NL

SMART 04

Persoonlijke mobiele beveiliging

Deze module beschrijft een aantal aspecten waar je op moet letten bij het gebruik van mobiele technologie.

Start cursus >

Co-funded by the Erasmus+ Programme of the European Union

SMART MODULE 4

Persoonlijke mobiele beveiliging

In de afgelopen decennia zijn mobiele apparaten niet langer alleen geschikt voor het voeren van gesprekken, maar ook voor vele andere doeleinden. Dit heeft geleid tot mobiele toegang tot bankieren, apps en internet. Met deze nieuwe mogelijkheden komt ook de zorg over gegevensbeveiliging. In deze module geven we uitleg over gegevensbescherming, hoe je wachtwoorden aanmaakt en wijzigt, veilige wifi-navigatie, en hoe je jezelf beschermt tegen cyberpesten en oplichters.

Doelgroep

Deze module is bedoeld voor iedereen die wil leren over veilig online navigeren, gegevensbescherming, cookies en hoe de wet persoonlijke gegevens beschermt (AVG).

Dit module kan voor sommige cursisten een uitdaging vormen. In dat geval zou het nuttig zijn om de inhoud samen met een begeleider of vriend(in) door te nemen.

Begeleiders kunnen deze module gebruiken om zichzelf te informeren en advies te geven over de veiligheidsaspecten van digitale technologieën.

Wat je zult leren in deze module

1. AVG en toestemming voor cookies
2. Wachtwoorden aanmaken en wijzigen
3. Wat is hacken en hoe kun je jezelf beschermen?
4. Hoe je jezelf beschermt tegen cyberpesten

Hoofdstukken in deze module

SMART | MODULE 4 | HOOFDSTUK 1

Inleiding tot mobiele beveiliging en gegevenseigendom

Informatie is macht!" Persoonlijke informatie is een van onze meest waardevolle bezittingen. In de moderne tijd wordt deze belangrijke bron volledig onderschat door consumenten, maar niet door bedrijven! Een aantal van de grootste bedrijven ter wereld zijn succesvol geworden door slim gebruik te maken van jouw gegevens. Dit hoofdstuk geeft uitleg over het eigendom van gegevens in het tijdperk van mobiel computergebruik en "de cloud".

Wat je zult leren in deze module

1. Wat is de Algemene Verordening Gegevensbescherming (AVG).
2. Bescherming van persoonsgegevens onder AVG.
3. Hoe cookies beheren.
4. Soorten persoonsgegevens.
5. Waar worden je gegevens opgeslagen?
6. Een back-up maken van je mobiele apparaat.

Gegevensanalyse – de snelst groeiende nieuwe “bedrijfstak”

Het verzamelen en analyseren van gegevens is belangrijk voor bedrijven om de behoeften van de klant te begrijpen. Gegevensanalyse heeft bedrijven geholpen hun diensten voor klanten te verbeteren.

Gegevensanalyse maakt websites en apps beter bruikbaar, en laat bijvoorbeeld een gebruiker van een smartwatch zien hoeveel stappen hij op een dag heeft gezet. Gegevensanalyse wordt vaak toegepast op (jouw) **persoonlijke gegevens**.

Persoonsgegevens en mobiele en draagbare apparaten

Persoonsgegevens is informatie die betrekking heeft op een identificeerbaar individu.

Bedrijven moeten persoonlijke informatie van burgers beschermen onder de wet **Algemene Verordening Gegevensbescherming (AVG)** door gevoelige **informatie** die wordt opgeslagen of via openbare netwerken wordt verzonden te coderen.

AVG wordt later in dit hoofdstuk besproken.

Waarom het belangrijk is gegevens te beveiligen die door mobiele apparaten worden verzameld

Wanneer een persoon of organisatie zonder toestemming of goedkeuring toegang krijgt tot persoonlijke informatie (adres, leeftijd en geslacht, gezondheidskwesties, financiële status, interesses) kan dit problemen opleveren voor de persoon van wie de gegevens worden verzameld.

Persoonsgegevens zijn gegevens die betrekking hebben op een identificeerbare persoon. Dergelijke informatie helpt om een dienst voor jou te personaliseren. Bedrijven moeten onder de **AVG-wetgeving** jouw persoonlijke gegevens beschermen door gevoelige **informatie** die via openbare netwerken naar derden worden gestuurd, te versleutelen. Zoals bijvoorbeeld met de hierboven getoonde voorbeelden van persoonlijke gegevens.

Meer informatie is te vinden op https://autoriteitpersoonsgegevens.nl/.

Wat is AVG?

Om te voorkomen dat bedrijven persoonlijke gegevens van burgers krijgen zonder hun toestemming, heeft de Europese Commissie de Algemene Verordening Gegevensbescherming (AVG) ingevoerd.

De AVG beschermt de persoonsgegevens van burgers die binnen de Europese Unie wonen en werken. Organisaties die actief zijn in de EU moeten toestemming hebben om persoonsgegevens te verwerken.

AVG - welke rechten biedt het binnen de EU?

AVG biedt personen de volgende rechten

- het recht om geïnformeerd te worden
- het recht op toegang
- het recht op rectificatie en wissing
- het recht op beperking van de verwerking
- het recht op overdracht van gegevens
- het recht op bezwaar
- het recht op geautomatiseerde profilering

Welke soorten gegevens kunnen als persoonsgegevens worden beschouwd?

Om het belang van privacyrechten in de EU te begrijpen, moeten we weten welke soorten persoonsgegevens onder de AVG kunnen vallen.

Laten we eens kijken naar enkele typische voorbeelden van soorten gegevens die als persoonsgegevens kunnen worden beschouwd en dus het beschermen waard zijn.

Voorbeelden van persoonsgegevens

1

2

3

Demografische gegevens zijn persoonsgegevens

Wanneer iemand een formulier invult om bijvoorbeeld een subsidie aan te vragen, vertrouwt hij de organisatie die het formulier maakt, om gevoelige informatie vertrouwelijk te behandelen. Dit is een vorm van persoonsgegevens.

Voorbeelden van persoonsgegevens

1

2

3

Zorgdossiers bevatten persoonsgegevens

Een bezoek aan een arts wordt beschouwd als een vertrouwelijke ervaring. De gegevens die over een individuele patiënt worden vastgelegd, zijn ook zeer vertrouwelijk en kunnen dus als persoonsgegevens worden beschouwd.

Voorbeelden van persoonsgegevens

1

2

3

Een verslag van dagelijkse activiteiten is een persoonsgegeven

Een overzicht van aankopen, bezochte locaties en gemaakte reizen van een geregistreerd persoon zijn ook persoonsgegevens.

Dagelijkse activiteiten

Mobiele apparaten en draagbare apparaten registreren buitengewoon veel details over iemands dagelijkse activiteiten. Veel van deze persoonlijke gegevens belanden in de cloud databases van mobiele en draagbare apps. Door over deze gegevens te beschikken, kunnen technologiebedrijven je gedetailleerde informatie geven over je activiteiten.

Voorbeelden van persoonsgegevens

4

5

Individuele financiële informatie

Financiële overzichten, kredietbeoordelingen en informatie over banksaldo zijn een andere categorie van persoonsgegevens. Het kan gebruikt worden om je te categoriseren als een grote verteerder, of een voorzichtige koper.

Voorbeelden van persoonsgegevens

4

5

Beelden of opnames van mensen

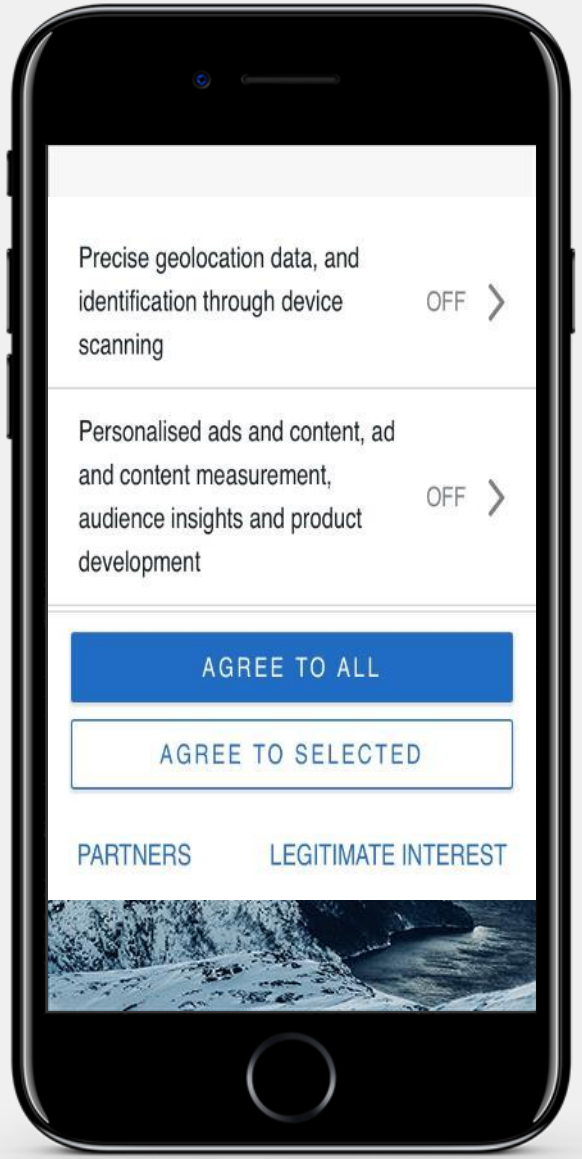
Eigenaren van beveiligingscamera's moeten voorzichtig zijn met het opslaan van videobeelden, omdat deze persoonsgegevens kunnen bevatten. Hetzelfde geldt voor geluidsopnamen. Beide mogen alleen worden bewaard met toestemming van degenen die worden opgenomen.

