TRAINING:

VEILIGHEID

TRAINING VEILIGHEID

Bij deze training hoort de Factsheet ‘Veiligheid’. Lees deze eerst en gebruik deze bij de training. In de training over Veiligheid leer je hoe je veiliger om kunt gaan met informatie. Je leert waarom een wachtwoord nodig is en wanneer een wachtwoord veilig is. Ook leer je meer over encryptie en waarom dit belangrijk is. Daarnaast leer je verschillende manieren van schermvergrendeling. Ook leer je wat een virusscanner is. Tot slot wordt ingegaan op het gebruik van USB-sticks. De training bestaat uit elf opdrachten, waarin deze onderwerpen worden behandeld.

Beveiliging door wachtwoorden

Wachtwoorden hebben we allemaal. Voor je telefoon, je pc of een account van je werk bijvoorbeeld. Door een wachtwoord zorg je ervoor dat niemand anders bij bepaalde informatie kan komen. Dit is belangrijk voor zowel jezelf, als voor een ander!

Opdracht 1

Zoek op YouTube het filmpje ‘Hoe kraakt iemand een wachtwoord?’ Of klik op https://www.youtube.com/watch?v=sCMotoEV3TY. Bekijk dit filmpje en beantwoord dan de onderstaande vragen.

a. Waar voldoet een goed wachtwoord aan? Noem tenminste drie eisen.

1

2

3

b. Welke wachtwoorden zijn veilig volgens het filmpje? Vink het groene vakje aan als een wachtwoord veilig is. Vink het rode vakje aan als een wachtwoord onveilig is.

☐ ☐	Nina1234	☐ ☐	H!nT$sp3\
☐ ☐	Januari01!	☐ ☐	L!VVi3@
☐ ☐	R1@#yR?	☐ ☐	YruNi9Hr?&
☐ ☐	24917415	☐ ☐	Lu(A$d3J0^G
☐ ☐	Max rijdt in een grote Mercedes!		

Opdracht 2

Welke wachtwoorden gebruik jij allemaal? Denk aan je mobiele telefoon, je iPad, je e-mailaccount, LinkedIn, Dropbox. Verschillen ze van elkaar?

Ga naar de volgende site: www.veiliginternetten.nl/wachtwoord-check/

Beantwoord de twee vragen op de site voor enkele wachtwoorden die je gebruikt.

- Uit hoeveel tekens bestaat je wachtwoord?
- Welke tekens gebruik je in jouw wachtwoord?

Scroll daarna op de site naar beneden. Hier zie je hoelang het duurt, voordat je wachtwoord is gekraakt. Dit is verschillend voor een standaard, gezamenlijke of een mega aanval.
Vul het schema hieronder in voor een paar van je wachtwoorden:

Wachtwoord	**Hoelang duurt het voordat het wachtwoord is gekraakt?**		
	Standaard aanval	**Gezamenlijke aanval**	**Mega aanval**
Werk e-mail			
Pc/laptop			
Ipad			
LinkedIn			
Anders			

Wachtwoorden onthouden

Het is belangrijk om een veilig wachtwoord te verzinnen. En daarnaast om voor elke dienst een ander wachtwoord te gebruiken. Maar hoe onthoud je die dan allemaal?

Zonder dat je het weet, gebruik je voor veel verschillende accounts een wachtwoord. In Nederland hebben mensen gemiddeld 22 wachtwoorden! Dit is natuurlijk erg veel en lastig te onthouden. Wat je nooit moet doen, is je wachtwoorden ergens opschrijven. Wat dan wel? Opdracht 3 en 4 gaan hierover.

Opdracht 3

Bedenk hoeveel wachtwoorden je ongeveer hebt. Denk hierbij aan een wachtwoord voor je e-mailadres, online bankieren, het aanzetten van je pc/laptop, je account bij je werk, of sociale media zoals LinkedIn en Facebook.

a. Hoeveel verschillende wachtwoorden die je zelf gebruikt, kun je bedenken?

Tip 1: Wachtwoordmanager

b. Bekijk de volgende site: www.vaulteq.com. Op welke manier kan deze site je helpen om je wachtwoorden te onthouden?
Tip: Kijk bijvoorbeeld onderaan de homepage onder ‘Ondersteuning’ en klik op ‘Over Vaulteq’.

Tools zoals Vaulteq worden *wachtwoordmanagers* genoemd. In zo’n wachtwoordmanager kun je al je wachtwoorden opslaan. Je hoeft dan nog maar één wachtwoord onthouden, namelijk die om de wachtwoordmanager te openen!

Wil je een wachtwoordmanager gebruiken voor al je wachtwoorden?
Er zijn verschillende aanbieders. Belangrijk is dat je een veilige aanbieder kiest. Amerikaanse aanbieders zoals 1Password of KeePass zijn volgens de Consumentenbond veilig. Informeer eens bij je organisatie of zij een wachtwoordmanager gebruiken!
Er zijn ook Nederlandse aanbieders zoals Vaulteq die een app aanbieden, die je kunt vinden in de Google Playstore of via www.vaulteq.com.

