VOORBEELDCASE

INLEIDING

In oktober is Hogeschool Harderwijk getroffen door een grootschalige phishingaanval. Oscar is Security Officer op Hogeschool Harderwijk. Na de aanval constateert hij dat de impact van de aanval veel kleiner had kunnen zijn als medewerkers en studenten zich meer bewust waren geweest van de risico's van phishing. Daarom heeft Oscar besloten om op zijn hogeschool een awareness-programma te starten. Hij hoopt zo te voorkomen dat phishingaanvallen als deze ook in de toekomst plaatsvinden.

Oscar heeft niet eerder een awareness-programma ontwikkeld. Voor wat extra hulp heeft hij daarom de Cybersave Yourself-wiki geraadpleegd. Aan de hand van de zeven fasen in het stappenplan ontwikkelt hij een Plan van aanpak voor Hogeschool Harderwijk.

We hopen dat dit ook jouw instelling inspiratie en inzichten biedt om met een eigen awareness-programma aan de slag te gaan.

**Deze voorbeeldcase is fictief en niet gebaseerd op een bestaande instelling of een bestaand awareness-programma.*

OSCAR

PLAN VAN AANPAK

WAAROM EEN AWARENESS-PROGRAMMA?

1.1 De aanleiding
1.2 De huidige privacy- en security-awareness-status van mijn instelling
1.3 Lessons learned
1.4 Betrokkenen
1.5 Overtuig stakeholders

1

DE DOELGROEP

2.1 Wie willen we bereiken
2.2 Doelgroepen in beeld
2.3 Risicoanalyse

2

HET DOELGEDRAG

3.1 Het programmadoel
3.2 Concrete gedragsdoelen

3

GEDRAGS FACTOREN

4.1 Factoren die van invloed zijn op het gedrag

4

STRATEGIE

5.1 Welke communicatie-middelen gaan we inzetten?

5

TOETSING

6.1 Hoe gaan we meten?

6

UITVOERING

7.1 Planning
7.2 Team
7.3 Tref voorbereidingen
7.4 Aan de slag

7

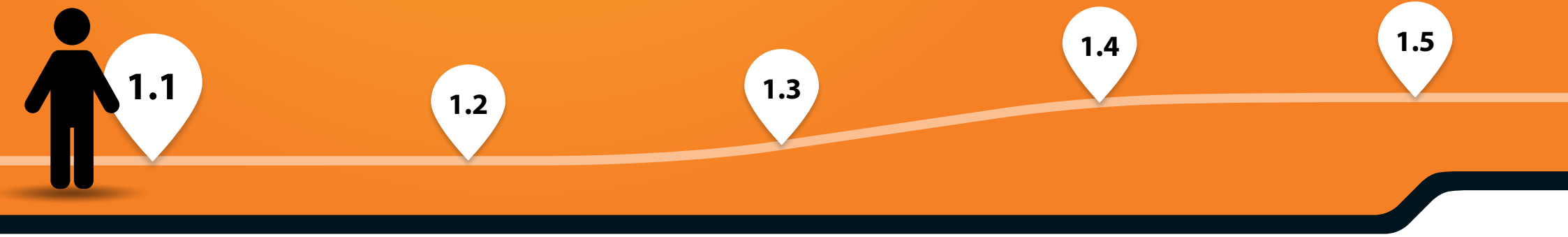
WAAROM EEN AWARENESS-PROGRAMMA

1.1 DE AANLEIDING

De phishingaanval in oktober heeft Oscar wakker geschud. Gegevens van een groot aantal studenten en medewerkers zijn afhandig gemaakt. Iets dat voorkomen had kunnen worden als zij zich meer bewust waren geweest van de gevaren van phishing. Daarom besluit Oscar een awareness-programma op te zetten. De aanleiding voor het awareness-programma verwerkt hij als volgt in het Plan van aanpak.

IN HET PLAN VAN AANPAK:

Op 18 oktober 2018 zijn diverse medewerkers en studenten slachtoffer geworden van een phishingaanval op onze instelling. Dit heeft ons doen constateren dat medewerkers en studenten niet of onvoldoende weten hoe ze een phishingmail moeten herkennen en wat de gevaren van phishing zijn. Met de komst van een awareness-programma hopen we dat we meer bewustzijn kunnen creëren binnen de instelling op het gebied van online privacy en veiligheid. Dit zodat we de veiligheid van onze instelling, maar ook van medewerkers en studenten in de toekomst, beter kunnen waarborgen.



1.2 DE HUIDIGE PRIVACY- EN SECURITY-AWARENESS-STATUS VAN MIJN INSTELLING

Oscar beseft dat er waarschijnlijk meer problemen spelen rondom privacy- en security-awareness op Hogeschool Harderwijk. Hij besluit onderzoek te doen naar de huidige awareness-status van de instelling.

Oscar neemt interviews af en voert panelgesprekken met diverse medewerkers en studenten. De steekproef is zo divers mogelijk. Hij praat bijvoorbeeld met eerstejaarsstudenten én afstudeerders, met nieuwe medewerkers én medewerkers die al wat langer in het onderwijs zitten, met bestuursleden, onderwijzend personeel en niet-onderwijzend personeel, onder wie communicatiemedewerkers en een aantal directe ICT-collega's.

De risico's heeft Oscar vastgelegd met behulp van het risico-inventarisatiedocument. Deze zijn vervolgens samengevat in het Plan van aanpak.

