SAXION UNIVERSITY OF APPLIED SCIENCES

DE HAAGSE HOGESCHOOL

VAR VeiligheidsAlliantie regio Rotterdam

Ministerie van Veiligheid en Justitie

Cyberweerbaarheid

Risicobewustzijn en zelfbeschermend gedrag rondom cybercrime onder jongeren en mkb'ers

Lectoraat Maatschappelijke Veiligheid,
Hogeschool Saxion &
Lectoraat Cybersecurity in het mkb,
De Haagse Hogeschool.

In opdracht van Veiligheidsalliantie Regio Rotterdam.

Onder financiering van het Ministerie van Justitie en Veiligheid.

Cyberweerbaarheid

Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers

Februari 2020

Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion

Lectoraat Cybersecurity in het mkb, De Haagse Hogeschool.

In opdracht van Veiligheidsalliantie Regio Rotterdam,

onder financiering van het Ministerie van Justitie en Veiligheid.

Colofon

Titel: Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers

Uitvoerende organisaties: Lectoraat Maatschappelijke Veiligheid Hogeschool Saxion &
Lectoraat Cybersecurity in het mkb, De Haagse Hogeschool

Auteurs:
dr. Ellen Misana-ter Huurne (Hogeschool Saxion)

dr. Ynze van Houten (Hogeschool Saxion)

dr. Remco Spithoven (Hogeschool Saxion)

Raoul Notté MSc. (De Haagse Hogeschool)

dr. Rutger Leukfeldt (De Haagse Hogeschool)

In opdracht van de Veiligheidsalliantie Regio Rotterdam

Onder financiering van het Ministerie van Justitie en Veiligheid

© 2020, Hogeschool Saxion & De Haagse Hogeschool

Inhoudsopgave

Samenvatting

Cybercriminaliteit is een serieus en urgent maatschappelijke probleem. De winst in het tegengaan van cybercriminaliteit zal op korte termijn niet liggen in het opsporen van daders of het vergroten van toezicht op internet, maar eerder in het verbeteren van de cyberweerbaarheid van internetgebruikers. Het gedrag van mensen heeft invloed op de kans slachtoffer te worden van cybercriminaliteit zoals *phishing* en *ransomware*.

Effectieve risicocommunicatie en voorlichting kunnen een belangrijke bijdrage leveren aan het zelfbeschermend en voorbereidend gedrag van eindgebruikers, en daarmee hun capaciteit om zichzelf en/of hun organisatie te beschermen tegen de mogelijke risico's en effecten. Risicocommunicatie is maatwerk en is idealiter gebaseerd op de beleving en percepties van de doelgroep. Daarom is het van belang voor iedere doelgroep de communicatiestrategie te laten aanpassen aan hun kenmerken, percepties en gedragingen. Aangezien vooral jongeren en mkb'ers relatief vaak slachtoffer zijn van verschillende vormen van cybercriminaliteit, zijn deze twee groepen onderwerp van deze studie.

Dit rapport beschrijft een exploratief onderzoek in opdracht van de VeiligheidsAlliantie regio Rotterdam (VAR), en uitgevoerd door Hogeschool Saxion en de Haagse Hogeschool. Het doel is het in kaart brengen van factoren die bijdragen aan zelfbeschermend gedrag door jongeren en mkb'ers ten aanzien van cybercriminaliteit en hoe dit gedrag door middel van effectieve risicocommunicatie kan worden gestimuleerd.

Hiertoe is een conceptueel model ontwikkeld (het *Cyber Resilience Model*), dat inzicht geeft in de mogelijke factoren die de weerbaarheid en zelfbeschermend gedrag kunnen verklaren en voorspellen. Op basis van diepte-interviews en vragenlijstonderzoek onder jongeren en mkb'ers, is onderzocht hoe deze groepen scoren op de verklarende factoren en welke factoren het zelfbeschermend gedrag beïnvloeden.

Uit de resultaten blijkt dat bij zowel jongeren als mkb'ers er sprake is van een sterke '*optimistic bias*'. Deze bias houdt in dat men het risico ziet en zich ervan bewust is, maar zichzelf veel minder vatbaar acht om slachtoffer te worden dan anderen. De meeste respondenten beschouwen cybercriminaliteit als een (groot) maatschappelijk risico, maar zien het niet als iets dat hen persoonlijk snel zal overkomen.

Verder blijkt dat over het algemeen zowel jongeren als mkb'ers het nuttig vinden om zelfbeschermende of voorbereidende maatregelen te treffen tegen cybercriminaliteit. Zowel jongeren als mkb'ers voeren

reeds verschillende zelfbeschermende maatregelen uit, maar de meerderheid is ook voornemens om in de toekomst aanvullende maatregelen te treffen.

De analyses laten zien dat het zelfbeschermend gedrag van jongeren vooral wordt ingegeven door persoonlijke kenmerken (opleidingsniveau, leeftijd, geslacht en risicogevoeligheid), effectiviteitsverwachtingen, ervaring met slachtofferschap en de perceptie van eigen verantwoordelijkheid om jezelf te beschermen. Daarnaast blijkt dat de intenties om in de toekomst aanvullende zelfbeschermende maatregelen te nemen samenhangen met leeftijd en geslacht, waarbij jongere vrouwen de laagste intenties hebben om zichzelf (beter) te gaan beschermen tegen cybercriminaliteit. Opvallend is, dat de lager opgeleide, jonge vrouwen (jonger dan 18 jaar) het laagst scoren op zelfbeschermend gedrag. Bij mkb'ers wordt zelfbeschermend gedrag vooral bepaald door persoonlijke kenmerken (geslacht, slachtofferschap en risicogevoeligheid), effectiviteitsverwachtingen en subjectieve normen.

1. Inleiding

Nederland is in korte tijd sterk gedigitaliseerd. Sinds de intrede van de *personal computer* begin jaren ’80 van de vorige eeuw en de introductie van het voor het brede publieke toegankelijke internet medio jaren ’90, is informatietechnologie onderdeel geworden van ons dagelijks leven. Met de komst van de smartphone zijn Nederlanders massaal online. Nagenoeg ieder huishouden is aangesloten op internet en een overgrote meerderheid van de Nederlanders is inmiddels elk wakker uur continu online (de Heij, 2019). Naast dat dit de samenleving veel gemakken biedt, maakt de massale verbondenheid de samenleving ook kwetsbaar.

Criminelen zagen al snel de voordelen van het internet. Met de maatschappelijke omarming van nieuwe technologie is het risicobewustzijn niet evenredig meegegroeid: mensen ervaren vooral de dagelijkse gemakken en staan niet stil bij de risico’s die als neveneffect van het gebruik van deze technologie ontstaan. Daarbij komt dat internet drijft op de vrije en ongecontroleerde deling van informatie, dat grote delen van de infrastructuur in private handen zijn en dat overheden niet tot nauwelijks toezicht hebben op wat er op het internet gebeurt. Ook is het met de juiste technische kennis mogelijk om je als crimineel redelijk makkelijk aan toezicht te onttrekken. Internet is met andere woorden een honingpot voor criminelen: een enorme groep onwetende, potentiële slachtoffers verspreidt bijna automatisch – vaak onbewust – enorme hoeveelheden interessante informatie en betaalt ook grote bedragen argeloos via online bankieren. Actief toezicht is er niet en je kan je kunt er relatief anoniem opereren.

De impact van cybercriminaliteit wordt langzaam maar zeker duidelijk. De beperkte cijfers die beschikbaar zijn, tonen aan dat cybercriminaliteit een serieus en urgent maatschappelijke probleem betreft. In 2018 werd 5% van de Nederlandse internetgebruikers het slachtoffer van één of meerdere online vermogensdelicten (CBS, 2019). De totale, maatschappelijke schade van cybercriminaliteit in Nederland werd voor dat jaar op 10 miljard euro geschat. Dat is omgerekend 1% van Bruto Nationaal Product (BNP). De omvang en impact van cybercriminaliteit op de Nederlandse samenleving heeft er toe geleid dat het kabinet in 2019 is gaan investeren op de aanpak van cybercriminaliteit. Ook stelde het Ministerie van Justitie en Veiligheid in 2019 een miljoen euro extra beschikbaar aan initiatieven van lokale overheden om cybercriminaliteit tegen te gaan.

Het gedrag van eindgebruikers heeft invloed op de kans slachtoffer te worden van cybercriminaliteit zoals *phishing* en *ransomware* en de mogelijk schadelijke gevolgen hiervan. De factoren die bijdragen aan het risicobewustzijn en het zelfbeschermend gedrag hebben daarmee een groot effect op (het voor-

komen van) mogelijk schadelijke effecten van deze risico's. Uit onderzoek is gebleken dat effectieve risicocommunicatie en voorlichting een significante bijdrage leveren aan het zelfbeschermend en voorbereidend gedrag van eindgebruikers, en daarmee hun capaciteit om zichzelf en/of hun organisatie te beschermen tegen de mogelijke risico's en effecten (Sheng et al., 2010). Risicocommunicatie is maatwerk en is idealiter gebaseerd op de beleving en percepties van de doelgroep (ter Huurne, 2008). Daarom is het van belang voor iedere doelgroep de communicatiestrategie te laten aanpassen aan hun kenmerken, percepties en gedragingen.

