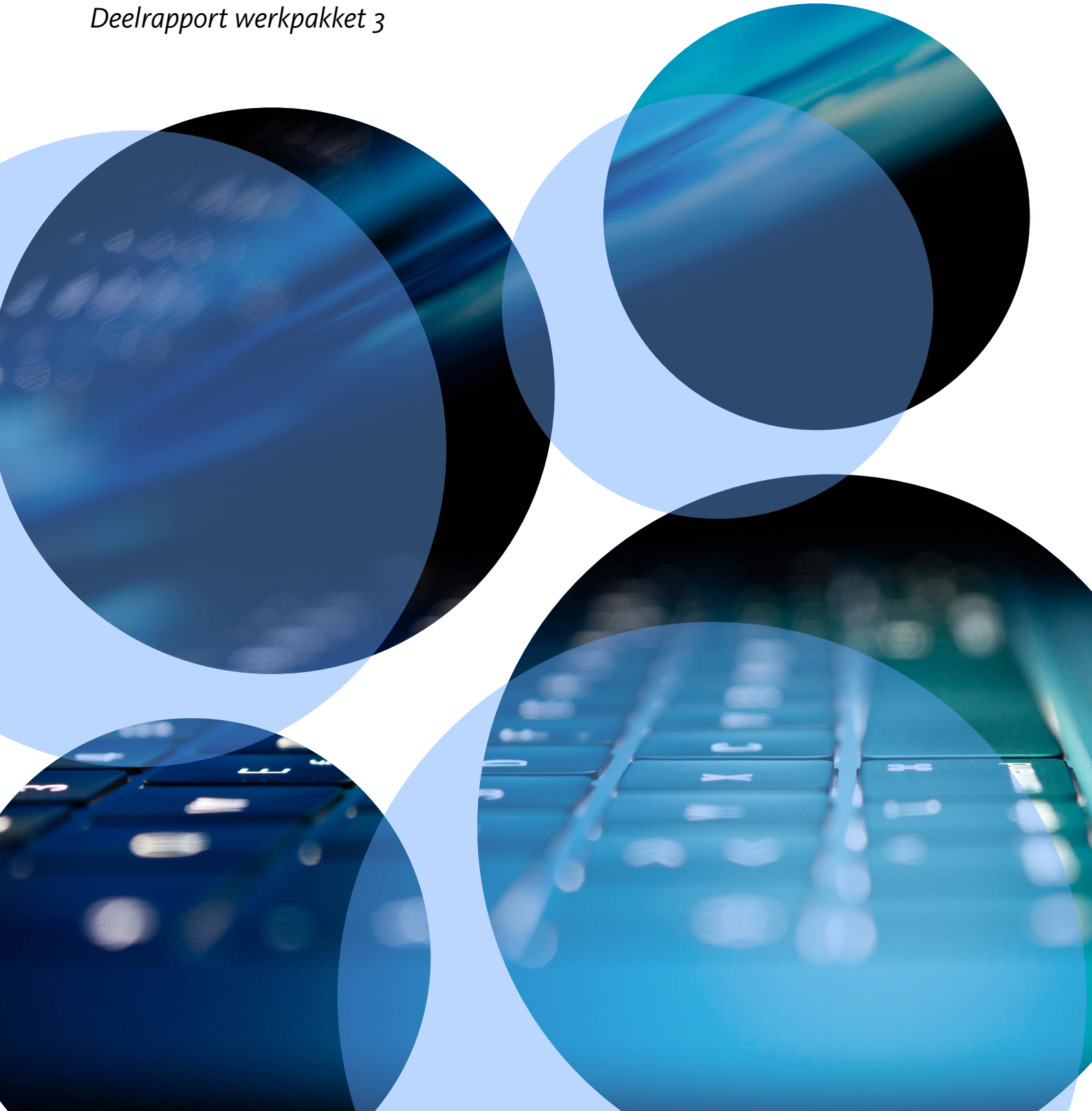
CYBERWEERBAARHEID

Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime.

Risicobewustzijn, preventief gedrag en de verklaringen daarvoor

Deelrapport werkpakket 3



COLOFON

Dit onderzoek is uitgevoerd door onderzoekers van het lectoraat Cybersecurity in het mkb van de Haagse Hogeschool en Maatschappelijke Veiligheid van Hogeschool Saxion:

Dr. Ellen Misana-ter Huurne[1]
Luuk Bekkers, MSc.[2]
Dr. Susanne van 't Hoff-de Goede[2]
Dr. Ynze van Houten[1]
Senna Hansen, MSc.[1]
Elsa Foppen, MSc.[1]
Sarah Ebrahem, MSc.[1]
Dr. Remco Spithoven[1]
Dr. Rutger Leukfeldt[1,3]

in samenwerking met de consortiumpartners binnen het project *'Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime'*:

Veiligheidsalliantie Regio Rotterdam
Noord-Holland Samen Veilig
Gemeente Almere
Gemeente Apeldoorn
Gemeente Den Helder
Gemeente Ede
Gemeente Haarlem
Gemeente Utrecht
Regionale Veiligheidsstrategie Midden-Nederland
Veiligheidsnetwerk Oost-Nederland
Gemeente Amersfoort
Gemeente Capelle a/d IJssel
Gemeente Dordrecht
Gemeente Enschede
Gemeente Rotterdam
Gemeente Zoetermeer
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Dit onderzoek is medegefinancierd door Regieorgaan SIA, onderdeel van de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO).

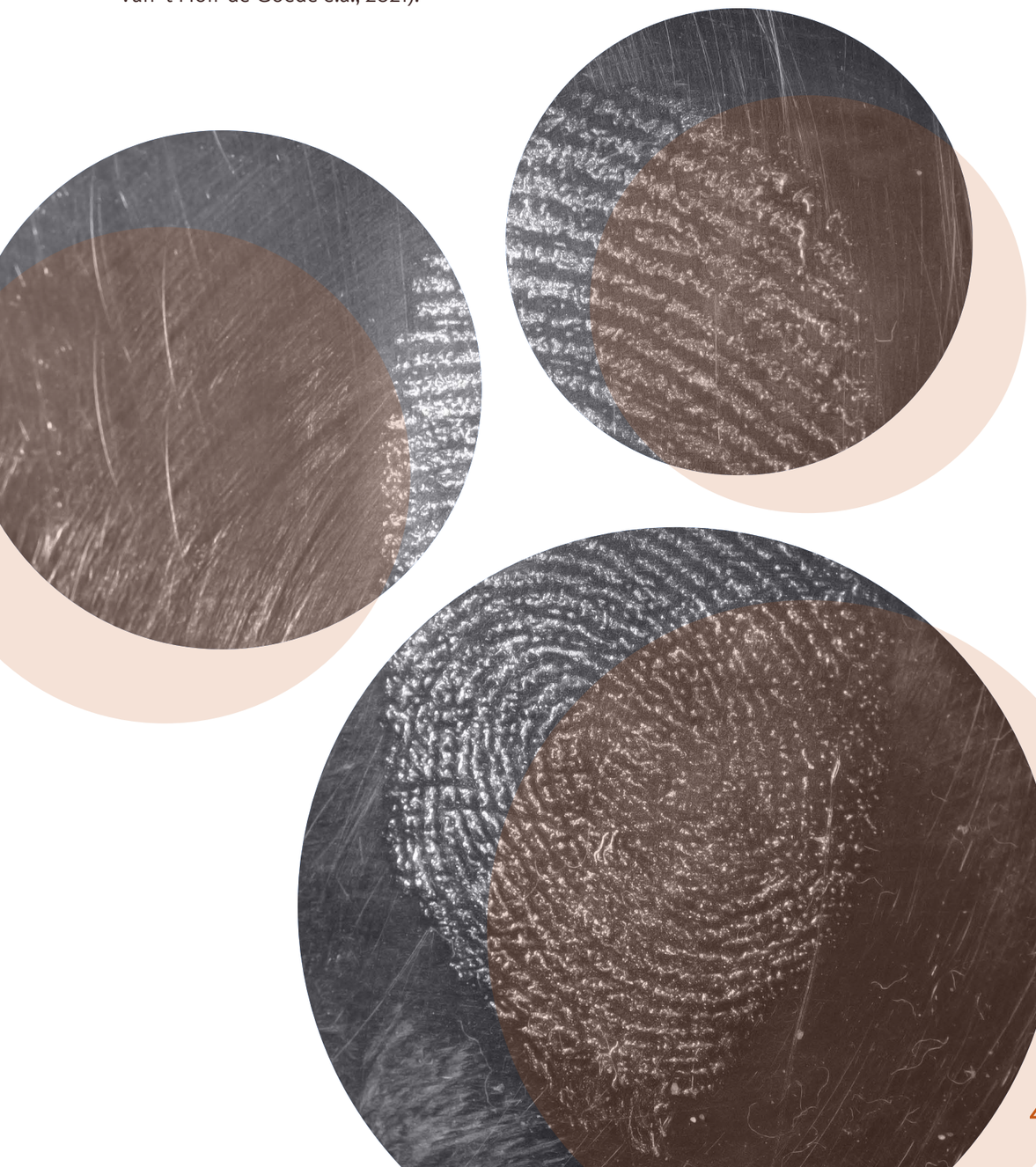
---

[1] Hogeschool Saxion
[2] De Haagse Hogeschool
[3] Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Inhoud

OPMERKING VOORAF

Dit rapport geeft een samenvatting van de resultaten van het onderzoek naar de sociaalpsychologische factoren en hun onderlinge samenhang die bijdragen aan de cyberweerbaarheid van jongeren, ouderen en mkb'ers ten aanzien van de geselecteerde typen cyberdelicten, als onderdeel van het project 'Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime'. Voor een gedetailleerde uitwerking van de onderzoeksmethoden en -resultaten van alle doelgroepen, verwijzen wij naar de volledige onderliggende deelrapporten per doelgroep (jongeren: Misana-ter Huurne e.a., 2021; ouderen: Van Houten e.a., 2021, mkb'ers: Van 't Hoff-de Goede e.a., 2021).



1. INLEIDING

1.1. Cyberweerbaarheid bij verschillende doelgroepen en typen delicten

Waar traditionele criminaliteit zoals woninginbraak en winkeldiefstal de laatste jaren afneemt, is er een sterke toename van cybercriminaliteit. Een groeiend aantal mensen en bedrijven wordt slachtoffer van verschillende en steeds weer nieuwe vormen van online criminaliteit. De vraag is nu hoe we slachtofferschap zoveel mogelijk kunnen voorkomen en mensen kunnen helpen zichzelf (of hun bedrijf) te beschermen tegen cybercriminelen. Een belangrijk aanknopingspunt hierin is online gedrag: steeds weer blijkt dat het menselijk handelen de belangrijkste oorzaak is van slachtofferschap.

In het project "Cyberweerbaarheid: een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime"[4] zoeken we naar manieren om mensen weerbaarder te maken tegen slachtofferschap van cybercriminelen. Hierbij wordt dus ingezet op preventie. Dit is maatwerk. Soms gaat het om het vergroten van de kennis en het risicobewustzijn van de mensen, in andere gevallen weten mensen wel dat er risico's zijn, maar hebben ze geen idee hoe ze zichzelf kunnen beschermen, of zien ze het niet als een risico voor hen persoonlijk. Wanneer mensen zich bewust zijn van de risico's van online criminaliteit, kennis hebben over hoe ze zichzelf kunnen beschermen en zichzelf ook daadwerkelijk gaan beschermen, verkleint dat de kans om slachtoffer te worden van cybercriminelen. We noemen dat 'cyberweerbaarheid'. Een grotere cyberweerbaarheid resulteert in een grotere mate waarin iemand in staat is tegenstand te bieden tegen cybercriminaliteit, ofwel zelfbeschermend gedrag te vertonen met betrekking tot cybercriminaliteit (Jansen, 2018; Van der Kleij en Leukfeldt, 2019). Het is daarom essentieel om inzicht te hebben in welke factoren een rol spelen bij het risicobewustzijn en het online zelfbeschermende gedrag van mensen. Dit inzicht is nodig om interventies te kunnen ontwikkelen die inspelen op de specifieke behoeften en gedragingen van de doelgroep.

We hebben in voorgaand onderzoek (werkpakketten 1 en 2 van dit project) inmiddels drie doelgroepen geïdentificeerd waarvoor het vergroten van de cyberweerbaarheid het meest wenselijk is, te weten: 1) jongeren van 16-25 jaar, 2) ouderen vanaf 55 jaar en 3) ondernemers in het midden- en kleinbedrijf (mkb'ers met maximaal 250 medewerkers) (Misana-ter Huurne e.a., 2021a). Deze groepen lijken relatief vaak slachtoffer te worden van cybercriminaliteit en bovendien zijn de emotionele en/of financiële gevolgen van slachtofferschap groot.

Binnen deze doelgroepen zijn specifieke delicten in het domein cybercrime geïdentificeerd waarvan slachtofferschap relatief vaak voorkomt. Voor jongeren is dit het misbruik van seksuele beelden, voor ouderen de zogenaamde vriend-in-noodfraude en voor mkb'ers is dat ransomware. Phishing blijkt daarnaast relevant te zijn voor alle eindgebruikers en is niet verbonden aan een specifieke doelgroep. Daarom is gekozen om voor alle drie de doel-

4 In dit tweejarig project werken professionals uit twaalf gemeenten en vier regionale veiligheidsnetwerken samen met onderzoekers van de Haagse Hogeschool, Hogeschool Saxion en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) aan het verhogen van de cyberweerbaarheid van de lokale samenleving. Het doel is om te komen tot beproefde interventies die lokale overheden kunnen inzetten om de cyberweerbaarheid onder inwoners en ondernemers binnen hun gemeente te vergroten.

groepen de cyberweerbaarheid ook te vergroten voor phishing. In Tabel 1 is een overzicht opgenomen met de doelgroep-delictcombinaties van deze studie.
Dit onderzoek (werkpakket 3) richt zich op de vervolgvraag hoe het gesteld is met het risicobewustzijn en het zelfbeschermende gedrag van de doelgroepen ten aanzien van de genoemde cyberdelicten, en op welke beïnvloedende sociaalpsychologische factoren interventies zich moeten richten om de cyberweerbaarheid te verhogen.

