet groter zijn dan 4 GB (in verband met de formatmogelijkheden, zie hieronder).
- Vervolgens word je gevraagd het wachtwoord voor het volume in te stellen. Kies een veilig wachtwoord (zie hoofdstuk 8) en ... vergeet deze niet!!!
- Het volgende venster is getiteld 'Format Options'. Selecteer 'FAT'.
- Het programma gaat nu het volume versleutelen. Maak een paar willekeurige muisbewegingen – daarmee kan de computer een betere encryptiesleutel aanmaken – voordat je op 'Format' (formatteren) klikt. Vervolgens wordt het volume aangemaakt. Afhankelijk van de grootte, het gekozen encryptie-algoritme en de snelheid van je computer duurt het aanmaken een paar seconden of wat langer.
- Als het volume is aangemaakt, klik dan op 'Exit' om naar het hoofdscherm van het programma terug te keren.




Gefeliciteerd – je hebt nu een veilig volume aangemaakt.

2. Te versleutelen bestanden in het volume met encryptie plaatsen

Nu kun je het volume openen en daar bestanden in plaatsen. Binnen VeraCrypt kies je een Drive en vervolgens ga je naar 'Select File' (selecteer bestand) → zoek het bestand dat je als container hebt aangemaakt en selecteer deze, kies vervolgens 'Mount' (activeren). Voer het wachtwoord in en klik op OK.

De VeraCrypt-container verschijnt nu op je systeem als een aparte drive (op dezelfde wijze als je C:-schrijf, een USB-stick of een externe harde schijf). Je kunt nu bestanden in de container plaatsen op dezelfde manier zoals je dat met een USB-stick zou doen. Ga naar Mijn Computer of de Finder (Mac), selecteer de gewenste bestanden en sleep ze naar de container.

Als je de bestanden in de container hebt geplaatst, kun je de container sluiten door te klikken op 'Dismount' in VeraCrypt. Het extra volume verdwijnt en de container ziet er nu uit als een willekeurig bestand op je computer.

## Harde schijf versleutelen

Naast het gebruik van bestanden als VeraCrypt-containers kun je er ook voor kiezen om de complete harde schijf te versleutelen. De meeste actuele besturingssystemen hebben een ingebouwde optie om de harde schijf te versleutelen. Zorg ervoor dat je de systeembestanden en programma's op een andere schijf opslaat als je data. De schijf met de data versleutel je.

**Windows** – Zoek op 'Bitlocker' (Configuratiescherm\Systeem en beveiliging\BitLocker-stationsversleuteling) → kies welke schijf je wilt versleutelen en stel eventueel een wachtwoord in. Je kunt er ook voor kiezen om een externe schijf of USB-stick te versleutelen met 'Bitlocker to go'.

**Mac** – Ga naar Systeemvoorkeuren → Security en Privacy → FileVault (kluis) →zet FileVault aan.


**Linux –** Bij installatie kies je voor versleuteling van de home-directory.

## Bestanden veilig online opslaan en delen

Doordat we al jarenlang wereldwijd met software van Microsoft (One Drive, Dropbox) en Google (Drive) werken, kunnen we nauwelijks nog om hun producten heen. Dat is een probleem zodra je gevoelige data toevertrouwt aan de cloud-omgeving van zulke organisaties. Kies liever voor dataopslag in Europa (bij een Europees bedrijf) en betaal er eventueel voor. Die organisaties moeten zich aan de strengere Europese wetgeving houden.


Bijvoorbeeld Stack van TransIP is een goede clouddienst voor opslag (tot 1TB gratis opslagruimte). De data worden automatisch versleuteld opgeslagen. Stack geeft bovendien goede mogelijkheden voor het uitwisselen van grotere bestanden (inclusief vervaldatum, downloadlink en wachtwoord-beveiliging). Stack is een aanrader boven bijvoorbeeld WeTransfer of Dropbox. Overweeg eventueel om de bestanden met VeraCrypt te versleutelen als je die toch via WeTransfer of Dropbox wilt uitwisselen. Kleinere bestanden kun je ook versleutelen en als bijlage met een e-mail meesturen.