Vanuit het besef dat de winst in het tegengaan van cybercriminaliteit *niet alleen* zal liggen in het opsporen van daders of het vergroten van toezicht op het internet, hebben de Veiligheidsalliantie regio Rotterdam (VAR), Hogeschool Saxion en de Haagse Hogeschool de handen ineengeslagen om op zoek te gaan naar praktische handvatten om inwoners en bedrijven meer bewust te maken van de risico's die zij lopen om het slachtoffer van cybercriminaliteit te worden en hen in hun zelfbeschermend gedrag te bevorderen. Om hierbij doelgroepgericht te werk te kunnen gaan, is gezamenlijk gekozen voor de focus op twee doelgroepen: jongeren en mkb'ers.

1.1 Doel en vraagstelling

Het doel van dit exploratieve onderzoek is het in kaart brengen van factoren die bijdragen aan zelfbeschermend gedrag door jongeren en mkb'ers ten aanzien van cybercriminaliteit en onderzoeken hoe dit gedrag door middel van effectieve risicocommunicatie kan worden gestimuleerd. De hoofdvraag van dit onderzoek luidt dan ook:

Welke factoren dragen bij aan het uitvoeren van zelfbeschermend gedrag door jongeren en mkb'ers ten aanzien van cybercriminaliteit en hoe kan dit gedrag door middel van effectieve risicocommunicatie worden gestimuleerd?

Bij deze doelstelling en hoofdvraag zijn de volgende deelvragen geformuleerd:

1. Hoe beleven jongeren en mkb'ers de risico's en mogelijke schade van cybercriminaliteit?
2. In hoeverre weten jongeren en mkb'ers hoe zij zichzelf kunnen beschermen tegen of voorbereiden op de risico's van cybercriminaliteit?
3. In welke mate vertonen jongeren en mkb'ers zelfbeschermend gedrag ten aanzien van cybercriminaliteit?
4. Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren en mkb'ers bij cybercriminaliteit?

5. Op welke factoren ten aanzien van cybercriminaliteit moeten campagnes zich richten om gedragsverandering bij jongeren en mkb'ers te stimuleren?

1.2 Afbakening

Risicocommunicatie is alleen effectief als er een afgebakende doelgroep is. Eerder onderzoek naar slachtofferschap van cybercriminaliteit wijst uit dat vooral *jongeren* slachtoffer worden (Domenie et al., 2013; Jansen, Leukfeldt, Wilsem, & Stol, 2013; Ngo & Paternoster, 2011; Sheng et al.,, 2010; Van de Weijer & Leukfeldt, 2017; Van Wilsem, 2013). Andere studies vonden geen verband tussen leeftijd en online slachtofferschap van onder andere oplichting, malware en identiteitsfraude (Bossler & Holt, 2009; Leukfeldt & Yar, 2016). De samenhang met andere persoonskenmerken is sterk afhankelijk van het type cybercriminaliteit. Zo worden hoger opgeleiden met hogere inkomens vaker slachtoffer van identiteitsfraude (Paulissen & Van Wilsem, 2015) en worden lager opgeleiden naar verhouding vaker slachtoffer van hacken (Domenie et al., 2013). Hoewel er discussie is over de invloed van persoonskenmerken als leeftijd, is leeftijd tot op heden het meest in onderzoek bevestigde persoonskenmerk dat met slachtofferschap van cybercriminaliteit samenhangt. Daarnaast zijn jongeren meer online en meer online zijn betekent een grotere vatbaarheid en daarmee een grotere kans op slachtofferschap van cybercriminaliteit (Leukfeldt en Yar, 2016; Leukfeldt, 2018).

Het midden- en kleinbedrijf (mkb) is een belangrijke pijler van de Nederlandse economie met drie miljoen banen en een totale omzet van bijna 860 miljard euro. Mkb'ers zijn met grote regelmaat doelwit van cybercriminelen, terwijl zij vaak niet de kennis en/of capaciteit hebben zich tegen deze aanvallen te wapenen (Leukfeldt, 2018; Notté et al., 2019). De omvang van cybercriminaliteit in het mkb is in aantal inmiddels ongeveer gelijk aan het aantal inbraken en fraude (WODC, 2011). De digitale vorm van criminaliteit is daarmee voor mkb'ers even reëel als de klassieke vormen van criminaliteit. Toch wordt er weinig onderzoek naar deze belangrijke doelgroep gedaan (Leukfeldt, 2018) en is er nog weinig bekend over in hoeverre zij in staat zijn zich te beschermen tegen en voor te bereiden op cybercriminaliteit. Wel is bekend dat attitudes en het gedrag van medewerkers belangrijke factoren zijn in vergroten of verkleinen van de risico's van cybercriminaliteit voor een organisatie (Vos, 2017; Alcatara & Riglietti, 2015).

Naast de algemene beleving van cybercriminaliteit onder de twee specifieke doelgroepen, richten wij ons in dit onderzoek verdiepend op twee specifieke vormen van cybercriminaliteit: *phishing* en *ransomware*. *Phishing* is een vorm van internetfraude waarbij oplichters pogen persoonlijke informatie als (bank)gegevens, inlogcodes en creditcardnummers te achterhalen en zodoende slachtoffers geld afhan-

dig te maken (Jagatic et al., 2005). *Phishing* is één van de meest voorkomende vormen van cybercriminaliteit en zal dat naar verwachting ook blijven (Domenie e.a., 2013; Leukfeldt, 2018). *Ransomware* – kortweg kwaadaardige software die bestanden op computers versleuteld en waar het slachtoffer geld moet betalen om weer toegang te krijgen tot die bestanden – is de laatste jaren een veelvoorkomend delict geworden waar burgers en ondernemers het slachtoffer van worden (Leukfeldt, 2018). Voor deze prominente vormen van cybercriminaliteit is de kans zeer aannemelijk is dat onze gekozen doelgroepen – jongeren en mkb'ers – enerzijds vatbaar zijn voor de risico's en anderzijds door middel van effectieve risicocommunicatie gestimuleerd kunnen worden om hun zelfbeschermend gedrag te vergroten. Het doel is om inzicht te krijgen in de beïnvloedende factoren voor zelfbeschermend gedrag onder deze doelgroepen om op basis daarvan effectieve communicatie te ontwikkelen waarmee mogelijke schade en effecten geminimaliseerd kunnen worden.

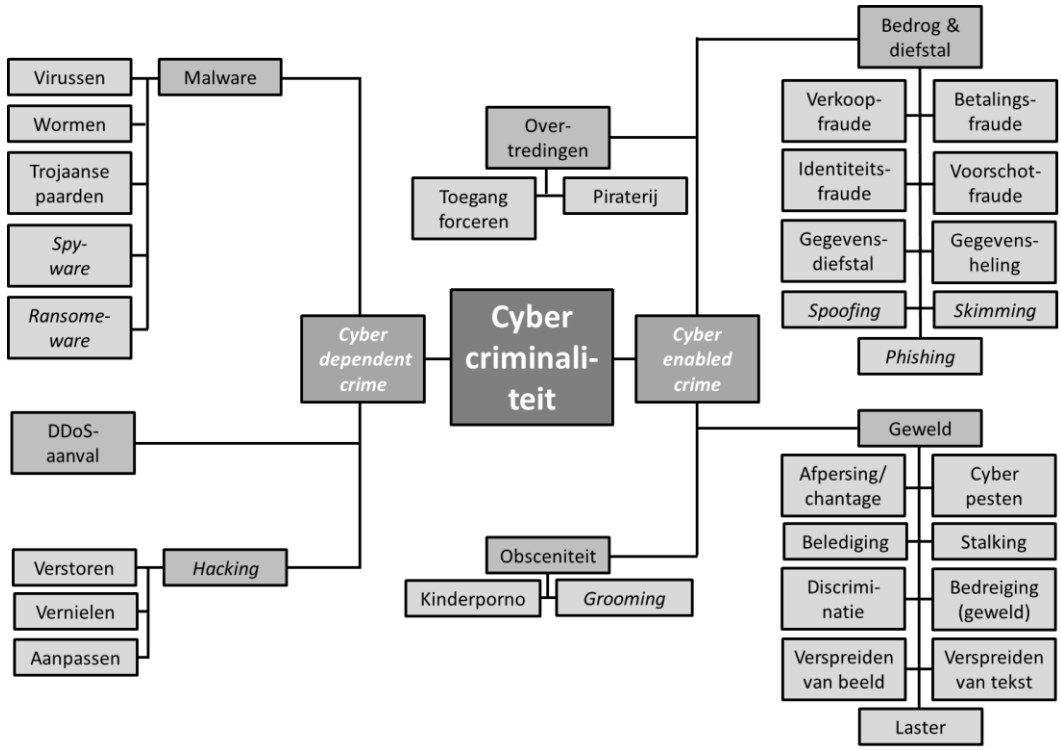
2. Cybercriminaliteit en cyberweerbaarheid

In dit hoofdstuk gaan we in op onderliggende theorie en belangrijke empirische kennis met betrekking tot de centrale begrippen in dit onderzoek.

2.1. Cybercriminaliteit

Cybercriminaliteit gaat in de basis over het gebruiken van informatietechnologie (IT) ten behoeve van het plegen van criminaliteit. Het begrip valt uiteen in twee subcategorieën: (I) *Cyber-enabled crime* en (II) *Cyber-dependent crime*. De eerste categorie betreft spreekwoordelijk oude wijn in nieuwe zakken. Hierbij worden aloude vormen van criminaliteit langs digitale wegen op grote schaal toegepast. Holt en Bosseler (2014) onderscheiden vier hoofdvormen van cyber-enabled crime waarbij IT het middel voor de uitvoering is: (A) overtredingen; (B) bedrog & diefstal; (C) geweld en (D) obsceniteit. Bij cyber-dependent crime is IT niet alleen het middel maar ook direct het doel. Middels (A) malware; (B) DDoS-aanvallen en (C) hacking worden slachtoffers digitale schade toegebracht.