1.2. Doelstelling

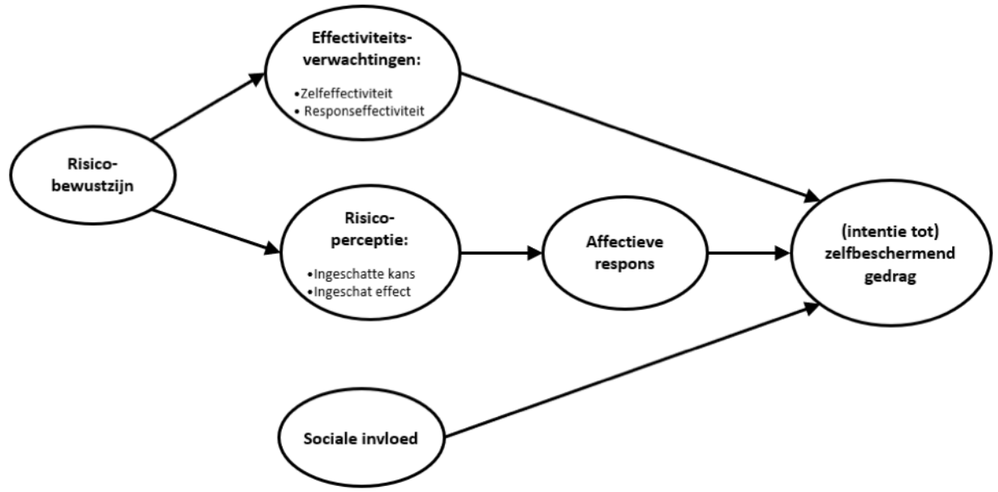
Dit onderzoek richt zich op het het inzichtelijk maken van de sociaalpsychologische factoren en hun onderlinge samenhang die bijdragen aan de cyberweerbaarheid van jongeren, ouderen en mkb'ers ten aanzien van de geselecteerde typen cyberdelicten. Hiermee wordt verder inzicht gegeven in de factoren waarop de te ontwikkelen interventies zich moeten richten om de cyberweerbaarheid (het risicobewustzijn en zelfbeschermend gedrag te bevorderen.

1.3. Onderzoeksvragen

De centrale onderzoeksvraag is:
Hoe is het gesteld met het risicobewustzijn en het zelfbeschermende gedrag van jongeren, ouderen en mkb'ers ten aanzien van de geselecteerde typen cybercrime en wat zijn de verklaringen voor het risicobewustzijn en het zelfbeschermende gedrag?
Om deze vraag te beantwoorden, zijn de volgende deelvragen gesteld:
1. Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van de doelgroepen ten aanzien van de cyberdelicten?
2. In welke mate vertonen leden van de doelgroepen zelfbeschermend gedrag ten aanzien van de cyberdelicten?
3. Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van leden van de doelgroepen ten aanzien van de cyberdelicten?

2. ZELFBESCHERMEND GEDRAG: HET CYBERWEERBAARHEIDSMODEL

Het Cyberweerbaarheidsmodel (Spithoven, 2020) dient als basis en als leidraad voor het inzichtelijk maken van het zelfbeschermend gedrag ten aanzien van cybercriminaliteit. Dit model geeft inzicht in hoe risicobewustzijn en zelfbeschermend gedrag ontstaat en welke factoren hierop van invloed zijn (Figuur 1).



Figuur 1. Het Cyberweerbaarheidsmodel (deels; cf. Spithoven, 2020)

De gedragsintentie komt volgens het model tot stand door een combinatie van verschillende factoren. Ten eerste de risicobeleving van mensen. Op basis van het risicobewustzijn (kennis, ervaring, etc.) vormt iemand een mate van risicoperceptie. Risicoperceptie is de persoonlijke inschatting van de risico's door een individu. Dit is gebaseerd op inschattingen van de kans dat een persoon wordt blootgesteld aan dat risico en de ernst van mogelijke effecten. De risicoperceptie beïnvloedt de affectieve respons. Affectieve respons heeft betrekking op de gevoelsmatige beleving van het risico, zoals angstig zijn, zich zorgen maken, etc. Prikkels uit de omgeving, bijvoorbeeld aandacht voor het risico op sociale media, kunnen bepaalde emotionele reacties teweegbrengen, zoals angst. Dit heeft invloed op de risicobeleving. Deze affectieve respons bepaalt in hoeverre iemand zichzelf beschermt. Ten tweede zijn de effectiviteitsverwachtingen direct van invloed op iemands (voornemen tot) zelfbeschermend gedrag. De effectiviteitsverwachtingen bestaan uit zelfeffectiviteit ('Ben ik in staat om het zelfbeschermend gedrag uit te voeren?') en responseffectiviteit ('Vind ik dit zelfbeschermend gedrag effectief om slachtofferschap te voorkomen?'). De derde factor die een belangrijke invloed heeft op de intentie om zelfbeschermend gedrag te vertonen is sociale invloed in de vorm van subjectieve normen. Dit is het beeld dat iemand heeft van de sociale norm wat betreft

het beschermen tegen cybercriminaliteit. Hoe groter de ervaren subjectieve normen en sociale invloed, hoe meer iemand geneigd is om zelfbeschermend gedrag te vertonen.
Met interventies willen we bereiken dat mensen beseffen dat (I) zij persoonlijk kans lopen om slachtoffer te worden en (II) de ernst en de gevolgen van slachtofferschap goed inschatten. Met andere woorden: een hoge risicoperceptie hebben. Pas dan zullen zij geneigd zijn zelfbeschermend gedrag te (willen) gaan uitvoeren. Daarvoor hebben zij hoge effectiviteitsverwachtingen nodig. Dat betekent dat zij (III) vertrouwen hebben dat zij het aanbevolen gedrag zelf goed kunnen uitvoeren (zelf-effectiviteit) en (IV) vinden dat dit gedrag ook effectief is om slachtofferschap te voorkomen (responseffectiviteit).
Wanneer deze vier elementen hoog zijn, is de motivatie voor zelfbeschermend gedrag het grootst. Echter, wanneer de waargenomen dreiging als laag wordt ervaren, dan is er geen motivatie of prikkel om preventief gedrag te gaan uitvoeren (men heeft immers niet het idee dat men gevaar loopt). Wanneer de waargenomen dreiging als hoog wordt ervaren, maar de effectiviteitsverwachtingen laag zijn, dan gaat angst of onrust een grote rol spelen. Immers, men heeft dan het idee dat men gevaar loopt en dat dit ernstige gevolgen kan hebben, maar heeft niet het idee hier zelf effectief op te kunnen anticiperen. Dit kan leiden tot het 'fear-control-process', waarbij men niet het risico of het gevaar zelf wil minimaliseren, maar alleen de gevoelens van angst die ontstaan. Dan gaan mensen bijvoorbeeld informatie over het risico vermijden, het risico bagatelliseren, of andere activiteiten ondernemen om de negatieve beleving op te heffen. In aanvulling hierop kan de intentie tot zelfbeschermend gedrag ook direct worden beïnvloed door subjectieve sociale normen (V). Deze bestaan uit de perceptie van sociale aanmoediging van het gedrag en de waargenomen geldende normen wat betreft het omgaan met het risico van cybercriminaliteit in de sociale omgeving van een persoon.

3. ONDERZOEKSMETHODEN

Om deze onderzoeksvragen te beantwoorden is een combinatie van onderzoeksmethoden ingezet. Bij iedere doelgroep (jongeren, senioren, mkb'ers) zijn 1) vragenlijsten afgenomen onder een representatieve steekproef en 2) interviews afgenomen. Middels de vragenlijsten is inzicht verkregen in risicobewustzijn, zelfbeschermend gedrag en verklarende factoren. Achterliggende overtuigingen en aanvullende verklaringen zijn via interviews in beeld gebracht. De combinatie van deze twee onderzoeksmethoden geeft een gedegen beeld van de cyberweerbaarheid en de verklarende factoren hiervan per doelgroep ten aanzien van de onderzochte cyberdelicten.

3.1. Vragenlijsten

De vragenlijsten zijn uitgezet in een representatieve steekproef van de doelgroepen (jongeren, senioren en mkb'ers) uit een panel van een gerenommeerd onderzoeksbureau. Voor iedere doelgroep zijn minimaal 1000 respondenten geworven.[5] Om de representativiteit van respondenten te waarborgen is de steekproef geselecteerd op basis van persoonlijkheidskenmerken, zoals leeftijd en opleidingsniveau (bij jongeren en senioren), bedrijfsomvang en de aanwezigheid van kennis/expertise op het gebied van cybercriminaliteit (bij mkb'ers). Respondenten vulden de vragenlijsten online in. Van iedere doelgroep
De vragenlijst bestond bestond uit Likert-type schalen met items (stellingen en vragen) die de onderzoekconcepten uit het Cyberweerbaarheidsmodel meten. De schalen zijn getoetst op betrouwbaarheid en blijken allemaal betrouwbaar.
De vragenlijstdata zijn geanalyseerd met behulp van beschrijvende en verklarende sta-

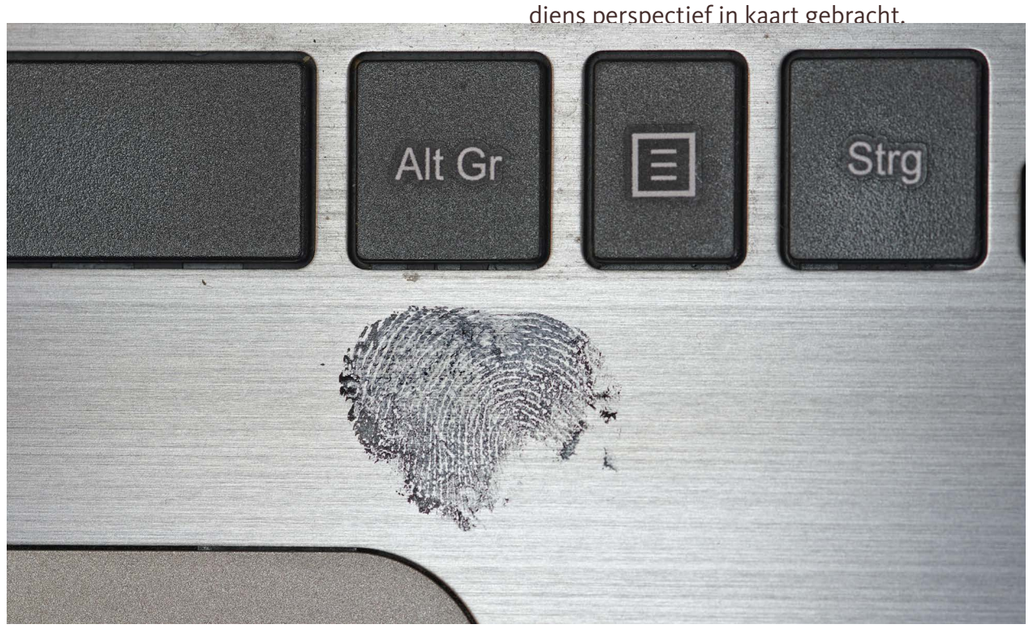
5 Voor een beschrijving van de kenmerken van de respondenten per doelgroep, zie Bijlagen 1 t/m 3.

tistieken. Door middel van Structural Equation Modelling (SEM) is het conceptueel model getoetst, waarbij inzicht is verschaft in welke factoren daadwerkelijk (het meest en significant) bijdragen aan het beïnvloeden van het zelfbeschermende gedrag.

3.2. Interviews

De inzichten op basis van de vragenlijsten zijn aangevuld met interviews; dertig per doelgroep. De vragen waren gestructureerd rondom de concepten uit het cyberweerbaarheidsmodel en verder gespecificeerd op de onderzoeksvragen. Centrale concepten waren de risicoperceptie, het risicobewustzijn, het zelfbeschermend gedrag en de verklarende factoren hierbij. De vraagstelling was open van aard. Dit bood de interviewer de mogelijkheid om door te vragen, waarbij ook dieper ingegaan kon worden op achterliggende overtuigingen of motieven.

Respondenten zijn geworven via persoonlijke netwerken van de onderzoekers, onder anderen via sociale media. Hierbij is gestreefd naar een grote diversiteit binnen de doelgroepen op basis van leeftijd, geslacht en opleidingsniveau bij jongeren en ouderen en voor mkb'ers op sector en aantal medewerkers. De interviews zijn via een videoverbinding afgenomen in verband met de coronacrisis en de bijbehorende beperkende maatregelen in het voorjaar van 2021.
Van alle interviews zijn met toestemming van de respondent geluidsopnames gemaakt. Deze opnames zijn getranscribeerd, waarna het geluidsfragment direct van de opnameapparatuur is verwijderd en de transcripten zijn geanonimiseerd. De transcripten zijn vervolgens met behulp van ATLAS.ti[6] geanalyseerd, waarbij na open codering netwerken van codes zijn gezocht om mechanismen in de data te ontwaren. Op deze manier zijn onderliggende verklaringen voor het risicobewustzijn en preventief gedrag van de respondenten vanuit diens perspectief in kaart gebracht.



6 ATLAS.ti is software gericht op de analyse van kwalitatieve onderzoeksgegevens.

4. RESULTATEN DOELGROEP JONGEREN

In dit hoofdstuk worden de resultaten van de vragenlijst en de interviews met jongeren over phishing en het misbruik van seksueel beeldmateriaal beschreven en afgesloten met een weergave van de conclusies en aanbevelingen.

4.1. Misbruik van seksueel beeldmateriaal

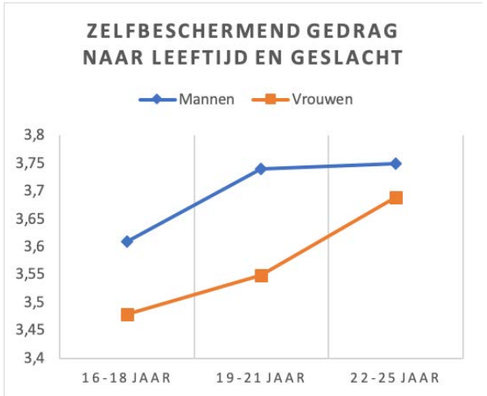
Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van jongeren ten aanzien van misbruik van seksueel beeldmateriaal?"

De gepercipieerde mate van risicobewustzijn impliceert dat jongeren zichzelf redelijk bewust vinden van de risico's gekoppeld aan misbruik van seksuele beelden (score van 3.68 op een vijfpuntsschaal). Uit de interviews is echter naar voren gekomen dat jongeren bij misbruik van seksueel beeldmateriaal voornamelijk denken aan de risico's gekoppeld aan het zelf maken en versturen van dergelijke beelden. Het risico op onrechtmatig verkregen beeldmateriaal, bijvoorbeeld door hacking of het creëren hiervan door middel van deep fakes, komt in eerste instantie niet op bij de respondenten. Daarmee is het bewustzijn van de risico's op handelingen van kwaadwillenden die doelbewust seksueel beeldmateriaal verkrijgen en/of creëren relatief laag te noemen.
De inschatting van de eigen kans om slachtoffer te worden wordt gemiddeld als (heel) klein ervaren (gemiddeld 1.33). Echter, de schade en emotionele impact worden veel hoger ingeschat (gemiddeld 4.48). Opvallend is, dat respondenten aangeven vooral te leunen op vertrouwen bij het maken en verzenden van seksueel beeldmateriaal; velen geven aan dat zij dit uitsluitend of eerder zouden doen wanneer zijn in een langdurige relatie zitten en/of degene waar zij de beelden naar versturen vertrouwen.
De ondervraagde jongeren achten de kans dat een leeftijdsgenoot van hetzelfde geslacht komend jaar slachtoffer wordt van misbruik van seksuele beelden veel hoger in (gemiddeld 3.41) dan hun eigen kans op slachtofferschap (gemiddeld 1.33). Hiermee is een sterke optimistic bias waargenomen; de kans dat anderen slachtoffer worden, wordt ruim twee keer zo groot ingeschat. De verklaring hiervoor lijkt te liggen in dat zij van zichzelf weten dat zij geen seksuele beelden delen, zelf bewuster zijn van risico's, minder online zijn dan leeftijdsgenoten en sterker in hun schoenen staan. Echter, het risico van deep fakes en dergelijke wordt wel hoog ingeschat, maar tegelijkertijd geven de jongeren aan geen idee te hebben hoe zij zich daartegen zouden kunnen beschermen.