Cookies: overeenkomsten om persoonlijke gegevens aan een bedrijf te geven

Cookies zijn kleine bestanden die websites naar je apparaat sturen om bepaalde informatie over jou te onthouden. Bijvoorbeeld je sportvoorkeuren of inloggegevens.

Volgens de AVG-voorschriften moet een website toestemming van de gebruiker krijgen om cookies op zijn apparaat te installeren.

Als je je zorgen maakt over de analyse van je gegevens, kun je de opties "Alles weigeren" of " Akkoord met gekozen " selecteren (zoals in de afbeelding hier). Het uitschakelen van cookies betekent dat de website niet gepersonaliseerd is en geen details zoals een wachtwoord of aankopen kan onthouden.



Nepberichten - een waarschuwing!

Soms verschijnen er interessante berichten op je mobiele apparaat. Wanneer je een bericht ziet voor een prijs of een verhaal dat te mooi lijkt om waar te zijn, is het meestal een truc om je geld misschien te stelen.

Wanneer je zo'n bericht ontvangt, is het belangrijk om geen formulier in te vullen, niet op een link te klikken of geen persoonlijke informatie te delen, zoals telefoonnummers, e-mail of adres, tenzij je weet dat het van een geldige bron komt.

Ook nieuwsberichten die je op je telefoon leest kunnen "nepnieuws" zijn - nieuws dat vals of verzonnen is.

Wat is de cloud?

De zogenaamde cloud is een wereldwijd netwerk van krachtige computers, en de software die op die computers draait. Je persoonlijke gegevens kunnen van je worden verzameld en opgeslagen in de cloud computer waar ook ter wereld. Ook door jou gecreëerde gegevens kunnen in de cloud worden opgeslagen en je hebt vanaf meerdere apparaten toegang tot die gegevens.

De opslag en analyse gebeuren op cloud computers in een gegevenscentrum, in plaats van lokaal op het apparaat van de gebruiker.

https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud

De cloud is erg handig voor mobiele apparaten

Probleem: apparaatopslag is beperkt

De meeste mobiele apparaten hebben slechts een beperkte opslagruimte. Op een gegeven moment raakt de opslagruimte op en wordt de verwerking traag.

Oplossing: gegevens opslaan en analyseren in de cloud

Bestanden, foto's, video's kunnen naar de cloud worden gekopieerd. Het is goed om kopieën te bewaren in de cloud. Het is echter belangrijk te onthouden dat cloud beveiliging een probleem kan zijn.

Cloud beveiliging

Hoe veilig zijn gegevens wanneer ze je mobiele apparaat hebben verlaten en zijn opgeslagen in de cloud?

Zelfs afgezien van bedrijven die gegevens van gebruikers gebruiken om meer producten te verkopen, kunnen persoonlijke gegevens in de cloud worden gehackt en gebruikt voor criminele doeleinden. Cloud beveiliging is belangrijk voor persoonlijke gegevens en mobiele apparaten. Zorg ervoor dat je serviceprovider en gegevens in de EU zijn gevestigd.

Cloud gegevens: waar bewaar je je bestanden? Lokaal of in de cloud?

Voordelen

- Personalisering en betere service
- Meer opslagruimte, aangezien een mobiel apparaat beperkte opslagruimte heeft
- Meer gegevens betekent "slimmere" beslissingen
- Alle gegevens lijken "op één plaats" te staan

Nadelen

- De gebruiker accepteert een verlies van gegevensprivacy aan de cloud provider
- Mogelijkheid van diefstal en fraude
- Als gegevens eenmaal in de cloud staan, is het uiterst moeilijk ze te verwijderen

Quiz

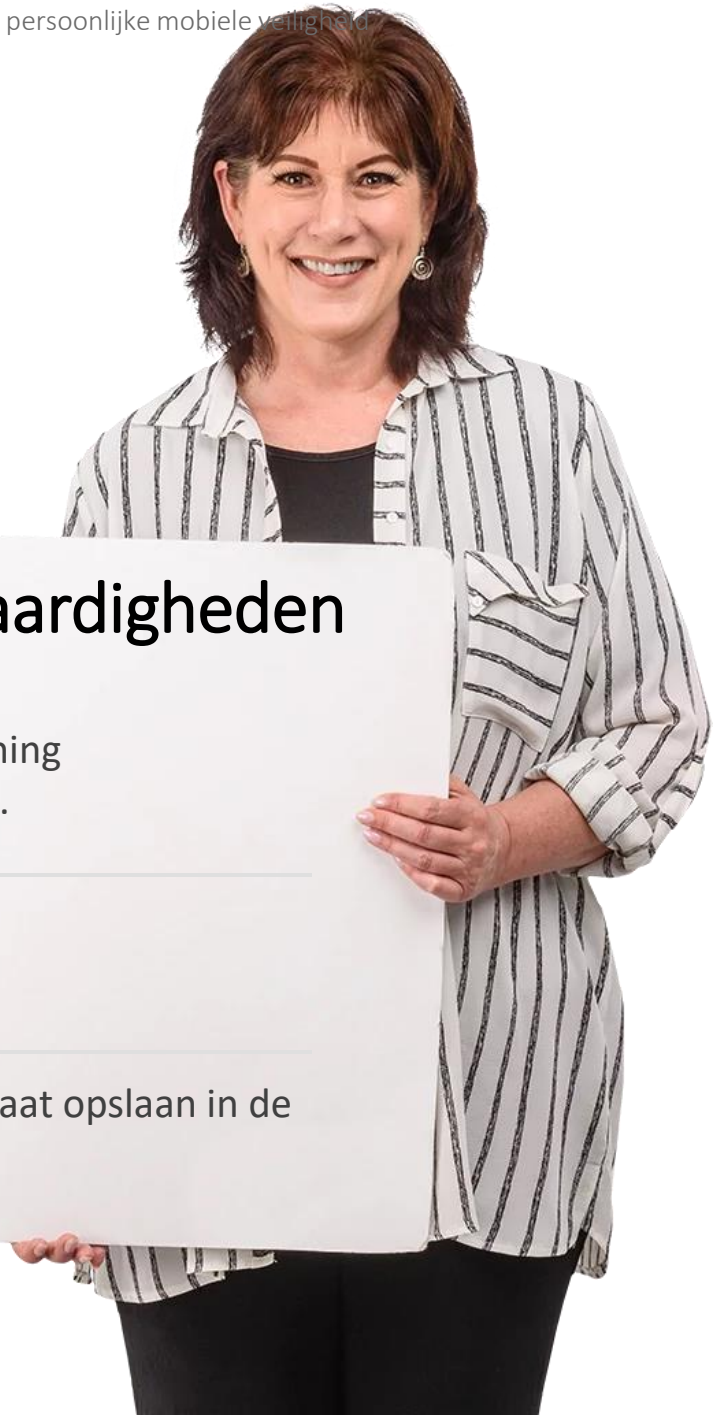
Click the **Quiz** button to edit this object

Samenvatting van het hoofdstuk

1. Privacy van gegevens.
2. Hoe de Algemene Verordening Gegevensbescherming jouw gegevens beschermt.
3. Cookies beheren.
4. De cloud begrijpen.
5. Begrijpen hoe je gegevens in de cloud worden opgeslagen.
6. In dit hoofdstuk krijg je een goed beeld van de privacy van mobiele gegevens.

Hoofdstuk voltooid!

Gefeliciteerd! Je hebt dit hoofdstuk met succes afgerond!



Samenvatting van vaardigheden

1. De Algemene Verordening Gegevensbescherming.
2. Cookies beheren.
3. Gegevens van je apparaat opslaan in de cloud.

Wat is het volgende?