Op https://www.consumentenbond.nl/veilig-internetten/test-wachtwoordmanagers kun je een aantal tips lezen over het gebruik van de wachtwoordmanager.

Wachtzinnen

Er is ook een andere veilige optie om wachtwoorden te onthouden. Maak gebruik van een wachtzin, in plaats van een wachtwoord! Zinnen bestaan namelijk uit meer letters en tekens. Hierdoor zijn ze al snel een stuk veiliger. Daarnaast is een zin gemakkelijker te onthouden. Een voorbeeld van een wachtzin is: ‘Dankzij e-mail gebruik ik zelden de telefoon!’

Opdracht 4

Tip 2: Wachtzinnen

Stel: Je moet voor de toegang tot je zorgdossiers een nieuw wachtwoord instellen. Je vindt de zin ‘Mijn 1e zoon Victor houdt van voetbal!’ een mooie wachtzin. Je wilt je wachtwoord veranderen, maar je krijgt een foutmelding:

‘Sorry, je wachtwoord mag maximaal 12 tekens bevatten.’

Hoe zou jij de wachtzin veranderen, zodat het uit maximaal 12 tekens bestaat?

Tips over het veranderen van een wachtzin?
Zoek bijvoorbeeld naar 'Van wachtwoord naar wachtzin' op de website van Nederlands Cyber Collectief of klik op https://nederlandscybercollectief.nl/nl/tip/van-wachtwoord-naar-wachtzin.

Beveiliging door versleuteling

We beveiligen dingen door ze op slot te doen.
Denk aan je fiets, je voordeur, of een kluis. Dit kun je alleen openmaken met een originele sleutel.

Ook op het internet heeft veel informatie een eigen sleutel. Hiermee beveilig je de informatie. Zo kan bijvoorbeeld niet iedereen jouw mails naar je leidinggevende of WhatsApp gesprekken meelezen. Deze digitale sleutel wordt *encryptie* (versleuteling) genoemd. Wanneer digitale informatie toch geopend wordt, zonder de originele sleutel te gebruiken, heet dit *hacken*.

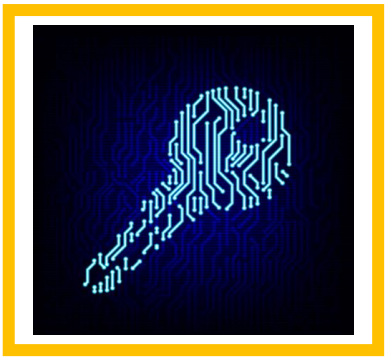
Zoek op YouTube het filmpje 'Hoe beschermt versleuteling jouw bestanden? NOS op 3' of klik op https://www.youtube.com/watch?v=hvvw48FV4G0. Bekijk het filmpje.

Opdracht 5

Lees de volgende casus:

Rianne werkt bij de administratie en moet nieuwe werklaptops bestellen. Ze gaat naar de website van de leverancier en bestelt tien laptops. Vervolgens gaat ze naar de website van de bank en betaalt online de bestelling. In haar mail opent zij de factuur en mailt die door naar haar leidinggevende.

Noem relevante websites uit de casus waarbij encryptie erg belangrijk is.



Tip! Je kunt zelf zien of een site is beveiligd met encryptie:

- Een site begint dan met *https://*
- En in de adresbalk staat een slotje

Opdracht 6

a. Onderzoek eens van de verschillende sites hieronder of ze veilig zijn.

Site	Begint met https://	Heeft een slotje	Veilig?
Je e-mail	ja/nee	ja/nee	ja/nee
De site van je werkgever	ja/nee	ja/nee	ja/nee
www.zorgvisie.nl	ja/nee	ja/nee	ja/nee
www.vgn.nl	ja/nee	ja/nee	ja/nee
www.zorgwacht.nl	ja/nee	ja/nee	ja/nee
www.reinaerde.nl	ja/nee	ja/nee	ja/nee

b. Welke sites zijn niet veilig? Welk teken wordt gebruikt in plaats van het slotje? En wat staat er als je hierop klikt?

Niet-veilige sites	Welk teken?	Wat staat er?
1		
2		

Beveiliging door vergrendeling

De WhatsApp berichten die je stuurt zijn ook beveiligd met encryptie. Informatie via WhatsApp blijft dus alleen tussen jou en de andere persoon. Ook als je met een collega of een ouder/verzorger appt over je cliënt. Maar wat als je telefoon wordt gestolen?

