Workshop persoonlijke informatiebeveiliging en privacy online - door Helma de Boer

10 simpele manieren om je privacy online te vergroten

Je wilt graag meer privé zijn als je online bent en minder sporen achterlaten, maar je weet niet waar je moet beginnen? Met deze tien simpele manieren ben je al een heel eind onderweg. Jij kunt dit ook. Met deze tips kun je uit de voeten op zowel je laptop, p.c. als mobiele telefoon.

Wees niet bang, ik ga niet in clichés vallen en het gebruik van Facebook of Google ontraden, want ik weet dat dit niet realistisch is. Mijn tips zijn dus ook bruikbaar als je Facebook of Google gebruikt. Onder de tips volgt een toelichting per onderdeel.

1. Gebruik Firefox als standaardbrowser.
2. Gebruik de zoekmachine Google, maar doe dat via www.startpage.com.
3. Blijf na gebruik niet ingelogd bij sociale platforms als Twitter, Facebook, Microsoft en Google en koppel geen diensten.
4. Verstrek geen echte gegevens over jezelf als dat niet nodig is. Zalando heeft je geboortedatum niet nodig.
5. Neem nu een keer de tijd om de instellingen van je mobiele telefoon en de geïnstalleerde apps na te lopen. Zet bijvoorbeeld overal 'locatie delen' uit en trek onnodige machtigingen in.
6. Installeer niet de eerste de beste app op je telefoon, maar kijk eerst of er alternatieven zijn die geen overbodige toegang tot onderdelen van je telefoon vragen en die je geen advertenties voorschotelen.
7. Gebruik een apart of tijdelijk e-mailadres voor flutdingen op internet (reacties, bestellingen, sociale media, registraties, ondertekening van petities, etc.).
8. Gebruik Telegram, Signal of Wire als chatapp in plaats van Whatsapp. Zelfde look & feel, maar veiliger en beter (mijn persoonlijke voorkeur gaat uit naar Signal).
9. Vermeld alleen je voornaam als je reageert op berichten op het internet zoals een blog of forum.
10. Gebruik een veilige online e-mailservice in plaats van Gmail. Kies bijvoorbeeld voor Protonmail (schitterende, superhandige mailapp voor je mobiele telefoon en gratis tot 500 mb opslag) of Startmail (niet gratis).

Toelichting per onderdeel

1. Surfen via Firefox

Firefox maakt jou de baas over je browser in plaats van andersom. Mozilla, de ontwikkelaar, zegt dat de browser is gemaakt voor mensen en niet voor winst. Als non-profitorganisatie zal Mozilla geen browsegegevens verzamelen en verkopen. Jouw privacy staat voorop. Verder zijn er allerlei uitbreidingen gemaakt waarmee je de browser nóg veiliger (en leuker!) kunt maken dan hij standaard al is. Je kunt Firefox helemaal naar jouw wensen instellen en trackers standaard uitschakelen. En dat is handig, want er zijn vele websites en advertenties die verborgen trackers toevoegen aan je browser, waardoor jouw surfgegevens nog worden verzameld lang nadat je weg bent. Dat kun je gemakkelijk

voorkomen met Firefox. Gedownload? Stel dan meteen Startpage als standaard in op het openingstabblad en als standaardzoekmachine.

2. Zoeken via Startpage

Als je Startpage een week hebt gebruikt om te zoeken, dan kun je niet meer terug naar Google. Het is dan namelijk ineens pijnlijk duidelijk dat ze je daar met advertenties om de oren smijten. Alleen dat zou al voldoende reden moeten zijn om Startpage te proberen. Een ander groot voordeel is dat je bij het zoekresultaat ervoor kunt kiezen om deze via 'proxy' te bekijken. Zo blijft jouw ip-adres onbekend bij de site die je bezoekt. Er zijn ook alternatieven, zoals DuckDuckGo.