Uiteraard is fysieke uitwisseling (in persoon) de veiligste manier om grote hoeveelheden data uit te wisselen. Dat kun je doen via een versleutelde stick of externe harde schijf die met een wachtwoord is beveiligd. Alles wat je nodig hebt voor het fysiek uitwisselen van gegevens is versleutelingssoftware (zoals VeraCrypt), een USB-stick en het wachtwoord.

## Bestanden veilig verwijderen

Op de meeste systemen verdwijnt een bestand niet van de harde schijf of USB-stick als je het verwijdert. Het bestand blijft bestaan, maar de plek waar het staat krijgt het label 'niet meer in gebruik'. Hierdoor weet het systeem dat het die plek mag overschrijven met andere data. Maar het oude bestand blijft onzichtbaar aanwezig tot die plek wordt overschreven en het kan ook worden teruggehaald met (vaak eenvoudige) forensische tools en ervaring.

Om ervoor te zorgen dat een bestand echt veilig en compleet wordt verwijderd, kun je een hulpmiddel gebruiken dat de ruimte waar het bestand was opgeslagen een paar keer overschrijft. Dat kan overigens wat tijd in beslag nemen, afhankelijk van het datavolume van de verwijderde data.

**Windows, Linux**
Op Linux- en Windows-systemen is BleachBit de belangrijkste opensource-verwijdertool die als zeer betrouwbaar staat aangeschreven. Een alternatief is bijvoorbeeld CC-Cleaner. Deze tools overschrijven de ruimte waar de bestanden stonden meerdere malen, waardoor het terughalen onmogelijk wordt.

**Mac**
Op een wat nieuwere Mac is er geen manier om losse bestanden op een veilige manier te verwijderen. Het is daarom belangrijk dat je de harddrive versleutelt, en toegang alleen mogelijk maakt met een wachtwoord.

**Kies liever voor USB-sticks**
Het opslaan van data op de harde schijf van een laptop zorgt ervoor dat je gegevens aan meer risico's blootstaan en vaak is het moeilijk om ze veilig te verwijderen. Daarom is het aan te raden om gevoelig materiaal op een extern opslagmedium op te slaan, zoals een USB-stick of een externe harde schijf (voor grotere volumes). Versleuteling van die apparaten en van de bestanden erop is ook belangrijk om ze te beschermen tegen verlies of diefstal.

Voor het veilig wissen/opschonen van een USB-stick (of willekeurige externe harde schijf): doe de USB-disk in het apparaat: start 'Disk Utility' → selecteer de drive die je wilt wissen (kijk in het menu links) → selecteer de erase-tabe (verwijder-tab). Selecteer 'Security Options' en schuif de slider naar 'Most Secure'* → 'OK' → "Erase'.

**Fysiek vernietigen van gegevens**
Als een volledige disk wilt wissen, is vernietiging daarvan ook een optie. Wil je er zeker van zijn dat er geen data meer kan worden teruggehaald, moet je het apparaat in kleine stukjes verdelen. Een hamer of onderdompelen in water werkt onvoldoende tegen goede forensische technieken. Bedenk ook dat een moderne printer/copier een harde schijf heeft die je wilt wissen als je deze afdankt.

# Hoofdstuk 4: onlinecommunicatie

## Metadata

Metadata zijn de data over data. Digitale bestanden bevatten verschillende metadata die als het ware in een schil om het bestand hangen. Die kunnen veel informatie weggeven. Je moet daarbij denken aan de auteur van een Word-document, de GPS-coördinaten van de locatie van een foto. Audio, video, en PDF-bestanden bevatten ook metadata en verborgen data (zoals commentaar, tracking-gegevens, bestandsnamen, etc.). De meeste kleurenlaserprinters printen hun type- en serienummer in onzichtbare puntjes op iedere vierkante centimeter van het papier. De herkomst van het papier of stukjes daarvan zijn dus te traceren naar de printer en uiteindelijk naar jou als die printer naar jou leidt (bijvoorbeeld als je de printer online hebt besteld). Ook de metadata van e-mails kunnen veel informatie over jou vertellen (zie hieronder 'e-mail').