Onderzoeksvraag 2: "In welke mate vertonen jongeren zelfbeschermend gedrag ten aanzien van misbruik van seksuele beelden?"

Gemiddeld treffen de jongeren 'soms' tot 'vaak' zelfbeschermende maatregelen tegen cybercriminaliteit in zijn algemeenheid. Hierbij blijken achtergrondkenmerken van invloed te zijn; mannen vertonen een significant hogere mate van zelfbeschermend gedrag dan vrouwen. Daarnaast is ook leeftijd van invloed; de mate van zelfbeschermend gedrag neemt toe met de leeftijd. Samengenomen is gebleken dat jongere meisjes (16-18 jaar)

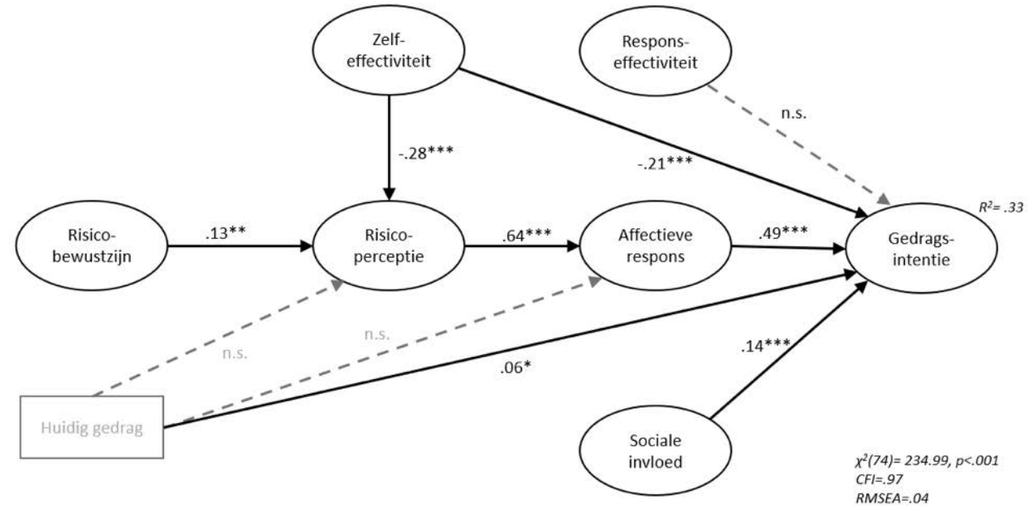
de laagste mate van zelfbeschermend gedrag tegen cybercriminaliteit in zijn algemeenheid vertonen en de oudere jongens (22-25 jaar) de hoogste mate. In Figuur 2 is te zien dat de jongere vrouwen het laagst scoren op algemeen zelfbeschermend gedrag en de 'oudere' jongens de hoogste mate van zelfgerapporteerd zelfbeschemend gedrag vertonen.



Figuur 2 Zelfbeschermend gedrag naar leeftijd en geslacht

Toegespitst op zelfbeschermend gedrag specifiek ter voorkoming van misbruik van seksueel beeldmateriaal, is gebleken dat de maatregel die het vaakst wordt uitgevoerd door de respondenten is het voorkomen dat er seksueel beeldmateriaal van ze bestaat (gemiddeld 4.35), gevolgd door het vermijden van opslag in de cloud van seksueel beeldmateriaal (gemiddeld 4.18) en het voor zichzelf houden van seksueel beeldmateriaal (4.09). Dit impliceert dat zelfbeschermend gedrag vooral bestaat op basis van 'voorkomen is beter dan genezen'. Dit moet echter in de context van de hele respondentengroep gezien worden; bijna alle respondenten hebben aangegeven tot nu toe (nog) niet aan sexting te hebben gedaan. Wanneer het gaat om kwaadwillenden die doelbewust seksueel beeldmateriaal afhandig maken, creëren of verzenden, is het zelfbeschermend gedrag erg laag. Jongeren zien dit als een risico voor iedereen, maar hebben weinig beeld van hoe je jezelf daartegen beschermt. Het gevoel van gebrek aan controle speelt hier een rol. De maatregelen die ze dan wel nemen zijn bijvoorbeeld het afplakken van webcams of het controleren op de aanwezigheid van camera's in bijvoorbeeld hotelkamers.

Onderzoeksvraag 3: "Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren ten aanzien van misbruik van seksuele beelden?"
Respondenten achten zichzelf redelijk goed in staat om zichzelf te beschermen tegen misbruik van seksuele beelden zolang het binnen hun eigen invloedssfeer ligt. Wanneer het gaat om kwaadwillenden is er volgens hen niets tot weinig aan te doen. Over het algemeen vinden ze het treffen van zelfbeschermende maatregelen wel effectief om slachtofferschap te voorkomen. Omdat weinig respondenten aangeven zelf aan sexting te doen, is hun risicoperceptie relatief laag en maken ze zich daarom ook weinig zorgen over hun veiligheid. Hun gedragsintenties zijn daarmee ook relatief laag.
Uit de verklarende analyses (Figuur 3) blijkt, dat deze gedragsintenties beïnvloed worden door verschillende voorspellers uit het Cyberweerbaarheidsmodel: hoe meer zorgen men zich maakt over de eigen risico's in combinatie met een lager beeld van zichzelf om zich te kunnen beschermen en de opvatting dat mensen in de omgeving van je verwachten dat je zelfbeschermend gedrag vertoont, hoe sterker de motivatie om dit ook te gaan doen. De responseffectiviteit is echter niet significant van invloed hierop.



Figuur 3 Paddiagram gedragsintentie alle ondervraagde jongeren (N=1179)

De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie. Deze inschatting van persoonlijk risico wordt vervolgens negatief beïnvloed door de mate van zelfeffectiviteit en positief beïnvloed door het risicobewustzijn. Met andere woorden, hoe meer men zich bewust is van de risico's van cybercriminaliteit in combinatie met een lagere inschatting van de eigen capaciteiten om zichzelf te beschermen, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen men zich maakt. Risicobewustzijn, zelfeffectiviteit en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan vertonen.

4.2. Phishing

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van jongeren ten aanzien van phishing?".

De mate van risicobewustzijn impliceert dat jongeren zichzelf redelijk bewust vinden van de risico's gekoppeld aan phishing met gemiddeld 3.41 op een vijfpuntsschaal. Uit de interviews blijkt dat respondenten op de hoogte zijn van wat phishing is. Zij omschrijven phishing als een techniek waarbij iemand zich voordoet als een andere organisatie of een ander individu om gevoelige informatie te ontfutselen. Dit wordt volgens respondenten vaak gedaan door het versturen van een nepmail waarbij de ontvanger vervolgens zelf vrijwillig de gevoelige informatie invult/opstuurt.
Ongeveer een derde van de ondervraagde jongeren (32%) geeft aan behoefte te hebben aan meer informatie. De respondenten die aangeven meer informatie te willen, willen met name weten wat ze kunnen doen om zichzelf te beschermen (86%), wat ze moeten doen bij slachtofferschap (68%) en hoe ze (een poging tot) phishing kunnen herkennen (59%). Dit betreft dus met name behoefte aan informatie over het verhogen van de zelfeffectiviteit.
De inschatting van de eigen kans om slacht-

“ Respondenten omschrijven phishing als een techniek waarbij iemand zich voordoet als een andere organisatie of een ander individu om gevoelige informatie te ontfutselen. ”

offer te worden wordt gemiddeld als (heel) klein ervaren (gemiddeld 1.82). Echter, de schade en impact worden met gemiddeld 3.90 veel hoger ingeschat. Dit impliceert dat respondenten van mening zijn dat ze weinig vatbaar zijn voor slachtofferschap, maar dat onverhoopt slachtofferschap wel grote schade en impact voor henzelf zou hebben.

Gemiddeld schatten de jongeren de kans dat een leeftijdsgenoot van hetzelfde geslacht komend jaar slachtoffer wordt van phishing veel hoger in (gemiddeld 2.67). Hiermee is een sterke optimistic bias waargenomen; slachtofferschap van phishing overkomt vooral anderen. Dit wordt in de interviews door de ondervraagde jongeren verklaard doordat ze denken zelf meer kennis te hebben over phishing en hoe zij slachtofferschap kunnen voorkomen dan leeftijdsgenoten. Daarnaast is in hun opvoeding benadrukt dat voorzichtigheid belangrijk is om slachtofferschap te voorkomen.

Onderzoeksvraag 2: “In welke mate vertonen jongeren zelfbeschermend gedrag ten aanzien van phishing?”.

Gemiddeld passen de respondenten ‘vaak’ zelfbeschermende maatregelen tegen phishing toe (gemiddeld 3.76). De maatregel die het vaakst wordt uitgevoerd is alleen op links klikken en alleen bijlagen openen van e-mails die zij vertrouwen (gemiddeld 4.53), gevolgd door het vermijden of direct verlaten van onbetrouwbare websites (gemiddeld 4.43) en het goed kijken naar de betrouwbaarheid van de afzender van een e-mail (gemiddeld 4.41). Uit de interviews komt naar voren dat respondenten zich beschermen tegen phishing door e-mails te negeren en te verwijderen, 2-staps verificatie in te stellen en bij twijfel over de echtheid van een bericht hulp te vragen bij het beoordelen van een bericht of de organisatie/afzender te benaderen. Daarnaast klikken respondenten überhaupt niet op een link in een bericht en hebben ze technische beveiligingsmaatregelen genomen, zoals het installeren van een virusscanner. Om te voorkomen dat respondenten spammails binnenkrijgen zijn zij kritisch bij het achterlaten van hun mailadres. Dit doen zij alleen indien het echt noodzakelijk is.

Onderzoeksvraag 3: “Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren ten aanzien van phishing?”.

Het merendeel van de respondenten acht zichzelf goed in staat om zichzelf te beschermen tegen phishing. Zij vinden bijvoorbeeld dat ze in staat zijn risico’s in te schatten en zichzelf te beschermen. Zij geven relatief minder vaak aan in staat te zijn om effectief te handelen als zij slachtoffer zouden worden van phishing. Over het algemeen vinden ze het treffen van maatregelen tegen phishing nuttig en effectief, maar ze zijn niet helemaal zeker of hun huidige maatregelen hen voldoende beschermen.

Toch maken jongeren zich maar een beetje of enigszins zorgen over hun risico op slachtofferschap van phishing. Uit de resultaten komt naar voren dat respondenten niet weten welke extra beschermende maatregelen zij kunnen nemen om slachtofferschap van phishing te voorkomen. Hierdoor staan ze dan ook gemiddeld redelijk neutraal tegenover het nemen van meer zelfbeschermende maatregelen tegen phishing. Ze geven aan dat ze meer ken-

nis nodig hebben om meer zelfbeschermende maatregelen te kunnen of willen uitvoeren. In Figuur 4 is te zien dat de intentie tot zelfbeschermend gedrag significant beïnvloed wordt door drie directe voorspellers uit het Cyberweerbaarheidsmodel: De mate waarin jongeren zich zorgen maken over hun eigen risico ten aanzien van phishing is hierbij de sterkste voospeller (β=0.38, p<0.001), implicerend dat hoe meer zorgen ze zich maken hoe meer ze geneigd zijn (aanvullende) maatregelen te gaan treffen. Daarnaast speelt de mate van zelfeffectiviteit een significante rol (β= -0.25, p<0.001); jongeren die zichzelf momenteel minder goed in staat achten zich te beschermen tegen phishing, zijn meer geneigd dat in de toekomst wel te gaan doen. Tot slot is de invloed vanuit de sociale omgeving ook een significante voorspeller (β=0.10, p<0.001); hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te gaan treffen.

De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie (inschatting van de persoonlijke kans op slachtofferschap en het effect daarvan; β=0.55, p<0.001). Deze inschatting van persoonlijk risico wordt vervolgens negatief beïnvloed door de mate van zelfeffectiviteit (β=-0.45, p<0.001) en positief beïnvloed door het risicobewustzijn (β=0.15, p<0.001). Met andere woorden, hoe meer men zich bewust is van de risico's van phishing in combinatie met een lagere inschatting van de eigen capaciteiten om zichzelf te beschermen, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen men zich maakt. Risicobewustzijn, zelfeffectiviteit en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan uitvoeren.

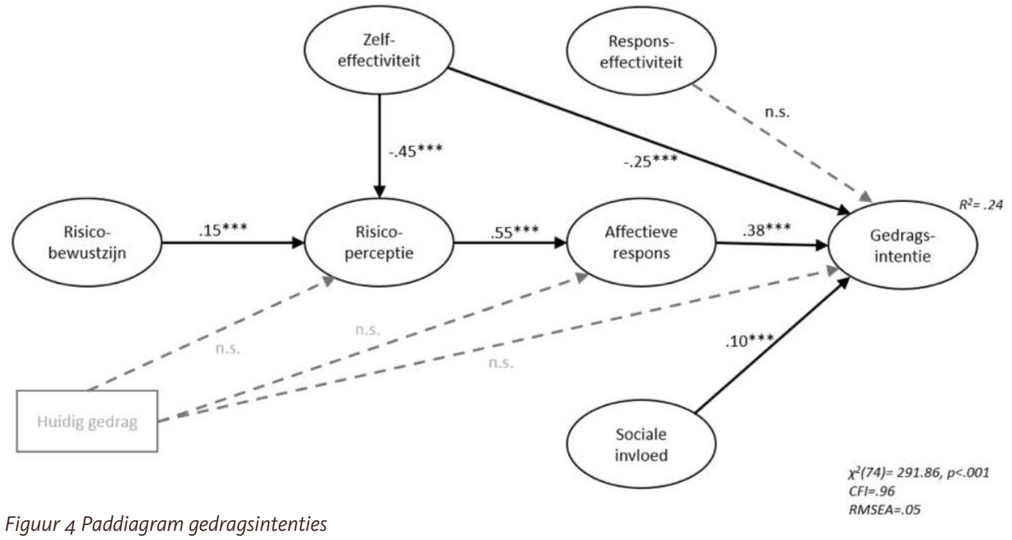
4.3 Geldezelen

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van jongeren ten aanzien van geldezelen?".

