INFORMATIEBLAD

VEILIGHEID

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG
IN DE ZORG

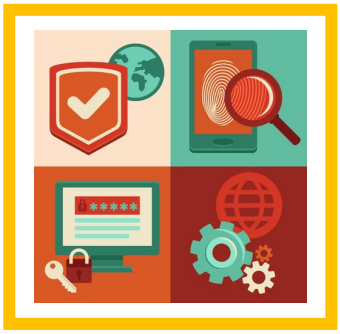
INFORMATIEBLAD VEILIGHEID

Deze lesmodule bestaat uit een Informatieblad, Opdrachtblad en Antwoordblad. Lees eerst dit Informatieblad en maak daarna de opdrachten van het Opdrachtblad. De juiste antwoorden vind je ten slotte in het Antwoordblad.

Veiligheid

In ons dagelijks leven zijn we omringd door digitale apparaten. Met onze computer, telefoon of tablet maken we gebruik van digitale diensten op verschillende websites, apps en sociale media. We delen er gegevens mee bij de vleet. Maar hoe doe je dat nu op een veilige manier? In deze lesmodule krijg je handvatten aangereikt om veilig om te kunnen gaan met digitale apparaten en diensten.

Veilige wachtwoorden



Of het nu gaat om een account voor je computer of voor een website, je moet op verschillende plekken een wachtwoord invullen om gebruik te kunnen maken van digitale diensten.
Een *veilig wachtwoord* instellen is daarom belangrijk. Het zorgt ervoor dat alleen jij toegang hebt tot bepaalde gegevens.
Het kan lastig zijn om verschillende wachtwoorden te onthouden. Veel mensen gebruiken daarom voor elke dienst hetzelfde wachtwoord. Of ze maken een wachtwoord aan dat gemakkelijk te onthouden is, zoals de eigen naam plus geboortejaar (bijv. Nina1985). Ook schrijven veel mensen wachtwoorden ergens op, om ze maar niet te vergeten. Maar je wachtwoord is hierdoor niet veilig voor anderen. Hackers kunnen er je wachtwoord gemakkelijk mee achterhalen.

Stel je voor dat iemand anders met jouw wachtwoord inlogt op een digitale dienst. Hij zou dan misschien je salaris kunnen zien, rare mails kunnen versturen via jouw naam, of onbetrouwbare websites kunnen bezoeken. Je snapt dan ook wel dat het helemaal niet verstandig is om voor werk én privé hetzelfde wachtwoord te gebruiken. Dan zou hij bijvoorbeeld op jouw naam cliëntdossiers kunnen wijzigen. Als dit negatieve gevolgen heeft voor een cliënt, ben jij verantwoordelijk. Jouw inloggegevens zijn namelijk verbonden aan die wijzigingen. Niet alleen jijzelf maar ook anderen hebben er dus belang bij dat jij een veilig wachtwoord gebruikt. Je eigen persoonlijke gegevens, maar ook die van je collega's en cliënten zijn daarmee goed beschermd.

Maar wat is een veilig en sterk wachtwoord? Lees de volgende zes tips:

1. Gebruik minimaal *acht tekens*. Hoe langer het wachtwoord, hoe moeilijker het te kraken te is.
2. Gebruik *letters, cijfers* en *symbolen*. Door deze variatie wordt het nog lastiger een wachtwoord te kraken.
3. Gebruik een *wachtwoordzin*. Deze is vaak moeilijk te raden voor buitenstaanders maar makkelijk te onthouden voor jouzelf. Verder op lees je meer over wachtwoordzinnen.
4. Gebruik *geen voor de hand liggende informatie*. Makkelijk te raden informatie zoals persoonsgegevens (bijvoorbeeld de naam van je kind) of veelgebruikte wachtwoorden zoals '123456' of 'password' worden afgeraden om te gebruiken.
5. Gebruik *niet steeds hetzelfde wachtwoord* voor verschillende diensten. Als je wachtwoord gekraakt wordt, geeft dit ook toegang tot andere diensten waar je dit wachtwoord gebruikt.
6. *Verander* je wachtwoord regelmatig! In veel organisaties is het verplicht om na een bepaalde tijd je wachtwoord te veranderen. Dit verkleint de kans dat iemand anders kan inloggen bij digitale diensten onder jouw naam.

