FACTSHEET: TRAINING VEILIGHEID

In deze factsheet voor de training Veiligheid, vind je alle relevante informatie over het omgaan met wachtwoorden, encryptie en virussen.

Wachtwoorden

Waarom heb je een wachtwoord?

Het is belangrijk om een wachtwoord te hebben. Een wachtwoord zorgt ervoor dat alleen jij toegang hebt tot bepaalde gegevens en diensten.

Als eerste heb jijzelf belang bij een (veilig) wachtwoord. Stel je voor dat iemand anders met jouw wachtwoord inlogt. Hij zou dan misschien je salaris kunnen zien, rare mails kunnen versturen via jouw naam, of onbetrouwbare websites kunnen bezoeken. Ook 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.

Daarnaast hebben ook anderen er belang bij dat jij een (veilig) wachtwoord gebruikt. In het genoemde voorbeeld hierboven over cliëntdossiers bijvoorbeeld. Het is in het belang van de cliënten dat alleen de juiste mensen toegang hebben tot hun gegevens.

Een wachtwoord zorgt er dus voor, dat niet alleen je eigen persoonlijke gegevens, maar ook die van je collega's en cliënten goed beschermd zijn. Daarom is het belangrijk dat je een veilig wachtwoord hebt en dat niemand anders dit wachtwoord weet.

Waar bestaat een veilig wachtwoord uit?

Een veilig wachtwoord moet aan drie dingen voldoen:

- *Variatie*:
  Het wachtwoord moet niet voor elke dienst hetzelfde zijn. Als iemand je wachtwoord achterhaalt, kan die persoon gelijk overal bij.
- *Sterk wachtwoord*:
  - Minstens 8 tekens.
  - Niet alleen maar een bestaand woord.
  - Een combinatie van verschillende tekens, zoals hoofdletters, kleine letters, cijfers en tekens.
- *Niet te raden*:
  - Geen reeks van opeenvolgende cijfers of nummers (bijv. Qwerty)
  - Geen persoonsgegevens (bijv. je naam of de naam van je kind)
  - Geen veelgebruikte wachtwoorden, zoals password, wachtwoord, voorjaar2018, geheim. Ook geen variaties hierop.

- De beveiligingsvraag voor als je je wachtwoord bent vergeten moet niet te makkelijk zijn. Het antwoord ook niet.

Tip: Controleer online hoe sterk jouw wachtwoord is
Op de website https://veiliginternetten.nl/wachtwoord-check/ kun je dit checken. Let erop dat je niet alleen bestaande woorden of gemakkelijke cijferreeksen in je wachtwoord hebt zitten.

Fouten bij het maken en onthouden van wachtwoorden

Het kan lastig zijn om verschillende wachtwoorden te onthouden. Veel mensen maken daarom een wachtwoord aan, dat gemakkelijk te onthouden is, zoals je eigen naam plus geboortejaar (bijv. Nina1985). Of gebruiken voor elke dienst hetzelfde wachtwoord, zodat ze niet steeds een ander wachtwoord hoeven te onthouden. Ook worden wachtwoorden vaak ergens opgeschreven, om ze maar niet te vergeten. Tot slot worden wachtwoorden ook vaak automatisch opgeslagen in de internetbrowser. De voorbeelden geven de meest gemaakte fouten aan bij het maken én onthouden van wachtwoorden. Hierdoor is je wachtwoord niet veilig voor anderen. Hackers kunnen je wachtwoord dan gemakkelijk achterhalen.

Google eens op 'meest gebruikte wachtwoorden 2017', of een ander jaartal. Kijk eens of jouw wachtwoord ertussen staat. Ook zal je zien dat 123456 het meest gebruikte wachtwoord is. Nooit doen dus!

Hoe onthoud je een sterk wachtwoord?

Om je wachtwoord gemakkelijker te onthouden, zijn er enkele tips. Deze worden hieronder uitgebreid besproken:

1. Maak gebruik van een wachtwoordmanager.
2. Maak een wachtzin.
3. Extra geheugensteuntjes.

Het opschrijven in een boekje is nooit een goed idee. Je hangt je sleutels toch ook niet aan de buitenkant van je voordeur!

De wachtwoordmanager – Tip 1

Je kunt een *wachtwoordmanager* gebruiken.
Dit is een app die je kunt gebruiken op je pc/laptop, telefoon of iPad. Een wachtwoordmanager is eigenlijk een digitale kluis. Hier bewaar je al jouw wachtwoorden in. Je hoeft alleen het wachtwoord voor het openen van de wachtwoordmanager te onthouden.