Spithoven (2020) heeft de onderstaande taxonomie voor cybercriminaliteit ontwikkeld om een overzicht te geven van de verschillende vormen van cybercriminaliteit (Figuur 1).



Figuur 1 – Taxonomie van cybercriminaliteit (Spithoven, 2020).

In dit onderzoek richten wij ons naast cybercriminaliteit in het algemeen op twee specifieke vormen: phishing en ransomware. Onder phishing verstaan wij: *'(t)he process whereby criminals use digital means such as email to try to retrieve users' personal information by posing as a trusted authority* (Leukfeldt, 2016, p. 58; zie ook Lastdrager, 2014). Onder ransomware verstaan wij: *'(…) a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. More modern ransomware families, collectively categorized as crypto-ransomware, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key'* (Trendmicro, z.d.).

2.2 Cyberweerbaarheid

Cyberweerbaarheid betreft de mate waarin iemand in staat is tegenstand te bieden tegen cybercriminaliteit, of, met andere woorden, zelfbeschermend gedrag te vertonen met betrekking tot cybercriminaliteit (zie bijvoorbeeld Van der Kleij en Leukfeldt, 2019). Onder zelfbeschermend gedrag verstaan wij: die acties of gedragingen die mensen uitvoeren om zichzelf te beschermen tegen risico's, gevaren of de gevolgen daarvan (inclusief (negatieve) emoties). Het onderzoek naar online beleving van veiligheid komt nog maar mondjesmaat op gang (Brunton-Smith, 2018; Brands & van Wilsem, 2019; Jansen, Kop & Stol, 2017). In de literatuur worden verschillende factoren beschreven waarom mensen wel of niet zelfbeschermend gedrag vertonen. Daarbij neemt de beleving van risico's een centrale plek in: voordat men zelfbeschermend gedrag ten opzichte van een risico vertoont, dient men het risico als persoonlijk relevant te beleven.

Voorspellers van inschattingen van de kans om slachtoffer van cybercriminaliteit te worden zijn gevonden in (I) het zelfvertrouwen dat mensen hebben in het gebruikmaken van de computer en internet en (II) sociale status. Geslacht, leeftijd, opleidingsniveau en eerder slachtofferschap van cybercriminaliteit leiden - als gevolg van verschillende metingen - tot gemengde resultaten (Brands & Van Wilsem, 2019; Jansen et al., 2017; Virtanen, 2017; Powell, 2013; Yu, 2014; Roberts, Indermaur & Spiranovic 2013). Brands en van Wilsem (2019) troffen in hun representatieve steekproef voor de Nederlandse bevolking aan dat oudere en lager opgeleide respondenten zich meer zorgen maakten, maar dat de sterk bezorgden minder online actief waren met bankieren en winkelen. Ook Brunton-Smith (2018) trof een sterke samenhang tussen zorgen over slachtofferschap van cybercriminaliteit en verklaringen van meer algemene gevoelens van onveiligheid. Er zijn dus zeer waarschijnlijk goede lessen over de verklaring van de online beleving van veiligheid te vinden in de inzichten over de verklaring van offline veiligheidsbeleving.

2.3 Risicocommunicatie

Er ligt een maatschappelijke uitdaging in het bevorderen van het risicobewustzijn en preventief gedrag om slachtofferschap van cybercriminaliteit te voorkomen. Burgers en bedrijven moeten in staat worden gesteld om hun gedrag aan te passen en daarvoor is het nodig te weten *hoe* en *waarom* zij dat moeten doen. Uit eerder onderzoek is gebleken dat effectieve risicocommunicatie en voorlichting een stevige bijdrage leveren aan het preventief gedrag van eindgebruikers en daarmee hun capaciteit om zichzelf of hun organisatie te beschermen tegen de mogelijke risico's en effecten van cybercriminaliteit (Sheng et al., 2010). Risicocommunicatie is in essentie bedoeld om individuen te ondersteunen om geïnformeerde beslissingen te nemen ten aanzien van de risico's waarmee zij worden geconfronteerd (Wade et al., 1992). Risicocommunicatie is maatwerk. Om optimaal effect te sorteren, wordt de communicatie gebaseerd op de beleving en percepties van de doelgroep (ter Huurne, 2008). Het is daarnaast van belang om voor iedere doelgroep de communicatiestrategie te laten aansluiten op hun voorkeuren, kenmerken, percepties en huidige gedragingen.

Juist bij het bevorderen van preventief gedrag speelt risicocommunicatie een rol die verder gaat dan louter informeren. Het doel is immers om individuen daadwerkelijk in staat te stellen en te stimuleren om zichzelf (beter) te beschermen. Hiervoor zijn een aantal aspecten belangrijk. Mensen moeten: (I) *weten* (risicobewustzijn); (II) *willen* (perceptie eigen verantwoordelijkheid); (III) *kunnen* (zelfeffectiviteit) en (IV) *doen* (gedrag). In de wetenschappelijke en praktijkgerichte discipline van risicocommunicatie zijn aanvullende inzichten opgedaan over hoe gedragsverandering ten aanzien van risico's tot stand komt. In de basis kunnen mensen daarom op twee manieren reageren op informatie over mogelijke risico's: *problem-focused coping* of *emotion-focused coping*. Deze begrippen leggen we hierna verder uit.

2.3.1 Problem vs. emotion focused coping

Bij problem-focused coping is het doel om het 'probleem' – in dit geval het risico of de dreiging van cybercriminaliteit – te minimaliseren. In het Exended Parallel Processing model (EPPM) (Witte, 1992) en de Protectie Motivatie Theorie (PMT; Rogers, 1975; Rogers, 1983, Rogers & Prentice-Dunn, 1997) wordt dit het 'danger control process' genoemd. Dit is het gedrag dat men door middel van campagnes beoogt te bereiken: mensen gaan hun gedrag aanpassen op basis van de gegeven gedragsadviezen met als doel zichzelf tegen het gevaar te beschermen. Deze communicatie speelt in op de waargenomen gedragscontrole. Bij waargenomen gedragscontrole gaat het om de mate waarin men zichzelf in staat acht het gewenste gedrag ook echt te kunnen uitvoeren en in hoeverre het uitvoeren van dit gedrag in hun bele-

ving bijdraagt aan het minimaliseren van het gevaar of de mogelijke gevolgen daarvan. Hierbij doorlopen individuen vier inschattingsstadia: (I) Inschatting van de eigen kwetsbaarheid ten opzichte van het gevaar; (II) Inschatting van de ernst van de dreiging en gevolgen daarvan; (III) Inschatting van de effectiviteit van het aanbevolen gedrag; (IV) Inschatting van de eigen effectiviteit (de mate waarin een persoon zichzelf in staat acht het aanbevolen gedrag uit te kunnen voeren).

Stadia 1 en 2 vormen samen de waargenomen dreiging of risicoperceptie. Stadia 3 en 4 vormen samen de effectiviteitsverwachting. Volgens PMT en EPPM zijn mensen geneigd het preventieve gedrag uit te voeren wanneer zowel de waargenomen dreiging als de effectiviteitsverwachting als hoog worden ingeschat. Met andere woorden: een individu moet het idee hebben dat hij/zij vatbaar is voor het risico en dit risico als ernstig inschatten. Daar komt nog bij dat het individu het idee moet hebben dat hij/zij het aanbevolen gedrag kan uitvoeren en dat het nuttig is dit gedrag te gaan uitvoeren. Wanneer één van deze factoren door het individu als (te) laag wordt inschat, dan is de kans klein(er) dat het individu over zal gaan tot het uitvoeren van preventief gedrag dat wordt geadviseerd.

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). Maar wanneer de waargenomen dreiging als hoog wordt ervaren, maar de effectiviteits-verwachtingen 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. Hier ligt een belangrijke theoretische link met de eerder behandelde psychologische beschermingsmechanismen.