Nu kan je dit hoofdstuk herhalen of onze studieaanbevelingen volgen door op een van de onderstaande knoppen te klikken:

Opnieuw

Volgende

SMART | MODULE 4 | HOOFDSTUK 2

Authenticatie

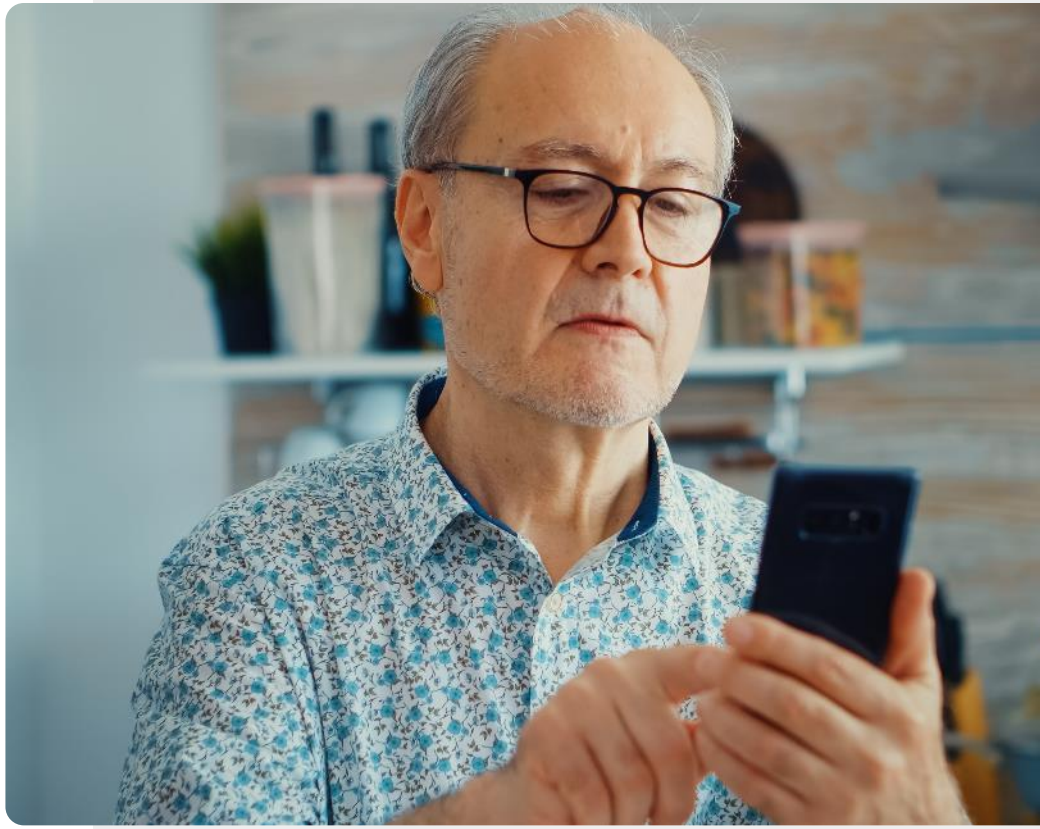
In dit hoofdstuk leer je over authenticatie, het proces waarbij de identiteit van een gebruiker wordt herkend om toegang te verlenen tot diensten. De technologie voor authenticatie ondersteunt de veiligheid en bescherming van persoonlijke informatie. Hier leer je verschillende soorten authenticatie en biometrische authenticatie en hoe je sterke wachtwoorden maakt.

Authenticatie - hoe apparaten weten wie de huidige gebruiker is

Authenticatie is de procedure om de identiteit van een gebruiker te herkennen. Het gebeurt vaak bij het openen van een app en controleert gebruikers om er zeker van te zijn dat een andere gebruiker niet in hun gegevens kijkt.

Verschillende systemen vereisen verschillende informatie, **credentials** genaamd, om een identiteit te bevestigen. Credential is vaak een wachtwoord, maar het kan ook gaan om andere vormen van authenticatie.

(https://www.veriff.com/blog/what-is-authentication)



Wat je zult leren in dit hoofdstuk

1. Wat is authenticatie en waarom heb je die nodig?
2. Soorten authenticatie.
3. Hoe maak je een sterk wachtwoord?
4. Verschillende soorten biometrische authenticatie.

Soorten authenticatie

Het aantal manieren om een gebruiker van een mobiel apparaat te authenticeren is de afgelopen decennia snel toegenomen.

Laten we snel enkele van de belangrijkste soorten authenticatie bekijken die op een mobiel apparaat beschikbaar kunnen zijn.

Soorten authenticatie

1
2
3

Authenticatie met wachtwoord

Wachtwoorden zijn waarschijnlijk de meest voorkomende vorm van authenticatie. Veilige wachtwoorden bevatten meestal letters, cijfers en andere tekens. Dit onderwerp wordt later in dit hoofdstuk behandeld.

Soorten authenticatie

1

2

3

Certificaatgebaseerde authenticatie

Een digitaal certificaat is een elektronisch document dat gebaseerd is op het idee van een rijbewijs of een paspoort. Een voorbeeld is het digitale certificaat met de volledige vaccinatiegegevens voor een COVID-19 vaccin.

Soorten authenticatie

1

2

3

Biometrische authenticatie

Biometrische authenticatie is een beveiligingsproces dat berust op unieke kenmerken van de eigenaar van het apparaat, zoals gezicht, stem of vingerafdrukken. We zullen zien dat mobiele apparaten verschillende soorten biometrische authenticatie benaderingen ondersteunen.

Soorten authenticatie

4

5

Authenticatie met een token

Bij deze aanpak hoeven gebruikers hun referenties slechts één keer in te voeren en wordt een geheime digitale sleutel gecreëerd - **het token**. De gebruiker kan het token net als dit treinkaartje gebruiken om toegang te krijgen tot systemen in plaats van opnieuw referenties in te voeren.

Soorten authenticatie

4

5

Multi-factor authenticatie (MFA)

Zodra de gebruiker op één manier is geïdentificeerd, wordt een code naar het mobiele apparaat gestuurd die de gebruiker moet invoeren in een app of website. Dit is **twee factor authenticatie**.

Wachtwoordverificatie

Laten we een paar van deze vormen van authenticatie selecteren en ze nader bekijken.

Waarschijnlijk de populairste vorm van authenticatie, en degene die al vele jaren op mobiele apparaten wordt gebruikt, is het wachtwoord.

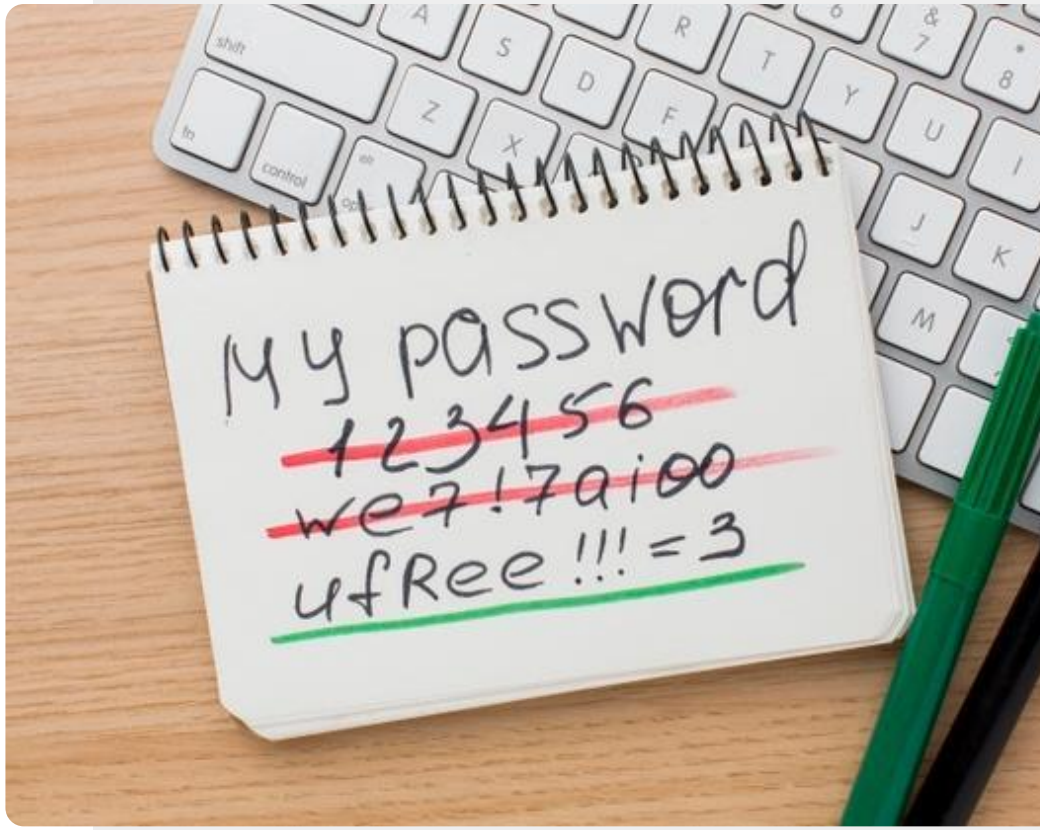
Het wachtwoord op de foto is gemakkelijk te raden, en dus niet erg veilig. Kan het beter?