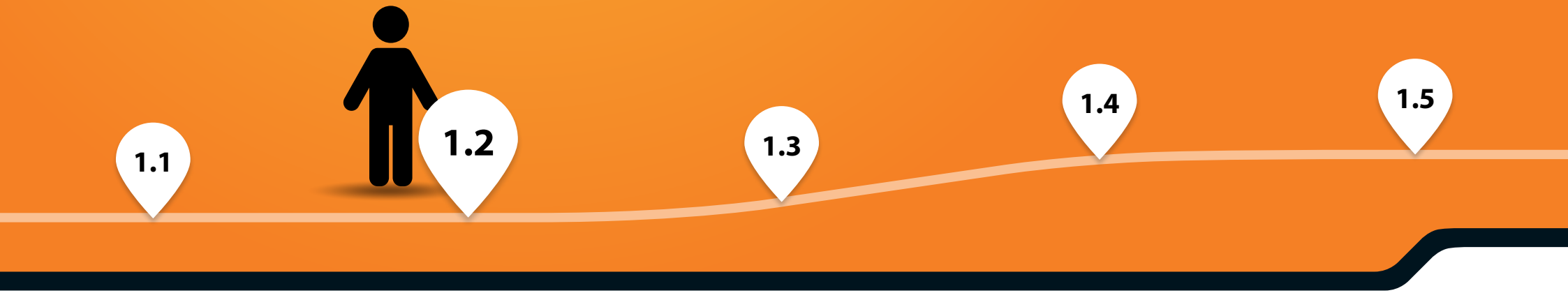
IN HET PLAN VAN AANPAK:

De phishingaanval op 18 oktober jongstleden heeft geleid tot verder onderzoek naar de privacy- en security-awareness-status op Hogeschool Harderwijk. Uit dit onderzoek komen de volgende risico's naar voren.

Phishing
Er heerst te weinig bewustzijn rondom de gevaren van phishing. Medewerkers en studenten weten onvoldoende waaraan ze een phishingmail kunnen herkennen en hoe ze moeten handelen wanneer ze geconfronteerd worden met een phishingmail.

Omgaan met data
Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming van toepassing. Dat betekent extra verantwoordelijkheden voor medewerkers als het aankomt op de bescherming van persoonlijke gegevens van (toekomstige) studenten en medewerkers. Uit het onderzoek blijkt echter dat medewerkers niet zorgvuldig omgaan met de opslag van data. Er wordt te weinig gebruikgemaakt van de veilige opslagdiensten van de instelling. Data zwerft rond in e-mails, op usb-sticks, of blijft staan op het bureaublad van de desbetreffende medewerker.

Wachtwoordgebruik
Zwakke wachtwoorden veroorzaken regelmatig datalekken. Idealiter zijn wachtwoorden uniek, lang en bestaan ze uit symbolen, cijfers, letters en hoofdletters. In slechts 15% van de gevallen voldoet een wachtwoord aan bovenstaande eisen. Bovendien zien we dat wachtwoorden regelmatig hergebruikt worden.



1.3 LESSONS LEARNED

Oscar weet dat er binnen Hogeschool Harderwijk een aantal activiteiten zijn georganiseerd om privacy- en security-awareness te stimuleren. Samen met een aantal directe collega's heeft hij geïnventariseerd wat er de afgelopen jaren georganiseerd is. De belangrijkste lessen die ze hieruit kunnen trekken omschrijft Oscar vervolgens kort in het Plan van aanpak.

IN HET PLAN VAN AANPAK:

Hieronder staat kort omschreven wat Hogeschool Harderwijk de afgelopen jaren heeft georganiseerd om privacy- en security-awareness te verbeteren. Evenals de belangrijkste lessen die hieruit getrokken kunnen worden.

1. Aan het begin van ieder nieuw studiejaar worden aan nieuwe studenten **gadgets** uitgedeeld met daarop de contactgegevens van de ICT-helpdesk. Het effect van deze actie op de awareness van nieuwe studenten is onbekend. Studenten lijken de ICT-helpdesk wel te vinden, maar dat is voornamelijk voor hulp met bijvoorbeeld het installeren van software.
2. Op het moment dat een medewerker in dienst komt van onze hogeschool krijgt hij of zij een **document** toegestuurd met daarin uitleg over hoe binnen onze instelling met data om te gaan. We zien echter dat er met enige regelmaat data zoekraakt, dat docenten veel gebruikmaken van usb-sticks en dat Dropbox en WeTransfer door veel van hen gebruikt worden. Gedrag dat we liever niet terug zouden zien.