De wachtwoordmanager onthoudt ook je wachtwoorden. Hij vult op een veilige manier automatisch je gebruikersnaam en wachtwoord in bij het inloggen op je accounts van websites. Ook controleert de wachtwoordmanager de sterkte van je wachtwoorden en maakt hij zelf sterke wachtwoorden aan.

Kortom, wat doet een wachtwoordmanager:

1. Je wachtwoorden bewaren.
2. Je wachtwoorden onthouden.
3. Sterke wachtwoorden aanmaken.

Waarom is een wachtwoordmanager een veilige manier voor het opslaan van wachtwoorden? Ten eerste maak een wachtwoordmanager vaak gebruik van *twee-factor-authenticatie*. Dit betekent dat je in twee stappen inlogt. Eerst gebruik je je inloggegevens (gebruikersnaam en wachtwoord). Vervolgens krijg je een code via bijvoorbeeld de sms. In het verdiepingskader op de volgende pagina wordt meer uitleg gegeven over twee-factor-authenticatie.

Ten tweede is de wachtwoordmanager versleuteld. Dit betekent dat de opgeslagen wachtwoorden onherkenbaar voor anderen worden gemaakt. Om ze herkenbaar te maken, is een sleutel nodig die niemand anders heeft. Dit heet ook wel *encryptie*. Meer uitleg over encryptie lees je verderop onder ‘Beveiliging door encryptie’.

Verdieping: Twee-factor-authenticatie.
'Twee-factor-authenticatie' en 'tweestapsverificatie' worden vaker door elkaar gebruikt omdat het principe hetzelfde is. Alleen de achterliggende techniek verschilt een beetje. Twee-factor-authenticatie is een veiligere manier van inloggen. Wanneer een cybercrimineel aan je gebruikersnaam en wachtwoord is gekomen, zou hij bij één van je diensten in kunnen loggen. Als jij dan de twee-factor-authenticatie hebt ingesteld, kan dit niet. Hij krijgt namelijk niet de extra controle sms binnen op zijn telefoon, die krijg alleen jij binnen.

Twee-factor-authenticatie is niet iets wat alleen bij een wachtwoordmanager kan voorkomen. Ook andere diensten bieden dit aan. Heb je bijvoorbeeld een DigiD, waarmee je kunt inloggen op websites van de overheid en zorg? Hiervoor gebruik je in ieder geval je DigiD-gegevens (je speciale gebruikersnaam en wachtwoord). Daarnaast kun je kiezen voor een extra controle via sms.

Meer uitleg over twee-factor-authenticatie vind je op: www.veiliginternetten.nl. Zoek op 'Wat is tweestapsverificatie' of klik op https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/.

De wachtzin – Tip 2

In plaats van een wachtwoord kun je ook een wachtzin maken. Omdat een zin uit meer letters en tekens bestaat, is het al snel een stuk veiliger. Ook is een zin makkelijker te onthouden.

Voorbeelden van wachtzinnen zijn:

- Dankzij e-mail gebruik ik zelden de telefoon!
- Brood bestaat uit gezonde vezels en mineralen!
- 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 @. Je kan bijvoorbeeld de zin *Liever U2 dan de 6e van Beethoven!* veranderen in *LU2dd6vB!*

Een veilige wachtzin:

- Bestaat uit minstens 5 woorden
- Bevat minstens een teken

Extra geheugensteuntjes– Tip 3

Je kunt ook gebruik maken van extra geheugensteuntjes om je wachtwoord gemakkelijk te onthouden. Hieronder staan twee tips.

- Bedenk een woord dat je in tweeën kunt hakken, bijvoorbeeld ‘paashaas’. Zet het systeem waar je in wilt loggen ertussen, bijvoorbeeld Dropbox. Zet een cijfer en teken achter het wachtwoord. Je krijgt dan: PaasDropboxHaas1@. Om dit te onthouden kun je Dropbox1@ als geheugensteun opschrijven.
  Zo kun je dus Paashaas onthouden voor elk apparaat. Want voor inloggen bij bijvoorbeeld Gmail, maak je PaasGmailHaas1@.
- Kies een artiest die je leuk vindt. Gebruik alle eerste letters van één van zijn/haar 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.