Wachtwoordverificatie: sterke wachtwoorden

Veel websites vereisen dat u een wachtwoord kiest dat enkele van de volgende eigenschappen heeft

- Minstens 8 tekens lang
- Bevat hoofdletters en kleine letters
- Bevat een cijfer
- Bevat een leesteken

Laten we nu eens kijken hoe een gemakkelijk te onthouden wachtwoord kan worden gemaakt met behulp van deze elementen.



Een sterk wachtwoord maken

1

2

3

Kies een woord dat je kent

Pak een pen en een stuk papier. Schrijf een lang woord of woorden op met een sterke betekenis voor jou, maar die voor iemand anders niet vanzelfsprekend is. Het kan "geduld" zijn of "Byzantium" of "antilope".

Een sterk wachtwoord maken

1

2

3

Vervang enkele tekens in het woord of de zin

Gebruik tekenvervangingen, bijvoorbeeld:

1 = ! e = 3 a = @ 8 = % E =£ I =| S = $ S = 5

C =(T = + G = 6 O = 0 I = 1 Z = 2 B = 8

Caroline zou bijvoorbeeld **(@rol1nE** kunnen worden.

Een sterk wachtwoord maken

1

2

3

Gebruik het wachtwoord voor een apparaat of een website

Vernietig nu zorgvuldig het wachtwoord op het papier of leg het op een zeer veilige plaats zoals een kluis.

Je kunt nu het nieuwe sterke wachtwoord invoeren op een apparaat of website.

Bescherm uw wachtwoord

Zodra je je wachtwoord hebt aangemaakt, moet je het beschermen.

Het beste is om te proberen het gewoon te onthouden, maar als je besluit het op te schrijven, moet je het op een echt veilige plaats bewaren.

Je moet een wachtwoord NOOIT ergens bij of in de buurt van je telefoon bewaren.

Doe de opdracht!

Antonio wil een veilig wachtwoord maken. Hoe moet hij dat doen?

✓Ontmoet en leer António kennen. Informatie over António vind je hier.

✓ António kiest de zin ‘nolimits’ als basiswoord voor zijn wachtwoord.

✓Gebruik de beschreven stappen om António te helpen met het maken van een sterk wachtwoord van ‘nolimits’.

Telefoonwachtwoorden en SIM-codes

Mobiele apparaten kunnen worden ingesteld met **wachtwoorden** om bestanden te beschermen. **SIM-kaarten** op een apparaat verbinden het met een telefoonnetwerk en zijn voorzien van een **PIN-code** die je invoert om toegang te krijgen tot het netwerk. Ze geven toegang tot de contacten op uw SIM en als het apparaat wordt gestolen, kan de SIM ook naar een ander apparaat worden verplaatst om je tegoed te gebruiken. Als de PIN-code 3 keer verkeerd wordt ingevoerd, is een tweede code nodig, een zogenaamde **PUK-code**. Daarom is het belangrijk om je PIN-code en PUK-code op een veilige plaats te bewaren zodra je ze bij je toestel of SIM krijgt.

Biometrische authenticatie

Een biometrisch authenticatiesysteem herkent unieke kenmerken van de gebruiker van het apparaat om hem toegang te verlenen tot het apparaat of het systeem.

Laten we nu enkele van deze benaderingen bekijken.

Biometrische authenticatie voor mobiele technologie

1
2
3

Vingerafdrukscanners

Vingerafdrukken zijn uniek en kunnen dus worden gebruikt om een gebruiker te identificeren. Veel moderne mobiele apparaten hebben ingebouwde vingerafdrukscanners, en de telefoon kan worden ontgrendeld door de vinger van de gebruiker over de vingerafdrukscanner te leggen.

Biometrische authenticatie voor mobiele technologie

1

2

3

Oogscan

Net als vingerafdrukken zijn de patronen in het oog uniek voor elke persoon. De camera in sommige mobiele apparaten kan het netvliespatroon van de eigenaar herkennen en gebruiken om het apparaat voor de eigenaar te ontgrendelen.

Biometrische authenticatie voor mobiele technologie

1
2
3

Gezichtsherkenning

Een andere soortgelijke methode voor gebruikersauthenticatie is een gezichtsscan. Ook hier wordt een camera gebruikt om de unieke gezichtskenmerken van de eigenaar van het apparaat te herkennen om het apparaat te ontgrendelen.

Doe de opdracht!

Tom wil authenticatie gebruiken op zijn telefoon. Kun je hem helpen een geschikte aanpak te kiezen?

✓Maak kennis met Tom. Informatie over Tom vindt u hier.

✓ Tom werkte vroeger bij een IT-bedrijf, dus hij is een vertrouwd gebruiker van technologie, maar hij is niet vertrouwd met moderne authenticatiebenaderingen. Hij wil graag zijn smartphone beveiligen, zodat anderen geen toegang tot zijn informatie kunnen krijgen.

✓Geef Tom op basis van de informatie in de vorige dia's advies over welke authenticatie-aanpak hij zou willen gebruiken.

Autorisatie

Zodra het apparaat de gebruiker heeft geauthenticeerd, heeft de gebruiker autorisatie (toestemming) voor toegang tot het apparaat of systeem.

Een gebruiker kan toestemming hebben om alle of slechts enkele functies van het apparaat te gebruiken.

Het is gemakkelijk om **authenticatie**, die de gebruiker identificeert, en **autorisatie**, die daarna plaatsvindt, door elkaar te halen.

Quiz

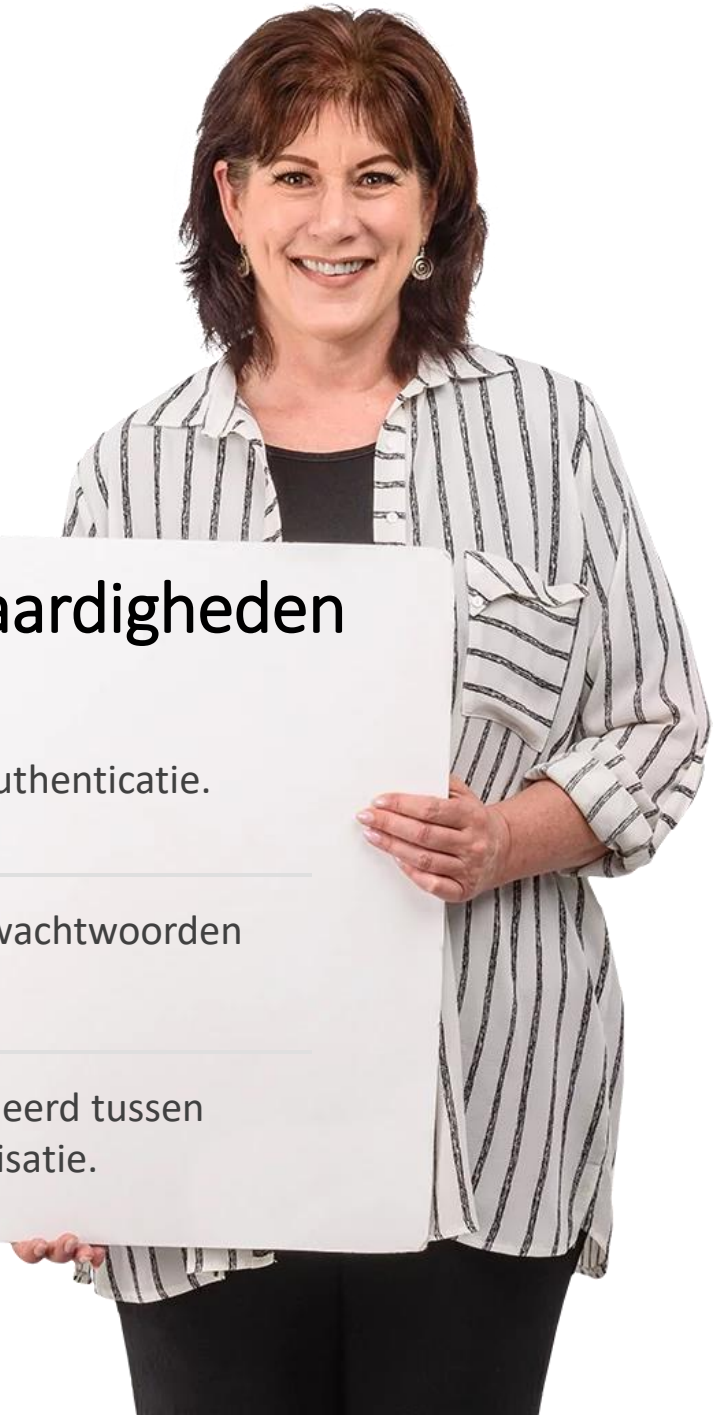
Click the **Quiz** button to edit this object

Samenvatting van het hoofdstuk

1. Je hebt geleerd over authenticatie en hoe deze wordt gebruikt om je toegang en informatie te beschermen.
2. Je hebt een aantal soorten authenticatie gezien.
3. Je hebt geleerd hoe je wachtwoorden moet maken en onthouden.
4. Probeer alstublieft de beveiligingsfuncties van je mobiele apparaat uit.
5. Wij hopen dat je de techniek voor het aanmaken van wachtwoorden zult oefenen om veilige wachtwoorden te maken.