3. Uitloggen

Dit is voor de meeste mensen waarschijnlijk het allermoeilijkst: uitloggen van een dienst als je deze niet meer gebruikt. Dat klinkt zo onhandig. Maar door ingelogd te blijven, worden werkelijk al je online-activiteiten vastgelegd. Laat je niet tegenhouden door het idee dat je dan allerlei wachtwoorden moet onthouden: als je LastPass gebruikt, hoef je maar één wachtwoord te onthouden, de rest onthoudt die digitale kluis voor je. En alles wat ze kunnen koppelen aan jouw surfgedrag, geeft een steeds beter (lees ook: financieel waardevoller) beeld van jou als persoon. Ze weten dan bijvoorbeeld precies waar je bent, wat je van bepaalde onderwerpen vindt en met wie je afspreekt, etc. Koppel daarom ook geen diensten aan elkaar. Dat geldt ook voor nieuwe diensten waarmee je met je Facebook- of Gmail-account kunt inloggen. Dat is handig omdat je dan geen apart account hoeft aan te maken, maar je geeft dan weer extra informatie aan die bedrijven weg. Kies er dus voor om toch een apart account aan te maken.

4. Ik ben geboren in juni in het jaar 1891

Vraag jezelf steeds af waarom je bepaalde informatie over jezelf aan een organisatie moet verstrekken. Dient dat een doel? Als Zalando om je geboortedatum vraagt, is dat uitsluitend om een beter profiel van je te krijgen (om te verkopen aan derden). Altijd gaat dat onder het mom van 'verbetering van diensten want: gepersonaliseerd' en altijd is dat onzin. Soms moet je verplicht iets invullen voordat je een bestelling kunt doen. Wees zuinig op je echte gegevens. Dan kan bijvoorbeeld door nepgegevens te verstrekken. Zo heb ik onlangs een foto online besteld en gedownload. Het adres dat ik verplicht moest invullen, leidt naar Duckstad.

5. Locatie uit

Ook wat lastiger voor veel mensen om de telefoon te gebruiken zonder locatie, stel ik mij zo voor. Maar echt; je went er snel aan en het geeft je enorm veel meer privacy. Zeer veel apps willen je locatie weten, ook als dat helemaal niet nodig is. Waarom moet Wordfeud weten waar je bent als je aan het puzzelen bent? Zelfs dat klompenpad kun je lopen zonder dat je je locatie met de app deelt. Loop eens al je apps na en kies bewust welke toestemmingen je verstrekt. Vaak zijn dat veel meer dan nodig. Zet alles uit en je merkt snel genoeg welke je toch nodig hebt.

6. Bewust zoeken naar goede apps

Voor veel diensten kun je kiezen uit verschillende apps. De meestgebruikte in de store zijn niet altijd de beste. Om te bekijken welke app het beste bij jou past, kun je eerst een onderzoekje doen. Er is een schat van informatie over apps te vinden op het internet en voor je het weet heb je een fotogalerij gevonden die alles alleen lokaal opslaat, die géén advertenties toont (een must wat mij betreft) en die niets deelt met de maker van de app. O ja, ik weet dat 'alleen lokaal' onhandig klinkt, maar het overzetten van je foto's met een USB-kabeltje is echt zo gebeurd.

7. Extra e-mailadres voor flutdingen

Je hoeft niet per se je persoonlijke e-mailadres overal achter te laten. Soms is een extra mailadres (bijvoorbeeld – ik noem maar iets – webhelma@….) praktisch om flutdingen te regelen op het internet. Onderteken er een petitie mee, log ermee in op je sociale media (ja, bijvoorbeeld Facebook of Twitter), bestel ermee bij die ene webshop waar je nooit meer terugkomt. Je "echte" PostvakIn zal flink opfleuren zonder al die troep. Een extra adres voorkomt spam en het zorgt ervoor dat je echte adres niet op straat ligt als er onverhoopt data wordt gelekt of gehackt. Niet alle sites hebben hun beveiliging op orde en zelfs als dat wel zo is, is dat helaas nog geen garantie tegen datalekken.