Ruim 8% van de jongeren is weleens direct benaderd om als geldezel op te treden. 0,8% heeft dat naar eigen zeggen ook daadwerkelijk gedaan. 12% van de jongeren heeft in zijn/haar omgeving gehoord dat andere jongeren zijn benaderd en 4% kent een geldezel uit zijn/haar omgeving. Bijna 60% heeft weleens een online advertentie gezien waarin geldezels worden geronseld. Het contact wordt vooral online via Snapchat en Instagram gelegd. Ook wordt er – in mindere mate - offline geronseld op school en op straat. Ronselaars zijn vooral via social media, via vrienden en via school bekend bij jongeren. Het fenomeen geldezelen is nog vrij onbekend. Minder dan de helft van de jongeren wist wat dit fenomeen inhoudt, degenen die dat wel wisten waren bekend met de risico's van geldezelen. Een klein deel van de jongeren vindt geldezelen echter stoer en acceptabel.

Onderzoeksvraag 2: "In welke mate vertonen jongeren zelfbeschermend gedrag ten aanzien van geldezelen?".

De jongeren vertonen een lage mate van zelfbeschermend gedrag want zij schatten de kans om zelf door ronselaars benaderd te worden laag in, men denkt vooral dat leeftijdsgenoten daar een grotere kans op lopen. De kans om vervolgens daadwerkelijk als geldezel op te treden wordt doorgaans ook laag ingeschat. De jongeren schatten immers de kans om door de bank en de politie ontdekt te worden vrij hoog in. Maar de jongeren hebben een vrij milde inschatting van de gevolgen: ze denken er met een waarschuwing of verscherpt toezicht vanaf te komen. Dat ze als fraudeur worden geregistreerd, vervolgd kunnen worden voor witwassen en een strafblad krijgen was slechts bij een deel van de jongeren bekend.



Figuur 4 Paddiagram gedragsintenties

Onderzoeksvraag 3: "Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren ten aanzien van geldezelen?".

Het is duidelijk dat de lage kansinschatting om als geldezel te worden geronseld en de milde inschatting van de gevolgen van het geldezelen leiden tot een lage mate van zelfbeschermend gedrag. Ook is het fenomeen geldezelen onder jongeren nog vrij onbekend en is er een deel van de jongeren wat positieve associaties heeft met geldezelen.

4.4. Geleerde lessen en aanbevelingen

4.4.1. Conclusies

Voor beide onderzochte delicten (misbruik van seksueel beeldmateriaal en phishing) kan worden gesteld dat het risicobewustzijn redelijk hoog is; jongeren geven aan op de hoogte te zijn van de risico's en hoe slachtofferschap ontstaat van zowel misbruik van seksueel beeldmateriaal als van phishing. Opvallend is, dat voor beide delicten een sterke optimistic bias is gevonden: men schat de kans dat een ander slachtoffer wordt veel groter in dan de eigen kans op slachtofferschap. Over het algemeen achten jongeren zichzelf dan ook redelijk tot goed in staat om zichzelf te beschermen tegen beide cyberdelicten en maken ze zich weinig zorgen over hun eigen online veiligheid. Het nemen van zelfbeschermende maatregelen wordt wel als nuttig en effectief beschouwd om jezelf te beschermen tegen slachtofferschap, en ze voeren voor beide delicten dan ook een redelijke mate van zelfbeschermend gedrag uit.

Gekeken naar dit huidige zelfbeschermende gedrag, dan zien we duidelijke verschillen tussen beide delicten. Bij het tegengaan van misbruik van seksueel beeldmateriaal zien jongeren vooral een taak voor zichzelf om te zorgen dat er geen beeldmateriaal beschikbaar is. Risicovermijding dus. Jongeren die wel seksueel beeldmateriaal van zichzelf verzenden, leunen vooral op vertrouwen in de ontvanger van de beelden. Jongeren hebben daarnaast geen idee hoe ze zich moeten beschermen tegen het doelbewust buitmaken van seksueel beeldmateriaal dat ze niet zelf verzenden, maar bijvoorbeeld gestolen wordt door hackers of gecreëerd wordt met behulp van deep fake. Dit ligt voor hun gevoel buiten hun persoonlijke invloedssfeer en daar hanteren ze dan ook weinig tot geen zelfbeschermende maatregelen voor. Daarentegen lijkt bij phishing voornamelijk alertheid een rol te spelen bij het vermijden van het risico, zoals het niet klikken op verdachte bijlagen of linkjes.
Gekeken naar de voorspellende variabelen bij de intenties om in de toekomst (aanvullend) zelfbeschermend gedrag te gaan uitvoeren, zien we dat met name de affectieve respons, de zelfeffectiviteit en de sociale invloed bij beide delicten direct invloed hebben op het voornemen voor toekomstig zelfbeschermend gedrag. Het risicobewustzijn, de risicoperceptie en de zelfeffectiviteit hebben daarbij een belangrijke indirecte invloed, via de affectieve respons. Bij beide delicten is de affectieve respons de belangrijkste directe voorspeller van gedragsintenties, gevolgd door een lagere zelfeffectiviteit. Daarnaast speelt de sociale omgeving – in de vorm van subjectieve normen bij misbruik van seksueel beeldmateriaal een gelijkwaardige voorspellende rol.

4.4.2. Aanbevelingen vergroten cyberweerbaarheid jongeren ten aanzien van misbruik seksueel beeldmateriaal

Op basis van de onderzoeksresultaten worden de volgende aanbevelingen gedaan om de cyberweerbaarheid van jongeren tegen misbruik van seksueel beeldmateriaal te vergroten:
• Ga specifiek in op de rol van vertrouwen bij het verzenden van seksueel beeldmateriaal.
• Geef concrete en makkelijk uitvoerbare handelingsperspectieven die als nuttig worden ervaren.
• Geef daarbij vooral informatie over hoe jongeren zichzelf kunnen beschermen, wat ze kunnen doen en waar ze terecht kunnen bij onverhoopt slachtofferschap.
• Schenk aandacht aan de sociale normen.
• Besteed specifieke aandacht aan jongeren die seksueel beeldmateriaal van zichzelf hebben en/of versturen.

4.4.3. Aanbevelingen vergroten cyberweerbaarheid jongeren ten aanzien van phishing

Op basis van de onderzoeksresultaten worden de volgende aanbevelingen gedaan om de cyberweerbaarheid van jongeren tegen phishing te vergroten:
• Vergroot de persoonlijke risicoperceptie en verklein de optimistic bias.
• Geef aan waarom aanvullende maatregelen nodig zijn om jezelf goed te beschermen en welke concrete handelingsperspectieven jongeren kunnen uitvoeren om dit te bereiken.
• Heb hiernaast specifieke aandacht voor het vergroten van het kennis- en risicobewustzijnsniveau van jongere en lager opgeleide jongeren.

4..4. Aanbevelingen vergroten cyberweerbaarheid jongeren ten aanzien van geldezelen

Zet naast algemene voorlichting over het fenomeen in op een afschrikwekkende campagne die de jongeren bereikt die gevoelig zijn om als geldezel op te treden. Dit betreft vooral de groep die positieve associaties heeft met ‘snel en gemakkelijk geld verdienen’. In beide vormen van voorlichting dient de nadruk te liggen op de hoge pakkans (deze is nagenoeg 100%) en de zware gevolgen die er aan het optreden als geldezel zijn verbonden: (I) je bankrekening wordt geblokkeerd en kan geen nieuwe rekening meer bij je bank openen; (II) je kan ook bij andere banken geen nieuwe rekening meer openen omdat je als fraudeur bent geregistreerd; (III) je kan voor een lange tijd geen leningen of hypotheek meer afsluiten; (IV) je komt als geldezel in beeld bij de politie; (V) je kan door justitie worden vervolgd voor witwassen en (VI) slachtoffers van oplichting kunnen hun schade op jou verhalen als je dit geld al niet meer hebt.

5. RESULTATEN DOELGROEP OUDEREN

5.1. Vriend-in-noodfraude

In deze paragraaf volgt een samenvatting van de belangrijkste uitkomsten met betrekking tot vriend-in-noodfraude, besproken aan de hand van de onderzoeksvragen.

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van ouderen ten aanzien van vriend-in-noodfraude?".

Ouderen zijn zich redelijk bewust van de risico's van vriend-in-noodfraude, van hoe je slachtoffer kunt worden en hoe daders te werk gaan (gemiddeld 3.67) . Tijdens de interviews is naar voren gekomen dat ouderen hun kennis hebben verkregen via televisieprogramma's, zoals Radar, Opgelicht?! en Opsporing Verzocht, de krant, het internet, zoals via SeniorenWeb of een digitale gids van de Consumentenbond, of zij hebben deze informatie ontvangen vanuit hun sociale omgeving. Eén op de vijf ondervraagde ouderen heeft behoefte aan meer informatie over vriend-in-noodfraude, met name over hoe je jezelf ertegen kunt beschermen, wat de ontwikkelingen zijn (nieuwe vormen van fraude) en welke vormen bestaan.

De eigen kans om slachtoffer te worden van vriend-in-noodfraude wordt laag ingeschat (gemiddeld 1.50). De affectieve respons van ouderen is dan ook laag; zij maken zich weinig zorgen om slachtoffer te worden en de schade die slachtofferschap van vriend-in-noodfraude zou veroorzaken (gemiddeld 1.74). De mogelijke schade en emotionele impact wordt echter als hoog gezien (gemiddeld 3.79). Er is sprake van een grote optimistic bias: Gemiddeld schatten de ouderen de kans dat een leeftijdsgenoot van hetzelfde geslacht komend jaar slachtoffer wordt van vriend-in-nood-fraude als veel hoger in (3.57) dan dat ze zelf slachtoffer worden (1.50).

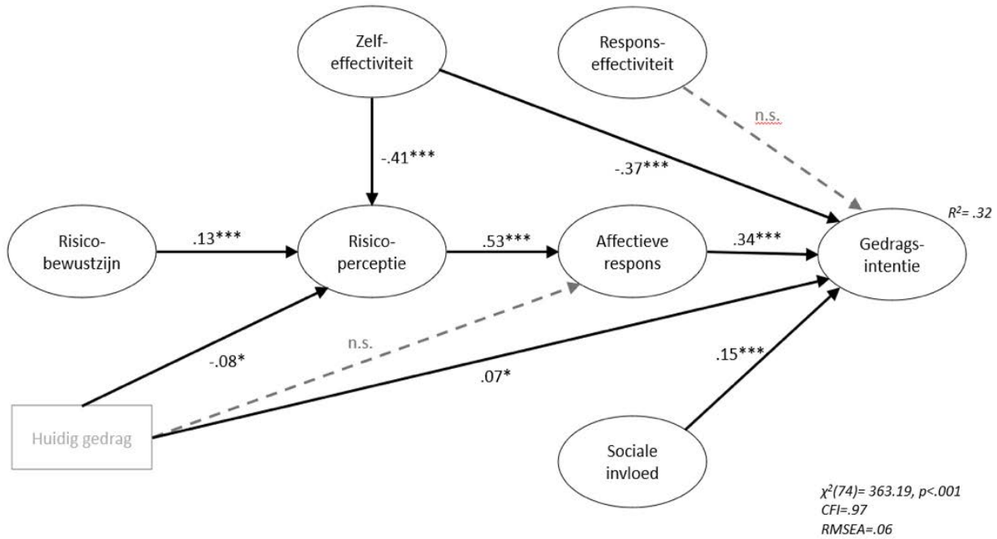
Onderzoeksvraag 2: "In welke mate vertonen ouderen zelfbeschermend gedrag ten aanzien van vriend-in-noodfraude?".

Ouderen rapporteren dat ze vaak zelfbeschermend gedrag ten aanzien van vriend-in-noodfraude vertonen (gemiddeld 3.90), met name eerst telefonisch of in de fysieke wereld spreken met de persoon die zegt geld nodig te hebben voordat zij geld overmaken (gemiddeld 4.84), gevolgd door het controleren van de profielfoto wanneer zij onverwacht een betaalverzoek krijgen van een bekende die aangeeft een nieuw telefoonnummer te hebben (gemiddeld 4.31) en het bellen van het oude nummer (gemiddeld 4.12). Het minst vaak geven ouderen aan afspraken te hebben gemaakt met vrienden/familie over betaalverzoeken (gemiddeld 1.18).

Ouderen ervaren belemmeringen bij het nemen van (meer) beschermende maatregelen tegen cybercrime in het algemeen, vooral omdat het te ingewikkeld is (47%). Daarnaast hebben ze de veronderstelling dat aanvullende maatregelen niet beter zouden beschermen (39%).

Onderzoeksvraag 3: "Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van ouderen ten aanzien van vriend-in-noodfraude?".

Ouderen staan negatief tot neutraal tegenover het nemen van meer zelfbeschermende maatregelen tegen vriend-in-noodfraude in de toekomst (gemiddeld 2.60). Hiermee is hun gedragsintentie relatief laag te noemen. Tegelijkertijd lijken zij niet volledig overtuigd te zijn dat de maatregelen die zij nu nemen, hen beschermen tegen vriend-in-noodfraude (gemiddeld 3.59). Ouderen achten zichzelf echter wel goed in staat risico's in te schatten en zichzelf te beschermen tegen vriend-in-noodfraude (zelfeffectiviteit; gemiddeld 3.96). Ze vinden het wel erg nuttig en effectief om zelfbeschermende maatregelen te treffen (gemiddeld 4.25).



Figuur 5. Paddiagram gedragsintentie (vriend-in-noodfraude)

In Figuur 5 is te zien dat de intentie tot zelfbeschermend gedrag significant beïnvloed wordt door drie directe voorspellers uit het Cyberweerbaarheidsmodel. Hierbij is de mate van zelfeffectiviteit de belangrijkste voorpeller (β= -0.37, p<.001); ouderen die zichzelf momenteel minder goed in staat achten zichzelf te beschermen tegen vriend-in-noodfraude, zijn meer geneigd dat in de toekomst wel te gaan doen. Daarnaast worden gedragsintenties sterk beïnvloed door de affectieve respons; de mate waarin ouderen zich zorgen maken over hun eigen risico ten aanzien van vriend-in-noodfraude, heeft een positieve invloed op gedragsintenties (β=0.34, p<.001). Dit impliceert dat hoe meer zorgen ze zich maken, hoe meer ze geneigd zijn aanvullende maatregelen te treffen. Tot slot is de invloed vanuit de sociale omgeving ook een significante voorspeller (β=0.15, p<.001). Hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te gaan treffen. De responseffectiviteit is echter niet significant van invloed hierop.