Hoofdstuk voltooid!

Gefeliciteerd! Je hebt dit hoofdstuk met succes afgerond!



Samenvatting van vaardigheden

1. Je hebt geleerd over authenticatie.
2. Je weet hoe je sterke wachtwoorden maakt.
3. Je hebt het verschil geleerd tussen authenticatie en autorisatie.

Wat is het volgende?

Nu kan je dit hoofdstuk herhalen of onze studieaanbevelingen volgen door op een van de onderstaande knoppen te klikken:

Opnieuw

Volgende

SMART MODULE 4 HOOFDSTUK 3

Een mobiel apparaat beschermen

In de fysieke wereld kunnen je bezittingen, waaronder je mobiele apparaat, worden gestolen. In de digitale wereld is je toestel ook kwetsbaar voor hacken en virussen. Dit hoofdstuk gaat over hoe je jouw smartphone, privacy en informatie kunt beschermen tegen cyberaanvallen, zoals virussen.

Wat je zult leren in dit hoofdstuk

1. Hoe je jouw apparaten tegen ongeautoriseerde toegang beschermt.
2. Hoe je jouw apparaten tegen virussen beschermt.
3. Ransomware, malware en DDoS.
4. Een hotspot veilig gebruiken.

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

1

2

3

Vergrendel je mobiele apparaat

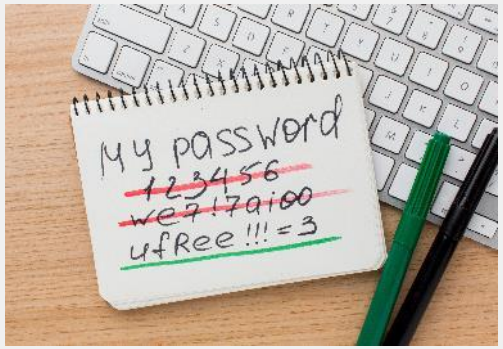
Vergrendel je mobiele apparaat met wachtwoorden of, nog beter, met ingeschakelde biometrische verificatie. Vergrendel je SIM met een PIN-code en bewaar je PIN- en PUK-codes op een gemakkelijk te onthouden maar veilige plaats.

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

1

2

3



Gebruik sterke wachtwoorden

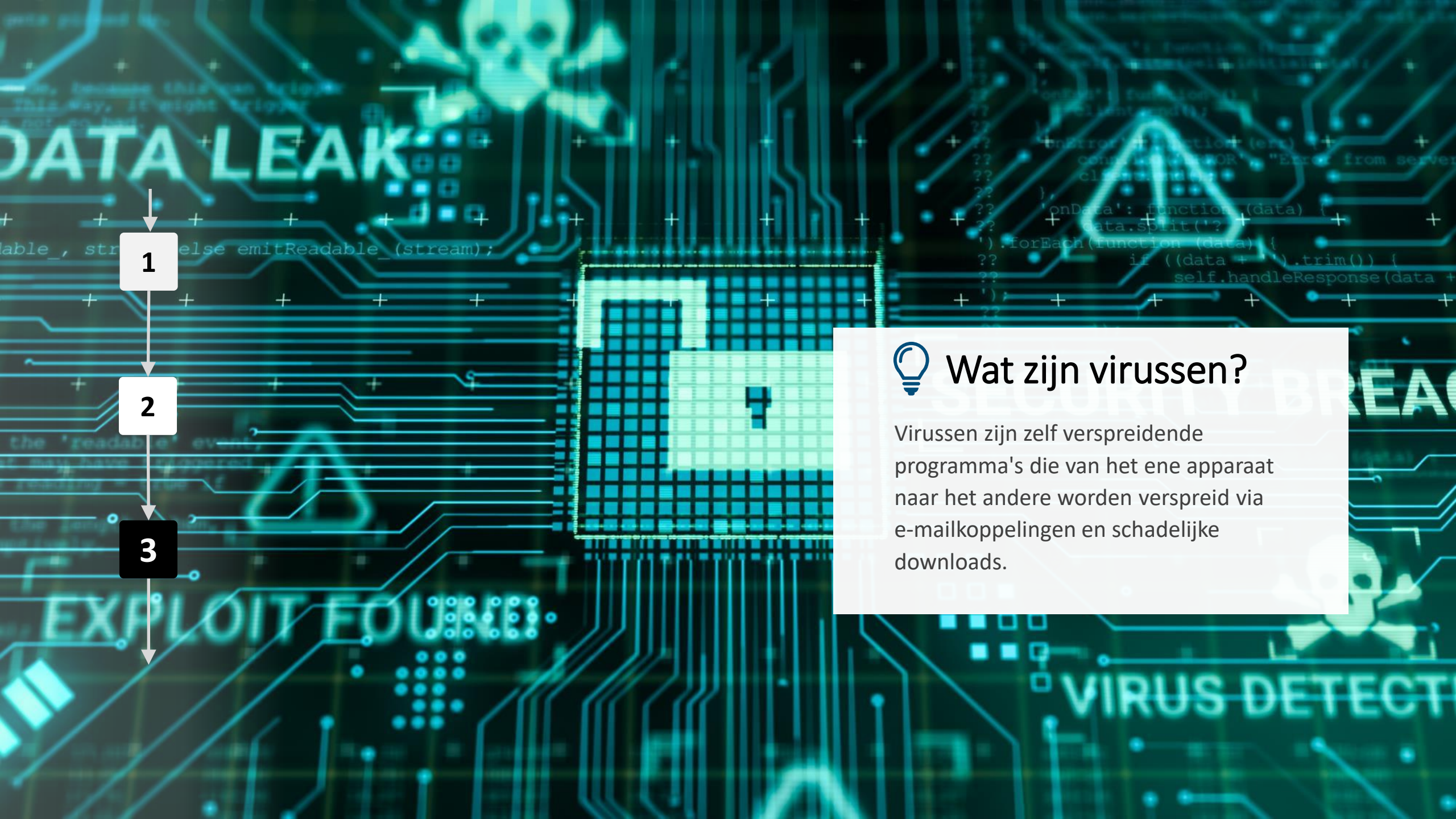
In het vorige hoofdstuk heb je geleerd wachtwoorden te maken en te gebruiken die sterk zijn, met hoofdletters en kleine letters, cijfers en speciale tekens. Het is de moeite waard om hiervoor met pen en papier te gaan zitten.

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

1
2
3

Let op je downloads

Download alleen bestanden, zoals documenten, video's, muziek of afbeeldingen, van websites die je vertrouwt, zoals fabrikanten van apparaten, grote softwarebedrijven of mediabedrijven. Sommige bestanden die worden gedownload van niet-vertrouwde sites kunnen virussen bevatten en je hardware beschadigen. Websites met adressen die beginnen met https, beschermen hiertegen.



Wat zijn virussen?

Virussen zijn zelf verspreidende programma's die van het ene apparaat naar het andere worden verspreid via e-mailkoppelingen en schadelijke downloads.

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

4

5

6

Houd het apparaat up-to-date met software-updates

De fabrikant van het mobiele apparaat stuurt meldingen over nieuwe software-updates. Updates helpen een apparaat te beschermen tegen beveiligingsfouten waardoor iemand gegevens van je apparaat kan halen. Download deze software-updates op het apparaat en werk het bij.

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

4

5

6

Versleutel de gegevens op het mobiele apparaat

De meeste mobiele apparaten hebben een optie om je gegevens te versleutelen. Als een telefoon wordt gestolen, maakt encryptie het moeilijker voor iemand zonder toestemming om de gegevens op het apparaat te zien. Een geautoriseerde gebruiker kan het toestel gewoon gebruiken.

Wat is encryptie?

Encryptie is de methode waarbij informatie wordt omgezet in onleesbare codes die de ware betekenis van de informatie verbergen, behalve voor de gebruiker die over de sleutel beschikt.
Facebooks sociale media-app WhatsApp heeft end-to-end-encryptie zodat de communicatie tussen twee gebruikers niet door een andere persoon kan worden "afgeluisterd".

Een mobiel apparaat beschermen tegen ongeautoriseerde toegang

4

5

6

Wees voorzichtig met openbare Wi-Fi

Wi-Fi in openbare ruimtes zoals luchthavens en cafés kan riskant zijn. Soms is wat je denkt dat de Wi-Fi van het café is, eigenlijk de laptop van een hacker die de verbinding met je telefoon voor verkeerde doeleinden kan gebruiken. Bij twijfel, maak geen verbinding!

Wi-Fi en criminaliteit

Cybercriminelen bespioneren soms openbare Wi-Fi-netwerken en verzamelen gegevens die via Wi-Fi worden overgedragen.