Methode 1: Wachtwoord opknippen

Een sterk wachtwoord kan een woord zijn dat je in tweeën hakt: bijvoorbeeld 'paashaas'. Zet de digitale dienst ertussen, bijvoorbeeld Dropbox. Je kunt ook een cijfer en teken erachter gebruiken. Je krijgt dan: PaasDropboxHaas1@. Om dit te onthouden kun je Dropbox1@ als geheugensteun opschrijven. Zo hoef je alleen Paashaas te onthouden voor elke dienst. Want om in te loggen bij bijvoorbeeld Gmail, gebruik je PaasGmailHaas1@.

Nog veiliger is om niet het woord Paashaas op te schrijven maar bijvoorbeeld alleen het ezelsbruggetje woorddeel1 -gmail-woordeel2-1@.

Als je je wachtwoord later wilt veranderen, kun je het cijfer veranderen. Dan krijg je PaasDropboxHaas2@.

WEETJE?! 80% van de jongeren gebruikt hetzelfde wachtwoord voor meerdere accounts. Ouderen gebruiken juist meer en betere wachtwoorden. Dit betekent echter niet dat ouderen per se verstandiger omgaan met hun wachtwoorden. Zij schrijven ze namelijk op een briefje en dat is ook niet veilig! Bron: NOS 25 nov 2015

Methode 2: De wachtzin

In plaats van een wachtwoord kun je ook een wachtzin maken. Een veilige wachtzin bestaat uit minstens vier woorden en één teken. Omdat een zin uit meer letters en tekens bestaat dan een woord, is het al snel een stuk veiliger. Ook is een zin meestal makkelijker te onthouden.

Voorbeelden van wachtzinnen zijn:

- Dankzij e-mail gebruik ik zelden de telefoon!
- BroodBestaatUitGezondeVezelsEnMineralen!
- Liever U2 dan de 6e van Beethoven!

Soms mag een wachtwoord niet te lang zijn. In dat geval kun je een wachtzin ombouwen tot een wachtwoord. Gebruik bijvoorbeeld alle eerste letters, of maak van een ‘a’ een @. Zo kan je de zin *Liever U2 dan de 6e van Beethoven!* veranderen in *LU2dd6vB!*

Tip: Kies een artiest die je leuk vindt als wachtwoord. Gebruik alle eerste letters van één van jouw favoriete nummers. Bijvoorbeeld Wzgimzztioa! Dit zijn alle eerste letters van de zin ‘Want zij gelooft in mij, zij ziet toekomst in ons allebei!’ Als geheugensteun zou je Hazes kunnen opschrijven.

WEETJE?! Op de website https://veiliginternetten.nl/wachtwoord-check/ kun je checken hoe veilig jouw wachtwoorden zijn!

*W*achtwoorden onthouden en opslaan

Het is niet slim om overal hetzelfde wachtwoord voor te gebruiken. Maar veel verschillende wachtwoorden onthouden is moeilijk. Het is heel onveilig om je wachtwoord ergens op te schrijven, dat moet je nooit doen. Je kan hooguit een ezelsbruggetje noteren. Gelukkig is er een goed hulpmiddelen voor het veilig onthouden én opslaan van wachtwoorden: **de wachtwoordmanager**

De wachtwoordmanager

Om je wachtwoorden of wachtzinnen te onthouden en op te slaan, kun je een *wachtwoordmanager* gebruiken. Dit is een tool of een app die je kunt gebruiken op je computer, telefoon of tablet.
Een wachtwoordmanager is eigenlijk een digitale kluis. Hierin bewaar je al jouw wachtwoorden en de wachtwoordmanager onthoudt ze ook meteen.
Hij vult op een veilige manier automatisch je gebruikersnaam en wachtwoord in bij het inloggen op je digitale accounts. Ook controleert de wachtwoordmanager de sterkte van je wachtwoorden en maakt hij zelf sterke wachtwoorden aan. Je hoeft dus alleen het wachtwoord voor het openen van de wachtwoordmanager te onthouden.

Twee-factor-authenticatie

Een wachtwoordmanager is bijzonder veilig omdat hij gebruikmaakt van:

1. *Twee-factor-authenticatie (2FA)*. Dit betekent dat je in twee stappen inlogt. Je opent het digitale slot als het ware niet met één sleutel, maar met twee sleutels. Eerst gebruik je je inloggegevens (gebruikersnaam en wachtwoord). Daarna vraagt de wachtwoordmanager om een tweede factor om je identiteit te verifiëren. Je krijgt bijvoorbeeld een code per sms. Maar een vingerafdruk, een melding die je accepteert in een mobiele app of gezichtsherkenning kan ook een tweede factor zijn.