Elk programma wat je gebruikt kan dus specifieke metadata-instellingen hebben. Zorg er dus voor dat je weet welke metadata wordt opgeslagen in de schil van de bestanden van het programma dat je wilt gebruiken en of/hoe je die informatie kunt verwijderen. Zo zorg je ervoor dat de metadata onschadelijk voor je zijn. Je kunt dit bijvoorbeeld achterhalen via onlineonderzoek naar het bewuste programma en de gebruikte bestandsformaten.

## E-mail

Je loopt verschillende risico's met e-mailcommunicatie. De kans bestaat dat je metadata wordt bekeken ( (je locatie/de onderwerpregel, met wie je contact hebt/hoe vaak/wanneer), dat men je e-mailinhoud leest en dat men de e-mailbijlagen onderschept. Men kan zich zelfs als jou voordoen.

Acties rondom informatiebeveiliging:

- gebruik sterke wachtwoorden
- gebruik een betrouwbare e-mailprovider
- gebruik TLS/SSL voor de verzending
- zorg voor goede e-mailinstellingen, zoals controle van e-mailadres/afzender via DMARC, DKIM en SPF zodat zeker is dat jij de afzender bent van een bericht (bijvoorbeeld onze eigen @tweedekamer.nl had dit nog niet op orde in oktober 2017);
- gebruik tijdelijk e-mailadressen voor specifieke doeleinden om je identiteit en locatie te beschermen

Een sterk wachtwoord is voldoende als basisbescherming tegen ongeautoriseerde toegang tot je e-mailaccount. Bedenk wel dat je e-mailberichten – als ze niet zijn versleuteld – in verhouding gemakkelijk te bekijken zijn door e-mailprovider. Kies daarom voor een betrouwbare provider. Een betrouwbare provider heeft een goed beveiligde infrastructuur, geeft je de mogelijkheid om mails tijdens het transport te beveiligen en geeft je data niet zomaar aan een inlichtingendienst.

Als je het land waar je e-mailprovider is gevestigd, niet vertrouwt, dan kun je beter geen e-mailadres in dat land gebruiken. Bijvoorbeeld de inlichtingendiensten van de USA en de UK slaan zoveel mogelijk e-mailcommunicatie op. Zelfs als je denkt dat je e-mails niet van belang zijn voor deze diensten, kan dat in de toekomst wel het geval zijn en men kan dan met terugwerkende kracht inzicht in die gegevens krijgen.

**Je identiteit en locatie beschermen als je e-mailt**

Degenen die hun werkelijke identiteit of die van anderen verborgen willen houden in de communicatie, moeten anonieme e-mailaccounts gebruiken. Dat moeten accounts zijn die niet met iets anders van die persoon online kan worden geassocieerd, op wat voor manier dan ook. Gmail en Hotmail vragen om een telefoonnummer of een alternatief e-mailadres, waardoor deze providers niet zo geschikt zijn voor anonieme accounts. Als je een anoniem account aanmaakt, moet je rekening houden met een aantal dingen. Bijvoorbeeld als je je anonieme e-mailadres aanmaakt via een internetverbinding die met jou kan worden geassocieerd, dan is je anonimiteit niet meer gegarandeerd. Bovendien, als je e-mails stuurt en ontvangt via zo'n internetverbinding, dan is je locatie bekend bij de internetprovider.