8. Veilige chatapp

De belangrijkste reden om zo weinig mogelijk gebruik te maken van Whatsapp is de hoeveelheid metadata die Facebook over jou in handen krijgt als je deze app gebruikt. Immers, Whatsapp is gekoppeld aan Facebook. Metadata = registratie van je online-activiteiten (maar niet de inhoud van het bericht). De app hoeft echt niet meteen weg hoor, maar verwonder je eens over de prachtige, veiliger alternatieven Telegram, Signal en Wire. Het leuke van Telegram en Wire is dat je je telefoonnummer niet aan de ander hoeft te verstrekken (geef je gekozen gebruikersnaam).

Ben je eenmaal een beetje bekend met je alternatieve chatapp, wees dan een held en verwijder Whatsapp. Je moet inderdaad je account helemaal verwijderen, anders zien mensen je nog steeds in de app. Je zult je erover verbazen hoeveel van je vrienden bereid zijn om een extra chatapp te installeren om met jou in contact te kunnen blijven.

9. Wie is die Helma?

Zodra je je voor- en achternaam publiek achterlaat op een blog of forum, ben je vrij gemakkelijk te vinden. Met alleen je voornaam kan het om duizenden personen gaan, maar met je achternaam erbij is dat een ander verhaal. Als je alleen je voornaam gebruikt, geeft je dat op zijn minst al direct bescherming tegen lurkers, de gluurders. Mensen die van alles over je willen weten en via het lurken informatie kunnen combineren die jij zelf hebt achtergelaten. Informatie waarmee ze soms een griezelig diepgaand plaatje kunnen maken.

10. E-maildienst

Voor gratis diensten betaal je met jouw privacy en dat van anderen. Gmail is van Google. Gmail koppelt diensten en ziet al je metadata (onderwerp, met wie je mailt, op welke tijdstippen, etc.) en wie je contactpersonen zijn. Je kunt je Gmail versleutelen, maar dat is niet zo gemakkelijk. Overweeg

daarom te betalen voor je mail. Wil je net zo eenvoudig werken als met Gmail, vergelijk dan bijvoorbeeld Protonmail en Startmail van Startpage. Bij beide heb je de mogelijkheid om je eigen domeinnaam te gebruiken en beide versleutelen je mail.

Het kan nog veel beter

Je ziet dat meer privacy vooral betekent dat je voor een andere werkwijze durft te kiezen. Ik weet dat dit voor velen het moeilijkst is: veranderen. Maar je plukt er wel de vruchten van. En "anders" betekent trouwens echt niet altijd dat je inlevert op gemak. Daarvan vind ik Protonmail een goed voorbeeld, want de mailapp is echt heel fijn.

Tien technieken om je privacy online verder te vergroten

In 10 simpele manieren om je privacy online te vergroten gaf ik je tien basistips om minder sporen achter te laten op het internet. Nu gaan we een stapje verder. Het wordt iets technischer, maar ik bespreek niets wat jij niet zelf kunt. Onder de tips volgt uitleg over de installatie van een browser-plugin.

Tien tips

1. Browser-plug-in – Tegen de advertentiegekte: gebruik Ghostery of Privacy Badger om cookies die je tracken te blokkeren in je browser. Daarmee voorkom je deels dat je over verschillende sites wordt gevolgd en blokkeer je advertenties, trackmogelijkheden en locatiediensten.
2. Browser-plug-in – Gebruik een advertentieblokker zoals Adblock Plus in je browser om te surfen zonder vervelende advertenties.
3. Browser-plug-in – Gebruik HTTPS Everywhere om je communicatie online te beveiligen.
4. Browser-plug-in – Gebruik voor ieder account een ander wachtwoord. Onthoud die met één overkoepeld wachtwoord. Dat kan met bijvoorbeeld met wachtwoordmanagers Keepass of Lastpass.
5. Zet webgeschiedenis uit in je browser en in je Google-account (accountinstellingen -> services -> webgeschiedenis verwijderen en onderbreken). Dit kan ook fijn zijn als je de p.c. deelt met huisgenoten.
6. Gebruik het proxy-adres van je zoekmachine (Startpage.com) om sites of anoniem te bezoeken. Klik daarvoor in het zoekresultaat niet op de link naar de site, maar op 'proxy'. Zie de afbeelding hieronder:

7. Zorg ervoor dat er op sociale media altijd om jouw toestemming wordt gevraagd voordat iemand je in een foto kan taggen (o.a. Facebook, je kunt dit instellen bij de privacy-instellingen).
8. Stel een tweestapsverificatie (2FA, tweefactorauthenticatie) in als extra beveiliging van je account. Zo kan iemand anders die over je schouders heeft meegekeken, toch niet in jouw account komen

of je krijgt een seintje als iemand ongeautoriseerd op je account inlogt. Je kunt dit voor alle veelgebruikte diensten instellen.

9. Gebruik vimeo in plaats van YouTube. De eerste is namelijk niet van Google. Je kunt eventueel de browser-plugin Adblock for YouTube installeren die de video-advertenties op de YouTube-site uitschakelt.
10. Gebruik een VPN-dienst om anoniem te surfen, bijvoorbeeld NordVPN of VyprVPN van Golden Frog. Hier lees je meer over VPN-diensten. De VPN-verbinding verbergt onder andere je IP-adres en je kunt geografische blokkades omzeilen.

Er is meer!

Ten slotte nog dit: bekijk de overzicht en toolbox van Bits of Freedom en leer hoe je nog meer stappen kunt zetten voor bescherming van je privacy online. Of beter nog: word donateur. BoF strijdt voor internetvrijheid en voor ieders privacy online en ze kunnen jouw steun goed gebruiken (want om onafhankelijk te kunnen blijven, moeten de donaties vooral van particulieren komen).

Oefening 1 – Startpage als standaardzoekmachine

In twee stappen stellen we Startpage in als standaardzoekmachine: in de eerste stap maken we Startpage de standaardpagina waarmee de browser opstart. In de tweede stap voegen we Startpage als zoekmachine toe aan de browser.

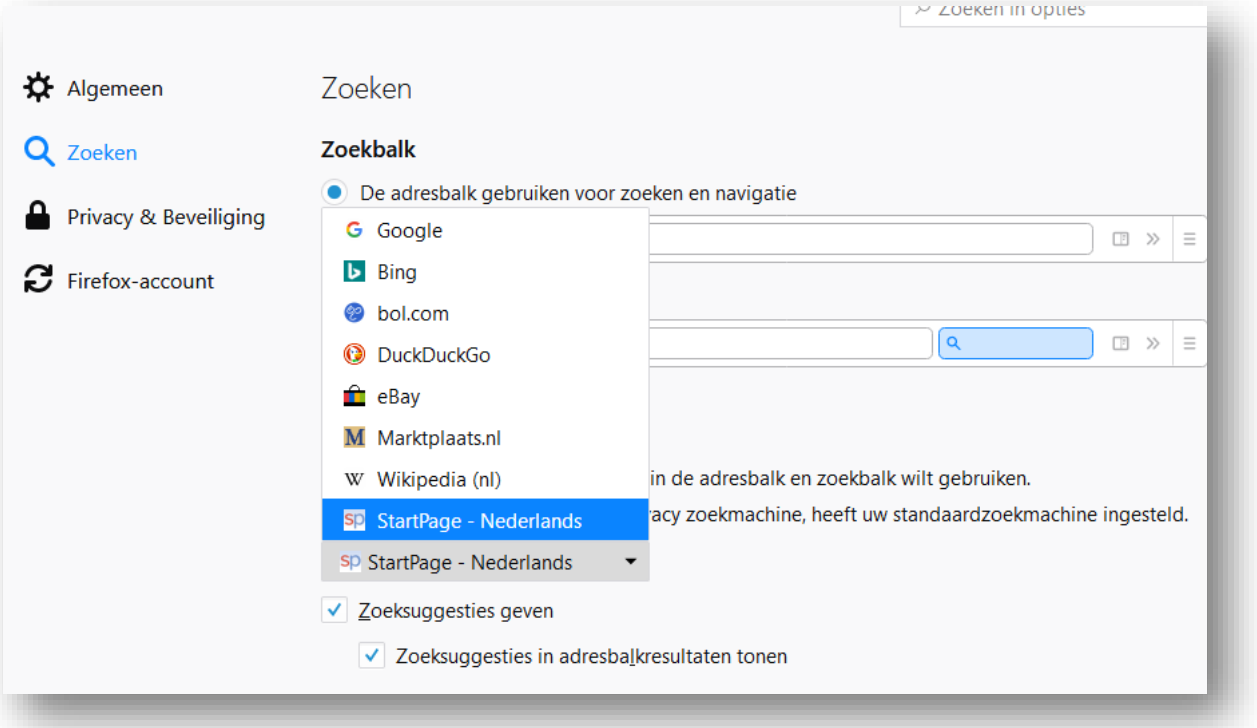
- Ga naar startpage.com/ned en selecteer 'Instellen als startpagina'