De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie (inschatting van persoonlijke kans op slachtofferschap en het effect daarvan; β=0.53, p<.001). Deze inschatting van persoonlijk risico wordt ver-

volgens negatief beïnvloed door de mate van zelfeffectiviteit (β=-0.41, p<.001) en in mindere mate door de mate van huidig zelfbeschermend gedrag (β= -0.08, p<.05). Daarnaast is ook het risicobewustzijn van invloed op de risicoperceptie (β=0.13, p<.001).
Met andere woorden, hoe lager de inschatting van de eigen capaciteiten om zichzelf te beschermen in combinatie met een lagere mate van huidig zelfbeschermend gedrag, maar een hoger risicobewustzijn, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen men zich maakt. Zelfeffectiviteit, risicobewustzijn en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan uitvoeren. Daarnaast is de huidige mate van zelfbeschermend gedrag (in mindere mate) van invloed op de intenties om aanvullend zelfbeschermende maatregelen te gaan treffen tegen vriend-in-noodfraude (β= 0.07, p<.05), wat betekent dat wanneer men momenteel meer zelfbeschermende maatregelen treft tegen vriend-in-noodfraude, men ook geneigd is in de toekomst meer aanvullende maatregelen te gaan treffen.

5.2. Phishing

In deze paragraaf volgen de resultaten met betrekking tot phishing, besproken aan de hand van de onderzoeksvragen.

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van ouderen ten aanzien van phishing?".
Ouderen zijn zich redelijk bewust van de risico's met betrekking tot phishing met een gemiddelde score van 3.66. Deze kennis hebben respondenten verworven via televisieprogramma's, nieuwsberichten, e-mails van hun bank, SeniorenWeb en/of zij hebben deze informatie ontvangen vanuit hun sociale omgeving. Bijna de helft (46%) van alle ondervraagden heeft behoefte aan meer informatie over phishing, met name over hoe ze zichzelf kunnen beschermen (76%), hoe ze (een poging tot) phishing kunnen herkennen (66%), ontwikkelingen op het gebied van phishing (bijvoorbeeld nieuwe vormen; 61%) en wat ze moeten doen bij slachtofferschap (56%).
De inschatting van de eigen kans om slachtoffer te worden is laag: deze wordt gemiddeld als 2.08 ingeschat. Het effect (schade en impact) wordt veel hoger ingeschat; gemiddeld 4.12 op een vijfpuntsschaal. Dit impliceert dat respondenten van mening zijn dat ze weinig vatbaar zijn voor slachtofferschap, maar dat onverhoopt slachtofferschap wel grote schade en impact voor henzelf zal hebben. Ondervraagde ouderen schatten hun risico om zelf slachtoffer te worden van phishing erg laag in en ook dat ze zelf minder kans lopen om slachtoffer te worden van phishing dan hun leeftijdsgenoten.

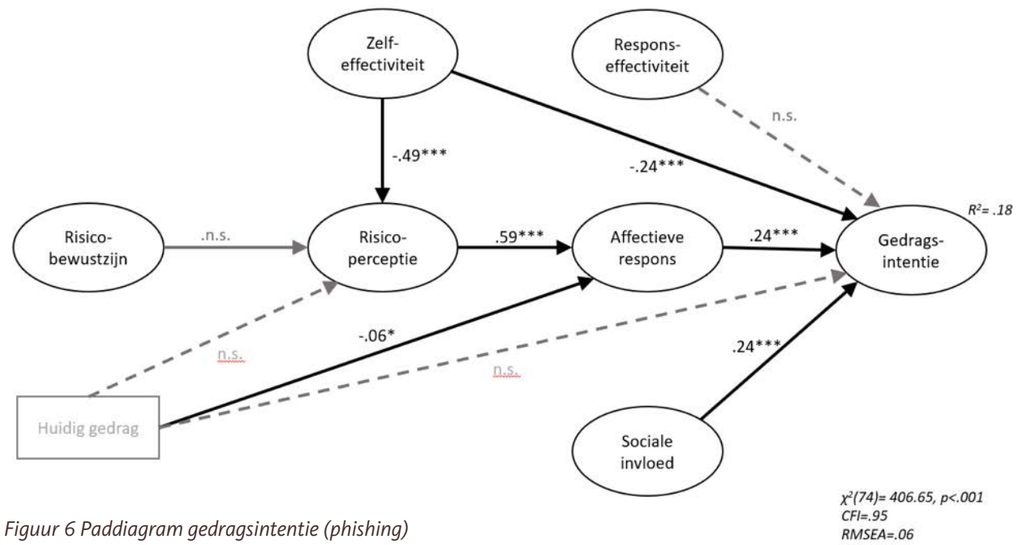
Onderzoeksvraag 2: "In welke mate vertonen ouderen zelfbeschermend gedrag ten aanzien van phishing?".
De ondervraagde ouderen rapporteren dat ze vaak zelfbeschermend gedrag ten aanzien van phishing vertonen (gemiddeld 4.22 op een vijfpuntsschaal), waarbij de maatregel die het vaakst wordt uitgevoerd door de respondenten het vermijden van onveilige websites is (4.79), gevolgd door alleen op links te klikken en bijlagen te openen van e-mails die ze vertrouwen (4.75), en het goed kijken naar de afzender van een e-mail (4.69). Het minst vaak geven ze aan de betrouwbaarheid van links te checken via daarvoor bestemde websites, en het nooit inloggegevens te verstrekken via internet of telefoon. Het blijkt dat onder de mensen die minder zelfbeschermend gedrag ten aanzien van phishing vertonen relatief veel laagopgeleiden en ook vrouwen zitten. In de interviews geven ouderen aan dat ze daarnaast hun apparaten goed beveiligd hebben, met een virusscanner of een tweetrapsverificatie waarbij de respondent via zijn telefoon toestemming moet geven om een bedrag over te maken. Op deze manier proberen respondenten te voorkomen dat ze slachtoffer worden van phishing.
Ouderen ervaren belemmeringen bij het nemen van (meer) beschermende maatregelen tegen cybercrime in het algemeen, onder meer dat het te ingewikkeld is. De interviews schetsen een beeld dat ouderen naast de maatregelen die ze zelf nemen om zich te beschermen tegen phishing niet zo goed weten hoe ze zich nog meer zouden kunnen beschermen hiertegen.

Onderzoeksvraag 3: "Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van ouderen ten aanzien van phishing?".
Wat betreft phishing geven ouderen aan een neutraal tot redelijke zelfeffectiviteit te hebben; gemiddeld scoren zij 3.64 op een vijfpuntsschaal. Ouderen die zichzelf momenteel minder goed in staat achten zich te beschermen tegen phishing, zijn meer geneigd dat in de toekomst wel te gaan doen.
Ouderen zijn wat neutraler betreffende hun gedragseffectiviteit; gemiddeld 3.44. Dit geeft aan dat zij niet volledig overtuigd lijken te zijn dat de maatregelen die zij nemen, hen beschermen tegen phishing. Hun responseffectiviteit is echter hoog met gemiddeld 4.21; ouderen ervaren het treffen van zelfbeschermende maatregelen als nuttig en effectief om slachtofferschap van phishing te voorkomen.
Ouderen zijn gemiddeld neutraal wat betreft de sociale norm (de invloed vanuit de sociale omgeving op beschermend gedrag ten aanzien van cybercriminaliteit in het algemeen). De invloed vanuit de sociale omgeving is wel een belangrijke voorspeller van de intentie tot zelfbeschermend gedrag: hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te gaan treffen.
De affectieve respons is met gemiddeld 2.67 relatief laag, maar hoger dan bij vriend-in-noodfraude. Men maakt zich vooral zorgen over financiële schade of toegang tot persoonsgegevens bij slachtofferschap van phishing. Hoe meer zorgen ze zich maken, hoe meer ze geneigd zijn aanvullende maatregelen te treffen. Ook hier wordt de affectieve respons sterk beïnvloed door de persoonlijke risicoperceptie. Deze inschatting van persoonlijk risico wordt vervolgens negatief beïnvloed door de mate van zelfeffectiviteit. De mate van risicobewustzijn heeft echter geen invloed op de risicoperceptie van ouderen ten aanzien van phishing.
Ouderen staan gemiddeld neutraal tegenover het nemen van meer zelfbeschermende maatregelen tegen phishing in de toekomst met 3.12. Dit betekent dat zij tot op zekere hoogte voornemens zijn aanvullende zelfbeschermende maatregelen te gaan treffen tegen phishing.
In Figuur 6 is te zien dat de intentie tot zelfbeschermend gedrag significant beïnvloed

wordt door drie directe voorspellers uit het Cyberweerbaarheidsmodel. De mate waarin ouderen zich zorgen maken over hun eigen risico ten aanzien van phishing, heeft een positieve invloed op gedragsintenties (β=0.24, p<0.001), implicerend dat hoe meer zorgen ze zich maken hoe meer ze geneigd zijn aanvullende maatregelen te treffen. Daarnaast speelt de mate van zelfeffectiviteit een significante rol (β= -0.24, p<0.001); ouderen die zichzelf momenteel minder goed in staat achten zich te beschermen tegen phishing, zijn meer geneigd dat in de toekomst wel te doen. Tot slot is de invloed vanuit de sociale omgeving ook een significante voorspeller (β=0.24, p<0.001). Hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te treffen.

Alle drie voorspellers vertonen een even sterke invloed op gedragsintenties. Met andere woorden, hoe meer zorgen men zich maakt over de eigen risico's in combinatie met een lager beeld van zichzelf om zich te kunnen beschermen en de opvatting dat mensen in

De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie (inschatting van persoonlijke kans op slachtofferschap en het effect daarvan; β=0.59, p<0.001). Deze inschatting van persoonlijk risico wordt vervolgens negatief beïnvloed door de mate van zelfeffectiviteit (β=-0.49, p<0.001). De mate van risicobewustzijn heeft echter geen invloed op de risicoperceptie van ouderen ten aanzien van phishing. Met andere woorden, hoe lager de inschatting van de eigen capaciteiten om zichzelf te beschermen, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen men zich maakt. Zelfeffectiviteit en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan uitvoeren. Daarnaast is de huidige mate van zelfbeschermend gedrag (in mindere mate) negatief van invloed op de affectieve respons (β= -0.06, p<0.05), wat betekent dat wanneer men momenteel minder zelfbeschermende maatregelen treft tegen phishing, men zich meer zorgen maakt over de persoonlijke risico's hiervan.



Figuur 6 Paddiagram gedragsintentie (phishing)

5.3. Geleerde lessen en aanbevelingen

5.3.1. Conclusies

Uit de resultaten is gebleken dat ouderen voor zowel phishing als vriend-in-noodfraude een relatief lage persoonlijke risicoperceptie hebben, terwijl ze beide delicten wel degelijk als een groot actueel risico zien voor ouderen in het algemeen. Dat betekent, dat zij een sterke optimistic bias ervaren. Deze optimistic bias kan leiden tot een verhoogde kans op slachtofferschap, juist door matig zelfbeschermend gedrag of minder oplettendheid vanwege het gebrek aan het ervaren van persoonlijk risico. Naast een lage risicoperceptie is er wel veel angst voor de schade en mogelijke impact bij slachtofferschap van vriend-in-noodfraude. Het appelleren in interventies aan deze schade/impact kan ouderen verleiden tot meer zelfbeschermend gedrag. De affectieve respons heeft sterke invloed op de intentie van ouderen om zichzelf te beschermen. Dat geldt ook voor zelfeffectiviteit, dus moet een "fear appeal" bij voorkeur samengaan met verhoging van de zelfeffectiviteit door heldere beschermingsmaatregelen te bieden.
In het algemeen geldt dat ouderen belemmeringen ervaren bij het nemen van (meer) beschermende maatregelen tegen cybercrime omdat ze het te ingewikkeld vinden, en vanwege de veronderstelling dat aanvullende maatregelen niet beter zouden beschermen. Een belangrijk deel van de ouderen heeft behoefte aan meer informatie over cybercrime, met name over 1) hoe ze zichzelf kunnen beschermen, 2) hoe ze (een poging tot) phishing kunnen herkennen, 3) wat ze moeten doen bij slachtofferschap, en 4) welke vormen bestaan. De informatiebehoefte bij phishing is echter hoger dan bij vriend-in-noodfraude.

5.3.2. Aanbevelingen vergroten cyberweerbaarheid ouderen ten aanzien van vriend-in-noodfraude

Op basis van de onderzoeksresultaten worden de volgende aanbevelingen gedaan om de cyberweerbaarheid van ouderen tegen vriend-in-noodfraude te vergroten:

- Leg in de voorlichting de nadruk op (mogelijke) varianten van deze fraudevorm ("WhatsApp-fraude 2.0", zie bijvoorbeeld Pietersz (2021)), of social engineeringtechnieken van criminelen in het algemeen.
- Doorbreek de optimistic bias door een campagne waarbij ouderen in de val worden gelokt doordat een surrogaat slachtoffererva-ring geleverd wordt (slachtofferschap leidt tot aanpassing gedrag).
- Besteed bij de handelingsperspectieven aandacht aan concrete en makkelijk uitvoerbare handelingen. Maak duidelijk dat aanvullende maatregelen weldegelijk effect hebben op wat ze al doen wat betreft zelfbeschermend gedrag. Weten wat je moet doen wanneer je slachtoffer wordt van vriend-in-noodfraude is nog niet altijd bekend onder ouderen.
- Ouderen rapporteren al veel te doen aan zelfbeschermend gedrag ten aanzien van vriend-in-noodfraude, maar maken relatief weinig afspraken met vrienden/familie over betaalverzoeken. In een campagne zouden ze gestimuleerd kunnen worden die afspraken wel te maken, of bijvoorbeeld in het algemeen onderling codes af te spreken om zeker te weten dat er sprake is van een familielid die contact zoekt. Vergelijk de afspraken die

5.3.3. Aanbevelingen vergroten cyberweerbaarheid ouderen ten aanzien van phishing

Ten aanzien van phishing leveren de resultaten van dit onderzoek een aantal aanknopingspunten voor de ontwikkeling van interventies ter verhoging van de cyberweerbaarheid van ouderen.

- Doorbreek de optimistic bias door een campagne waarbij ouderen in de val worden gelokt doordat een surrogaat slachtoffervaring geleverd wordt (slachtofferschap leidt tot aanpassing gedrag).
- Ouderen geven aan al veel maatregelen tegen phishing te nemen. Geef aan waarom aanvullende maatregelen nodig zijn om jezelf goed te beschermen en welke concrete handelingsperspectieven men kan nemen om dit te bereiken.
- De voorgestelde maatregelen dienen gebruikersvriendelijk te zijn, en er dient helder te worden gecommuniceerd waarom deze maatregelen leiden tot een betere bescherming. Dat laatste is ook nodig om de gedragseffectiviteit te beïnvloeden, zodat ouderen overtuigd raken dat maatregelen nut hebben.
- Daarnaast kan ook de sociale invloed aangewend worden: laat zien dat anderen (familieleden, vrienden, peers) het belangrijk vinden dat ouderen zich beschermen.