Een ander verschijnsel in de rol die risicoperceptie speelt bij het al dan niet uitvoeren van zelfbeschermend gedrag, is de zogenaamde 'optimistic bias' (zie bijvoorbeeld Weinstein, 1989) of 'third-person perception (Sun et al., 2008). Dit verwijst naar het psychologisch fenomeen dat individuen geneigd zijn om risico's op een egocentrische wijze te beoordelen. Het komt er op neer dat individuen hun eigen vatbaarheid voor risico's vaak onderschatten, terwijl men de vatbaarheid van anderen vaak hoger inschat. In de basis komt het er op neer dat de optimistic bias door individuen wordt toegepast om een 'self-serving' inschatting van het risico te maken, waarbij een aantal factoren een rol speelt: 1) egocentrisme, 2) vergroting self-esteem, 3) psychologische afstand en 4) illusie van controle. Optimistic bias is

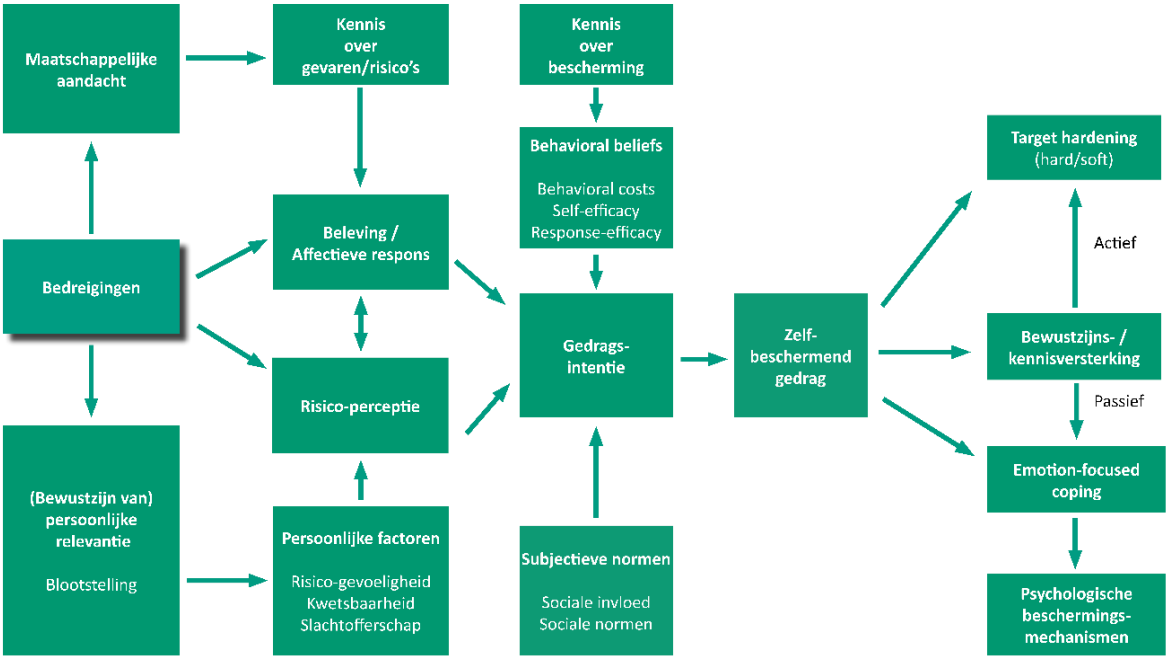
overigens ook van toepassing op positieve inschattingen van gebeurtenissen. Ook in relatie tot online risico's is deze optimistic bias gevonden (o.a. Rhee et al., 2005). Verschillende onderzoekers impliceren dat de optimistic bias, als onderdeel van risicoperceptie, een belangrijk concept is om aandacht aan te schenken in risicocommunicatie, aangezien juist de optimistic bias kan zorgen voor onveilig gedrag door onrealistische inschatting van persoonlijk risico.

2.3.2 Inspelen op de specifieke beleving

Het is van belang om de communicatie over cybercriminaliteit persoonlijk relevant en dichtbij te maken, zodat individuen de neiging hebben om hun gedrag aan te passen. Risicocommunicatie-boodschappen om gedragsverandering te stimuleren zijn het meest effectief, wanneer zij enerzijds inspelen op het verhogen van de risicoperceptie en anderzijds het aanbieden van concrete, als makkelijk uitvoerbare en nuttig ervaren, gedragsadviezen (ter Huurne, 2008; Kievik et al., 2018). De sleutel bij risicocommunicatie ligt in het denken in doelgroepen. Elke doelgroep vraagt om een op maat gemaakte aanpak en deze start bij het achterhalen en verklaren van het risicobewustzijn en het preventieve gedrag rondom het risico onder de doelgroep. Op deze wijze kan risicocommunicatie een bijdrage leveren aan het preventieve gedrag van eindgebruikers en daarmee hun capaciteit om zichzelf en/of hun organisatie te beschermen tegen mogelijke risico's en negatieve effecten (Sheng, et al., 2010). Deze inzichten zijn samengevoegd in het conceptuele model in Figuur 2.

2.4 Conceptueel model: Cyber resilience

Op basis van bovenstaande inzichten hebben we een conceptueel model ontwikkeld (Figuur 2). Dit model dient als (wetenschappelijke) basis en als leidraad voor het inzichtelijk maken van de factoren die een rol spelen bij de (intenties tot) zelfbeschermend gedrag ten aanzien van cybercriminaliteit onder de doelgroepen in dit onderzoek: jongeren en mkb'ers.



Figuur 2 –Het cyber resilience model.

De centrale begrippen in het model worden hieronder uitgelegd:

Onder **zelfbeschermend gedrag** verstaan wij: die acties of gedragingen die mensen uitvoeren om zichzelf te beschermen tegen risico's, gevaren of de gevolgen daarvan (inclusief negatieve emoties). In de basis kunnen mensen op twee manieren reageren op mogelijke risico's: problem-focused coping of emotion-focused coping. De intentie om dit gedrag uit te voeren is een belangrijke voorspeller van het daadwerkelijk gedrag (Ajzen, 1991).

Target hardening is het gedrag dat beoogd wordt te bereiken door middel van risicocommunicatie campagnes: mensen gaan hun gedrag aanpassen op basis van de gegeven gedragsadviezen met als doel zichzelf te beschermen tegen het gevaar. Toegepast op de risico's van cybercriminaliteit kan dit op verschillende manieren:

(I) Door fysieke maatregelen te treffen (wachtwoorden instellen, anti-phishing software, etc.)

(II) Door gedragsmatige maatregelen (informatie zoeken, alertheid, bewustzijn, veilig handelen)

De **gedragsintentie** om preventief gedrag ten aanzien van cybercriminaliteit te nemen komt tot stand langs verschillende factoren:

(I) de perceptie van het risico; Onder **risicoperceptie** verstaan wij de wijze waarop een individu het risico voor hem inschat, is afhankelijk van verschillende factoren. Ten eerste moet er een **dreiging** ervaren worden. Deze dreiging bestaat uit de inschatting van de **kans** dat de persoon blootgesteld wordt aan een risico en de ingeschatte **ernst** van de mogelijke effecten. Dit zijn de mate van **risicogevoeligheid, kwetsbaarheid en slachtofferschap**. Het hebben van ervaring, kennis en bewustzijn van de aanwezigheid van het risico of gevaar speelt hierbij een belangrijke rol. Zo is aandacht voor het risico in de **sociale omgeving** (een kennis is slachtoffer geworden van phishing of malware) of in de **media** een belangrijke trigger van risicoperceptie. De **kennis** die een persoon daardoor opdoet over het risico, beïnvloedt het risicobewustzijn. De mate waarin de persoon zich bewust is van zijn mogelijke persoonlijke risico door deze aandacht is van invloed op de risicoperceptie.

(II) de beleving van ofwel de **affectieve respons** op het risico. Risicoperceptie is niet alleen een puur cognitieve inschatting van het gevaar of het risico. Door kennis, informatie, (sociale of media) aandacht en bewustzijn, ontstaat er vaak een affectieve respons. Deze respons is voornamelijk gebaseerd op emoties, intuïtie en onderbuikgevoel en is vaak een onbewuste reactie (Lindell & Perry, 2012). Deze reactie is echter van grote invloed op de **risicobeleving** en het uiteindelijke gedrag van mensen (Slovic, 2004; Finucane et al., 2000).

(III) Onder **'behavioural beliefs'** verstaan wij de mate waarin men zichzelf in staat acht het gedrag echt te kunnen uitvoeren en in hoeverre het uitvoeren van dit gedrag bijdraagt aan het minimaliseren van het gevaar of de mogelijke gevolgen daarvan. Hierbij zijn vier inschattingsstadia aanwezig:

(I) Inschatting eigen kwetsbaarheid ten opzichte van het gevaar;
(II) Inschatting van de ernst van de dreiging en gevolgen daarvan;
(III) Inschatting van de effectiviteit van het aanbevolen gedrag;
(IV) Inschatting van de eigen effectiviteit (de mate waarin een persoon zichzelf in staat acht het aanbevolen gedrag uit te kunnen voeren).

Stadia 1 en 2 vormen samen de **risicoperceptie**. Stadia 3 en 4 vormen samen de **effectiviteitsverwachting**.

(IV) De gedragsintentie wordt tevens beïnvloed door **subjectieve normen** - de sociale aanmoediging van gedrag en geldende normen in de omgang met het risico van cybercriminaliteit.

Gegeven de complexiteit van dit proces is het zaak om per doelgroep - op maat - in te spelen op deze samenhangende concepten om effect te sorteren en doelgroepen - in plaats van naar passieve (A) *emotion focused coping* onder invloed van psychologische beschermingsmechanismen – naar actieve (B) *target hardening* te brengen en zo hun cyberweerbaarheid te vergroten.

Het hierboven beschreven conceptuele model is gebaseerd op kennis over de offline wereld. Daarmee is dit onderzoek, ondanks dat het gebaseerd is op een conceptueel model, van *exploratieve* aard. Het is immers nog nooit toegepast op nieuwe vormen van criminaliteit. We kunnen zeker lessen uit de offline wereld in de online wereld toepassen, maar in de woorden van Manuel Castells (2000, p. xix) '*We are in a new world, and we need new understanding'.*

3. Onderzoeksopzet

Vanwege het exploratieve karakter van dit onderzoek is gebruik gemaakt van zowel kwantitatieve als kwalitatieve onderzoeksmethoden, te weten vragenlijsten en (diepte)interviews. Deze methoden worden hieronder eerst uitgelegd, waarna wordt beschreven hoe de concepten meetbaar zijn gemaakt (de operationalisatie), en hoe de deelnemers aan het onderzoek zijn geworven.