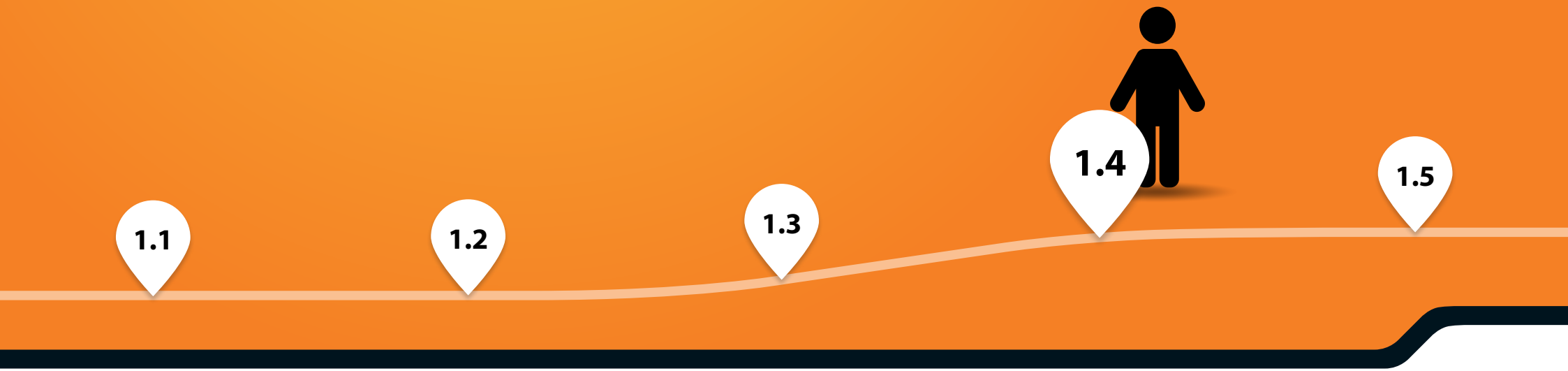
1.4 BETROKKENEN

Om het awareness-programma tot een succes te maken heeft Oscar hulp nodig uit verschillende hoeken. Dat beseft hij maar al te goed. De mensen/ functies die nodig zijn om dit project tot een succes te maken bepaalt hij aan de hand van een stakeholderanalyse. De belangrijkste stakeholders benoemt Oscar vervolgens kort in het Plan van aanpak.

IN HET PLAN VAN AANPAK:

Om dit project tot een succes te maken hebben we ondersteuning van de volgende mensen nodig:

- Het bestuur van Hogeschool Harderwijk. Onder wie in ieder geval de algemeen directeur.
- Leidinggevende ICT-afdeling
- Leidinggevende communicatieafdeling
- ICT-helpdesk
- Studentambassadeurs
- Docentambassadeurs

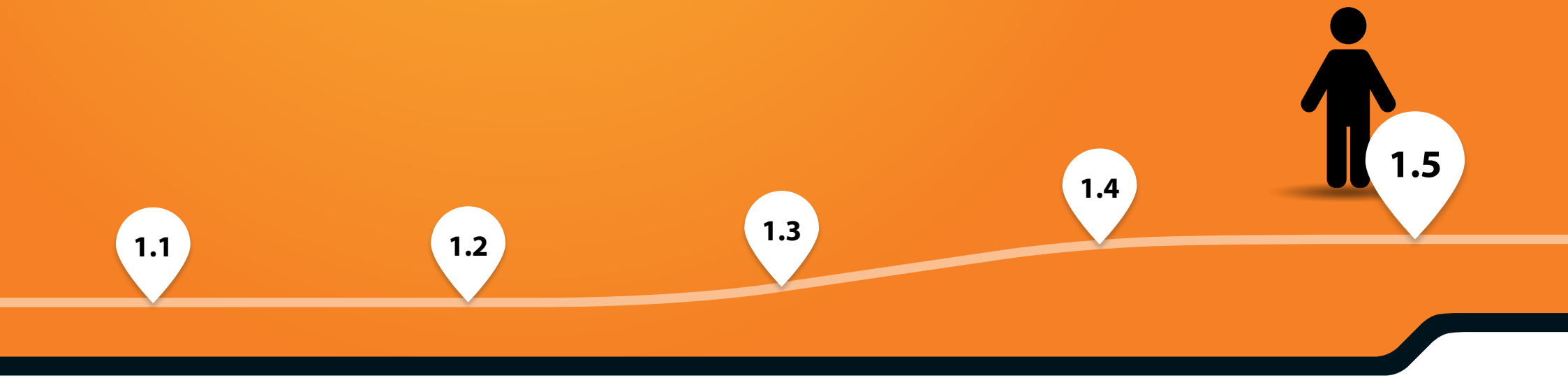


1.5 OVERTUIG STAKEHOLDERS

Om belangrijke stakeholders te betrekken bij het awareness-programma heeft Oscar een presentatie opgezet. Oscar heeft deze presentatie gegeven aan het management van de hogeschool en heeft het mandaat gekregen om een awareness-programma op te starten.

Inhoudelijk heeft Oscar in de presentatie belangrijke informatie rondom het awareness-programma verwerkt. Denk aan relevante inzichten uit het onderzoek van stap 1.2 en bijvoorbeeld een overzicht van alle recente incidenten, waaronder de grote phishingaanval in oktober. De presentatie maakte het voor Oscar mogelijk om de noodzaak van het programma kort en bondig uit te leggen aan zijn collega's.

KIJK OP DE WIKI VOOR EEN PRESENTATIEVOORBEELD



DE DOELGROEP

2.1 WIE WILLEN WE BEREIKEN

Oscar heeft relevante stakeholders overtuigd van het nut van een awareness-programma voor Hogeschool Harderwijk. Dat betekent dat Oscar aan de slag kan gaan met de ontwikkeling van het programma. Hij begint met het bepalen van zijn doelgroepen. Want hoewel het awareness-programma relevant is voor de gehele instelling, heeft het geen zin om iedereen te bereiken met dezelfde boodschap. Van verschillende gebruikers kan verschillend gedrag worden verwacht. In het Plan van aanpak omschrijft Oscar kort welke doelgroepen bereikt moeten worden en waarom.