2. *Encryptie*. Dit betekent dat de opgeslagen wachtwoorden onherkenbaar voor anderen worden gemaakt. De wachtwoordmanager is versleuteld. Om ze herkenbaar te maken, is een sleutel nodig die niemand anders heeft.

WEETJE?! Een bekend voorbeeld van twee-factor-authenticatie wordt gebruikt bij het pinnen van geld. De eerste factor waar je je identiteit mee bekend maakt is het invoeren van je bankpas. De tweede factor is het invoeren van je pincode.

Encryptie

Encryptie is dus het op slot zetten van digitale gegevens zodat ze alleen voor jou en degene aan wie jij ze stuurt leesbaar zijn. Door deze versleuteling wordt jouw communicatie, zoals bijvoorbeeld e-mails, beschermd. Het komt hierdoor minder snel bij verkeerde personen terecht. Sommige websites worden ook met encryptie beveiligd. Denk bijvoorbeeld aan internetbankieren. De website die je gebruikt om online te betalen moet natuurlijk goed beveiligd zijn. Hoe herken je een beveiligde website?

Check de adresbalk van de website. Er zijn twee kenmerken van een veilige website:

1. De URL (de naam van het webadres) begint met *https://*
2. In de adresbalk zie je een pictogram van een *gesloten slotje*.

De s in https:// staat voor ‘secure’, het Engelse woord voor veilig. Als je op het gesloten slotje klikt, wordt er gemeld dat de website veilig is.

Ontbreekt de https:// of het slotje? Of staat er een vreemde naam als je op het slotje klikt? Dan is het geen beveiligde website. Geef in dat geval nooit gevoelige gegevens door!

WEETJE?! ‘WhatsApp’ maakt ook gebruik van encryptie. Lees er meer over op de website van www.veiliginternetten.nl door te zoeken naar het artikel ‘WhatsApp versleutelt berichten’ of klik hier.

Beveilig netwerk

Veel zorgorganisaties werken met een beveiligde werkomgeving. Je moet eerst inloggen met jouw werkaccount voordat je bij de informatiesystemen van de organisatie kan. Vaak kan dit alleen via een internetverbinding. In het werkblad 'internet, de basis' besteden we aandacht aan het verschil tussen *openbare en beveiligde Wi-Fi netwerk*.

Een beveiligd Wi-Fi netwerk kun je herkennen aan het slotje. Om toegang te krijgen moet je het juiste netwerk kiezen en de *beveiligingssleutel* voor het netwerk invoeren. Oftewel het wachtwoord. Wanneer je via een onbeveiligd netwerk inlogt kunnen hackers toegang krijgen tot jouw computer zelfs al werk je in een beveiligde omgeving. Gebruik dus nooit een onbeveiligd Wi-Fi netwerk om in te loggen op je werkomgeving.

Digitale vingerafdruk

Je kunt je computer, telefoon of tablet ook beveiligen door deze goed te vergrendelen. Dat kan steeds vaker met een digitale vingerafdruk. Hierbij heb je voor het ontgrendelen van je beeldscherm jouw persoonlijke vingerafdruk nodig. Ook het autoriseren van betalingen en inloggen in apps gaat steeds vaker met de vingerafdrukscanner.

Vergrendeling met een vingerafdruk heeft een aantal voordelen:

- Je vingerafdruk is uniek. Alleen jij kunt met je eigen vingerafdruk inloggen.
- Anderen kunnen niet meekijken als jij je telefoon ontgrendelt. Dit is wel zo bij een pincode of patroon.
- Ontgrendelen met een vingerafdruk gaat erg snel.

Er zijn ook nadelen aan het gebruik van een vingerafdrukscanner:

- Er zit een groot verschil in kwaliteit van de verschillende vingerafdrukscanners. Ze zijn niet allemaal even geavanceerd en veilig.
- Je laat je vingerafdrukken ongemerkt overal achter. Het is mogelijk om vingerafdrukscanners daarmee te foppen.
- Met een vingerafdruk ben je ook makkelijker te dwingen je vinger te gebruiken om je telefoon te ontgrendelen.

Een goed wachtwoord of pincode heeft deze nadelen niet. Dat is de reden dat de meeste telefoons met een vingerafdrukscanner – na diverse mislukte scanpogingen – terugvallen op een code of wachtwoord.