- Een nieuw schermpje opent zich:

- Houd de linkerknop van de muis ingedrukt en sleep de afbeelding met de muis naar het 'home'-symbool en laat de muis los

- Er verschijnt een pop-up met de vraag 'Wilt u dat dit document uw nieuwe startpagina wordt? Klik op 'ja'
- Klik vervolgens op 'Toevoegen aan <browsernaam>' ← de naam van de browser hangt af van met welke browser u werkt:

- Volg de stappen die in beeld komen om Startpage als zoekmachine ook aan de browser toe te voegen
- Als dit is gebeurd, kun je Startpage ook als standaardzoekmachine instellen; dat gaat net een stapje verder dan Startpage alleen als startpagina te gebruiken. Ga hiervoor naar de opties/instellingen van de browser (bij bijna iedere browser rechtsboven via een menu te benaderen en kies uit de standaardlijst Startpage als standaard:



- 0 - 0 - 0 -

Oefening 2 - Extensie of plug-in: de browserfunctionaliteit uitbreiden

Er zijn een paar tips genoemd waarvoor je een extra functionaliteit aan je browser moet toevoegen: de zogenaamde browser-plugin (extensie, add-on). Het klinkt ingewikkelder dan het is. Het is een kwestie van opzoeken en installeren. Vervolgens moet je naar smaak een aantal instellingen aanpassen.

Zo installeer je een add-on: – zoek de add-on op en kies voor toevoegen aan de browser.
Bijvoorbeeld bij HTTPS Everywhere zie je in Firefox het volgende schermpje:

Hier beheer je je add-ons in Firefox (vergelijkbaar in andere browsers):

Oefening 3 – Versleuteld volume

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. Dat laatste behandelen we niet hier, maar als je dat wilt leren, bekijk je het gratis e-book 'Informatiebeveiliging voor o.a. journalisten'.

VeraCrypt voor versleuteling

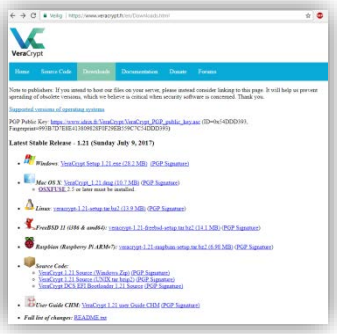
VeraCrypt is opensource-software voor het versleutelen van bestanden
Download: https://www.veracrypt.fr/en/Downloads.html
(Mac-gebruikers moeten ook FUSE voor macOS downloaden: https://osxfuse.github.io/)

Hier vind je goede, begrijpelijke documentatie over VeraCrypt:
https://www.veracrypt.fr/en/Documentation.html

Met VeraCrypt kun je een versleutelde container maken die als een soort digitale kluis voor bestanden werkt, beveiligd met een wachtwoord. 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 het bestand wordt onderschept kan niemand in de digitale kluis 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 als het bestand is versleuteld. Verlies van wachtwoord betekent verlies van data.**

Installatie van VeraCrypt/Fuse



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

Je voert twee stappen uit: eerst maak je een versleuteld volume, vervolgens plaats je er bestanden in.