IN HET PLAN VAN AANPAK:

De doelgroep van het awareness-programma is breed, want verandering is nodig binnen de gehele instelling. We maken om die reden onderscheid tussen vier doelgroepen:

- **Studenten**
  Het is onduidelijk hoeveel kennis zij bezitten over de verschillende onderwerpen. Veel van hen zijn waarschijnlijk niet op de hoogte van het privacy- en securitybeleid van onze hogeschool. De doorloop van studenten is bovendien aanzienlijk, omdat er elk jaar veel nieuwe studenten bijkomen én vertrekken na afronding van de studie.
- **Onderwijzend personeel**
  We verwachten dat ze in enige mate bekend zijn met het privacy- en securitybeleid van de instelling. Onderwijzend personeel heeft veel te maken met persoonlijke gegevens en bestanden van studenten. Denk aan cijferlijsten, tentamens, verslagen en scripties. Veilig omgaan met data en documenten vereist extra aandacht.
- **Niet-onderwijzend personeel**
  We verwachten dat ze in enige mate bekend zijn met het privacy- en securitybeleid van de instelling. Ook niet-onderwijzend personeel heeft te maken met bestanden die vertrouwelijke informatie bevatten, zoals persoonsgegevens met vertrouwelijke informatie voor de instelling. Veilig omgaan met data vereist om die reden extra aandacht.
- **Directie en hoger management**
  Betrokkenheid van het bestuur is onmisbaar voor een goede awareness-campagne. Directie en management vervullen een voorbeeldfunctie. Door zichtbaar veilig gedrag te vertonen, bevestigen zij dat dit het gewenste gedrag is.

2.2 DOELGROEPEN IN BEELD

Oscar wil een beter beeld krijgen van iedere doelgroep. Daarom ontwikkelt hij voor iedere doelgroep een uitgebreid doelgroepprofiel. Aan de hand van de vragen uit het stappenplan brengt hij belangrijke eigenschappen van de doelgroepen in kaart.

DOELGROEPPROFIEL STUDENTEN

Geslacht:
- Vrouw: 56%
- Man: 44%

Leeftijd:
- 15-24 jaar: 91,0%
- 25-34 jaar: 8,5%
- 35-44 jaar: 0,5%

Opleidingsniveau:
- 28,9% .....afkomstig van mbo
- 51,7% ..... afkomstig van havo
- 19,4% ..... afkomstig van vwo

Verdeling over de verschillende faculteiten:
- Business en economie 24,3%
- Bewegen, sport en voeding..... 6,2%
- Digitale media en creatieve industrie 9,3%
- Gezondheid..... 6,7%
- Maatschappij en recht..... 16,2%
- Onderwijs en opvoeding 12,5%
- Techniek 14,8%

Houding en gedrag t.o.v. online privacy en veiligheid
- Verandert regelmatig het wachtwoord..... 41%
- Gebruikt wachtwoord voor meerdere accounts 65%
- Deelt wachtwoord weleens met anderen 58%
- Opent geen e-mails van onbekende afzenders..... 34%
- Weet een phishingmail te herkennen 66%
- Gebruikt opslagdiensten van de instelling 15%
- Raakt wel eens data kwijt door deze onzorgvuldig op te slaan... 81%

Wat doen ze dagelijks?
De voornaamste bezigheid van studenten bestaat uit, hoe kan het ook anders, studeren. Daarnaast bezit een groot deel van de studenten een bijbaan (67%) en zijn ze actief in het verenigingsleven. Vrije tijd brengen ze graag door met vrienden of besteden ze aan hobby's, waaronder sport.

Gebruik van (IT-)middelen
Studenten zijn over het algemeen veel online. Ze maken veel gebruik van WhatsApp, Facebook, Instagram en andere social kanalen. Bovendien zijn ze vaak op de hoogte van de laatste online trends. Ze zijn gemiddeld beter technisch onderlegd dan andere doelgroepen, maar gaan van alle doelgroepen het minst zorgvuldig om met online veiligheidsregels.

Omgang met gevoelige informatie
Over het algemeen hebben studenten geen toegang tot gevoelige informatie. Wel is het van groot belang dat zij op een veilige manier omgaan met bestanden en overige data die noodzakelijk zijn voor de eigen studievoortgang. Daarnaast is het voor hen goed om zich nu en in hun latere loopbaan bewust te zijn van online privacy- en securityrisico's.

Voorbeeldgedrag
Studenten zijn niet primair de doelgroep die voorbeeldgedrag moet vertonen. Veel van ons gedrag wordt echter gestuurd door anderen en het is om die reden prettig als studenten het juiste voorbeeld laten zien aan andere studenten.

2.3 RISICOANALYSE

Niet iedere doelgroep loopt in dezelfde mate risico op de factoren die in stap 1 zijn bepaald. Met behulp van een risicomatrix kan Oscar eenvoudig systematisch weergeven hoe groot de risico's voor de verschillende doelgroepen zijn.
Hij gebruikt hiervoor de risicomatrix op de wiki als basis.