3.1 Vragenlijsten

Bij vragenlijsten vullen respondenten een lijst vragen met gestandaardiseerde antwoorden in. Deze methode is geschikt voor het meten van houdingen in grotere populaties (Babbie, 1998; De Vaus, 2001). Omdat alle data op een moment in de tijd wordt verzameld drijft deze methode op bestaande verschillen tussen groepen in plaats van verandering (De Vaus, 2001).

3.1.1. Deelnemers onderzoek

De vragenlijst is aan een grote groep respondenten voorgelegd om zo een breder inzicht te krijgen in de factoren die een rol spelen bij het al dan niet uitvoeren van zelfbeschermend gedrag bij cybercriminaliteit.

De vragenlijst is verspreid onder beide doelgroepen; in totaal hebben 2.115 jongeren en 631 mkb-ondernemers de vragenlijst ingevuld. Respondenten zijn geworven door (I) een online-ondernemerspanel van I&O research (mkb'ers) en (II) studenten van Saxion, die via hun eigen netwerk volgens de sneeuwbalmethode respondenten hebben geworven (jongeren).

3.1.2 Meetinstrument

Op basis van het conceptueel model zijn de volgende concepten gemeten in het onderzoek:

1. Persoonlijke kenmerken: leeftijd, geslacht, opleidingsniveau, blootstelling/kwetsbaarheid, recent slachtofferschap;
2. Risicoperceptie persoonlijk: inschatting kans en gevolgen persoonlijk risico;
3. Risicoperceptie algemeen: inschatting risico's voor iedereen in de samenleving;
4. Kennis over risico's en gevolgen;
5. Kennis over zelfbeschermende maatregelen en gedrag;
6. Subjectieve normen ten aanzien van zelfbeschermend gedrag;
7. Motivation to comply met betrekking tot subjectieve normen;

8. Behavioral beliefs: zelfeffectiviteit (uitvoerbaarheid), responseffectiviteit (beoordeeld nut) van zelfbeschermend gedrag en gedragseffectiviteit (beoordeling effectiviteit huidig zelfbeschermend gedrag);
9. Behoefte aan informatie/voorlichting over cyberrisico's;
10. Huidig zelfbeschermend gedrag;
11. Intenties tot zelfbeschermend gedrag.

De vragenlijst bestond uit Likert-type schalen met items (stellingen en vragen) die de onderzoeksconcepten meten. De schalen zijn getoetst op betrouwbaarheid, berekend met Cronbach's [1]alpha (α; bij schalen met meer dan twee stellingen) of de correlatie (r; bij schalen met twee stellingen[2]) en blijken allemaal betrouwbaar. De volledige vragenlijst is opgenomen in Bijlage 1.

Slachtofferschap

Respondenten is gevraagd of zij de afgelopen twaalf maanden slachtoffer zijn geworden van cybercriminaliteit. Antwoordmogelijkheden waren 'ja', 'nee' en 'weet ik niet'. Indien een respondent slachtoffer was geworden, is gevraagd wat de impact en effecten van de gebeurtenis waren en in hoeverre deze ervaring van invloed is geweest op hun online en zelfbeschermend gedrag ten aanzien van cybercriminaliteit.

Risicoperceptie persoonlijk

Persoonlijke risicoperceptie is gemeten met behulp van stellingen over de kans en effecten van de risico's. Kans is gemeten met drie vragen*: Hoe groot acht je de kans om <u>zelf</u> de komende twaalf maanden slachtoffer te worden van [cybercriminaliteit / phishing / ransomware]?* Antwoorden werden gegeven op een zespuntsschaal met categorieën van 'geen kans'(1) tot 'hele grote kans'(6). Deze schaal is betrouwbaar: α=.83. Ingeschat effect is gemeten door twee stellingen op een vijfpuntsschaal: *"Als ik slachtoffer zou worden van [cybercriminaliteit/phishing/ransomware] , dan levert dat ernstige schade voor mij op."* ('helemaal mee oneens'(1) tot 'helemaal mee eens'(5)); α=.86.

---

[1] **Cronbach's alpha** is een manier om vast te stellen of meerdere items samen één schaal mogen vormen. Het wordt ook wel een betrouwbaarheidsanalyse genoemd. De **Cronbach's alpha** zelf is de maatstaf. Dit wordt getoetst op basis van de onderlinge correlatie van de verschillende items. Een schaal met een Cronbach's alpha van minimaal .70 wordt als betrouwbaar beschouwd.

[2] Hierbij is het significantieniveau van de correlatie getoetst, waarbij p≤.05 wordt aangeduid met *; p ≤.01 wordt aangeduid met **; en p≤.001 wordt aangeduid met ***. Hoe kleiner de p-waarde, hoe sterker de significantie.

Risicoperceptie algemeen

Algemene risicoperceptie is gemeten door te vragen: *'Hoe groot acht je de kans dat een gemiddelde Nederlander de komende twaalf maanden slachtoffer wordt van [cybercriminaliteit / phishing / ransomware]*?. Antwoordcategorieën (zespuntsschaal) varieerden van ('geen kans' (1) tot 'hele grote kans' (6)).Deze schaal is betrouwbaar: α=.91.

Zelfeffectiviteit

Zelfeffectiviteit is gemeten met behulp van vier stellingen: *'Ik weet:… [hoe ik mij kan beschermen tegen cybercriminaliteit/ …welke risico's ik loop om slachtoffer te worden van cybercriminaliteit/ …hoe ik (een poging tot) cybercriminaliteit kan herkennen/ …wat ik moet doen wanneer ik slachtoffer word van cybercriminaliteit]'.* Antwoordcategorieën varieerden van 'helemaal niet' (1) tot 'volledig' (5) op een vijfpuntsschaal. Deze schaal is betrouwbaar: α=.83.

Responseffectiviteit

Twee items: *'Het is nuttig om maatregelen te treffen om je tegen cybercriminaliteit te beschermen.'* en *'Maatregelen treffen heeft weinig nut; het verkleint de kans om slachtoffer van cybercriminaliteit te worden niet of nauwelijks.'* Deze items op een vijfpuntsschaal van 'volledig mee oneens' (1) tot 'volledig mee eens' (5) correleren significant (r=.22***).

Gedragseffectiviteit

Gedragseffectiviteit is gemeten met twee items: *'De door mij genomen maatregelen zorgen ervoor dat ik minder kans heb om slachtoffer te worden van cybercriminaliteit'* en *'Ik vind dat ik mij voldoende bescherm tegen cybercriminaliteit'* op een vijfpuntsschaal van volledig mee oneens (1) tot volledig mee eens (5). Deze correleerden sterk r=.67***.

Subjectieve normen

Subjectieve normen zijn gemeten met twee items: *"Mensen in mijn omgeving vinden het belangrijk dat ik mezelf tegen cybercriminaliteit bescherm"* en *"Mensen in mijn omgeving verwachten dat ik mezelf tegen cybercriminaliteit bescherm"* op een vijfpuntsschaal van 'volledig mee oneens' (1) tot 'volledig mee eens'(5). Deze items vertonen een sterke correlatie, r=.60***.

Motivation to comply

Twee items: *"Ik ben geneigd om mezelf te beschermen, omdat anderen dat ook doen"* en *"Ik ben geneigd om mezelf te beschermen, omdat mensen om mij heen dat van mij verwachten"*. Vijfpuntsschaal

van 'volledig mee oneens' (1) tot 'volledig mee eens' (5). Deze items vertonen een sterke correlatie, r=.64***.

Sociale invloed

De items van subjectieve normen en motivation to comply vormen samen één schaal met sociale invloed. Deze schaal is betrouwbaar, α=.78.

(Intenties tot) zelfbeschermend gedrag

Gedragsintentie is gemeten door de vraag: *Bent u voornemens om in de toekomst aanvullende voorbereidende of zelfbeschermende maatregelen te treffen tegen cybercriminaliteit?* Vierpuntsschaal van 'zeker niet' (1) tot 'zeker wel' (4).

Daarnaast is aan respondenten is gevraagd welke zelfbeschermende maatregelen zij reeds uitvoeren. Zij konden van 24 maatregelen aangeven of zij deze uitvoeren en daarnaast of er andere, niet genoemde maatregelen zijn die zij uitvoeren.

Persoonlijke gegevens

Respondenten is gevraagd naar hun geslacht, leeftijd, opleidingsniveau en recent slachtofferschap.

3.1.3 Gereedschappen en analyse

De vragenlijst is afgenomen via Qualtrics[3]. Dit is een betrouwbare en gebruiksvriendelijke online tool voor vragenlijstonderzoek. De gegeven antwoorden worden geëxporteerd naar en geanalyseerd met behulp van SPSS[4]. Data zijn geanalyseerd op beschrijvende en verklarende statistieken. Gemiddelde scores, verschillen tussen doelgroepen en veronderstelde samenhang (correlaties) tussen relevante concepten uit het model zijn getoetst. Door middel van Structural Equation Modelling (SEM)[5] met behulp van STATA is het conceptueel model getoetst, waarbij inzicht wordt verschaft in welke factoren daadwerkelijk (het meest en significant) bijdragen aan het beïnvloeden van het zelfbeschermend gedrag.