6. RESULTATEN DOELGROEP MKB'ERS

In dit hoofdstuk worden de resultaten van de vragenlijst en de interviews met mkb'ers over ransomware en phishing beschreven.

6.1. Ransomware

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van mkb'ers ten aanzien van de ransomware?".

Mkb'ers zijn zich redelijk bewust van de risico's van ransomware (gemiddeld 3.34, op een vijfpuntsschaal). Uit de interviews komt naar voren dat de respondenten die bekend zijn met ransomware aan deze kennis komen via hun eigen werk, via experts, door het nieuws te volgen of omdat er in hun omgeving slachtofferschap van ransomware heeft plaatsgevonden. Minder dan de helft (41%) van de respondenten geeft aan behoefte aan aanvullende informatie over de risico's en hoe ze zichzelf hiertegen kunnen beschermen te hebben. De respondenten die aangeven meer informatie te willen, willen met name weten hoe ze zichzelf/hun bedrijf kunnen beschermen tegen ransomware (80%), hoe ze een poging tot ransomware kunnen herkennen (70%) en wat ze moeten doen wanneer ze/hun bedrijf slachtoffer is geworden van ransomware (62%). Mkb'ers achten de kans klein om zelf slachtoffer te worden (gemiddeld 2.15), terwijl de mogelijke schade en emotionele impact veel hoger wordt ingeschat (gemiddeld 3.82). Dit impliceert dat respondenten van mening zijn dat ze weinig vatbaar zijn voor slachtofferschap, maar dat onverhoopt slachtofferschap wel grote schade en impact voor henzelf zal hebben. Dit is in lijn met de bevindingen uit de interviews. Respondenten rapporteren namelijk dat hun bedrijf afhankelijk is van computersystemen en dat ze veel privacygevoelige data van klanten hebben opgeslagen. De voornaamste zorgen van respondenten hierbij zijn imagoschade doordat vertrouwelijke informatie van klanten in verkeerde handen zou kunnen vallen en financiële schade door de tijd die benodigd is om gegevens te herstellen. Mkb'ers schatten de risico's voor andere mkb'ers hoger in dan voor henzelf (respectievelijk gemiddeld 2.73 en 2.15). Dit impliceert een optimistic bias, waarbij mkb'ers de risico's van ransomware voor zichzelf lager inschatten in vergelijking met andere mkb'ers.

Onderzoeksvraag 2: "In welke mate vertonen mkb'ers zelfbeschermend gedrag ten aanzien van ransomware?".

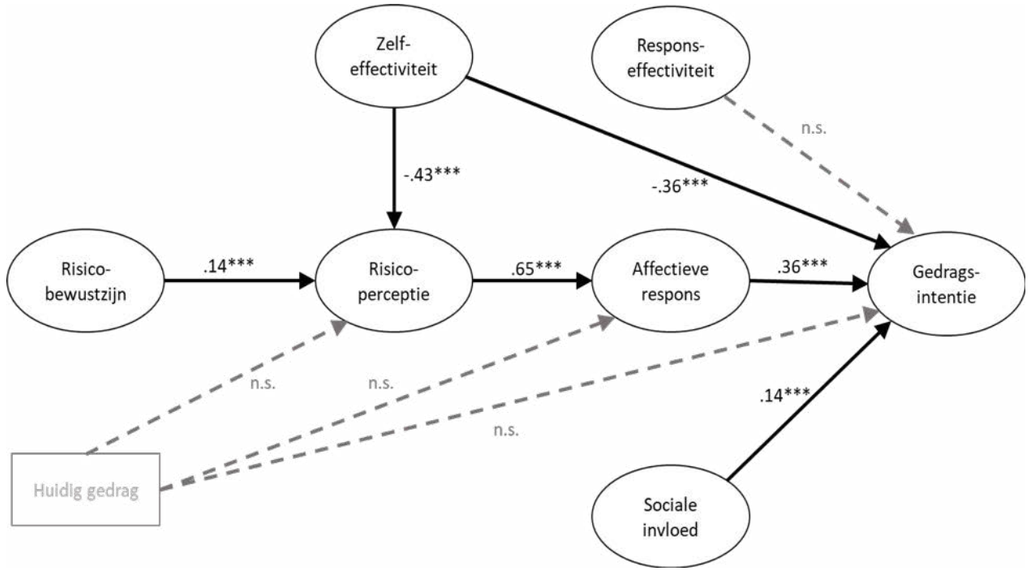
Respondenten is gevraagd in welke mate zij gebruikmaken van acht zelfbeschermende maatregelen op het gebied van cybercriminaliteit op een schaal van 1 (nooit) tot 5 (altijd). Gemiddeld scoren respondenten hier met 4.29 relatief hoog. De maatregel die het vaakst wordt uitgevoerd door de respondenten is alleen klikken op links en bijlagen openen van e-mails die ze vertrouwen (gemiddeld 4.71), gevolgd door goed naar de afzender van een e-mail kijken en alleen downloaden van websites die ze vertrouwen. Respondenten is ook gevraagd naar mogelijke belemmeringen bij het nemen van (meer) beschermende maatregelen tegen cybercriminaliteit in het algemeen. Hier benoemen ze het vaakst dat ze het als te ingewikkeld ervaren (38,9%), dat ze denken dat aanvullende maatregelen niet beter zouden beschermen (37,2%) en dat het

te veel tijd kost (33,7%).

Onderzoeksvraag 3: "Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb'ers ten aanzien van ransomware?".

Respondenten scoren met 3.20 een gemiddelde mate van zelfeffectiviteit. Tijdens de interviews is de meest genoemde reden ze al voldoende beschermd zouden zijn en tot dusver nog geen slachtofferschap hebben ervaren. De respondenten die zichzelf niet in staat achten zich te kunnen beschermen tegen ransomware wijten dit aan een gebrek aan kennis en geven aan hierin externe partijen met expertise nodig te hebben. De responseffectiviteit van de respondenten is relatief hoog met een gemiddelde van 4.11 op een vijfpuntsschaal. Dit impliceert dat respondenten het treffen van zelfbeschermende maatregelen als nuttig en effectief ervaren om slachtofferschap van ransomware te voorkomen. Respondenten ervaren enigszins subjectieve sociale normen om zelfbeschermend gedrag uit te voeren (gemiddeld 3.37). Mkb'ers lijken zich in lage mate zorgen te maken over de kans op slachtofferschap van ransomware (gemiddeld 2.37). En ondanks dat ze de schade en impact van slachtofferschap hoog inschatten, zorgt dit er niet voor dat ze zich daar veel zorgen om maken (gemiddeld 2.52). Tot slot scoren ze gemiddeld op de gedragsintentie om in de toekomst (aanvullend) zelfbeschermend gedrag te gaan uitvoeren (gemiddeld 3.05).

In Figuur 7 is te zien dat de intentie tot zelfbeschermend gedrag significant beïnvloed wordt door drie directe voorspellers: De mate waarin mkb'ers zich zorgen maken over hun eigen risico ten aanzien van ransomware (affectieve respons; β=0.36, p<0.001) en de mate van zelfeffectiviteit (β= -0.36, p<0.001) zijn hierbij de sterkste voospellers, implicerend dat hoe meer zorgen ze zich maken en hoe minder ze zichzelf nu in staat achten zich te beschermen tegen ransomware, hoe meer ze geneigd zijn aanvullende maatregelen te gaan treffen. Tot slot is de invloed vanuit de sociale omgeving ook een significante voorspeller (β=0.14, p<0.001); hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te treffen. Met andere woorden, hoe meer zorgen mkb'ers zich maken over de eigen risico's in combinatie met een lager beeld van zichzelf om zich op dit moment te kunnen beschermen en de opvatting dat mensen in de omgeving van je verwachten dat je zelfbeschermend gedrag uitvoert, hoe sterker de motivatie om dit ook te gaan doen. De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie (inschatting van persoonlijke kans op slachtofferschap en het effect daarvan; β=0.65, p<0.001). Deze inschatting van persoonlijk risico wordt vervolgens negatief beïnvloed door de mate van zelfeffectiviteit (β=-0.43, p<0.001) en positief beïnvloed door het risicobewustzijn (β=.14, p<.001). Met andere woorden, hoe meer mkb'ers zich bewust zijn van de risico's van ransomware en hoe meer kennis ze ervan hebben, in combinatie met een lagere inschatting van de eigen capaciteiten om zichzelf te beschermen, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen ze zich maken. Risicobewustzijn, zelfeffectiviteit en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan uitvoeren.



Figuur 7. Toetsing Cyberweerbaarheidsmodel ransomware

6.2. Phishing

Onderzoeksvraag 1: "Hoe is het gesteld met het risicobewustzijn en de risicoperceptie van mkb'ers ten aanzien van phishing?".

De ondervraagde mkb'ers achten zichzelf redelijk bewust van de risico's gekoppeld aan phishing; gemiddeld scoren ze 3.86. Zij geven gemiddeld aan beter te weten welke risico's hun bedrijf loopt als ze op een onbetrouwbare link klikken, dan hoe daders te werk gaan. Respondenten komen aan kennis over phishing via programma's en waarschuwingscampagnes op de televisie, via sociale media, door eerder slachtofferschap, via bekenden, vanuit hun werk, voorlichtingscampagnes op internet en andere niet-gespecificeerde bronnen.

Een derde van de respondenten (33%) geeft aan behoefte te hebben aan meer informatie. De respondenten die behoefte hebben aan meer informatie willen met name informatie over hoe ze zichzelf/hun bedrijf kunnen beschermen tegen phishing (80%), wat ze moeten doen bij slachtofferschap van phishing (66%) en wat de ontwikkelingen zijn op het gebied van phishing (62%).

De inschatting van de eigen kans om slachtoffer van phishing te worden is laag; deze wordt gemiddeld als 2.15 ingeschat. Het effect (schade en impact) wordt hoger ingeschat; gemiddeld 3.67 op een vijfpuntsschaal. Dit impliceert dat respondenten van mening zijn dat ze relatief weinig vatbaar zijn voor slachtofferschap, maar dat onverhoopt slachtofferschap wel grote schade en impact voor henzelf zal hebben. Uit de interviews blijkt dat vooral reputatieschade een zorg is: bedrijven beschikken over klantgegevens met gevoelige data, die niet in verkeerde handen mogen vallen.

Daarnaast valt ook hier een optimistic bias op: men schat de kans dat andere, vergelijkbare, ondernemers slachtoffer worden van phishing hoger in (gemiddeld 2.74) dan de eigen kans op slachtofferschap.

“ Men schat de kans dat andere, vergelijkbare, ondernemers slachtoffer worden van phishing hoger in dan de eigen kans op slachtofferschap. ”

Onderzoeksvraag 2: “In welke mate vertonen mkb’ers zelfbeschermend gedrag ten aanzien van phishing?”.

Respondenten is gevraagd van vijf zelfbeschermende maatregelen tegen phishing in hoeverre zij deze uitvoeren. Hierop scoren zij gemiddeld hoog met 4.29 op een vijfpuntsschaal. De maatregel die het vaakst wordt uitgevoerd door de respondenten is alleen klikken op links en bijlagen openen van e-mails die ze vertrouwen (gemiddeld 4.71), gevolgd door goed naar de afzender van een e-mail te kijken (gemiddeld 4.66) en het vermijden of verlaten van websites die ze niet vertrouwen (gemiddeld 4.66).

Respondenten lijken op basis van de interviews echter beperkte kennis te hebben over hun exacte huidige zelfbeschermende gedrag tegen phishing. Zo weet bijna geen respondent welke maatregelen zij zelf nog meer zouden kunnen treffen, anders dan een ICT-expert inschakelen.

Onderzoeksvraag 3: “Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb’ers ten aanzien van phishing?”.

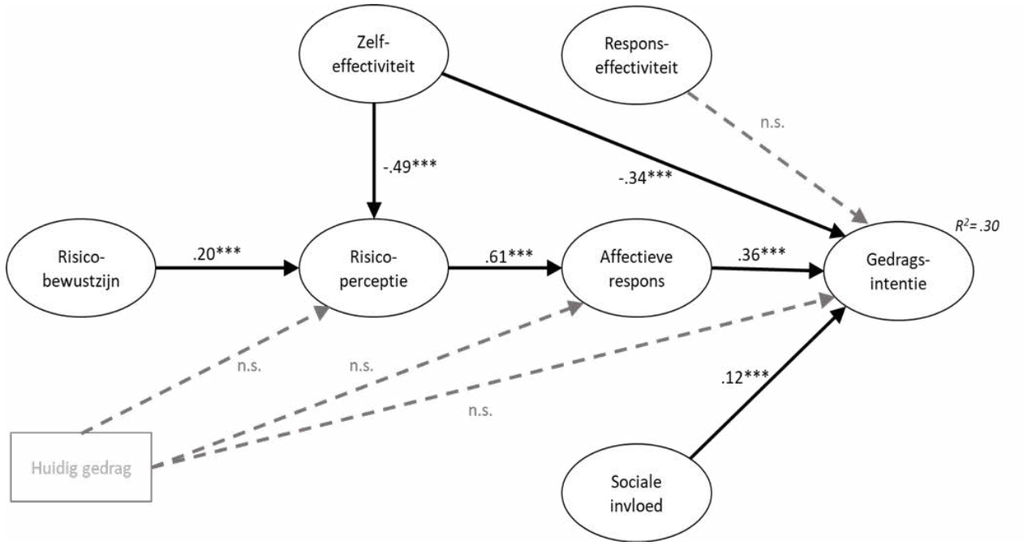
De ondervraagde respondenten achten zichzelf met een gemiddelde score van 3.57 op een vijfpuntsschaal redelijk in staat zichzelf te beschermen tegen phishing. De responseffectiviteit van de respondenten is relatief hoog met een gemiddelde van 4.11 op een vijfpuntsschaal. Dit impliceert, dat respondenten het treffen van zelfbeschermende maatregelen in het algemeen als nuttig en effectief ervaren om slachtofferschap van phishing te voorkomen.