Veranderen van wachtwoorden

In veel organisaties is het verplicht om na een bepaalde tijd je wachtwoord te veranderen. Dit verkleint de kans dat iemand anders jouw wachtwoord weet en met jouw inloggegevens kan inloggen. Bijvoorbeeld: iemand die naast je zat in de trein heeft meegekeken terwijl je aan het inloggen was op je werksysteem. Deze persoon weet hierdoor jouw inloggegevens.

Verander daarom je wachtwoord af en toe. Bij het voorbeeld PaasDropboxHaas1@, zou je het cijfer kunnen veranderen. Dan krijg je PaasDropboxHaas2@. Of je kiest een ander liedje van dezelfde artiest. In het voorbeeld hierboven kies je dan een ander liedje van André Hazes, denk aan Ihauhl,ddldo! (Ik haal alles uit het leven, drink de laatste druppel op!).

Deze tips en nog meer zijn te vinden in het artikel ‘Veilige wachtwoorden zijn makkelijk om te onthouden’. Dit is te vinden in de Digikrant, de krant van maart 2018 over digitale vaardigheden.
Deze krant is beschikbaar voor medewerkers van ’s Heeren Loo, maar voor anderen ook digitaal te downloaden op www.digitaal-vaardig.nl.

Beveiliging door encryptie

Bijna iedereen heeft wel een sleutelbos met sleutels voor zijn huis, auto, of fiets. Deze sloten kunnen alleen opengemaakt worden met een originele sleutel. Op internet wordt informatie en communicatie soms ook gesloten voor andere mensen. Het op slot zetten van digitale informatie en communicatie heet *encryptie* (versleuteling).

Waarom is encryptie zinvol?

Door encryptie wordt communicatie, zoals e-mail of WhatsApp, beschermd. Het komt hierdoor minder snel bij de verkeerde personen terecht. Ook sommige websites worden met encryptie beveiligd.

Denk bijvoorbeeld aan internetbankieren. Je kan je voorstellen, dat de website die je gebruikt om online te betalen goed beveiligd moet zijn. Anders kan iedereen zich bemoeien met jouw bankzaken.

Hoe vindt encryptie plaats?

Encryptie kan plaatsvinden op twee manieren.

1. De *opslag van informatie* kan worden versleuteld. Denk hierbij aan de wachtwoordmanager. De wachtwoordmanager versleutelt de opgeslagen wachtwoorden via encryptie. Er bestaan ook USB-sticks en harddisks waar je informatie versleuteld op kunt bewaren.
2. Het *transport van informatie* kan worden versleuteld. Dit is bij WhatsApp berichten het geval. Stel; je collega stuurt jou een berichtje via WhatsApp. Dit berichtje kan de tijd dat hij 'onderweg is' van de mobiel van je collega naar die van jou niet gelezen worden. Mocht het berichtje afgetapt worden onderweg, is alleen de code te achterhalen. Het berichtje achter de code kan niet gelezen worden, omdat deze versleuteld is.

Lees hoe 'WhatsApp' gebruik maakt van encryptie op: https://veiliginternetten.nl/nieuws/whatsapp-versleutelt-berichten/.

Sommige websites maken gebruik van encryptie via een beveiligingscertificaat. Bijvoorbeeld websites voor internetbankieren. Klik op https://veiliginternetten.nl/zakelijk/themas/bedrijfswebsite/beveiligingscertificaat/ voor meer informatie.

Hoe herken je of een website beveiligd is?

Je kunt zelf controleren of een website veilig is of niet. Kijk hiervoor naar de adresbalk bovenin de browser en let op twee dingen:

- De URL begint met *https://*
- 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? Verlaat dan de website en tik de URL nog een keer in. En geef dan nooit gevoelige gegevens door!

Kijk eens op de site www.testjewachtwoord.nl. Is het verstandig deze website te gebruiken? Waarom wel/niet?

Beveiliging door vergrendeling

Je moet je telefoon of tablet goed beveiligen. Als iedereen zomaar op jouw telefoon of tablet kan, is de informatie niet veilig. Daarom is het belangrijk om deze apparaten te vergrendelen.

Beveiligen via een digitale vingerafdruk

Een manier om te vergrendelen is met een digitale vingerafdruk. Hierbij heb je voor het ontgrendelen van je beeldscherm een vingerafdruk nodig. Je kunt de vingerafdrukscanner als schermvergrendeling zelf instellen. Dit kan per apparaat iets verschillen.