Opdracht 7

Op je zakelijke iPhone of iPad kunnen gevoelige gegevens staan. Dus deze kun je maar beter goed vergrendeld hebben. Als je telefoon in andermans handen terechtkomt, moet hij/zij er niet makkelijk in kunnen komen. Er bestaan verschillende manieren van vergrendelen. Niet op elk apparaat gebruik je alle manieren.

a. Kruis aan welke manier van vergrendelen jij gebruikt bij jouw telefoon.

- ☐ Geen
- ☐ Vergrendeling door een patroon
- ☐ Vergrendeling door een pincode
- ☐ Vergrendeling door een wachtwoord
- ☐ Vergrendeling door een vingerafdruk
- ☐ Vergrendeling door gezichtsherkenning

Misschien heb je op jouw telefoon nog niet je vingerafdruk ingesteld. Dit kan je doen door de onderstaande instructie te volgen.

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

b. Noem een voor- en nadeel van het gebruiken van je vingerafdruk voor vergrendeling.

Voordeel	
Nadeel	

Virussen

Het is dus belangrijk om je apparaten en websites te beveiligen. Maar ook is het belangrijk om je apparaten te beschermen tegen virussen. Zoek op YouTube het filmpje ‘Alert Online – Virussen NL’ of klik op https://www.youtube.com/watch?v=GR9tCE57nXw.

Opdracht 8

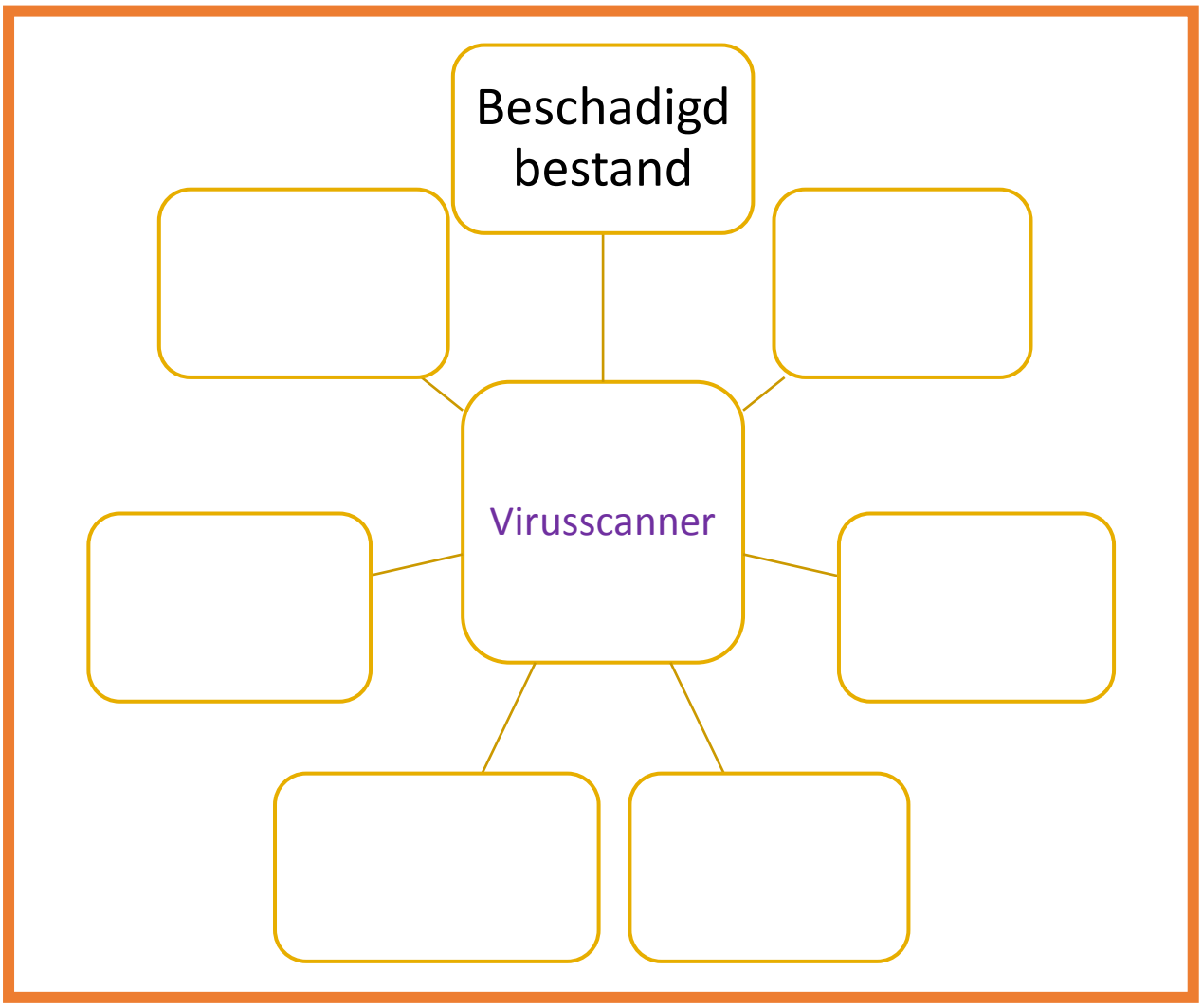
Een virus kan veel schade aanrichten aan je computer en bestanden. Ook voor bedrijven kunnen virussen voor veel problemen zorgen. Zo heeft het bedrijf TNT Express vorig jaar te maken gehad met een virusaanval. Deze aanval heeft grote gevolgen gehad voor het bedrijf. Zoek op RTLZ het artikel ‘Cyberaanval kost FedEx minstens 250 miljoen euro’ of klik op https://www.rtlz.nl/beurs/bedrijven/cyberaanval-kost-fedex-minstens-250-miljoen-euro.