Zo kan de crimineel bankgegevens, wachtwoorden en andere gevoelige informatie bemachtigen.

Voor- en nadelen: openbare Wi-Fi gebruiken of niet?

Voordelen

- Gratis
- Uw mobiele datategoed wordt niet gebruikt
- Gemakkelijk te verbinden
- Beschikbaar

Nadelen

- Niet veilig
- Wi-Fi van een organisatie kan worden vervalst
- Meestal minder snelheid dan je eigen mobiele dekking

Wat is een hack aanval?

Het doel van een hackaanval is zich toegang te verschaffen voor kwade bedoelingen, diefstal van gegevens of met de bedoeling de gegevens van een organisatie te vernietigen.

Malware, Ransomware, DDoS

*"**Malware** is alle software die opzettelijk is ontworpen om schade toe te brengen aan een computer, server, client of computernetwerk. Software die onbedoeld schade veroorzaakt door een of andere tekortkoming wordt daarentegen meestal omschreven als een softwarebug. Er bestaat een grote verscheidenheid aan soorten malware, waaronder computervirussen, wormen, Trojaanse paarden, ransomware, spyware, adware, wiper en scareware."(Bron: https://en.wikipedia.org/wiki/Malware)*

*"**Ransomware** is een soort malware die het slachtoffer de toegang tot veel bestanden op zijn computer verhindert. Het wordt meestal gedownload via een link in een e-mail, op een website of op sociale media. Eenmaal gedownload, versleutelt het alle gegevensbestanden op de computer en verschijnt er een blokkeringsscherm dat een losgeldbetaling eist om de bestanden vrij te geven. Klik NIET op links in verdachte teksten of e-mails!" (Bron: https://www.bankofireland.com/security-zone/protect-your-business/ransomware/)*

*"**DDoS**-mitigatie verwijst naar het proces van succesvolle bescherming van een gerichte server of netwerk tegen een gedistribueerde denial-of-service-aanval (DDoS). Door gebruik te maken van speciaal ontworpen netwerkapparatuur of een cloud-gebaseerde beschermingsdienst kan een slachtoffer de inkomende aanval tegengaan."(Bron: https://www.cloudflare.com/en-gb/learning/ddos/ddos-mitigation/)*

Doe de opdracht!

Tom heeft authenticatie toegevoegd aan zijn telefoon. Kun je nog andere manieren voorstellen om zijn informatie te beschermen?

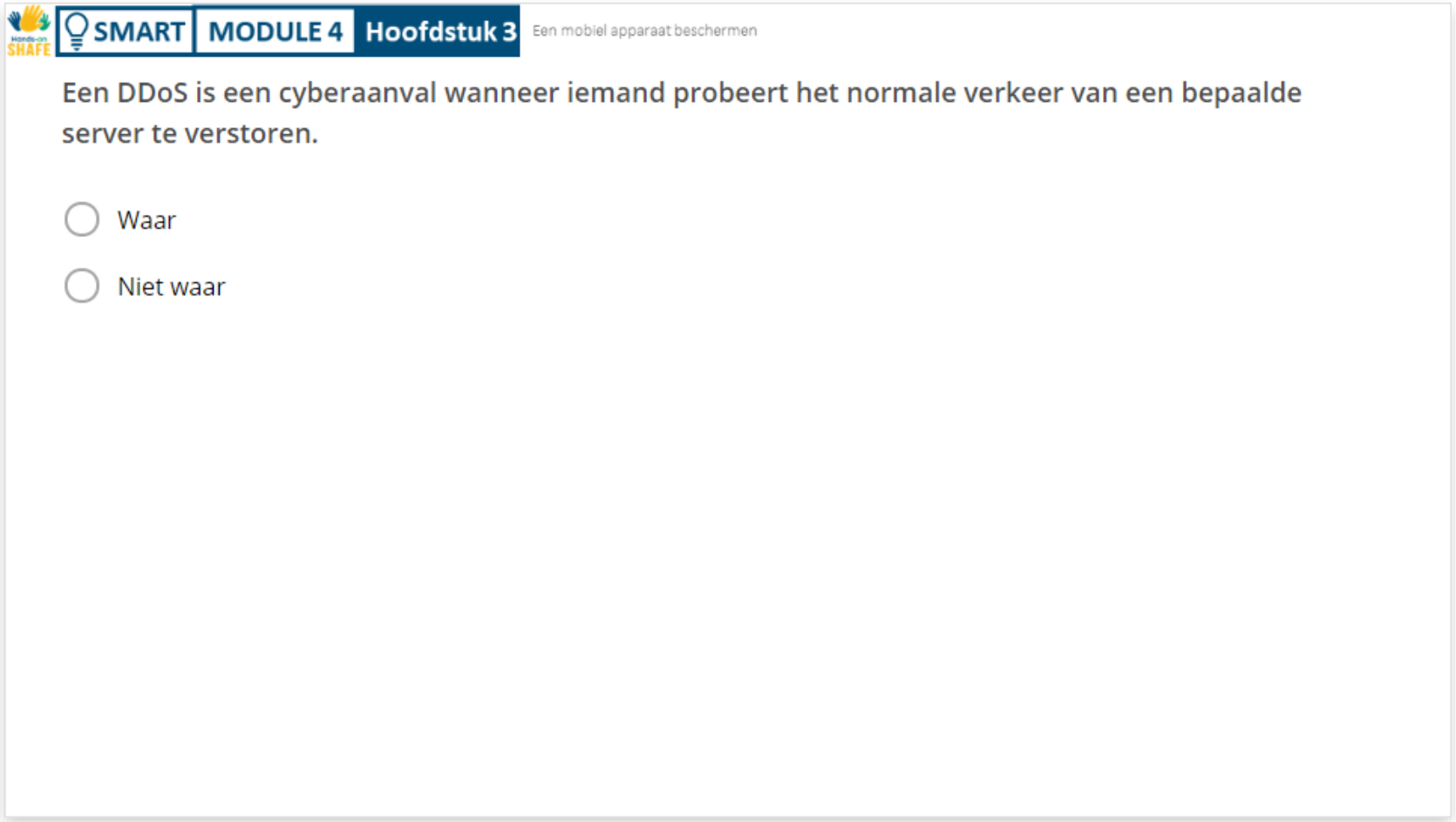
✓Maak kennis met Tom. Informatie over Tom vindt je hier.

✓ Tom werkte vroeger bij een IT-bedrijf en is dus een vertrouwd gebruiker van technologie. Hij gebruikt nu authenticatie, maar wil zijn smartphone op een veilige manier gebruiken, zodat anderen niet bij zijn informatie kunnen.

✓Stel op basis van de informatie die je in de vorige dia's hebt geleerd andere acties voor die Tom kan nemen om zijn informatie te beschermen.

Quiz

Click the **Quiz** button to edit this object



Samenvatting van het hoofdstuk

1. Je hebt geleerd hoe je een mobiel apparaat moet beschermen.
2. Je hebt het verschil geleerd tussen virussen en hackaanvallen.
3. Je hebt geleerd wat ransomware, malware en DDoS betekenen.
4. Je bent je bewust van de gevaren van het gebruik van openbare Wi-Fi.

Hoofdstuk voltooid!

Gefeliciteerd! Je hebt dit hoofdstuk met succes afgerond!

Samenvatting van vaardigheden

1. Je hebt geleerd hoe je een mobiel apparaat kunt beschermen tegen hackaanvallen en virussen.
2. Je hebt geleerd hoe je een mobiel apparaat op openbare plaatsen kunt beschermen.
3. Je hebt geleerd over hackers tools zoals malware.

Wat is het volgende?

Nu kan je dit hoofdstuk herhalen of onze studieaanbevelingen volgen door op een van de onderstaande knoppen te klikken:

Opnieuw

Volgende

SMART | MODULE 4 | HOOFDSTUK 4

Cyberpesten en omgaan met ongepaste inhoud

Wat moet je doen als je doelwit wordt van cyberpesten? Als mensen de persoon niet zien, is het gemakkelijker om de schade die cyberpesten aanricht niet te beseffen. In dit hoofdstuk bekijken we de menselijke aspecten van digitale communicatie en wat wel en niet gepast is om online te delen.

Wat je zult leren in dit hoofdstuk

1. Je bewust te zijn van cyberpesten.
2. Hoe met ongepaste inhoud om te gaan.
3. Wat wel of niet online te delen.
4. Online vrienden: hoe veilig is het?

Wat is cyberpesten?

Cyberpesten wordt gedefinieerd als **een agressieve, opzettelijke handeling door een groep of individu, met behulp van elektronische vormen van contact, herhaaldelijk en na verloop van tijd tegen een slachtoffer dat zich niet gemakkelijk kan verdedigen. - Smith 2018**

Van cyberpesten wordt meestal gezegd dat er drie elementen bij komen kijken:

- intentie om schade te berokkenen
- onevenwichtige machtsverhouding
- herhaling van de handeling

Soorten cyberpesten

Cyberpesten kan gebeuren via tekstberichten, telefoongesprekken, e-mails, chatrooms of platforms voor sociale media.