Mkb’ers lijken zich in lage mate zorgen te maken over de kans op slachtofferschap van phishing en de schade die slachtofferschap van phishing zou veroorzaken. Hun affectieve respons is daarmee relatief laag met gemiddeld 2.30. De gedragsintentie van de mkb’ers is niet hoog en niet laag met gemiddeld 3.05. In Figuur 8 is te zien dat de intentie tot zelfbeschermend gedrag significant beïnvloed wordt door drie directe voorspellers uit het Cyberweerbaarheidsmodel: De mate waarin mkb’ers zich zorgen maken over hun eigen risico ten aanzien van phishing is hierbij de sterkste voospeller (β=0.36, p<.001), implicerend dat hoe meer zorgen ze zich maken hoe meer ze geneigd zijn aanvullende maatregelen te gaan treffen. Daarnaast speelt de mate van zelfeffectiviteit een significante rol (β=-0.34, p<.001); mkb’ers die zichzelf momenteel minder goed in staat achten zich te beschermen tegen phishing, zijn meer geneigd dat in de toekomst wel te gaan doen. Tot slot is de invloed vanuit de sociale omgeving ook een significante voorspeller (β=0.12, p<.001); hoe sterker het idee dat anderen vinden dat ze zichzelf zouden moeten beschermen en hoe meer ze geneigd zijn aan deze subjectieve norm te voldoen, hoe groter de intentie om aanvullende maatregelen te gaan treffen. Met andere woorden, hoe meer zorgen mkb’ers zich maken over de eigen risico’s in combinatie met een lager beeld van zichzelf om zich op dit moment te kunnen beschermen en de opvatting dat mensen in de omgeving van je verwachten dat je zelfbeschermend gedrag uitvoert, hoe sterker de motivatie om dit ook te gaan doen.

De affectieve respons wordt sterk beïnvloed door de persoonlijke risicoperceptie (inschatting van persoonlijke kans op slachtofferschap en het effect daarvan; β=0.61, p<0.001). Deze inschatting van persoonlijk risico wordt

vervolgens negatief beïnvloed door de mate van zelfeffectiviteit (β=-0.49, p<0.001) en positief beïnvloed door het risicobewustzijn (β=0.20, p<0.001). Met andere woorden, hoe meer mbkb'ers zich bewust zijn van de risico's van phishing in combinatie met een lagere inschatting van de eigen capaciteiten om zichzelf te beschermen, hoe hoger de inschatting op persoonlijk slachtofferschap en hoe meer zorgen ze zich maken. Risicobewustzijn, zelfeffectiviteit en risicoperceptie hebben hiermee een belangrijke indirecte invloed op het voornemen om zelfbeschermend gedrag te gaan uitvoeren.

dan bij ransomware, maar de verschillen zijn klein. Het deel van de respondenten dat behoefte heeft aan meer informatie (ongeveer de helft bij ransomware en een derde bij phishing), wil vooral meer weten over hoe ze zichzelf/hun bedrijf kunnen beschermen.
Het blijkt dat mkb'ers over het algemeen een laag risico zien in ransomware en phishing voor hun bedrijf. Dit komt met name doordat respondenten de kans klein achten dat ze zelf slachtoffer worden. De schade en emotionele impact wordt veel hoger ingeschat, wat impliceert dat men verwacht dat onverhoopt slachtofferschap wel grote schade en impact



Figuur 8. Toetsing Cyberweerbaarheidsmodel phishing

6.3. Geleerde lessen en aanbevelingen

6.3.1. Conclusies

Uit de vragenlijst blijkt dat mkb'ers aangeven redelijk te weten wat de risico's van ransomware en phishing zijn voor hun bedrijf. Het risicobewustzijn omtrent phishing ligt hoger

voor henzelf zou hebben. Mkb'ers lijken zich hierbij vooral zorgen te maken over reputatieschade, bijvoorbeeld doordat vertrouwelijke informatie van klanten in verkeerde handen zou kunnen vallen en hun onderneming daardoor in een slecht daglicht komt te staan. Ook lijkt er sprake van optimistic bias: respondenten schatten de kans dat vergelijkbare mkb'ers slachtoffer worden van ransomware of phishing hoger in dan hun eigen kans. Toch wordt ook de kans dat vergelijkbare mkb'ers slachtoffer worden laag ingeschat, wat impliceert dat mkb'ers in het algemeen een laag risico zien in beide delicten.
Mkb'ers geven aan soms tot vaak zelfbeschermende maatregelen te nemen tegen ransomware en phishing, zoals het voor zichzelf houden van inloggegevens en goed kijken naar de afzender van een e-mail. In mindere mate hebben mkb'ers voorschriften over hoe te handelen bij slachtofferschap en controleren ze verdachte linkjes op betrouwbaarheid. Mogelijk is dit te wijten aan belemmeringen die mkb'ers ervaren bij het treffen van (meer) zelfbeschermende maatregelen. Hierbij lijkt vooral gebruiksvriendelijkheid een rol te spelen: mkb'ers geven aan dat het niet nemen van bepaalde maatregelen om hun bedrijf tegen cybercriminaliteit te beschermen, te wijten is aan dat het te veel tijd kost of te ingewikkeld is.

6.3.2. Aanbevelingen vergroten cyberweerbaarheid mkb'ers ten aanzien van phishing en ransomware

De bevindingen van dit onderzoek bieden een aantal aanknopingspunten voor interventies die gemeentes kunnen toepassen om de cyberweerbaarheid van mkb'ers in hun gemeente te verhogen voor ransomware en phishing. Deze interventies zijn op beide delicten toepasbaar, aangezien mkb'ers in vergelijkbare mate van plan zijn zelfbeschermende maatregelen te nemen tegen beide delicten en onderliggende verklaringen voor dat gedrag vergelijkbaar zijn.

- Vergroot de kennis van mkb'ers over mogelijke maatregelen die zij kunnen toepassen om slachtofferschap te voorkomen.
- Aangezien een groot deel van de respondenten geen behoefte heeft aan informatie, is enkel het verstrekken van informatie niet voldoende. Het is van belang eerst te zorgen dat mkb'ers open staan voor nieuwe informatie en zich bewust zijn dat dit belangrijk is, bijvoorbeeld door de persoonlijke risicoperceptie van mkb'ers te verhogen.
- Interventies zouden zich vanwege de lage risicoperceptie moeten richten op het verhogen van de persoonlijke risicoperceptie. Betrek hierbij specifiek de potentiële negatieve gevolgen van slachtofferschap: mkb'ers lijken gemotiveerd om zichzelf te beschermen vanwege de mogelijke impact en schade die ransomware en phishing kunnen hebben voor hun bedrijf (affectieve respons).
- Interventies kunnen daarnaast worden gericht op het verkleinen van de optimistic bias (de mate waarin mkb'ers inschatten dat soortgelijke bedrijven meer risico lopen dan zijzelf).
- De motivatie van mkb'ers om hun bedrijf te beschermen kan worden verhoogd door in te spelen op de subjectieve normen omtrent cyberweerbaarheid. Als mkb'ers namelijk het gevoel hebben dat bedrijven uit hun omgeving ook veilig gedrag vertonen en dit dus de 'heersende norm' is, zijn zij mogelijk eerder geneigd zelf ook zelfbeschermend gedrag te vertonen.
- Bij het ontwikkelen van interventies die het inzetten van zelfbeschermende maatregelen onder mkb'ers willen promoten zou in het bijzonder aandacht moeten worden besteed aan de gebruiksvriendelijkheid van deze maatregelen. Hiermee wordt de belangrijkste belemmering die mkb'ers ervaren overkomen: beperk waar mogelijk de mate van complexiteit en de tijd die het kost om het gewenste gedrag te vertonen.

LITERATUUR

Bekkers, L., Van 't Hoff-de Goede, S., Misana-ter Huurne, E., Houten, Y. van, Spithoven, R., & Leukfeldt, R. (2021). Cyberweerbaarheid. Een gemeentelijk offensief ter preven tie van slachtofferschap van cybercrime. Doelgroep mkb. Deelrapport werk pakket 3. Den Haag/Deventer: De Haagse Hogeschool, Lectoraat Cybersecurity in het mkb en Hogeschool Saxion, Lectoraat Maatschappelijke Veiligheid.

Houten, Y. van, Misana-ter Huurne, E., Hansen, S., Van 't Hoff-de Goede, S., Bekkers, L., Fop pen, E., Spithoven, R., Hansen, S., & Leukfeldt, R. (2021). Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cyber crime. Doelgroep ouderen. Deelrapport werkpakket 3. Den Haag/ Deventer: De Haagse Hogeschool, Lec toraat Cybersecurity in het mkb en Hogeschool Saxion, Lectoraat Maatschappelijke Veiligheid.

Misana-ter Huurne, E., Bekkers, L., Van 't Hoff-de Goede, S., Foppen, E., Ebrahem, S., Houten, Y. van, Spithoven, R., Hansen, S., & Leukfeldt, R. (2021a). Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Doelgroep jongeren. Deelrapport werkpakket 3. Den Haag/Deventer: De Haagse Hogeschool, Lec toraat Cybersecurity in het mkb en Hogeschool Saxion, Lectoraat Maatschappe lijke Veiligheid.

Misana-ter Huurne, E., Bekkers, L., Van 't Hoff-de Goede, S., Foppen, E., Ebrahem, S., Van Hou ten, Y., Hansen, S., Spithoven, R., & Leukfeldt, R. (2021b). Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime Deelrapport 2: Risicobewustzijn en preventief gedrag wat betreft ransomware en phishing. Doel groep mkb Den Haag/Deventer: De Haagse Hogeschool, Lectoraat Cybersecurity in het mkb en Hogeschool Saxion, Lectoraat Maatschappelijke Veiligheid.

Spithoven, R. (2020). Verbonden risico's. Maatschappelijke veiligheid in de black box society. Den Haag: Boom Criminologie (Lectorale rede, longread).

BIJLAGEN

Bijlage 1: Kenmerken respondenten doelgroep Jongeren

Vragenlijst (N=1179)

Tabel 1. Achtergrondkenmerken respondenten vragenlijst doelgroep jongeren

	Respondenten	
Kenmerk	**N**	**%**
Geslacht		
- Man	341	30,2%
- Vrouw	790	69,8%
Opleiding		
- LBO / VBO / VMBO (kader- of beroepsgerichte leerweg / MBO1	10	0,9%
- MAVO / HAVO / VWO (eerste drie jaar) / ULO / MULO / VMBO (TL of GL) / VSO	31	2,6%
- MBO 2, 3, 4 (basisberoeps-, vak-, middenkader- of specialistenopleiding) of MBO oude structuur (vóór 1998)	133	11,3%
- HAVO of VWO (klas 4 of hoger) / HBS / MMS / HBO propedeuse of WO Propedeuse	280	23,9%
- HBO (behalve HBO-master) / WO-kandidaats- of WO-bachelor	515	43,9%
- WO-doctoraal of WO-master of HBO-master / postdoctoraal onderwijs	203	17,3%
Leeftijd		
- 16 t/m 18	218	27%
- 19 t/m 21	374	31,7%
- 22 t/m 24	487	41.3%
Regio		
- West (UT, NH, ZH)	395	33,5%
- Noord (GR, FR, DR)	222	18,8%
- OOST (OV, GD, FL)	220	18,7%
- ZUID (ZL, NB, LB)	337	28,7%
Dagelijkse bezigheid		
- Scholier / student	925	78,5%
- Werkzaam in loondienst	206	17,5%
- ZZP'er / freelancer	10	0,8%
- Ondernemer met personeel	1	0,1%
- Werkloos / werkzoekend / arbeidsongeschikt / bijstand	26	2,2%
- Gepensioneerd	1	0,1%
- Huisvrouw / huisman	3	0,3%
- Anders	7	0,6%
Ervaring met misbruik van seksuele beelden en phishing		
- Seksuele beelden ontvangen van iemand met beelden van die persoon zelf	453	38,4%
- Seksuele beelden doorgestuurd gekregen met beelden van iemand anders	369	31,3%
- Seksuele beelden van jezelf doorgestuurd	291	24,7%
- Seksuele beelden van iemand anders doorgestuurd	35	3,0%
- Een phishing-bericht ontvangen	918	77,9%

Interviews

De interviews zijn gehouden met 29 jongeren, waarvan vijftien gericht op misbruik van seksueel beeldmateriaal en veertien op phishing. De respondenten zijn geselecteerd op basis van persoonlijke kenmerken; geslacht, leeftijd en opleidingsniveau. De gemiddelde leeftijd van de respondenten varieerde bij de interviews over misbruik van seksueel beeldmateriaal van 19 tot 24 jaar (gemiddeld 21 jaar) en bij phishing van 17 tot 23 jaar (gemiddeld 20 jaar). Ongeveer evenveel mannen als vrouwen hebben deelgenomen. Tabel 2 bevat een overzicht van de respondenten die zijn bevraagd over misbruik van seksueel beeldmateriaal en Tabel 3 bevat een overzicht van de respondenten die zijn bevraagd over phishing.

Tabel 2 Kenmerken respondenten interviews misbruik seksueel beeldmateriaal

Respondentcode	Geslacht	Leeftijd	Opleidingsniveau
IVS1	Man	21	HBO
IVS2	Man	24	HBO
IVS3	Vrouw	23	Universiteit
IVS4	Vrouw	22	HBO
IVS5	Vrouw	24	Universiteit
IVS6	Man	22	MBO
IVS7	Man	23	MBO / werkzaam
IVS8	Vrouw	20	HBO
IVS9	Vrouw	21	MBO
IVS10	Vrouw	22	HBO
IVS11	Man	23	MBO / werkzaam
IVS12	Man	20	MBO
IVS13	Vrouw	19	MBO
IVS14	Man	24	HAVO
IVS15	Vrouw	20	HBO

Tabel 3 Kenmerken respondenten interviews phishing

Respondentcode	Geslacht	Leeftijd	Opleidingsniveau
IVP1	Man	23	Hbo
IVP2	Man	21	Hbo
IVP3	Vrouw	17	Mbo
IVP4	Vrouw	20	Wo
IVP 5	Vrouw	17	Hbo
IVP 6	Man	21	Wo bachelor
IVP7	Man	20	Wo master
IVP8	Man	18	Havo
IVP	Man	18	Havo
IVP10	Man	22	WO Bachelor
IVP11	Man	17	Hbo
IVP12	Vrouw	22	Vmbo
IVP13	Vrouw	20	Hbo
IVP14	Vrouw	17	Havo

Bijlage 2: Kenmerken respondenten doelgroep Ouderen

Senioren

Vragenlijst (N=1191)

In totaal hebben 1191 respondenten de vragenlijst ingevuld. Aangezien voor vriend-in-noodfraude het bezit van een smartphone als selectiecriterium is gebruikt, is de uiteindelijke respons hier kleiner (N=1078). Mannen zijn licht oververtegenwoordigd in de steekproef (54% tegen 46% vrouwen). Qua opleiding is er een evenredige verdeling over laag-, middelbaar en hoogopgeleiden (respectievelijk 31%, 35% en 34%). De leeftijdsgroep van 55-64 jaar (52%) is sterk vertegenwoordigd in de steekproef. De groepen 65-74 jaar (28%) en ouder dan 75 jaar (20%) zijn minder sterk vertegenwoordigd. Bij de steekproef voor vriend-in-noodfraude (met het bezit van een smartphone als selectiecriterium) is de jongste groep nog wat groter (54%) en de oudste groep nog wat kleiner (18%). Het grootste deel van de respondenten is gepensioneerd (48%) of werkzaam in loondienst (31%). Van de gehele groep heeft 77% wel eens een phishingbericht ontvangen. Van de groep smartphonebezitters is 15% het afgelopen jaar benaderd via een chat-app als Whatsapp door een oplichter.
Er waren in totaal 1191 respondenten. De kenmerken van de respondenten zijn weergegeven in Tabel 1. Aangezien voor vriend-in-noodfraude het bezit van een smartphone als selectiecriterium is gebruikt, is de uiteindelijke respons hier kleiner (N=1078). Voor deze groep zijn de kenmerken apart gegeven in de tabel.