Is er binnen jouw organisatie wel eens een virus geweest? Of heb je zelf hier mee te maken gehad? Wat waren de gevolgen voor jouw organisatie en voor jezelf?

Bedrijf	Gevolgen
1 Bij mijn organisatie	
2 Bij mijzelf	

Opdracht 9

Een virusscanner is daarom erg belangrijk. Kijk op https://veiliginternetten.nl/themes/basisbeveiliging/virus/ voor meer informatie over hoe een virusscanner werkt.
Maak het woordweb af bij het onderwerp ‘Viruscanner’. Welke begrippen passen hierbij?



Opdracht 10

Lees de volgende casus:

Ronald heeft net een nieuwe computer gekocht. Hij wil zijn computer goed beveiligen en gaat op zoek naar een antivirusprogramma. Op internet vindt hij verschillende programma’s. Hij twijfelt welk programma hij zal installeren.

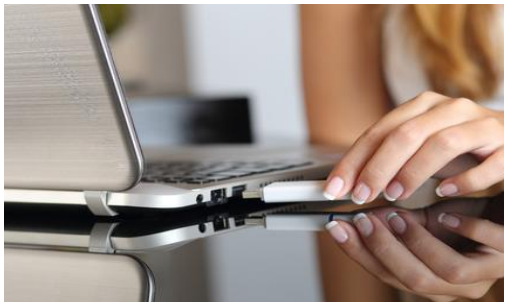
Welke kenmerken passen bij een veilige virusscanner? Vink het groene vakje aan als het een kenmerk van een veilige virusscanner is. Vink het rode vakje aan als het een kenmerk van een onveilige virusscanner is.

- ☐ ☐ Je kent veel mensen die dat programma gebruiken.
- ☐ ☐ Het programma wordt niet genoemd op vergelijkingssites.
- ☐ ☐ Het programma wordt aanbevolen op een blog.
- ☐ ☐ Het programma wordt genoemd op één website.
- ☐ ☐ Het programma wordt aanbevolen op de website van de consumentenbond.

Trap er niet in!
Veel mensen maken gebruik van een virusscanner. Cybercriminelen spelen daar graag op in. Zij maken nep-antivirusprogramma's. Bij een nep-antivirusprogramma lijkt het alsof je een echt antivirusprogramma hebt gedownload. Maar eigenlijk besmet het je computer juist! Het zorgt er bijvoorbeeld voor dat je bankgegevens gestolen worden.
Let dus goed op welk virusprogramma je installeert!

USB-sticks

Een USB-stick kan een handig middel zijn om bestanden op te bewaren. Je kunt de USB-stick namelijk overal mee naartoe nemen. Toch zijn er risico's aan verbonden.



Opdracht 11

Stel, jij hebt enkele dossiers van cliënten op je USB-stick gezet. Zo kun je er vanavond thuis nog even naar kijken. Welke risico's kun jij bedenken bij het gebruiken van je USB-stick? Trek lijnen van 'Risico's gebruik USB-sticks' naar de verschillende mogelijke risico's.

Risico's gebruik USB-sticks

Kans op datalek

Materiaal USB is van slechte kwaliteit

Kans dat gezinslid je USB gebruikt

Je vergeet waar je al je bestanden opgeslagen hebt

Kans dat mensen meelezen

Kans op het verspreiden van virussen

Je vergeet de USB-stick uit de computer te halen en mee te nemen

Veel USB-sticks openen de bestanden automatisch

WAT HEB JE ZOJUIST GELEERD?

Wachtwoorden:

- **Je weet wat veilige wachtwoorden zijn.**
- **Je weet waar je op een veilige manier je wachtwoorden kunt opslaan.**

Beveiliging:

- **Je weet wat encryptie betekent.**
- **Je kunt schermontgrendeling via vingerafdruk instellen.**

Virussen:

- **Je weet wat een virusscanner is.**
- **Je kent de risico's van het gebruik van een USB-stick.**