Wees je er daarom van bewust dat e-mailproviders in de USA (zoals Outlook, Gmail, etc.) de wetten en werkwijze van dat land toepassen. De ene e-mailprovider werkt daar wellicht meer aan mee dan andere, maar – tenzij je je eigen server draait of tenzij de organisatie waar je voor werkt heeft een server in een land met goede privacywetten, zoals Zwitserland of IJsland – moet je aannemen dat je mails en de metadata daarvan niet veilig zijn bij welke e-mailprovider dan ook. Als je account kiest, neem dan ook in overweging welke gegevens je daarvoor wilt verstrekken. Sommige providers vragen bijvoorbeeld om persoonlijke gegevens zoals je mobiele nummer, je adres/postcode, een ander e-mailadres. Het kan zijn dat je in de toekomst wilt voorkomen dat die informatie bekend wordt (in het bijzonder als je een anoniem e-mailadres gebruikt). Tip: kies bijvoorbeeld voor maildiensten als Protonmail en of Startmail. Protonmail heeft bovendien een fijne interface voor je smartphone.

**Metadata van e-mail**

E-mail-metadata bevatten informatie over de zender en ontvanger, de e-mailadressen, gebruikte IP-adressen, serverinformatie, datum, tijd, tijdzone, unieke identificatiecode van de e-mail en gerelateerde e-mails, soort inhoud en codering, inloggegevens van de mailclient met IP-adres, informatie over prioriteiten en categorieën, onderwerp, status en leesbevestigingen.

Het is niet eenvoudig om de metadata van e-mails te beschermen, dus je moet in de onderwerpregel zo kort mogelijk zijn en/of verhullende teksten gebruiken. Het kan ook verstandig zijn om je locatie/IP-adres te verbergen door gebruik te maken van de Tor-browser.

Je ziet dat deze informatie uitgebreid en onthullend is, maar veel inlichtingendiensten en justitiële instellingen (en in sommige gevallen individuele hackers) zijn in staat de hele inhoud van de e-mail te verkrijgen. Dat kun je alleen met encryptie voorkomen. Metadata kun je echter niet versleutelen.

**Zelf voorzichtig omgaan met e-mail**

Risico's met e-mail betreffen niet in de laatste plaats je eigen acties. Denk maar aan de bijlage die naar de verkeerde persoon wordt gestuurd. Dit is op verschillende manieren te voorkomen:

- zorg ervoor dat er geen automatisch e-mailadres uit het cachegeheugen van je mailprogramma wordt ingevuld als je een letter intypt;
- verstuur geen bijlage, maar geef een downloadlink die je beveiligt met een wachtwoord en een maximale beschikbaarheidstijd (gebruik bijvoorbeeld 'Stack' van TransIP);
- versleutel de bijlage (en eventueel je e-mailverkeer).

Verder kan je laptop worden gecompromitteerd via mail. Tips om dit te voorkomen:

- voorkom phishing en klik niet op links in mails van onbekende afzenders;
- trap niet in zogenaamde 'hoax'-berichten (vaak paniekzaaierige mails die je (dus niet) moet doorsturen aan iedereen die je kent);
- gebruik een goed antivirusprogramma (Windows/Mac);
- geef je zakelijke dragers niet aan derden/kinderen.

**E-mailencryptie**

Je kunt je e-mailinhoud beschermen tegen pottenkijkers door gebruik te maken van encryptie. Je verhaspelt dan de inhoud van je e-mailberichten in een (tot nu toe) onbreekbare code die alleen de ontvanger met de privé-encryptiesleutel kan lezen. Ieder ander ziet een berg code. Voor uitgebreide documentatie, zie:


Het versleutelen van e-mail maakt alleen je berichtinhoud onleesbaar en verbergt de metadata niet (zoals met wie je mailt, de onderwerpregel, je locatie, etc.). Als je niet wilt dat de onderwerpregel de inhoud van je bericht weggeeft, kies dan een onschuldig onderwerp dat niet gerelateerd is aan de werkelijke inhoud van het bericht. Ook de bijlagen worden niet versleuteld. Verder kun je alleen versleutelde berichten sturen naar mensen die ook encryptie gebruiken voor hun e-mail.