De risicomatrix van Hogeschool Harderwijk ziet er als volgt uit:

Risico:	Studenten	Onderwijzend personeel	Niet-onderwijzend personeel	Directie en hoger management
Gebrek aan bewustzijn rondom de gevaren van phishing	🔴	🟡	🟡	🟢
Niet kunnen herkennen van een phishingmail	🔴	🔴	🔴	🔴
Onjuist handelen in het geval van een phishingmail	🔴	🔴	🔴	🔴
Niet gebruiken van de veilige opslagdiensten van de instelling	N.v.t.	🔴	🟡	🟡
Rondzwerven van data in e-mail of op usb-sticks	N.v.t.	🔴	🔴	🔴
Aanmaken van een zwak wachtwoord	🔴	🔴	🔴	🔴
Hergebruiken van wachtwoorden	🔴	🔴	🔴	🔴

Laag risico	🟢
Gemiddeld risico	🟡
Hoog risico	🔴

HET DOELGEDRAG

3.1 HET PROGRAMMADOEL

Het is tijd om de doelen van het awareness-programma te bepalen. De risico's die Oscar heeft gevonden in de eerste fase en de doelgroepen die hij heeft vastgesteld in de tweede fase gelden daarvoor als basis.

Oscar wil met het awareness-programma aan drie onderwerpen aandacht besteden. Zo wil hij meer aandacht creëren rondom phishing, veilig datagebruik en veilig wachtwoordgebruik. Voor ieder van deze onderwerpen formuleert Oscar een concreet programmadoel. Deze verwerkt hij vervolgens in het Plan van aanpak.

IN HET PLAN VAN AANPAK:

In 2022 moeten met het awareness-programma de volgende doelen zijn bereikt:

- Studenten en medewerkers zijn op de hoogte van de gevaren van phishingaanvallen. Gebruikers weten wat phishing is, waaraan ze een phishingaanval kunnen herkennen en hoe ze moeten handelen op het moment dat ze met een phishingaanval te maken krijgen.
- Medewerkers weten hoe ze zorgvuldig met de opslag van data moeten omgaan en handelen hiernaar.
- Studenten en medewerkers zijn zich bewust van het belang van sterke wachtwoorden. Ze weten hoe ze een sterk wachtwoord moeten instellen en doen dat ook.

3.2 CONCRETE GEDRAGSDOELEN

Programmadoelen zijn doorgaans slecht meetbaar. Daarom stelt Oscar in deze stap voor ieder programmadoel meerdere concrete gedragsdoelen vast. Deze stellen Oscar in staat om te meten of hij met het opgestelde programma zijn programmadoelen behaalt.

De gedragsdoelen stelt Oscar vast aan de hand van het schema in het stappenplan. Zo weet Oscar zeker dat de gedragsdoelen die hij formuleert concreet genoeg zijn.

IN HET PLAN VAN AANPAK:

Concreet willen we met het programma in 2022 de volgende gedragsdoelen hebben bereikt:

Phishing

- Op het moment dat er een phishingmail binnenkomt weten onze medewerkers en studenten waaraan ze deze kunnen herkennen.
- Op het moment dat er een phishingmail binnenkomt melden onze medewerkers en studenten dit direct bij de ICT-helpdesk.
- Nadat studenten en medewerkers de phishingmail gemeld hebben bij de ICT-helpdesk verwijderen ze deze permanent uit hun inbox.

Veilig omgaan met data

- Op het moment dat medewerkers data op moeten slaan weten ze hoe én waar ze dit moeten doen (op beveiligde servers).
- Op het moment dat medewerkers data moeten delen weten ze hoe ze dit op een veilige manier kunnen doen (via beveiligd systeem/SURFdrive bijvoorbeeld).
- Op het moment dat medewerkers data op een onveilige manier toegestuurd krijgen van een collega spreken ze hem/haar daarop aan.

Wachtwoorden

- Op het moment dat medewerkers en studenten hun wachtwoord aanpassen weten ze aan welke eisen een wachtwoord moet voldoen om veilig te zijn.
- Medewerkers en studenten maken gebruik van tweefactorauthenticatie waar mogelijk.
- Medewerkers en studenten zijn op de hoogte van de mogelijkheid om een wachtwoordmanager te gebruiken.

GEDRAGSFACTOREN

4.1 FACTOREN DIE VAN INVLOED ZIJN OP HET GEDRAG

Gedrag is altijd afhankelijk van meerdere factoren. Om te bepalen welke factoren van invloed zijn op de gedragsdoelen die Oscar eerder heeft vastgesteld heeft hij het invulschema op de wiki gedownload. Met behulp van dit invulschema heeft Oscar een heleboel factoren kunnen vaststellen. Te veel om in het Plan van aanpak te vermelden.

In een volgende stap heeft Oscar dan ook bepaald wat precies de belangrijkste factoren zijn. Deze omschrijft hij vervolgens kort per gedragsdoel in het Plan van aanpak.

PHISHING

Op het moment dat er een phishingmail binnenkomt weten onze medewerkers en studenten waaraan ze deze kunnen herkennen.

1. **Kennis:** Medewerkers en studenten kunnen een phishingmail alleen herkennen als ze daar voldoende kennis over bezitten.
2. **Gewoonten en automatismen:** Medewerkers en studenten openen en lezen mails op de automatische piloot. Ze zijn zich niet bewust van het feit dat de mail ook een phishingmail zou kunnen zijn.
3. **Zelfbeeld:** Medewerkers en studenten schatten de kans dat ze zelf in een phishingmail trappen erg klein in. Dit zorgt voor een afnemen in alertheid.

Op het moment dat er een phishingmail binnenkomt melden onze medewerkers en studenten dit direct bij de ICT-helpdesk.