Het kan de vorm aannemen van kwetsende woorden, denigrerende opmerkingen, het plaatsen van valse informatie op openbare forums of blogs, het hacken van accounts voor persoonlijke bedreigingen van gewelddadige of seksuele aard.

- Rao 2018

Hoe om te gaan met cyberpesten

Volgens deskundigen zijn er een aantal manieren om met een cyberpester om te gaan.

Negeren: Waar mogelijk, negeer en kap de pester af.

Vastleggen: Houd de tijd, datum en inhoud van alle pesterijen bij, zodat je het kunt melden als dat nodig is.

Steun van vrienden: deel je ervaring met vrienden en familieleden, zodat je je niet geïsoleerd voelt.

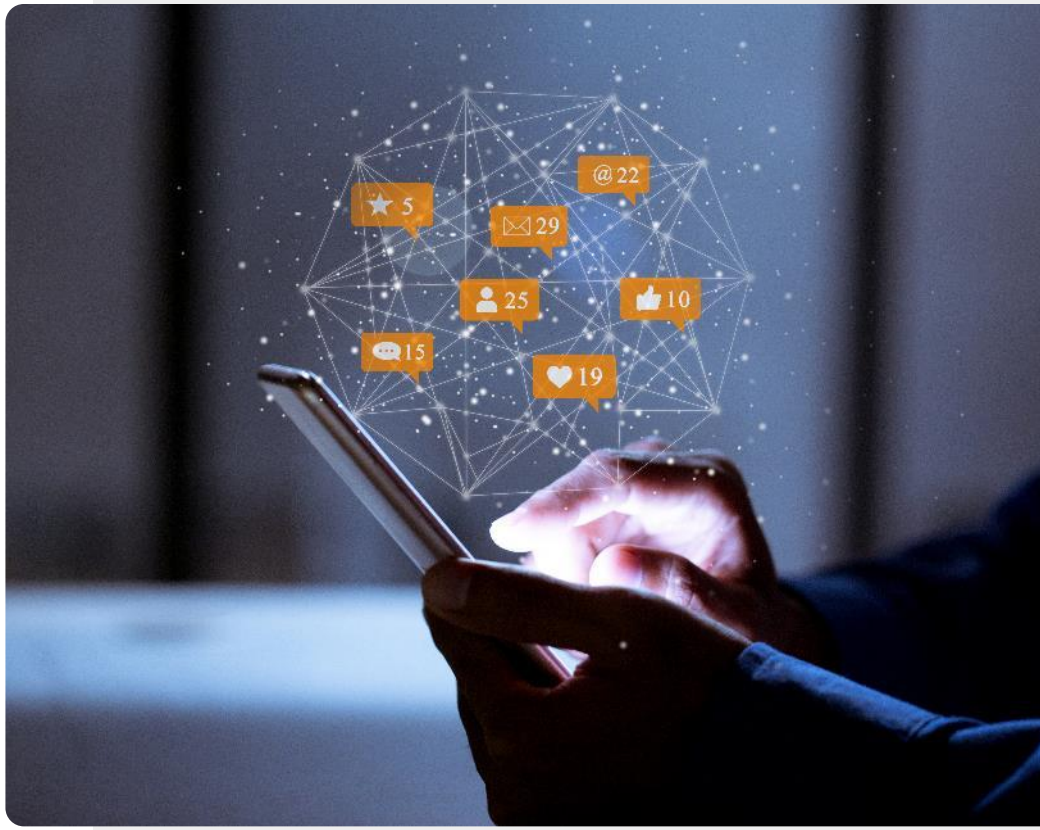
Rapporteren: Neem contact op met de moderator van de site of het forum.

Persoonlijke informatie delen op sociale media

Als je informatie deelt op sociale media, moet je ervan uitgaan dat die er lange tijd zal staan. Bedenk of je post problemen zal veroorzaken.

"Hoewel het misschien lijkt alsof de informatie wordt gedeeld met alleen je vrienden en familie, kan het ook worden gedeeld met hackers en oplichters die de sociale mediasites afstruinen." "Als je gegevens eenmaal op het internet staan, blijven deze nog jaren later vindbaar en kunnen ze door allerlei gewetenloze figuren worden gebruikt."

Joseph Turow - Penn State



Waar kan je cyberpesten melden?

Je serviceprovider of social media netwerk kan je helpen om ongewenste berichten en oproepen te blokkeren.

Als de situatie ernstiger is, kan de plaatselijke politie een onderzoek instellen naar bedreigende berichten.

Verwijderen van online identiteiten

Op sociale media apps kun je vaak je profiel wijzigen, zodat het niet zichtbaar is voor het grote publiek.

Het is niet altijd mogelijk om je berichten op sociale media of internetforum te verwijderen, maar je kunt wel je identiteit verwijderen, zodat die berichten anoniem worden.

In sommige gevallen kun je een verzoek sturen naar een zoekmachine, zoals Google, zodat je gegevens niet in zoekopdrachten verschijnen.

Ben je gehackt?

Als iemand toegang krijgt tot je e-mail of social media account, kan hij die gebruiken om valse mails naar je contactpersoon te sturen en ander onheil aan te richten. Dit wordt hacken genoemd.

Een manier waarop dit kan gebeuren is wanneer een groot datalek voor een online dienst ook jouw wachtwoord omvat. Als je hetzelfde wachtwoord gebruikt voor verschillende accounts, zoals e-mail, kan je account worden gehackt.

https://haveibeenpwned.com/

Kies je online vrienden zorgvuldig uit

Het kiezen van online vrienden: controleer de informatie die je krijgt van "nieuwe" vrienden.

Deel je persoonlijke informatie niet, voer neutrale gesprekken.

Leen geen geld aan een "nieuwe" vriend.

Een echte vriend zal geïnteresseerd zijn in je interesses en je niet gebruiken om problemen op te lossen.

Online nieuwe vrienden maken

Voordelen

- Je kunt in contact komen met mensen over de hele wereld.
- Je kunt online veel meer vrienden ontdekken die jouw interesses delen dan in een lokale gemeenschap.
- Online chats kunnen gemakkelijker zijn dan in persoon.
- Je kunt je account sluiten als er iets misgaat.

Nadelen

- Misschien communiceer je liever persoonlijk, de afstand kan een probleem zijn.
- Je moet voorzichtig zijn om geen persoonlijke informatie aan een vreemde te geven. Hun identiteit kan vals zijn.
- Het is gemakkelijker voor mensen om online te beledigen, wanneer ze de andere persoon niet zien.

Wat is ongepaste inhoud?

Tot de ongepaste inhoud behoren beelden van *"terreuraanslagen, onthoofdingen en bomaanslagen; wreedheden tegen mensen en dieren; sites met zelfbeschadiging; inhoud die aanzet tot anorexia en eetstoornissen; inhoud die aanzet tot zelfmoord; seksueel misbruik en verkrachting; geweld en verontrustende inhoud; haatsites; online porno".*

https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/

In internetjargon wordt iemand die ongepaste inhoud verstuurd met de bedoeling andere lezers te provoceren of te beledigen een **trol** genoemd.

Omgaan met ongepaste inhoud

De meeste zoekproviders hebben functies om dit te ondersteunen. Google's SafeSearch is bijvoorbeeld te vinden op https://www.google.com/preferences.

Het is het eerste op de pagina. Open die pagina en klik op het pictogram naast 'Schakel SafeSearch in'.

Je kunt er ook voor kiezen SafeSearch vast te zetten. Google blokkeert dan zowel teksten als afbeeldingen op websites voor volwassenen die met deze sites verband houden.

https://www.dragonblogger.com/how-to-block-inappropriate-content-on-google/

Doe de opdracht!

Teresa is boos over een cyberpest incident. Kun je haar helpen?

✓Ontmoet en leer Teresa kennen. Informatie over Teresa vind je hier.