## Chat/instant-messaging

Instant messaging is een prima manier om contacten te onderhouden en te communiceren. Het is tegenwoordig niet moeilijk om een chatapp te installeren die gebruikmaakt van versleuteling. We hebben wel wat suggesties die je privacy verhogen. Veelgebruikte chatapps zijn WhatsApp en Facebook Messenger.  Ze zijn weliswaar het meestgebruikt, maar niet het veiligst.

Veiliger zijn de chatapps Wire, Signal en Telegram. Ze hebben ook een desktop-versie, zodat je ze niet alleen op je telefoon maar ook op je laptop kunt gebruiken. Hier lees je precies welke van de drie het beste bij jou past. Overwegingen hierbij zijn bijvoorbeeld of je je telefoonnummer en/of contacten wilt delen met de app-aanbieder.

## Bellen (telefoon, voice, video) via internet

Velen van ons vinden smartphones belangrijk in het dagelijkse leven, zowel privé als op het werk. Het heeft veel voordelen om steeds online te zijn en toegang te hebben tot e-mail, webbrowsers, sociale media, en agenda's. Ook de hoge kwaliteit van de meeste camera's en de voicerecorder maken smartphones waardevolle hulpmiddelen. Maar juist die functionaliteit maakt een smartphone tegelijkertijd bijna letterlijk een surveillancetool, want smartphones zijn niet goed te beveiligen.

Risico's die je loopt met het gebruik van smartphones:

- automatisch loggen van je huidige en vorige locaties en verzamelen van metadata (telefoonnummer, locatie van iedere beller, unieke serienummers van de betreffende telefoons, tijd/lengte van een gesprek, kaartnummers van prepaidkaarten, etc).;
- diefstal en verlies van data;
- op afstand toegang krijgen tot data via verbinding met publieke wifinetwerken;
- op afstand toegang krijgen tot alle data op enig moment dat de telefoon aan staat;
- het aftappen van telefoongesprekken en voicemail, onderscheppen of opnemen;

- geheime automatische toegang op afstand tot de microfoon om geluid op te nemen;
- geheime automatische toegang op afstand tot de camera om foto's te maken.

Bij lage risiconiveaus is de dreiging vooral fysiek: iemand krijgt je telefoon in handen. Als dit gebeurt kan zelfs een minder vaardige hacker of de politie je wachtwoord kraken (als je een wachtwoordslot hebt ingesteld). Dit biedt dus minimale protectie. Zorg ervoor dat je je data back-upt en dat je video- of audio-opnames zo snel mogelijk opslaat naar een veilig opslagmedium.

Stel daarnaast in ieder geval gegevensversleuteling op je smartphone in. De meeste moderne smartphones hebben die optie standaad aan boord. Zorg ervoor dat je de gegevens op afstand kunt wissen. Gebruik ook de vergrendeling op de telefoon (pincode, swipe-patroon).

Je kunt ook tracking-apps gebruiken om je telefoon terug te vinden als deze wordt gestolen. Apple biedt bijvoorbeeld voor iPhones een gratis app aan, genoemd 'Find my iPhone'. Die vertelt je op welke locatie de telefoon zich op dat moment bevindt. Een andere anti-diefstal-app is 'Prey'. Deze rapporteert de telefoon als gestolen en slaat niet alleen de huidige locatie op, maar ook de locaties waar de telefoon is geweest nadat de telefoon als gestolen is gemeld.

**Een extra telefoon met prepaid SIM**
Een wegwerptelefoon is goedkope, contant betaalde telefoon met weinig techniek en met een prepaid SIM-kaart die niet op je naam staat. De telefoon gebruik je alleen voor specifieke doeleinden, bijvoorbeeld als je een bepaalde app wilt gebruiken en je daarvoor een verificatieproces via een SMS moet doorlopen. De SIM-kaart wisselen met je huidige smartphone is daarvoor niet afdoende, omdat je je identiteit dan alsnog via het IMEI-nummer weggeeft.