3.2 Interviews

De respondenten kregen in de interviews semigestructureerde vragen voorgelegd door een interviewer in een *face-to-face* interview. Gezien de kennis over online veiligheidsbeleving nog in de kinderschoenen

[3] https://www.qualtrics.com/
[4] Statistical Package for the Social Sciences; https://www.ibm.com/analytics/nl/nl/technology/spss/index.html
[5] Het doel van SEM is het opstellen en toetsen van een model omtrent de interrelatie tussen een geheel van geobserveerde (manifeste) en niet-geobserveerde (latente) variabelen.

staat (Brunton-Smith, 2018; Brands & Van Wilsem, 2019; Jansen, Kop & Stol, 2017) is er gekozen voor het maximaliseren van de vrijheid die respondenten hadden in het antwoorden op vragen en de volgorde waarin de vragen door de interviewer werden gesteld: *'the qualitative interviewing design is flexible, iterative and continuous, rather than prepared in advance and locked in stone'* (Rubin & Rubin 1995, p. 43). De respondenten waren met andere woorden *'(…) free to answer questions in their own words rather than required to choose one or another predetermined alternative'* (Weiss 1995, p. 12).

3.2.1. Deelnemers onderzoek

In totaal zijn 29 jongeren en 25 mbk-ondernemers geïnterviewd. Werving vond plaats via het uitgebreide netwerk van de onderzoekers verbonden aan beide lectoraten en het principe van de sneeuwbalmethode, ofwel de *re-assuring informant* (Weiss, 1995): bekenden van bekenden van de onderzoekers die op basis van de vertrouwensband met de onderzoekers een goed woordje kunnen doen en potentiële respondenten kunnen polsen of zij aan het onderzoek willen bijdragen.

3.2.2. Meetinstrument

De semigestructureerd vragenlijst was – net als de in de vorige paragraaf beschreven vragenlijst – gebaseerd op het conceptuele model uit onderdeel 2.5. Het interviewschema is beschreven in Bijlage 2.

3.2.3 Gereedschappen en analyse

De interviews zijn volgens afspraak individueel op locatie en in enkele gevallen via skype met de respondenten mondeling afgenomen door een onderzoeker. Van alle interviews zijn geluidsopnames gemaakt. Vervolgens zijn deze opnames volledig getranscribeerd. Analyses zijn met behulp van het softwarepakket ATLAS.ti[6] uitgevoerd op basis van een systematische codering, waarbij de volgende stappen worden doorlopen: 1) open coderen, 2) axiaal coderen, 3) selectief coderen.

[6] https://atlasti.com/

4. Cyberweerbaarheid bij jongeren

De uitkomsten van de analyses van de enquête en interviews gehouden onder jongeren worden hieronder aan de hand van de deelvragen gepresenteerd. Indien relevant, worden effecten van geslacht, opleiding, en leeftijd aangegeven.

4.1 Steekproef en respondenten

In totaal hebben 2.115 jongeren onze vragenlijst ingevuld. Van de respondenten was 53% man. De gemiddelde leeftijd is 20 jaar, waarvan 29% jonger was dan 18 jaar, 50% tussen de 18 en 21 jaar en 21% tussen de 22 en 25 jaar oud. Het opleidingsniveau varieert; 26% gaf aan een middelbaar opleidingsniveau te hebben (vmbo, mbo), 56% hoger (havo, hbo) en 18% wo-niveau (vwo, universiteit). Onder de Nederlandse bevolking is de verdeling in de onderzochte leeftijdscategorie (16-25 jaar) in het schooljaar 2018-2019 respectievelijk 36%, 36%, en 27% (CBS, 2019)[7]. In dit onderzoek is dus de groep havoleerlingen en hbo-studenten oververtegenwoordigd, wat te verklaren is door de manier van werven vanuit een hbo-instelling.

De respondenten zijn gemiddeld veel online: 94% is minimaal dagelijks online. Een aanzienlijk deel is minstens ieder wakker uur online (34%) of zelfs (bijna) continu tijdens de wakkere uren (18%). De belangrijkste redenen om online te zijn, zijn: sociale contacten (73%), ontspanning (70%), studie (66%), bankieren (64%), winkelen (55%) en werk (51%).

Naast de enquête zijn er 29 diepte-interviews gehouden met jongeren. De groep bestond voor 43% uit mannen en 57% uit vrouwen. De gemiddelde leeftijd was 21,5 jaar (range 18-25 jaar). De groep was relatief hoog opgeleid (15% (v)mbo, de overigen havo, hbo, en (v)wo). De voornaamste dagbesteding van de groep was het volgen van een opleiding (65%).

4.2 Deelvraag 1: Hoe beleven jongeren de risico's en mogelijke schade van cybercriminaliteit?

Voor het beantwoorden van deze deelvraag kijken we naar het slachtofferschap, de risicoperceptie en het bewustzijn met betrekking tot risico's en mogelijke schade van cybercriminaliteit.

4.2.1 Slachtofferschap

De beleving van risico's wordt sterk beïnvloed door de eigen ervaring die jongeren hebben met cybercriminaliteit. Een klein deel van de respondenten van de enquête (4%) is het afgelopen jaar slachtoffer

[7] Aangezien de cijfers voor deze leeftijdsgroep niet als zodanig beschikbaar zijn, betreft het hier een schatting op basis van CBS-gegevens over het schooljaar 2018-2019

geworden van cybercriminaliteit. Het overgrote merendeel (87%) geeft aan de afgelopen twaalf maanden geen slachtoffer te zijn geworden van cybercriminaliteit, en 9% van de respondenten weet niet zeker of ze wel of geen slachtoffer zijn geworden. De personen die slachtoffer zijn geworden noemen vooral het verlies van geld en (persoonlijke) bestanden als geleden schade. Op de vraag wat de impact was van hun slachtofferschap geven de meesten aan dat, naast het verlies van geld of bestanden, men is geschrokken en zich minder veilig voelt online. Ook schaamte wordt door enkele respondenten benoemd. De meeste slachtoffers hebben hun online gedrag aangepast door voorzichtiger en oplettender te zijn, meer research te doen naar websites en betere beveiliging op hun *devices* te installeren.

De geïnterviewde jongeren meldden o.a. de volgende ervaringen met cybercriminaliteit:

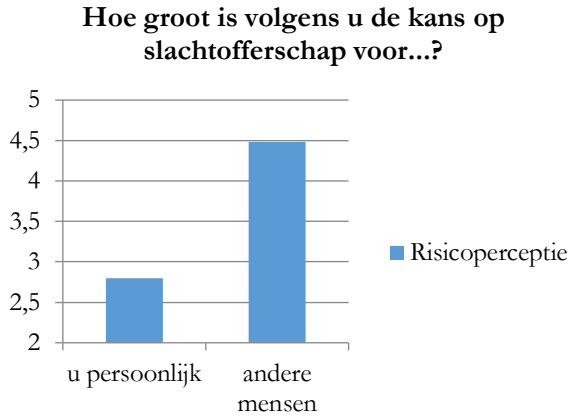
> *"Ik had ook iets gedownload voor muziek, allemaal virussen en toen werd mijn computer steeds langzamer en opeens deed ie het niet meer."* (jongere4)
>
> *"Ik heb zelf kaartjes van de Efteling gekocht die niet echt waren. Daar kwamen we achter bij het pretpark zelf."* (jongere15)
>
> *"(…) Vanaf toen kreeg ze [een vriendin] berichtjes dat ze haar foto's zouden gaan publiceren. Ze dacht van: ''yo, het is gewoon een grap''. Uiteindelijk is het wel gebeurd, echt heel erg."* (jongere17)
>
> *"Ik heb dus een keer een scherm gekregen van volgens mij 'de politie die zei dat ze gedetecteerd hadden dat er getorrent was op de PC en dat ik een boete moest betalen."* (jongere22)

4.2.2 Risicoperceptie

De kansinschatting om persoonlijk slachtoffer te worden is beneden gemiddeld onder de respondenten van de enquête: 2,80 (op een 6-puntsschaal), modus (64%): "(heel) klein". Echter, de respondenten schatten de kans dat een gemiddelde Nederlander slachtoffer wordt van cybercriminaliteit significant[8] hoger in: 4,48 (modus (62%): "(heel) groot"). Er is hier sprake van een 'optimistic bias' (Figuur 3), waarbij men cybercriminaliteit als risico beschouwt, maar zichzelf minder kwetsbaar acht dan anderen. Daarbij schatten mannen de kans op slachtofferschap nog eens significant[9] lager in dan vrouwen (gemiddeld

[8] $t(1689)=56{,}89$; $p<.001$
[9] $t=4{,}46$; $p<.001$

resp. 2,70 en 2,91). Wat betreft opleiding en leeftijd zijn er geen significante verschillen in de risicoperceptie gevonden.



Figuur 3. Optimistic bias met betrekking tot de kans op slachtofferschap

Uit de interviews komt een beeld naar voren dat jongeren zichzelf zeer vaardig inschatten wat betreft het herkennen van bedreigingen (zoals een phishing-mail). Over de toekomst zijn ze wat onzekerder, omdat criminelen steeds slimmere technieken in zullen zetten. Als ze al slachtoffer worden, ligt de schuld vaak bij iemand anders (bijvoorbeeld door een datalek). Ze zien zichzelf ook niet als een interessant doelwit.