WEETJE?! Gebruik je een vingerafdrukscanner op je telefoon? Houd deze dan up-to-date en kies het liefst voor fabrikanten die vaak en veel updaten. Installeer alleen apps van betrouwbare bronnen zoals de Google Playstore of iOS App store.

USB-sticks

Met een USB-stick heb je overal en op elk moment toegang tot bepaalde gegevens. Dat is heel handig maar het gebruik ervan is niet altijd veilig. Het vergroot de kans op:

- Een *datalek*. Als een USB-stick roekeloos wordt gebruikt kunnen persoonsgegevens of gevoelige informatie in verkeerde handen terecht komen. Dat kan bijvoorbeeld gebeuren als je de USB-stick kwijtraakt of als je hem deelt met anderen.
  Meer weten over een datalek? Volg dan de module Persoonsgegevens!
- Een *virus*. Via een USB-stick kunnen virussen makkelijk op een computer terechtkomen en zich verspreiden. Op veel apparaten opent een USB-stick namelijk direct nadat deze in het apparaat is gestoken. Als een onveilig programma op de USB-stick staat, wordt dit geopend zonder dat je er iets aan kan doen. Andersom kan een USB-stick zo makkelijk een virus overnemen van een besmet apparaat.

Het is steeds minder vaak nodig om USB-sticks te gebruiken. Redenen om wel een USB-stick te gebruiken zijn:

- '*Ik weet niet zeker of er internet is op de plek waar ik een presentatie houd.*' Maar de voorzieningen zijn laatste jaren veel beter geworden, je kunt zelfs een laptop aansluiten op de wifi van je telefoon en je telefoon via je mobiele databundel het internet op laten gaan.
- '*Ik kan op de locatie niet inloggen op mijn bedrijfsnetwerk*.' Maar dan is het vaak toch nog veiliger gebruik te maken van een privéclouddienst als gmail, dropbox of WeTransfer.

WEETJE?! Er bestaan ook USB-sticks waar je informatie versleuteld op kunt bewaren.

Virusscanners

Niet alleen mensen, ook computers, telefoons en tablets kunnen getroffen worden door een virus. Een computervirus is kwaadaardige software die je bestanden beschadigd of verwijderd, zonder dat je er iets aan kunt doen. Met behulp van een virusscanner bescherm je computer, telefoon en tablet tegen een virus. Het is niet gebruikelijk dat je een virusscanner kan downloaden op apparatuur van jouw werk. Gelukkig houdt de ICT afdeling dat voor jou in de gaten. Als je thuis ook werkt in zorgsystemen vanaf je privé computer of laptop is het verstandig een goede virusscanner aan te schaffen. Wat is een goede virusscanner?

Een goede virusscanner doet twee dingen:

1) Hij *controleert op virussen*. Dat doet de virusscanner aan de hand van een lijst met actuele informatie over bekende virussen. De bestanden, programma's en documenten op je apparaat worden vergeleken met de gegevens uit deze lijst. Bij overeenkomsten met de lijst probeert de scanner het virus te verwijderen.

2) Hij *houdt verdacht gedrag tegen*. De virusscanner zoekt *verdacht gedrag* op van programma's, documenten en bestanden op je apparaat. Verdacht gedrag kan namelijk betekenen dat er een virus is. Vervolgens zal hij het virus verwijderen.

Virusscanner installeren
Wil je een virusscanner installeren? Er zijn veel mogelijkheden. Je kunt kiezen uit gratis of betaalde scanners. Maar let op: gratis bestaat niet! Als je niet hoeft te betalen in geld, betaal je in iets anders, bijvoorbeeld door jouw persoonlijke gegevens ter beschikking te stellen aan derden. Kijk ook uit voor nep-antivirusproducten. Sommige programma's doen zich voor als virusscanner, maar besmetten je in werkelijkheid juist met een virus.

Zoek voor meer informatie op www.veiliginternetten.nl naar het artikel 'Wat is een goede virusscanner?' of klik hier.

Je weet nu hoe je veilig om kunt gaan met digitale apparaten en diensten. Je bent klaar om het Opdrachtblad te maken van de lesmodule Veiligheid.

Bronnen:

- T. van Steenbergen, *Jongeren slordiger met wachtwoorden dan ouderen*, 23 november 2015, www.nos.nl
- www.veiliginternetten.nl

Deze module is gemaakt door De Nova Learning in opdracht van 's Heeren Loo en bewerkt door Jongleert in opdracht van Utrechtzorg.

Heb je opmerkingen of vragen over deze module? Mail dan naar info@digivaardigindezorg.nl