## Overige risico's

**Social engineering**
Er zijn verschillende manieren waarop kwaadwillenden in het bezit kunnen komen van informatie die jij niet wilt delen. Een belangrijke daarin is social engineering: iemand probeert om rechtstreeks informatie van je los te krijgen door jouw vertrouwen te wekken. Een methode die we niet zo gauw herkennen, want mensen willen van nature de ander vertrouwen en juist daar wordt misbruik van gemaakt. Voorbeelden:

- Iemand die zich voordoet als een collega en zo jouw adres of geboortedatum te weten komt.
- Denk ook aan de telefoontjes die in naam van Microsoft worden gepleegd naar particulieren ("Er is iets mis met uw computer, met Windows."), de "Microsoft-scam".
- Ethische hackers hebben in een ziekenhuis vertrouwelijke informatie (tot en met wachtwoorden) weten te ontfutselen door zich voor te doen als medewerkers van een IT-bedrijf dat voor de beveiliging kwam.

Een nadeel van deze werkwijze (social enigineering) voor de kwaadwillende is de tijdrovendheid; dit kan niet geautomatiseerd plaatsvinden. Het is wel vaak effectief. Tip: vraag je altijd af of je de informatie die je deelt, wel met die persoon of partij zou moeten delen. Klopt het wel? En wat is het nadeel als je het niet geeft en eerst de geldigheid van de vraag controleert?

**Onveilige mail: phishing en hoax**

Hoe herken je een onveilige mail? Een van de meest duidelijke kenmerken van een mail die ervoor bedoeld is om je gegevens te ontfutselen (bijvoorbeeld een phishing-mail waarbij de afzender uw bank lijkt te zijn) is: angst in combinatie met snelheid. Je wordt ineens geconfronteerd met een probleem waar je vooraf niet van op de hoogte was en waar je snel actie voor moet ondernemen. Bijvoorbeeld:

> *"Als u niet binnen 24 uur de benodigde actie onderneemt, wordt uw creditcard geblokkeerd."*

Ga nooit op zo'n mail in. Bel je bank als je twijfelt. Een andere methode is de poging je te verleiden. Iedereen kent wel het voorbeeld van de Nigeriaan die uit het niets mailt om u te vertellen dat hij miljoenen voor u heeft.

Tip: er moeten altijd alarmbellen aangaan als iemand vraagt om geld (of u dat gratis lijkt aan te bieden), u wijst op een hack of een verlopen licentie, etc. zonder dat u zelf daarvan iets heeft gemerkt. Wees vooral op uw hoede als er snel iet moet gebeuren en u bent degene die de actie moet uitvoeren.

De hoax is een bijzonder geval. Een hoax is het verspreiden van valse geruchten per mail (of tegenwoordig bijvoorbeeld ook via WhatsApp) worden verspreid. Het zijn van die berichten waarin wordt gevraagd om het bericht zo snel mogelijk door te sturen aan zoveel mogelijk mensen die u kent. Mailboxen raken zo overbelast. Een hoax-mailbericht is meestal niet zozeer een onveilig als wel vervelend (pas wel goed op als er een bijlage bij zit!). Meestal is niet duidelijk waar de mail oorspronkelijk vandaan komt of wanneer de informatie voor het eerst is verspreid. Sommige berichten kunnen al jarenlang rondgaan. ZDNet.be schreef een goede uitleg over de hoax.

Tip: moet er massaal worden doorgestuurd en is de inhoud van het bericht schreeuwerig? Check dan via de zoekmachine of je met een hoax te maken hebt.

**Malware via een bekende**

Ten slotte nog dit: tegenwoordig zie je met enige regelmaat dat accounts op sociale media worden gehackt. Bekenden sturen een raar bericht (bijvoorbeeld, "Wat heb je nu gedaan?") met een link. Omdat je die persoon kent, klik je toch maar op die link uit nieuwsgierigheid, maar de kans is groot dat je malware binnenhaalt. Wees dus altijd op je qui-vive voordat je op links klikt.