Citaten uit de interviews over de eigen kans op slachtofferschap:

> *"Ik schat mij hoger in dan de gemiddelde Nederlander. Het klinkt misschien arrogant, maar het is wel realistisch."* (jongere2)
>
> *"Ik denk dat er wel een kans is dat mijn data gelekt wordt. Niet door mijzelf denk ik, nee. Dat er gewoon een bedrijf wordt gehackt waar mijn gegevens zijn."* (jongere6)
>
> *"Van phishing zou ik niet snel slachtoffer van zijn maar als je ook…. Ransomware en DDoS-aanvallen, daar kan iedereen slachtoffer van worden in principe."* (jongere10)
>
> *"Op het moment dat ik de phishingmails kan vermijden, waarvan ik overtuigd van ben dat ik dat kan, zie ik niet in hoe ik daarvan slachtoffer word."* (jongere11)
>
> *"Ik zou niet weten waarom mensen data, wachtwoorden of gegevens van mij nodig hebben."* (jongere19)

Wat betreft andere mensen worden door de geïnterviewde jongeren een aantal categorieën met name als kwetsbaar gezien: ouderen, kinderen, en mensen met een lager IQ.

In de enquête is gevraagd naar de potentiele, negatieve gevolgen van slachtofferschap. Deze worden relatief hoog ingeschat: 3,80 (op een schaal van 1 tot 6). Ook hier zien we dat mannen deze effecten significant[10] lager inschatten dan vrouwen (gemiddeld resp. 3,72 en 3,85). Vrouwen hebben daarmee een significant hogere risicoperceptie dan mannen. Wanneer we kijken naar opleidingsniveau, dan zien we dat hoger opgeleiden de negatieve gevolgen van slachtofferschap hoger inschatten dan lager opgeleiden. Met andere woorden, jongeren van het (V)MBO schatten hun kansen optimistischer in. Er zijn geen significante verschillen tussen leeftijdsgroepen gevonden.

4.2.3 Bewustzijn van mogelijke risico's en effecten van cybercriminaliteit (kwetsbaarheid)

Op de vraag of respondenten weten welke risico's zij lopen om slachtoffer te worden van cybercriminaliteit, geeft 41% aan het grotendeels of volledig te weten. Ruim de helft (52%) zegt een beetje of enigszins een beeld te hebben van zijn/haar persoonlijke risico's, terwijl 7% zegt dit helemaal niet te weten.

De interviews bevestigen dat jongeren niet zeker weten wat de risico's inhouden, wat criminelen bijvoorbeeld met hun gegevens kunnen doen. Genoemde risico's zijn de inbreuk op de persoonlijke levenssfeer (bijvoorbeeld door het verliezen van persoonlijk foto's, waaronder naaktfoto's) inclusief bijbehorende negatieve gevoelens en het verliezen van persoonlijke gegevens (inloggegevens) die gebruikt kunnen worden om geld afhandig te maken.

Citaten uit de interviews over risicobewustzijn:

> *"Je gevoel van privacy en je vertrouwen in de technische wereld zeg maar."* (jongere9)
>
> *"Materiële schade komt je wel overheen, maar het is geen prettig idee als je weet dat je gegevens op straat liggen."* (jongere10)
>
> *"Dan heb je bankgegevens ingevuld of inloggegevens en dan kunnen ze jou geld afhandig maken."* (jongere12)

[10] t=2,98; p<.01

"Stalken. Stel je bent op Facebook en je krijgt een bericht van John en die ziet er heel aantrekkelijk uit. Je begint met hem te praten en hij gaat je stalken." (jongere17)

"Dat is een van de grootste dingen die je in je leven tegen kunt hebben, dat naaktfoto's van jou op het internet zijn. Dat is iets wat je niet kan terugdraaien." (jongere20)

"Dat je een keylogger hebt. Dat alles wat je typt dat ze dat kunnen zien en dat ze al je wachtwoorden kunnen achterhalen." (jongere22)

"Als je mijn emailadres hebt dan weet je bijvoorbeeld waar ik deze week op naar vakantie ga. En dan weet je ook wat mijn vluchtnummer is en met wat voor creditcardnummer ik heb betaald. Dat weet je, dat staat in mijn email. Ik heb een paspoortfoto naar [noemt naam] toegestuurd. Dat is wel heel erg, hele persoonlijke dingen staan erin. Je kan denk ik heel veel met mijn emailadres. Eng veel." (jongere27)

"Persoonlijk een breuk denk ik. Daar zou ik mij echt voor schamen en daar zou ik mij echt onzeker over voelen. ''Waarom ik? Waarom hebben ze mij gepakt? Wat is er bijzonder aan mij of juist raar aan mij? Ben ik zo'n makkelijk doelwit? Ben ik zelf heel erg naïef geweest om alles op Facebook te zetten? Heb ik mijn profiel niet goed beschermd? Waarom ben ik doelwit? Hebben ze iets tegen mij?'' Dat zou ik echt eng vinden." (jongere27)

"Gehackt via facebook zeg je (…) Dan heb je wel veel gegevens van mij (…) Ik connect daar ongeveer alles aan. Het is wel gelinkt aan veel accounts." (jongere28)

4.3 Deelvraag 2: In hoeverre weten jongeren hoe zij zichzelf kunnen beschermen tegen of voorbereiden op de risico's van cybercriminaliteit?

Voor het beantwoorden van deze deelvraag kijken we naar hoe de jongeren hun eigen kennis inschatten over hoe ze zich kunnen beschermen, waar ze op letten om gevaren te herkennen, en wat ze zouden doen mochten ze toch onverhoopt slachtoffer worden.

Wanneer het gaat om zelfbeschermend gedrag, dan geeft 34% aan grotendeels of volledig te weten hoe hij/ zij zichzelf kan beschermen tegen de risico's van cybercriminaliteit, 60% een beetje of enigszins en 6% helemaal niet. Ongeveer twee derde van de geënquêteerden heeft dus twijfels over hoe ze zich kunnen beschermen.

De geïnterviewde jongeren zijn alert op bijvoorbeeld phishingmails en het veranderen van wachtwoorden. Echter, kennis over de werking van en het updaten van virusscanners ontbreekt nogal eens.

> *"Op mijn telefoon heb ik geen virusscanner en heel veel mensen niet. Soms zie je een reclame van: ''neem nu een virusscanner ook op je telefoon.'' En ik denk dat daar nog wel wat zinnigs in zit. Daar zou ik nog wat aan kunnen doen"* (jongere2)
>
> *"Door op zulke links te klikken of als je een mailtje krijgt, die onzin van: "je hebt dit en dit gewonnen.'' Als ik de afzender niet ken doe ik dat niet."* (jongere4)
>
> *"Ik denk dat het sowieso goed is om regelmatig je wachtwoord te veranderen. Dat het niet hetzelfde wachtwoord is bij 10 duizend miljoen verschillende dingen. En niet meer gegevens gegeven dan nodig is. Als een webshop vraagt om telefoonnummers, ja, alsof H&M mij ooit zou bellen"* (jongere6)
>
> *"Ik zorg dat ik van een veilige internetverbinding gebruik maak."*(jongere12)
>
> *"Geen gegevens op onbeveiligde netwerken versturen. Een back-up maken van belangrijke bestanden. Geen naaktfoto's sturen. Dat is het wel."* (jongere21)
>
> *"Laatst heb ik toevallig ook iets gedaan waar ik de hele nacht mee bezig was: mijn foto's van Facebook verwijderd. Dat ik wat minder zichtbaar ben online. Maar aan de andere kant staat mijn Instagram wel open."* (jongere28)

Van de geënquêteerden geeft 40% aan naar eigen inschatting grotendeels/volledig in staat te zijn een (poging tot) cybercriminaliteit te kunnen herkennen, 50% een beetje/enigszins, en 9% helemaal niet.

Met het herkennen van phishingmails hebben de meeste geïnterviewden naar eigen zeggen geen moeite: er wordt gelet op e-mailadres, de aanhef (met of zonder naam), taalgebruik, layout, of de mail verwacht wordt, et cetera. Ter illustratie enkele citaten uit de interviews:

> *"Een bank stuurt jou nooit een mailtje. Altijd een brief of ze bellen je, dus dan vind ik het niet betrouwbaar. (…) Bij track en trace ga ik kijken of mijn naam erbij staat, gaan ze het echt naar mij richten, zit mijn persoonlijke informatie erbij? Ja? Dan is het betrouwbaar, in ieder geval betrouwbaarder. Staan er rare links bij, dan is het niet betrouwbaar."* (jongere1)
>
> *"Niet persoonlijk aan mij geadresseerd, slecht Engels, slecht Nederlands bijvoorbeeld. Of een site waar ik nooit wat mee heb gehad die mij een bericht stuurt."* (jongere5)

> *"Als ik weet dat er een mail komt van de Rabobank of een dergelijke partij… Als ik dat weet open ik het. Als ik bijvoorbeeld een nieuwe bankpas aanvraag of een rekening open. Tuurlijk, dan weet ik dat er iets binnenkomt en verwacht ik het ook. Als het op een onverwachts moment komt over iets waarvan ik weet: ''daar heb ik mij de afgelopen weken helemaal niet mee bezig gehouden.'' Dan open ik het bij voorbaat al niet."* (jongere15)
>
> *"Nu begint mijn universiteit en dan krijg ik wel mailtjes van de Rijksuniversiteit van Groningen dat ik mij moet aanmelden voor de introductieweek. Stel iemand weet dat en maakt zo'n hele e-mail na, dat het er dan precies hetzelfde uitziet, dan zou ik er misschien wel voor vallen"* (jongere18)

Over de kans om ransomware te omzeilen is men minder positief:

> *"Ik ben bang voor het andere waar ik geen kennis van hebt, dat van die bitcoins in dat voorbeeld. Ja, daarvoor ben ik wel bang. Ik denk niet dat ik voldoende beschermd ben tegen ransomware."* (jongere17)
>
> *"Ik ken gewoon dingen niet. Dan kan ik er makkelijk intrappen. Ransomware. Ik ken dat niet."* (jongere24)

Over wat men moet doen wanneer men denkt slachtoffer te zijn geworden, zijn jongeren minder zelfverzekerd: slechts 24% geeft aan te weten wat dan te doen, terwijl ook 24% helemaal niet weet wat te doen en 53% denkt een beetje of enigszins te weten wat dan te doen. Hier zien we dat mannen significant[11] meer vertrouwen hebben in het eigen kunnen dan vrouwen (gemiddeld respectievelijk 3.14 en 2.69).