Vergrendeling met een vingerafdruk heeft een aantal voordelen. Je vingerafdruk is uniek. Alleen jij kunt met je eigen vingerafdruk inloggen. Daarnaast kunnen anderen niet meekijken, als jij je telefoon ontgrendelt. Dit is wel zo bij een pincode of patroon. Bovendien gaat het ontgrendelen sneller met een vingerafdruk.

Voor alle Apple apparaten kun je de volgende site raadplegen om je vingerafdruk (Touch ID) in te stellen. Klik op https://www.appletips.nl/touch-id-instellen/

Het gebruik van een vingerafdruk is erg veilig. Zitten er ook risico’s aan? Het is belangrijk om dit voor jezelf te bedenken. Google maar eens op ‘hoe veilig is je vingerafdruk’, en je leest verschillende meningen.

Virussen

Een virus is kwaadaardige software op je computer. Een virus kan je bestanden beschadigen of verwijderen, zonder dat je er iets aan kunt doen.

Wat is een virusscanner?

Een virusscanner is een computerprogramma dat controleert of een computer een virus heeft. Ook probeert een virusscanner een virus tegen te houden en te verwijderen.

Een virusscanner werkt op twee manieren:

1. De virusscanner heeft een *blacklist*: een lijst met alle informatie over bekende virussen. De bestanden, programma's en documenten op de computer worden vergeleken met de gegevens uit de blacklist. Bij overeenkomsten met de blacklist, wordt geprobeerd het virus te verwijderen.
2. De virusscanner zoekt *verdacht gedrag* op de computer van programma's, documenten en bestanden. Verdacht gedrag kan betekenen dat er een virus is. Wanneer een virus gevonden is, zal dit worden verwijderd.

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. Misschien worden jouw gegevens gedeeld met derden. De een vindt dat prima, de ander heeft er moeite mee. Bedenk voor jezelf wat jij oké vindt.

Zoek voor meer informatie op www.veiliginternetten.nl naar het artikel 'Een virusscanner voor je computer downloaden'. Of klik op https://veiliginternetten.nl/themes/situatie/ik-heb-een-virus-na-het-downloaden/

Soms is een virusscanner nep. Deze scanners besmetten computers juist met virussen. Voordat je een virusprogramma installeert moet je hier alert op zijn! Kijk bijvoorbeeld op Google of YouTube welke antivirusprogramma's te vertrouwen zijn. Kijk ook altijd op de site van het programma zelf. Download het niet via een andere website.

Het gebruik van USB-sticks

Het voordeel van een USB-stick is dat je overal en op elk moment toegang hebt tot bepaalde gegevens. Er zitten alleen ook grote risico's aan het gebruik van een USB-stick.

Risico's van het gebruik van USB-sticks

Allereerst kan een USB-stick de kans op een datalek vergroten, doordat een USB-stick kwijtraakt of in verkeerde handen valt. Verkeerde handen zijn bijvoorbeeld mensen die slechte bedoelingen hebben. Maar let op! Ook gezinsleden worden hiermee bedoeld. In veel gezinnen worden USB-sticks gedeeld. Hier zit geen verkeerde bedoeling achter, maar toch is het risicovol. Stel dat je kind een spreekbeurt houdt op school. Alle leerlingen en leerkrachten kunnen de andere bestanden op de USB-stick dan inzien. Of iemand uit je gezin raakt de USB-stick kwijt. Kijk hier dus mee uit.

De risico's van het gebruik van een usb-stick kunnen leiden tot een datalek. Wil je meer weten over een datalek? Volg dan ook de training Persoonsgegevens!

Daarnaast kunnen virussen makkelijk op een computer terechtkomen via een USB-stick. 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 direct geopend zonder dat je er iets aan kan doen.

Ook kunnen virussen gemakkelijk verspreid worden door een USB-stick. Stel dat op één apparaat een virus staat en de USB-stick wordt op dat apparaat gebruikt. Het virus kan op de USB-stick terecht komen. Vervolgens kan dit virus, doordat een USB-stick ook op andere computers wordt gebruikt, zich verspreiden.

Meer informatie over verschillende risico's van het gebruik van USB-sticks? Zoek dan het artikel 'Bescherming tegen onveilige USB-sticks' van Rijksoverheid. Of klik op https://www.rijksoverheid.nl/documenten/rapporten/2009/12/02/bescherming-tegen-onveilige-usb-sticks.

Bronnen:

- www.veiliginternetten.nl
- www.rijksoverheid.nl
- www.appletips.nl
- www.digitaal-vaardig.nl
- www.antivirus.nl
- www.digid.nl
- www.testjewachtwoord.nl