Stap 1 – maak een versleuteld volume
Om een volume met encryptie te maken, start je VeraCrypt. Je maakt van tevoren een leeg bestand aan op de plek die als container gaat fungeren (bijvoorbeeld een leeg kladblok-bestand). Dan voer je

de aanwijzingen uit voor ‘harde schijf’ of voor ‘USB-stick’, afhankelijk van waar je een versleutelde omgeving nodig hebt:

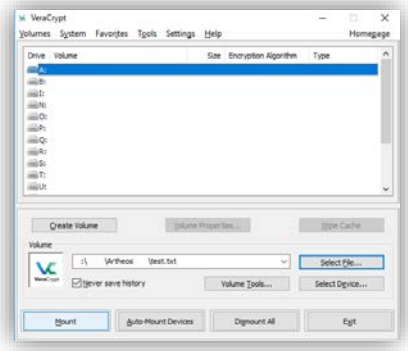
1. *Op harde schijf*: selecteer ‘Volumes’ → 'Create New Volume' (creëer nieuw volume) → ‘Create an encrypted file container’ (maak een versleutelde container voor bestanden) -> selecteer ‘Standard VeraCrypt volume’-> en selecteer het bestand waarin de container op je computer moet worden opgeslagen. Kies ‘ja’ als om overschrijven wordt gevraagd. Je kunt het bestand later verplaatsen. Geef de container een onopvallende naam.

2. *Op 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.

Daarna:

- Het volgende venster is getiteld ‘Encryption Options’ (versleutelingsopties). De standaard-instellingen volstaan.
- 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.



<u>Stap 2 – Te versleutelen bestanden in het volume met encryptie plaatsen</u>
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-schijf, 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. De container ziet er nu uit als een willekeurig bestand op je computer.

Oefening 4 – metadata

Weet jij wat metadata zijn? Weet je hoeveel ze over je kunnen verklappen? Of over anderen? Het is goed je ervan bewust te zijn dat alle bestanden metadata opslaan. Dat zijn alle gegevens die niet over de inhoud van je bestand of e-mail gaan, maar alle randzaken. Denk bij e-mail bijvoorbeeld aan de onderwerpregel, verzendtijdstip en afzender/geadresseerde.

Elk programma dat je gebruikt kan specifieke metadata-instellingen hebben. Zorg er daarom voor dat je weet welke informatie wordt opgeslagen in (bestanden van) het programma dat je wilt gebruiken en of en 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.

Open een willekeurig, bestaand Word-bestand uit je account en klik op ‘Bestand’. Bekijk welke gegevens er staan genoteerd (bewerkingstijd, maker, etc.). Je kunt hier gegevens aan toevoegen of verwijderen.

Oefening 5 – wachtwoordmanager en sterke wachtwoorden

Een wachtwoordmanager helpt je veilig omgaan met wachtwoorden. Je hoeft dan maar één overkoepelend wachtwoord te onthouden om de rest te kunnen gebruiken.

Er zijn twee manieren om het je gemakkelijk te maken om voor ieder account dat je online gebruikt een ander, ingewikkeld wachtwoord te gebruiken:

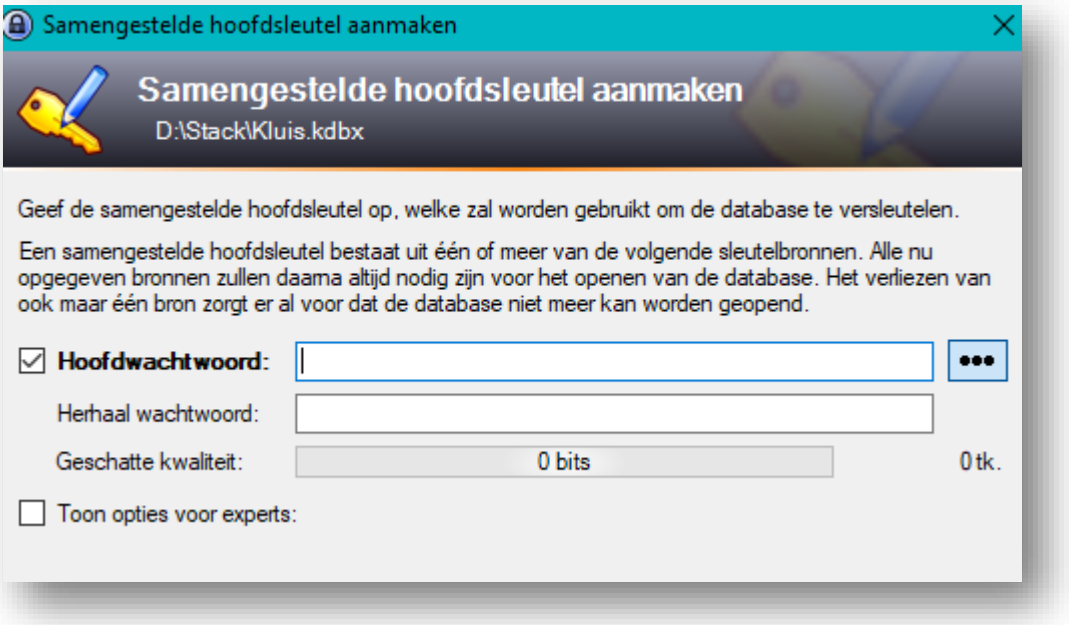
- via een lokale wachtwoordenkluis, zoals Keepass
- via een extensie/plug-in in je browser, zoals LastPass

Voor de eerste moet je een account aanmaken, voor het gebruik van Keepass is dat niet nodig. Loop altijd even de 'instellingen' van een programma of plug-in door na installatie. Je kunt hier allerlei basisinstellingen aangeven, bijvoorbeeld aangeven op welk moment de kluis moet sluiten (na bepaalde duur van inactiviteit).

Keepass (lokaal)

- Download Keepass
- Download eventueel de Nederlandse vertaling via Keepass, vertalingen

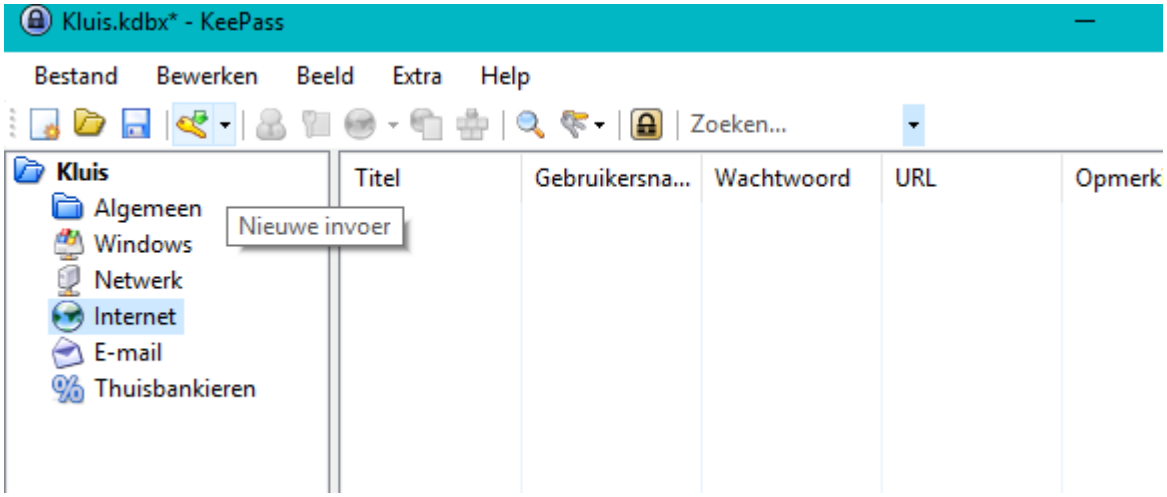
Keepass is een lokale database. Kies is voor 'bestand' → maak nieuw. Zo maak je een kluis aan voor je wachtwoorden. Je wordt gevraagd de kluis een naam te geven en ergens op te slaan. Vervolgens moet je een hoofdwachtwoord instellen:



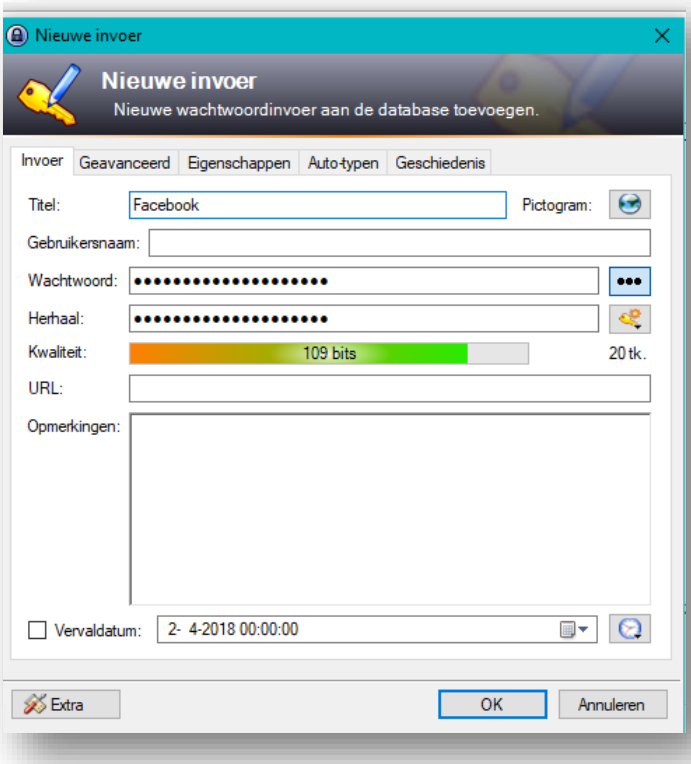
Kies hier een wachtwoordzin die je gemakkelijk kunt onthouden. Dat kan een favoriete dichtregel zijn of wat voor zin dan ook. Hoe langer de zin, hoe moeilijker het wachtwoord te kraken is. Je kunt

eventueel een noodblad aanmaken, printen en deze in een fysieke kluis leggen, zodat je later altijd in de kluis kunt komen, ook als je je wachtwoord toch bent vergeten.
Vervolgens kun je al je wachtwoorden in deze kluis opbergen en gebruiken als je aan het surfen bent. Het is een kwestie van knippen en plakken. Dat is de meest veilige manier om met wachtwoorden om te gaan.

Klik op het sleuteltje voor een nieuwe invoer. Dat ziet er zo uit:



Een nieuw scherm opent zich en je ziet dat er al een wachtwoord wordt gesuggereerd (via de puntjes wordt het wachtwoord leesbaar). Dit wachtwoord kun je kopiëren en plakken in het inlogveld.



LastPass – cloud

- Ga naar [LastPass Free]
- Voeg LastPass toe als extensie of add-on/plug-in

Je weet ondertussen hoe je een extensie of plug-in aan je browser kunt toevoegen en waar je deze kunt terugvinden.

- Ga naar 'add-ons' en vink aan 'Automatisch uitloggen wanneer alle browservensters en Firefox afgesloten is voor (mins)'. → mins = minuten
- Maak een account aan en volg de stappen van LastPass. Voor velen zal dit fijner werken omdat het iets minder omslachtig is dan het gebruik van Keepass. De laatste is minder gemakkelijk te onderscheppen door kwaadwillenden.