1. **Kennis:** Medewerkers en studenten kunnen alleen correct handelen als ze weten welke stappen ze moeten ondernemen nadat ze een phishingmail hebben ontvangen.
2. **Fysieke omgeving:** Het kost uiteraard tijd en energie om een phishingmail te melden bij de ICT-helpdesk. Voelt deze drempel als te hoog, dan zal dit voor een afname in correct gedrag zorgen.
3. **Sociale omgeving:** Er kan sprake zijn van diffusion of responsibility. Medewerkers en studenten gaan er in dat geval vanuit dat een ander de phishingmail meldt.

Nadat studenten en medewerkers de phishingmail gemeld hebben bij de ICT-helpdesk verwijderen ze deze permanent uit hun inbox.

1. **Kennis:** Medewerkers en studenten kunnen alleen correct handelen als ze weten welke stappen ze moeten ondernemen nadat ze een phishingmail hebben ontvangen.
2. **Zelfbeeld:** Medewerkers en studenten weten wellicht niet, of niet goed, hoe ze een phishingmail permanent uit hun inbox kunnen verwijderen. Dat kan zorgen voor onzekerheid en angst om iets verkeerd te doen.
3. **Houding:** Medewerkers en studenten hebben niet het gevoel dat het gevaarlijk is om een phishingmail in de inbox te laten staan. ‘Zolang ik maar geen bestanden open/download of op linkjes in de e-mail klik.’

VEILIG OMGAAN MET DATA

Op het moment dat medewerkers data op moeten slaan weten ze hoe én waar ze dit moeten doen (op beveiligde servers).

1. **Kennis:** Medewerkers kunnen alleen op een veilige manier data opslaan als ze weten hoe ze dit moeten doen.
2. **Gewoonten en automatismen:** Medewerkers slaan data dagelijks op. Daar hebben ze vaste patronen en gedragingen voor ontwikkeld. Langdurige gedragsverandering heeft tijd nodig.
3. **Houding:** Het verkeerd opslaan van data kan onvoldoende worden ingeschat als gevaarlijk. Totdat het een keer misgaat. Weerstand ligt bovendien op de loer. 'Ik bepaal zelf wel waar ik mijn data opsla.'

Op het moment dat medewerkers data moeten delen, weten ze hoe ze dit op een veilige manier kunnen doen (via beveiligd systeem/SURFdrive bijvoorbeeld).

1. **Kennis:** Medewerkers kunnen alleen op een veilige manier data delen als ze weten hoe ze dit moeten doen.
2. **Gewoonten en automatismen:** Medewerkers delen dagelijks informatie met collega's of studenten. Daar hebben ze vaste patronen en gedragingen voor ontwikkeld. Langdurige gedragsverandering heeft tijd nodig.
3. **Houding:** Het delen van data via onbeveiligde systemen wordt onvoldoende ingeschat als gevaarlijk. 'Even WeTransfer gebruiken kan geen kwaad.' Weerstand ligt op de loer. 'Ik bepaal zelf wel hoe ik mijn data deel.'

Op het moment dat medewerkers data op een onveilige manier toegestuurd krijgen van een collega spreken ze hem/haar daarop aan.

1. **Sociale omgeving:** Gedrag wordt voor een groot deel bepaald door onze sociale omgeving. Dit werkt twee kanten op. Ziet een medewerker dat collega's het juiste gedrag laten zien, dan stimuleert dit bij hem/haar ook het gewenste gedrag. Zien we echter veel verkeerd gedrag, dan zal het ongewenste gedrag de norm worden.
2. **Houding:** De attitude heerst dat het ieders eigen verantwoordelijkheid is om data op de juiste manier te delen. Dit verkleint de kans dat medewerkers elkaar hierop aanspreken.
3. **Zelfbeeld:** Het zorgt voor onzekerheid als een medewerker onvoldoende weet wat het juiste gedrag is. Dit kan ertoe leiden dat medewerkers elkaar er niet op durven aanspreken als een collega op een onveilige manier data deelt.

WACHTWOORDEN

Op het moment dat medewerkers en studenten hun wachtwoord aanpassen weten ze aan welke eisen een wachtwoord moet voldoen om veilig te zijn.

1. **Kennis:** Medewerkers en studenten kunnen alleen op een veilige manier hun wachtwoord aanpassen als ze weten aan welke eisen een wachtwoord moet voldoen.
2. **Gewoonten en automatismen:** Wachtwoorden aanpassen of aanmaken gebeurt vaak op de automatische piloot. We willen snel een account aanmaken en we vinden het lastig om wéér een nieuw wachtwoord te bedenken. Met als resultaat dat we wéér een wachtwoord gebruiken dat is afgeleid uit een eerder wachtwoord.
3. **Houding:** Medewerkers en studenten bezitten doorgaans veel verschillende inloggegevens. Weer een nieuw wachtwoord bedenken voelt als veel gedoe. En hoe groot is de kans nou eenmaal dat jouw wachtwoord wordt gekraakt?

Medewerkers en studenten maken gebruik van tweefactorauthenticatie waar mogelijk.

1. **Kennis:** Medewerkers en studenten kunnen alleen gebruikmaken van tweefactorauthenticatie als ze weten hoe ze dat moeten doen.
2. **Emoties en associaties:** Tweefactorauthenticatie is een technologisch afgedwongen maatregel. Dit kan negatieve emoties en weerstand veroorzaken bij de gebruiker.
3. **Houding:** Het gebruik van tweefactorauthenticatie voelt voor medewerkers en studenten als veel gedoe.