Mannen zijn lichtelijk oververtegenwoordigd in de steekproef (54% tegen 46% vrouwen). Qua opleiding is er een evenredige verdeling over laag-, middelbaar en hoogopgeleiden (respectievelijk 31%, 35% en 34%). De grootste leeftijdsgroep is 55-64 jaar (52%) is sterk vertegenwoordigd in de steekproef. De groepen 65-74 jaar (28%) en ouder dan 75 jaar (20%) zijn minder sterk vertegenwoordigd. Bij de steekproef voor vriend-in-noodfraude (met het bezit van een smartphone als selectiecriterium) is de jongste groep nog wat groter (54%) en de oudste groep nog wat kleiner (18%). De respondenten zijn verdeeld over het hele land, met een te verwachten oververtegenwoordiging van de meer dichtbevolkte regio's. Het grootste deel van de respondenten is gepensioneerd (48%) of werkzaam in loondienst (31%). Bij de smartphonebezitters zijn die percentages respectievelijk 46% en 33%. Van de gehele groep heeft 77% wel eens een phishingbericht ontvangen. Van de groep smartphonebezitters is 15% het afgelopen jaar benaderd via een chat-app als Whatsapp door een oplichter.

Tabel 1. Achtergrondkenmerken van onderzoekspopulaties voor phishing en vriend-in-noodfraude (de laatste groep betreft een subselectie van de eerste groep: respondenten in bezit van een smartphone)

	Respondenten phishing (N=1191)		**Respondenten vriend-in-noodfraude (N=1078)**	
Kenmerk	**n**	**%**	**n**	**%**
Geslacht				
- Man	644	54.1%	584	54.2%
- Vrouw	547	45.9%	494	45.8%
Opleiding				
- Geen onderwijs	8	0.7%	5	0.5%
- LBO/VBO/VMBO (kader- of beroepsgerichte leerweg/MBO1	95	8.0%	87	8.1%
- MAVO/HAVO/VWO (eerste drie jaar)/ULO/MULO/VMBO (TL of GL)/VSO	268	22.5%	238	22.1%
Totaal Laagopgeleiden	*371*	*31.2%*	*330*	*30.7%*
- MBO 2, 3, 4 (basisberoeps-, vak-, middenkader- of specialistenopleiding) of MBO oude structuur (vóór 1998)	239	20.1%	220	20.4%
- HAVO of VWO (klas 4 of hoger) / HBS / MMS / HBO propedeuse of WO Propedeuse	174	14.6%	159	14.8%
Totaal Middelbaar opgeleiden	*413*	*34.7%*	*379*	*35.2%*
- HBO (behalve HBO-master)/WO-kandidaats of -bachelor	264	22.2%	245	22.8%
- WO-doctoraal of WO-master of HBO-master / postdoctoraal onderwijs	141	11.9%	122	11.3%
Totaal Hoogopgeleiden	*405*	*34.0%*	*367*	*34.1%*
Leeftijd				
- 55 t/m 64 jaar	615	51.6%	580	53.8%
- 65 t/m 74 jaar	336	28.2%	306	28.4%
- 75+	240	20.2%	192	17.8%
Regio				
- West (UT, NH, ZH)	447	38.6%	406	38.8%
- Noord (GR, FR, DR)	181	15.6%	162	15.5%
- Oost (OV, GD, FL)	234	20.2%	212	20.2%
- Zuid (ZL, NB, LB)	296	25.6%	267	25.5%
Dagelijkse bezigheid				
- Werkzaam in loondienst	366	30.7%	353	32.7%
- ZZP'er / freelancer	34	2.9%	31	2.9%
- Ondernemer met personeel	9	0.8%	7	0.6%
- Werkloos / werkzoekend / arbeidsongeschikt / bijstand	116	9.7%	109	10.1%
	574	48.2%	496	46%
- Gepensioneerd	71	6.0%	64	5.9%
- Huisvrouw / huisman	21	1.8%	18	1.7%
Ervaring met vriend-in-noodfraude en phishing				
- In het afgelopen jaar benaderd via een chat-app als WhatsApp door een oplichter				
- Een phishingbericht ontvangen	912	76.6%	160	14.9%

Interviews (N=30)

De interviews zijn gehouden met dertig ouderen, waarvan vijftien gericht op vriend-in-nood-fraude en vijftien op phishing. De respondenten zijn geselecteerd op basis van leeftijd: mensen van 55 jaar en ouder. Er is waar mogelijk getracht de selectie van respondenten te weerspiegelen aan de verdeling in de gehele maatschappij. Tabel 2 bevat een overzicht van de respondenten die zijn bevraagd over vriend-in-noodfraude en Tabel 3 bevat een overzicht van de respondenten die zijn bevraagd over phishing

Tabel 2. Overzicht van respondenten voor het delict vriend-in-noodfraude

Respondentcode	Leeftijdscategorie	Geslacht	Duur van het interview
VIN1	75+	Man	42 minuten
VIN2	65 t/m 74 jaar	Man	40 minuten
VIN3	75+	Man	29 minuten
VIN4	75+	Vrouw	31 minuten
VIN5	55 t/m 64 jaar	Vrouw	33 minuten
VIN6	55 t/m 64 jaar	Man	26 minuten
VIN7	55 t/m 64 jaar	Man	26 minuten
VIN8	65 t/m 74 jaar	Vrouw	58 minuten
VIN9	75+	Vrouw	53 minuten
VIN10	55 t/m 64 jaar	Man	36 minuten
VIN11	65 t/m 74 jaar	Vrouw	29 minuten
VIN12	65 t/m 74 jaar	Man	25 minuten
VIN13	65 t/m 74 jaar	Vrouw	37 minuten
VIN14	75+	Vrouw	40 minuten
VIN15	55 t/m 64 jaar	Man	24 minuten

Tabel 3. Overzicht van respondenten voor het delict phishing

Respondentcode	Leeftijdscategorie	Geslacht	Duur van het interview
PHI1	75+	Man	37 minuten
PHI2	75+	Man	30 minuten
PHI3	65 t/m 74 jaar	Vrouw	19 minuten
PHI4	75+	Vrouw	31 minuten
PHI5	65 t/m 74 jaar	Vrouw	26 minuten
PHI6	75+	Vrouw	21 minuten
PHI7	65 t/m 74 jaar	Man	27 minuten
PHI8	55 t/m 64 jaar	Man	46 minuten
PHI9	75+	Man	49 minuten
PHI10	55 t/m 64 jaar	Man	28 minuten
PHI11	55 t/m 64 jaar	Vrouw	21 minuten
PHI12	75+	Man	25 minuten
PHI13	75+	Man	27 minuten
PHI14	55 t/m 64 jaar	Man	31 minuten
PHI15	55 t/m 64 jaar	Vrouw	23 minuten

Bijlage 3: Kenmerken respondenten doelgroep mkb'ers

Vragenlijst (N=1020)

In totaal hebben 1020 mkb'ers (respons van 51%) de vragenlijst volledig ingevuld. De achtergrondkenmerken van de 1020 respondenten zijn uiteengezet in Tabel 1. Respondenten zijn ongeveer gelijk verdeeld tussen mannen (56,4%) en vrouwen (43,6%). Ook komen de respondenten voornamelijk uit een van de Westelijke provincies (Utrecht, Noord Holland, Zuid Holland; 47,5%), terwijl 21,7% afkomstig is uit een oostelijke provincie en komt respectievelijk 21,3% en 9,5% uit het noorden of zuiden van Nederland. Dit lijkt een vrij accurate afspiegeling van de verdeling in de gehele Nederlandse bevolking (CBS, 2019). Ruim drie kwart van de respondenten zijn hoogopgeleid (75,7%; opleidingsniveau HBO of hoger), een stuk hoger dan het gemiddelde in de Nederlandse bevolking (CBS, 2019), en 80,4% is werkzaam als zzp'er, in lijn met de verdeling binnen alle mkb-bedrijven in Nederland (CBS, 2020). De overige 19,6% heeft een bedrijf met personeel, grotendeels met 1 tot 10 medewerkers in dienst (78,9%). De meeste respondenten zijn van middelbare leeftijd (68,4%; 39 tot en met 65 jaar), gevolgd door 18 tot en met 38 jaar (17,1%) en ouder dan 65 jaar (14,5%). Meer dan de helft van de respondenten verzorgen zelf de ICT-beveiliging van hun bedrijf (62,2%), ongeveer een derde heeft een extern bedrijf in dienst (33,4%) en een klein deel heeft intern een medewerker aangesteld (5,3%). Een aantal respondenten heeft niemand die de ICT-beveiliging van hun bedrijf verzorgt (7,2%). Ruim twee-derde van de bedrijven heeft wel eens phishing-bericht ontvangen en een kleine 20 procent heeft een poging tot een ransomware-aanval ervaren. In totaal geeft 2,6% van onze steekproef aan ook slachtoffer te zijn geweest van phishing in de afgelopen twaalf maanden, waarbij ook schade is geleden. In het geval van ransomware ligt dit percentage op 1,5%.

Tabel 1. Achtergrondkenmerken van onderzoekspopulatie (N=1020)

	Respondenten	
Kenmerk	**N**	**%**
Geslacht		
- Man	570	56,4%
- Vrouw	441	43,6%
Opleiding		
- LBO / VBO / VMBO (kader- of beroepsgerichte leerweg / MBO1	11	1,1%
- MAVO / HAVO / VWO (eerste drie jaar) / ULO / MULO / VMBO (TL of GL) / VSO	42	4,1%
- MBO 2, 3, 4 (basisberoeps-, vak-, middenkader- of specialistenopleiding) of MBO oude structuur (vóór 1998)	109	10,7%
- HAVO of VWO (klas 4 of hoger) / HBS / MMS / HBO propedeuse of WO Propedeuse	86	8,4%
- HBO (behalve HBO-master) / WO-kandidaats- of WO-bachelor	408	40,1%
- WO-doctoraal of WO-master of HBO-master / postdoctoraal onderwijs	362	35,6%
Leeftijd		
- 18 t/m 39	174	17,1%
- 39 t/m 65	698	68,4%
- 65+	148	14,5%
Dagelijkse bezigheid		
- ZZP'er / freelancer	820	80,4%
- Ondernemer met personeel	200	19,6%
Regio		
- Noord (GR, FR, DR)	97	9,5%
- Oost (OV, GD, FL)	217	21,3%
- West (UT, NH, ZH)	484	47,5%
- Zuid (ZL, NB, LB)	221	21,7%
Aantal medewerkers		

- 1-10	153	78,9%
- 11-50	29	15%
- 50-250	9	4,6%
- Meer dan 250	3	1,5%
ICT-beveiliging		
- Ondernemer zelf	634	62,2%
- Interne medewerker	54	5,3%
- Een extern bedrijf	341	33,4%
- Niemand	73	7,2%
Ervaringen met ransomware en phishing		
- Een phishing-bericht ontvangen	822	80,6%
- Een poging tot een ransomware- aanval ervaren	200	19,6%
- Slachtofferschap van phishing	26	2,6%
- Slachtofferschap van ransomware	15	1,5%

Interviews (N=30)

De interviews zijn gehouden met 30 eigenaren van mkb-bedrijven, waarvan 15 interviews waren gericht op ransomware en 15 interviews op phishing. Bij de selectie van de respondenten is rekening gehouden met de vertegenwoordiging van het klein mkb (minder dan 10 werknemers), middelgroot mkb (minder dan 50 werknemers) en groot mkb (minder dan 250 werknemers). In totaal zijn 15 klein mkb, 9 middelgroot mkb en 6 groot mkb eigenaren geïnterviewd, in lijn met het feit dat het mkb in Nederland voor het grootste deel bestaat uit bedrijven met minder dan 10 personen (CBS, 2020). Er is op voorhand geen rekening gehouden met de sector van het bedrijf, aangezien uit voorgaand onderzoek blijkt dat de sector slechts een beperkte invloed heeft op slachtofferschap van cybercriminaliteit (e.g. Notté e.a., 2019). Tabel 2 bevat een overzicht van de respondenten die zijn bevraagd over ransomware en Tabel 3 bevat een overzicht van de respondenten die zijn bevraagd over phishing.

Tabel 2. Overzicht van respondenten voor het delict ransomware

Respondentcode	Geslacht	Type bedrijf	Aantal medewerkers
RANSOM1	Vrouw	Financiële dienstverlening	9
RANSOM2	Man	Dienstverlening	90
RANSOM3	Man	Bouw en architectuur	4
RANSOM4	Man	Fotografie	Zzp
RANSOM5	Vrouw	Metaalbewerking	62
RANSOM6	Man	ICT-beheer	Zzp
RANSOM7	Vrouw	Jeugdzorg	17
RANSOM8	Man	Agrarische sector	10
RANSOM9	Vrouw	Sport en recreatie	4
RANSOM10	Man	Industriële automatisering	60
RANSOM11	Man	Automatisering	105
RANSOM12	Man	IT-leverancier	7
RANSOM13	Man	Bouw nijverheid	35
RANSOM14	Vrouw	Horeca	8
RANSOM15	Man	Technisch commercieel	Zzp

Tabel 3. Overzicht van respondenten voor het delict phishing

Respondentcode	Geslacht	Type bedrijf	Aantal medewerkers
PHISHING1	Man	Energiesector	13
PHISHING2	Man	Automobielsector	11
PHISHING3	Man	Fysiotherapeut	Zzp
PHISHING4	Vrouw	Detailhandel	1
PHISHING5	Man	Automobielsector	6
PHISHING6	Man	Dienstverband/retail	2
PHISHING7	Vrouw	Horeca	9
PHISHING8	Man	Horeca	20
PHISHING9	Vrouw	Detailhandel	2
PHISHING10	Man	Online retail	10
PHISHING11	Man	Facilitaire sector	130
PHISHING12	Man	Bouw	12
PHISHING13	Man	Detachering	Ca. 100
PHISHING14	Man	Fysiotherapie	7
PHISHING15	Man	Zakelijke dienstverlening	10