ANTWOORDBLAD

VEILIGHEID

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

ANTWOORDBLAD VEILIGHEID

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

Opdracht 1

a. Onderstaande punten komen in het filmpje naar voren. Kijk of je ze alle vijf hebt!
Een veilig wachtwoord:

1. Is sterk en niet te raden.
2. Bestaat uit minstens 8 tekens. Zowel hoofdletters, kleine letters, cijfers als tekens.
3. Bestaat niet alleen maar uit bestaande woorden.
4. Bevat geen reeks van opeenvolgende cijfers of letters.
5. Bevat geen persoonlijke gegevens. Een naam, geboortedatum of hobby mag niet uitgeschreven zijn in gewone letters in het wachtwoord.

b. In de tabel hieronder zie welke wachtwoorden veilig en welke onveilig zijn. Bij de onveilige wachtwoorden vind je de toelichting waarom het onveilig is.

Veilige wachtwoord	Onveilige wachtwoord	Waarom?
H!nT$sp3\	Nina1234	Persoonsgegevens + cijferreeks
YruNi9Hr?&	Januari01!	Heel woord (dat erg voor de hand ligt)
Lu(A$d3J0^G	R1@#yR?	Minder dan 8 tekens
Wachtzin: Max rijdt in een grote Mercedes!	24917415	Alleen cijfers en geen andere tekens
	L!VVi3@	Minder dan 8 tekens

Opdracht 2

Het antwoord is afhankelijk van jouw persoonlijk gedeelde informatie. Hoe lang het kraken duurt, hangt af van welk wachtwoord je gebruikt. In de regel geldt dat hoe langer het wachtwoord, hoe langer het duurt voordat hij gekraakt is.

Hoe langer een wachtwoord, hoe veiliger!

Opdracht 3

a. Het antwoord is afhankelijk van jouw persoonlijk gedeelde informatie.

b. Er bestaan veel verschillende wachtwoordmanagers. De wachtwoordmanagers 1Password en KeePass zijn volgens de Consumentenbond heel veilig. Ook LastPass en Dashlane zijn bekende en veelgebruikte wachtwoordmanagers.

Opdracht 4

a. Bijvoorbeeld alle eerste letters: M1zVhvv!
Ook kan je kiezen voor de eerste twee letters van sommige woorden: Mij1zooVhvv!
Let erop dat je bij zo'n wachtwoord in ieder geval hoofd- en kleine letters gebruikt, tekens, en cijfers.

Opdracht 5

a. In de casus bezocht Rianne verschillende websites om de laptops aan te kunnen schaffen. Op alle websites moest ze daarvoor belangrijke gegevens delen. Het is daarom belangrijk dat alle websites versleuteld zijn:

- De website van de webshop waar Rianne de laptops aanschaft.
- De website van de bank waar Rianne de laptops mee betaalt.
- De website die Rianne gebruikt om te e-mailen met haar leidinggevende.

Opdracht 6

a. Je kunt zien of een website veilig is als de URL begint met *https://* én als er een *slotje* in staat. In de tabel hieronder lees je welke websites veilig zijn. Je e-mail en website van je werkgever moet je zelf controleren, omdat dit per e-mailaccount en werkgever kan verschillen.

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

Let op: een site die vandaag veilig is, kan morgen onveilig zijn! Deze tabel is dus tijdgebonden.

Opdracht 7

a. Het antwoord is afhankelijk van jouw persoonlijk gedeelde informatie.

b. Hieronder staan een aantal mogelijke voordelen nadelen genoemd van vergrendeling met een digitale vingerafdruk.

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.

Nadelen

- 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.

Opdracht 8

a. Misschien ben je ooit getroffen door een virus, misschien ook niet. Bedenk dan wat de gevolgen zouden kunnen zijn in deze situaties. Hieronder staan een paar opties.

Bedrijf	Gevolgen
1 **Bij mijn organisatie**	Gegevens van cliënten gestolen Werkzaamheden liggen stil Herstelkosten Website offline
2 **Bij mijzelf**	Persoonlijke bestanden beschadigd Bestanden kunnen niet meer worden geopend Bestanden zijn verloren gegaan Computer loopt vast Ongewenste sites of reclames openen

Opdracht 9

a. Mogelijke voorbeelden van begrippen voor het woordweb van ‘Virusscanner’ zijn:

- virus
- malware
- geïnfecteerd bestand
- kwaadaardige software
- beschadigd bestand
- bestanden verwijderd

- blacklist
- verdacht gedrag
- virus verwijderen

Opdracht 10

a. Hieronder lees je de kenmerken die horen bij een veilige en bij een onveilige virusscanner.

Kenmerken van een veilige virusscanner:

- Je kent veel mensen die dat programma gebruiken.
- Het programma wordt aanbevolen op de website van de consumentenbond.

Kenmerken van een onveilige virusscanner:

- Het programma wordt niet genoemd op vergelijkingssites.
- Het programma wordt aanbevolen op een blog.
- Het programma wordt genoemd op één website.

Opdracht 11

a. De mogelijke risico's van het gebruiken van een USB-stick zijn:

- Kans op een datalek.
- Je vergeet je USB-stick uit de computer te halen en mee te nemen.
- Kans op het verspreiden van virussen.
- Veel USB-sticks openen de bestanden automatisch.
- Kans dat gezinslid je USB-stick gebruikt.

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