Medewerkers en studenten zijn op de hoogte van de mogelijkheid om een wachtwoordmanager te gebruiken.

1. **Kennis:** Medewerkers en studenten kunnen alleen gebruikmaken van een wachtwoordmanager als ze weten hoe ze dat moeten doen.
2. **Houding:** Mogelijk voelen medewerkers en studenten weerstand of wantrouwen ten aanzien van het gebruik van een wachtwoordmanager. Want wat als de wachtwoordmanager wordt gehackt?
3. **Fysieke omgeving:** Mogelijk zijn er kosten verbonden aan het gebruik van een wachtwoordmanager. Of heerst er onduidelijkheid over welke wachtwoordmanager het best te gebruiken is.

STRATEGIE

5.1 WELKE COMMUNICATIEMIDDELEN GAAN WE INZETTEN?

In stap 4 heeft Oscar bepaald welke factoren van invloed zijn op het gedrag dat hij met de awareness-campagne wil beïnvloeden. Daaruit komt naar voren dat hij:

- Medewerkers en studenten moet voorzien van **kennis** op het gebied van wachtwoorden en phishing. Medewerkers moeten daarnaast op de hoogte gebracht worden van regels omtrent veilig datagebruik.
- **Gewoonten en automatismen** van medewerkers en studenten moet je proberen te doorbreken.
- De **houding** van medewerkers en studenten ten aanzien van veilig wachtwoordgebruik, phishing en veilig datagebruik moet je zien te veranderen.

In deze fase bepaalt Oscar met welke middelen hij de doelen van het awareness-programma kan behalen. In het Plan van aanpak omschrijft hij kort welke middelen hij in wil gaan zetten en waarom.

IN HET PLAN VAN AANPAK:

Op het gebied van wachtwoorden, veilig omgaan met data en phishing heerst nog veel onduidelijkheid bij medewerkers en studenten van onze hogeschool. Daarom is het op de eerste plaats van belang dat we de doelgroep informeren en voeden met de benodigde kennis. Om dit te bereiken willen we in ieder geval de volgende middelen inzetten:

- Informatie over de drie onderwerpen in de nieuwsbrief.
- Informatie over de drie onderwerpen op de website.
- Informatie over de drie onderwerpen op intranet.
- Introductie van het awareness-programma via e-mail.
- Introductie van het awareness-programma via televisieschermen/informatieborden.
- Verspreiding van posters binnen de instelling. Om aandacht te vragen voor het awareness-programma en om kennis over de drie onderwerpen te delen. Posters worden voornamelijk verspreid op relevante locaties, bijvoorbeeld waar veel met laptops wordt gewerkt.
- Verspreiding van koffiebekers met opdruk binnen de instelling. Om aandacht te vragen voor het awareness-programma.

Gewoonten en automatismen moeten worden doorbroken. Om dit te bereiken zetten we middelen in die studenten en medewerkers op belangrijke en relevante momenten uit hun gedragspatronen halen. Bijvoorbeeld door ze te toetsen of herinneren aan het gewenste gedrag.

- Gesimuleerde phishingacties.
- Pop-up die medewerkers herinnert aan het gewenste gedrag op het moment dat ze data opslaan.
- We voorzien medewerkers en studenten van een wachtwoordmanager.

De houding van medewerkers en studenten ten aanzien van de verschillende onderwerpen moet veranderen. Dit bereiken we onder meer door onze doelgroep te inspireren.

- De inzet van een ambassadeursprogramma onder medewerkers en studenten.
- Workshops en trainingen voor directie en personeelsleden.

TOETSING

6.1 HOE GAAN WE METEN?

Om te achterhalen of de middelen die Oscar tijdens het programma inzet ook daadwerkelijk het gewenste gedrag opleveren moet hij metingen uitvoeren. Daarom bedenkt hij in stap 6 hoe hij gaat toetsen of de doelen van het programma behaald worden.

Hiervoor vraagt hij advies aan data-analisten van de ICT-afdeling. Ook haalt hij inspiratie uit de tabel met meetmogelijkheden op de wiki. Dit zorgt ervoor dat hij op de hoogte is van de mogelijkheden om data te verzamelen. In het Plan van aanpak benoemt hij kort hoe hij gaat meten of de gedragsdoelen worden behaald.

PHISHING

Doel: *Op het moment dat er een phishingmail binnenkomt weten onze medewerkers en studenten waaraan ze deze kunnen herkennen.*

Wordt gemeten door:
het aantal mensen dat klikt op de link of een bijlage opent tijdens een phishingsimulatie.

Doel: *Op het moment dat er een phishingmail binnenkomt melden onze medewerkers en studenten dit direct bij de ICT-helpdesk.*

Wordt gemeten door:
het aantal mensen dat een phishingmail detecteert en rapporteert tijdens een phishingsimulatie.

Doel: *Nadat studenten en medewerkers de phishingmail gemeld hebben bij de ICT-helpdesk verwijderen ze deze permanent uit hun inbox.*

Wordt gemeten door:
het aantal mensen dat de phishingmail na detectie permanent verwijdert tijdens een phishingsimulatie.

VEILIG OMGAAN MET DATA

Doel: *Op het moment dat medewerkers data op moeten slaan weten ze hoe én waar ze dit moeten doen (op beveiligde servers).*

Wordt gemeten door:
afname van een online vragenlijst.