# Hoofdstuk 5: veilig wachtwoordengebruik

Een dilemma van het werken met wachtwoorden is veilig wachtwoordengebruik. Mensen gebruiken graag dezelfde wachtwoorden voor verschillende websites en systemen, maar dat is onveilig. Wachtwoorden gebruik je om jezelf (of anderen) als geautoriseerde gebruikers te identificeren. Sterke wachtwoorden zijn de sleutel in informatiebeveiliging. Dit begint bij de beveiliging van je apparaat met een wachtwoord dat op je apparaat is opgeslagen, en het gaat natuurlijk verder in de cloud waar wachtwoorden ergens blijven voor gebruik.

Infobeveiliging-acties:

- gebruik een wachtwoordmanager (als KeePassX, gratis/opensource) en een adblocker;
- leer hoe je sterke wachtwoorden kunt maken;
- weet wanneer je wachtwoord veilig is;
- bewaar de belangrijkste wachtwoorden alleen in je geheugen.

**Onthoud slechts één wachtwoord met een wachtwoordmanager**
Als je een wachtwoordmanager gebruikt, is het gemakkelijk om voor alle accounts verschillende wachtwoorden te gebruiken. Je hoeft er namelijk maar één te onthouden: zo'n manager slaat al je verschillende wachtwoorden op in een database en de toegang wordt beschermd door een hoofdwachtwoord. Zodra je het hoofdwachtwoord van de database hebt ingetoetst, staan al je wachtwoorden tot je beschikking. De manager vult je wachtwoorden aan of je kopieert/plakt ze uit de database. Voor onlinegebruik kun je hiervoor bijvoorbeeld het gratis programma KeePassX gebruiken. Een betaald alternatief is LastPass. Vergeet je hoofdwachtwoord niet, want alle informatie wordt versleuteld opgeslagen en zonder hoofdwachtwoord zijn de gegevens onleesbaar. In een artikel van The Verge van december 2017 wordt uitgelegd dat het ook belangrijk is om adblockers te activeren, omdat die tegenwoordig soms ook scriptjes gebruiken waarmee gebruikersnamen en wachtwoorden via formulieren in browsers worden opgepikt als je de autofill gebruikt.

**Zo maak je een sterk wachtwoord**
Je kunt programma's om wachtwoorden mee te kraken gewoon online kopen. Goede software kan tot acht miljoen wachtwoorden per seconde proberen. Daarom is het belangrijk dat je hoofdwachtwoord moeilijk te kraken is. Het hoofdwachtwoord moet dus ingewikkeld zijn, maar ook te onthouden. Wij raden daarvoor het 'Schneier-schema' aan: kies een zin kiezen die je kunt onthouden en symboliseren. Bijvoorbeeld, "This little piggy went to market" kan worden "tlpWENT2m". Zo'n wachtwoord met negen karakters staat in geen enkel woordenboek. Kies je eigen zin, iets persoonlijks maar niet iets dat duidelijk aan je publieke gegevens is gerelateerd.

**Herken niet-versleutelde wachtwoorden**
Bedenk ook dat er iets niet in de haak met de beveiliging van de partij die jouw je bestaande wachtwoord leesbaar toestuurt als je je wachtwoord bent vergeten. Dat wachtwoord is dan namelijk onversleuteld opgeslagen. Dat betekent dat iedereen die toegang tot de database heeft, jouw wachtwoord kan uitlezen (niet alleen hackers, ook medewerkers van die organisatie). Je moet altijd een link krijgen waarmee je je wachtwoord (opnieuw) kunt instellen. Geeft een organisatie je een eerste wachtwoord dat leesbaar is, dan moet er altijd worden gevraagd om een nieuw wachtwoord in te stellen zodra je de eerste keer inlogt. Gebeurt dat niet, dan is je wachtwoord niet veilig.