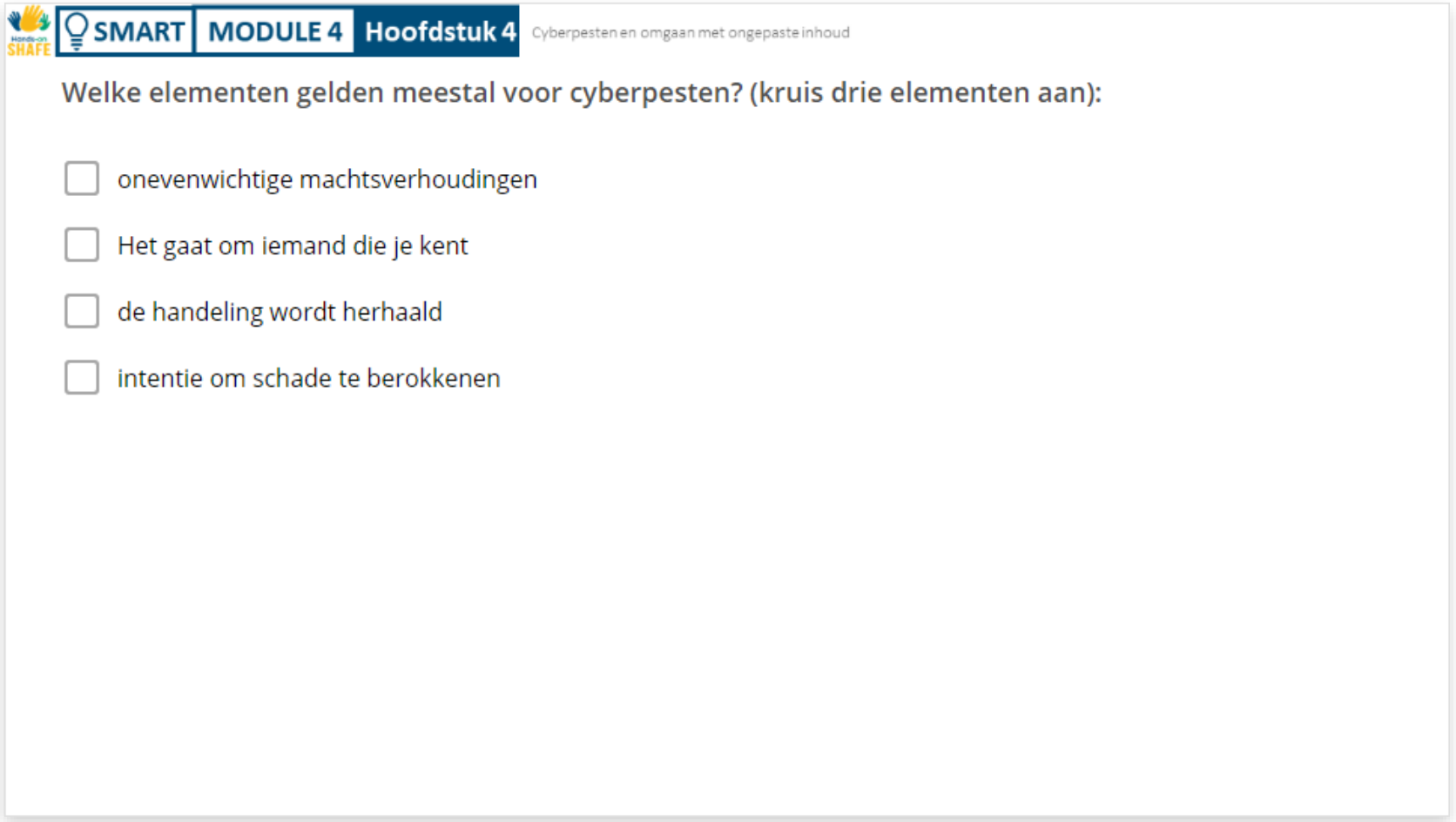
✓ Teresa gebruikt technologie om in contact te blijven met haar vrienden, maar onlangs werd ze getroffen door cyberpesten. Tot nu toe is het geen ernstig geval, maar toch wil ze graag weten hoe ze ermee om moet gaan - vooral als het doorgaat.

✓Geef Teresa op basis van de informatie die je in de vorige dia's hebt geleerd, advies over hoe ze met cyberpesten moet omgaan.

✓Als het cyberpesten ernstiger wordt, met wie moet Teresa dan contact opnemen?

Quiz

Click the **Quiz** button to edit this object



Samenvatting van het hoofdstuk

1. Je hebt geleerd over cyberpesten, hoe je het kunt herkennen en melden.
2. Je hebt geleerd over ongepaste inhoud en hoe je die kunt blokkeren.
3. Je hebt geleerd hoe je veilig kunt zijn als je online nieuwe vrienden ontmoet.
4. Je hebt geleerd voorzichtig te zijn met het delen van gegevens online - eenmaal geplaatst is het moeilijk ze te verwijderen.
5. Als iets je niet bevalt: kun je het blokkeren, rapporteren of je account sluiten.

Hoofdstuk voltooid!

Gefeliciteerd! Je hebt dit hoofdstuk met succes afgerond!

Samenvatting van vaardigheden

1. Hoe herken je cyberpesten.
2. Hoe blokkeer je ongepaste inhoud.
3. Hoe internet trollen te herkennen en niet in de val te lopen.

Wat is het volgende?

Nu kan je dit hoofdstuk herhalen of onze studieaanbevelingen volgen door op een van de onderstaande knoppen te klikken:

Opnieuw

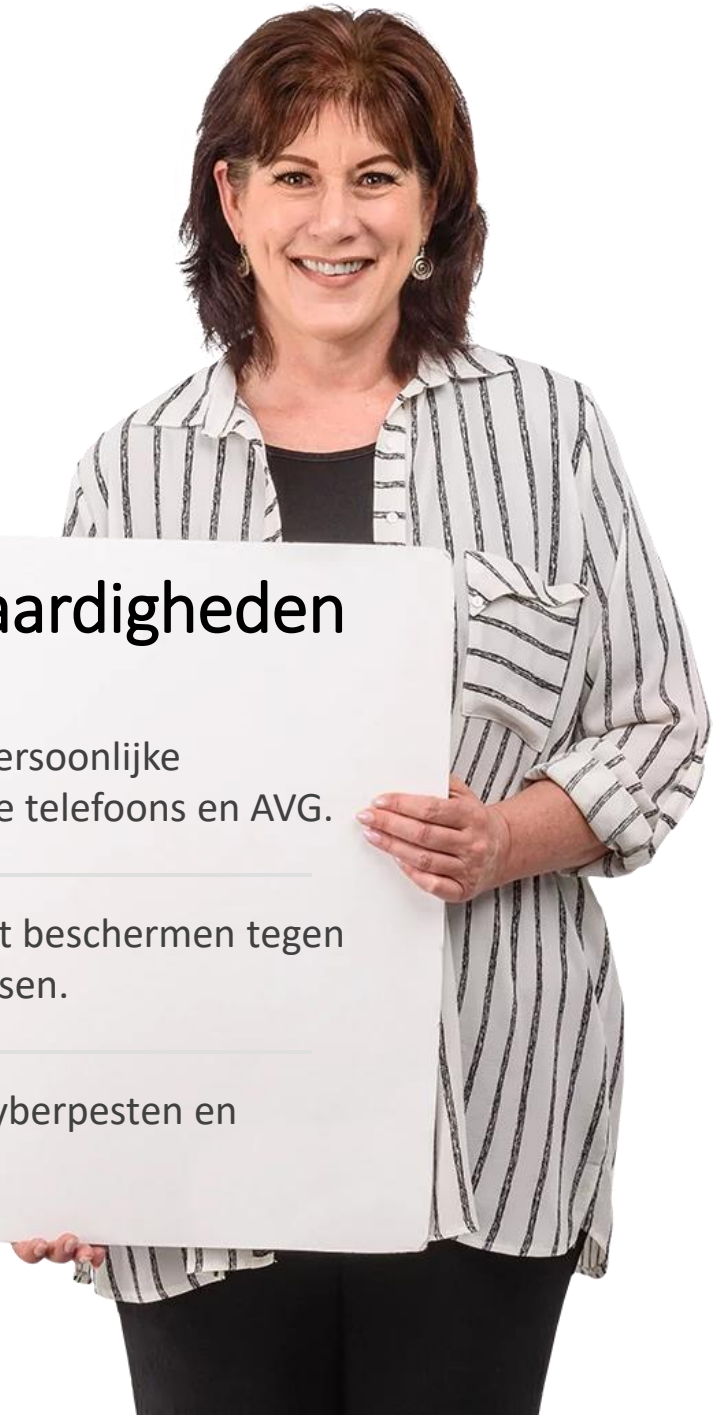
Volgende

Samenvatting van de module

1. Je hebt geleerd over beveiliging van mobiele telefoons.
2. Je hebt geleerd over de Algemene Verordening Gegevensbescherming, AVG.
3. Je hebt geleerd over soorten authenticatie.
4. Je hebt geleerd hoe je sterke wachtwoorden maakt.
5. Je leerde over de instrumenten van hackaanvallen: malware, ransomware, DDoS.
6. Je hebt geleerd over cyberpesten en hoe je geen slachtoffer kunt worden.
7. Je hebt geleerd hoe je de SafeSearch-instellingen van Google kunt aanpassen om ongepaste inhoud te voorkomen.

Module voltooid!

Gefeliciteerd! Je hebt deze module met succes afgerond!



Samenvatting van vaardigheden

1. Je hebt geleerd over persoonlijke beveiliging van mobiele telefoons en AVG.
2. Hoe je je apparaat kunt beschermen tegen hackaanvallen en virussen.
3. Hoe om te gaan met cyberpesten en ongepaste inhoud.

Wat is het volgende?

Nu kun je deze module herhalen of onze studieaanbevelingen volgen door op een van de onderstaande knoppen te klikken:

Opnieuw

Volgende