Doel: *Op het moment dat medewerkers data moeten delen weten ze hoe ze dit op een veilige manier kunnen doen (via beveiligd systeem/SURFdrive bijvoorbeeld).*

Wordt gemeten door:
afname van een online vragenlijst.

Doel: *Op het moment dat medewerkers data op een onveilige manier toegestuurd krijgen van een collega spreken ze hem/haar daarop aan.*

Wordt gemeten door:
afname van een online vragenlijst.

WACHTWOORDEN

Doel: *Op het moment dat medewerkers en studenten hun wachtwoord aanpassen weten ze aan welke eisen een wachtwoord moet voldoen om veilig te zijn.*

Wordt gemeten door:
afname van een online vragenlijst.

Doel: *Medewerkers en studenten maken gebruik van tweefactorauthenticatie waar mogelijk.*

Wordt gemeten door:
afname van een online vragenlijst.

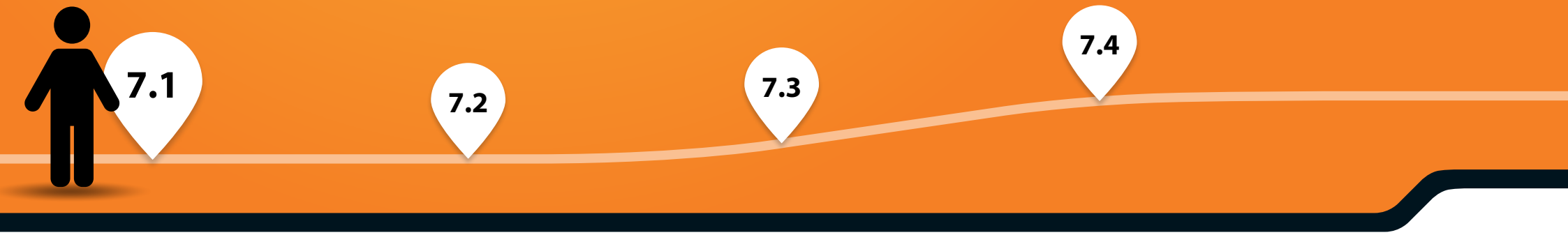
Doel: *Medewerkers en studenten zijn op de hoogte van de mogelijkheid om een wachtwoordmanager te gebruiken.*

Wordt gemeten door:
afname van een online vragenlijst.

UITVOERING

7.1 PLANNING

Nu Oscar de eerste zes stappen heeft doorlopen is het tijd om te beginnen met de uitvoering. Hij start daarbij met het maken van een planning. In die planning staat beschreven wanneer welk onderdeel van het programma aan bod komt. Hij wil graag starten met het programma op de eerste dag van het nieuwe schooljaar. De tijd die hem tot die tijd nog rest gebruikt hij om het programma verder uit te werken.
Je kunt daarbij bijvoorbeeld denken aan de ontwikkeling van middelen.



7.2 TEAM

Oscar is niet in staat om in z'n eentje het awareness-programma te ontwikkelen en te dragen. Daarom stelt hij een team samen én een stuurgroep.

Het team is verantwoordelijk voor de dagelijkse gang van zaken rond het awareness-programma. Oscar is zelf fulltime in dienst als Security Officer op Hogeschool Harderwijk. Naast hem wil hij graag nog een Security Officer aanstellen, zodat ze samen met hun leidinggevende en een medewerker van de afdeling Communicatie het programma kunnen dragen.

De stuurgroep omvat adviseurs uit verschillende lagen van de organisatie en komt één keer per kwartaal samen.

In het Plan van aanpak geeft Oscar aan hoe de teamsamenstelling eruit komt te zien.

IN HET PLAN VAN AANPAK:

Het privacy- en security-awareness-team zal bestaan uit de volgende functies/personen.

• Oscar Lodewijks	Security Officer	1.0 fte
• Angela de Jong	Security Officer	1.0 fte
• Bas Jansen	Manager Informatietechnologie	0.2 fte
• Mariska de Vries	Marketing- en communicatiemedewerker	0.2 fte

De adviesraad voor het awareness-programma zal bestaan uit de volgende functies/personen.

• Nicole van den Berg	Decaan
• Maikel Meijer	Hoofd Communicatie
• Dennis Janssen	Informatiemanager
• Kirsten van Dijk	Docent
• Maartje Bakker	Docent
• Jeffrey Visser	Student

7.3 TREF VOORBEREIDINGEN

De basis van het awareness-programma van Hogeschool Harderwijk staat. Maar voordat het programma echt van start kan moet Oscar er eerst zorg voor dragen dat de benodigde materialen ontwikkeld worden. Dit doet hij in overleg met de marketing- en communicatieafdeling. Zij hebben de kennis en connecties in huis om voor het awareness-programma een communicatieconcept te ontwikkelen.

Uiteindelijk maakt Oscar samen met zijn team de beslissing om gebruik te maken van het Cybersave Yourself-materiaal dat je terug kunt vinden op de wiki.

KIJK OP DE WIKI VOOR CYBERSAVE YOURSELF-MATERIAAL

7.4 AAN DE SLAG

Oscar heeft alle stappen doorlopen. Het awareness-programma van **Hogeschool Harderwijk** is er klaar voor om gelanceerd te worden!

7.1 7.2 7.3 7.4