# Verklarende woordenlijst

| Begrip | Definitie |
|---|---|
| AMT-chipset | chipset met 'Intel Active Management Technology' (AMT) voor geautomatiseerd management (kwetsbaarder dan oudere chipsets van voor 2008) |
| Besturingssysteem | de software die de computer bestuurt als deze opstart, vertelt wat er moet gebeuren en hoe dat moet worden gedaan. Het is de basisinterface van de computer, waarmee je met computer kunt werken |
| Encryptie | versleuteling van data tot onleesbare code die met een sleutel kan worden ontcijferd |
| Extensie | uitbreiding van je browser met een plug-in waarmee je de browser extra functionaliteit geeft (zoals een advertentieblocker of wachtwoordmanager) |
| Firmware | op hardware geprogrammeerde software die instructies geeft aan hoe het betreffende apparaat moet communiceren met de andere hardware van de computer (inclusief de BIOS) |
| Hardware | de fysieke componenten die samen het computersysteem vormen |
| Malware | kwaadaardige software, bijvoorbeeld spyware, ervoor bedoeld om een computersysteem te verstoren of beschadigen |
| Man-in-the-middle-aanval (MITM) | de heimelijke interceptie van communicatie waarbij een tussenpersoon zich gedraagt als doel/ontvanger/contactpersoon |
| Metadata | data over data, bijvoorbeeld verzenddatum, onderwerpregel |
| Opensource | gratis gedistribueerde software waarvan de broncode publiek beschikbaar is |
| Risiconiveau | de mate waarin je risico loopt dat iemand ongeautoriseerde toegang tot jouw gegevens wil krijgen, onderverdeeld in basisrisico, middelmatig risico, hoog risico en toprisico. Dit boek behandelt het basisrisico. |
| Tor | browser waarmee je anoniem kunt surfen |
| url | de adresbalk van de internetbrowser |
| VPN | VPN-verbinding (Virtueel Privé Netwerk), geeft je een beveiligde (versleutelde) en soms anonieme (omgeleide) toegang tot een netwerk en maakt daarmee de internetverbinding veiliger |

## Over de auteurs

**Helma de Boer** is privacy-professional, docent en activist. Ze leerde zichzelf programmeren in de jaren '90 en bouwde vele websites en databases voor het mkb. Ze studeerde Nederlands aan Hogeschool Windesheim en volgde opleidingen tot Data Protection Officer aan het HAN in Arnhem. In 2017 was ze gastschrijver bij Bits of Freedom. Via haar bedrijf Artheos (2004) adviseert ze bedrijven over de AVG en werkt ze als privacyfunctionaris. Verder geeft ze trainingen in onder andere informatica en privacy-awareness.

**Arjen Kamphuis** is co-founder en Chief Technology Officer van Gendo (2005). Daarvoor werkte hij voor IBM as IT-architect, trainer en IT-strategie-adviseur. Hij was tot oktober 2017 werkzaam als lead advisor information security bij Brunel en werkt nu als directeur van PG Knowledge. Als CTO van Gendo adviseert hij verschillende nationale overheden, non-profitorganisaties en Fortune-500 bedrijven over hun technologiebeleid. Sinds 2009 traint Arjen journalisten, politici, advocaten, mensenrechtenactivisten en klokkenluiders om hun communicatie en data te beschermen tegen inbreuk of manipulatie door bijvoorbeeld overheden en corporates.

Verbetertips, complimenten en feedback op dit boek zijn van harte welkom. Stuur daarvoor een e-mail naar: helma@artheos.nl (PGP-sleutel 0xEEA94382).

## Colofon

Persoonlijke informatiebeveiliging
Je digitale gegevens beschermen

Foto voorzijde/achterzijde: via Pixabay CC0
Omslagontwerp: Helma de Boer

De suggesties die in dit boek worden gedaan voor productmerken (hardware en software), zijn geen aanbevelingen voor de genoemde merken of hun producten. De besproken flexibiliteit is ook beschikbaar van andere merken.