Met betrekking tot de kans om het slachtoffer worden van phishing is er veel onduidelijkheid. De geïnterviewden zeiden o.a. het volgende:

> *"Ik denk dat als ik een mail zou hebben waar mijn bankgegevens gestolen worden, dan zou ik eerst naar de bank gaan en daarna naar de politie."*(jongere2)
>
> *"Geen idee. Ik denk dat ik zou googlen: 'Hackalert!', 'Hackpolitie, wat moet ik doen?'"* (jongere3)
>
> *"Als ze je betaalgegevens dan hebben zou ik het niet weten wat ik moet doen."*(jongere7)

[11] $t=10.86$; $p<.001$

"Als er echt geld verloren is gegaan, dan ben ik gewoon bang dat je het kwijt bent. Ik weet niet echt of er een oplossing voor is." (jongere19)

"Nee, ik denk dat ik niks zou doen eigenlijk. Ik zou er niet bij nadenken. Ik zou denken: 'O, ik heb hier op geklikt, ik sluit het weer snel.' Verder gewoon doorgaan met mijn leven en niet aan denken, totdat ik tegenkom van 'hee, dit klopt niet.' Dan zou ik denken: 'hee, ik heb laatst op dat mailtje gedrukt.'" (jongere24)

In het geval de geïnterviewden het slachtoffer zouden worden van ransomware, dan worden er vooral emotionele reacties getoond en psychologische beschermingsmechanismen tentoongesteld:

"Ik zou eerst een kwartier tot een half uur in paniek zijn en met dingen gaan gooien uit frustratie. En ook huilen trouwens. Zo van: ''waarom ik altijd?'' Daarna zou ik mijn laptop afsluiten en mijn vriend bellen. Dan zou ik gelijk de politie bellen omdat ik maar 3 dagen heb." (jongere3)

"Heel snel wegklikken alles. (…) ik zou niet weten wat ik anders zou kunnen doen. Ja, heel snel mijn computer laten scannen door de virusscan. Dan zou ik ook doen, een volledige systeemscan." (jongere4)

"Ik zou in paniek schieten. Ik zou heel erg in paniek schieten." (jongere25)

"Ik zou sowieso niet betalen. (…) Omdat ik weiger om te onderhandelen met zulke mensen zeg maar." (jongere8)

"Als het nu gebeurt en iemand heeft mijn laptop, dan denk ik: 'jochie, veel plezier ermee want ik zit er toch over te denken om een nieuwe te kopen'" (jongere11)

"Ik zou 'm uit het raam gooien want ik heb er niks belangrijks opstaan. (…) Ja, je laat je toch niet afpersen. Ik koop gewoon een nieuwe laptop." (jongere16)

"Ik zou schreeuwen: 'Joh fucking slim!' En dan zou ik boos worden en daarna zou ik 'm naar het reparatiecentrum brengen, klaar." (jongere17)

Effectiviteitsverwachtingen

Effectiviteitsverwachtingen betreffen: (I) de zelfeffectiviteit (in hoeverre acht men zichzelf in staat te beschermen tegen of adequaat te handelen bij cybercriminaliteit);(II) responseffectiviteit (in hoeverre

beoordeelt men handelingsperspectieven als nuttig) en (III) gedragseffectiviteit (in hoeverre acht men huidig zelfbeschermend gedrag als effectief).

Zelfeffectiviteit

De mate waarin respondenten zichzelf in staat achten zich tegen cybercriminaliteit te beschermen is gemiddeld (2.93). Opvallend is, dat mannen gemiddeld significant meer vertrouwen hebben in hun eigen kunnen dan vrouwen (3.13 vs. 2.67)[12] Op de stelling: *"Ik vind het lastig om me goed te beschermen tegen cybercriminaliteit"* scoren mannen (gemiddeld 3.11) dan ook significant lager dan vrouwen (gemiddeld 3.48).

Ook is er een significante, positieve samenhang tussen leeftijd en zelfeffectiviteit; hoe ouder de respondent, hoe meer vertrouwen hij/zij heeft in eigen kunnen om zichzelf te beschermen[13]. Dat betekent dat relatief jongere respondenten zichzelf minder goed in staat achten om zich tegen cybercriminaliteit te beschermen.

Responseffectiviteit

De respondenten zien zeker het nut in van het nemen van voorbereidingsmaatregelen of het uitvoeren van zelfbeschermend gedrag (gemiddeld 3.97). Maar liefst 91% is het (helemaal) eens met de stelling: *"Het is nuttig om maatregelen te treffen om jezelf te beschermen tegen cybercriminaliteit".*

Uit nadere analyses blijkt dat opleidingsniveau samenhangt met responseffectiviteit, waarmee hoger opgeleiden zelfbeschermend gedrag als nuttiger beschouwen dan lager opgeleiden.

Gedragseffectiviteit

Aan respondenten is gevraagd in hoeverre zij vinden dat hun huidige gedrag hen beschermt tegen de risico's van cybercriminaliteit. Dit wordt als gemiddeld beoordeeld (3.28 op een vijfpuntsschaal). De meningen zijn echter sterk verdeeld; 24% vindt dat hij/zij zich onvoldoende beschermt tegen cybercriminaliteit, tegenover 44% die van mening is dat hij/zij zich voldoende beschermt.

Bijna de helft van de respondenten (48%) vindt dat de door hem/haar genomen maatregelen ervoor zorgen dat hij/zij minder kans heeft om slachtoffer te worden van cybercriminaliteit. Wanneer we kijken naar verschillen tussen geslacht, leeftijd en opleiding, zien we dat mannen vinden dat zij zichzelf beter

[12] $t=10.43$; $p<.001$
[13] $r=.07$; $p<.01$

beschermen dan vrouwen (3.42 versus 3.11)[14]. Leeftijd is positief gecorreleerd met gedragseffectiviteit[15], wat betekent dat hoe ouder de respondent, hoe beter hij/zij vindt dat hij/zij beschermd is.

4.4. Deelvraag 3: In welke mate vertonen jongeren zelfbeschermend gedrag ten aanzien van cybercriminaliteit?

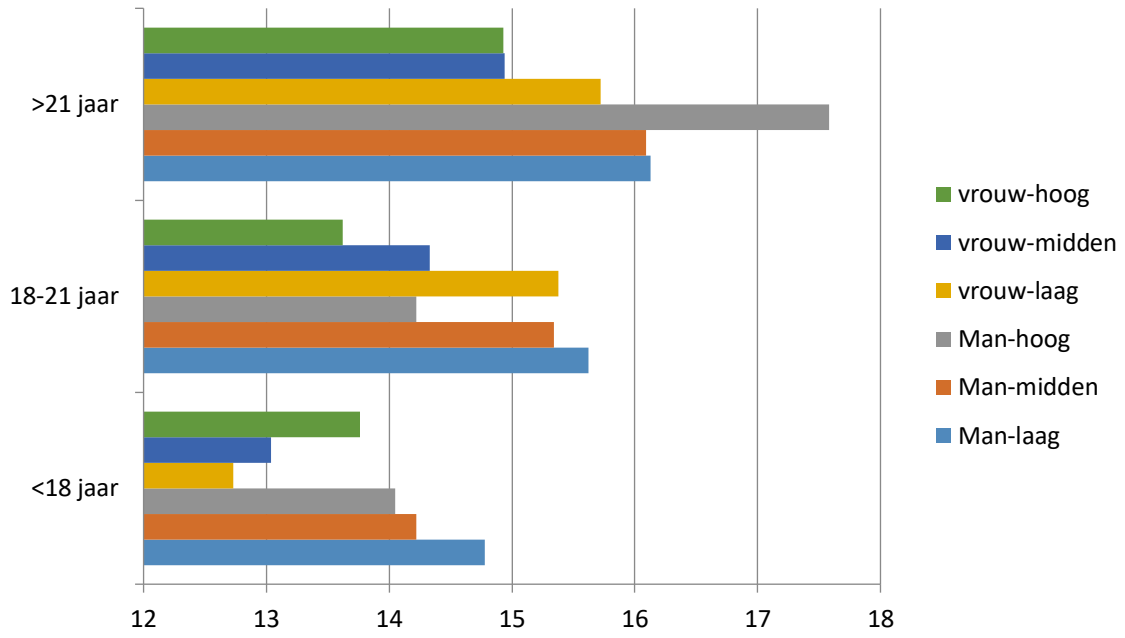
De geënquêteerde jongeren is gevraagd welke zelfbeschermende maatregelen zij reeds uitvoeren. Zij konden van 24 maatregelen aangeven of zij deze hanteren en daarnaast of er andere, niet in de vragenlijst aangedragen maatregelen zijn die zij uitvoeren. De respondenten voeren gemiddeld 15 van de 24 zelfbeschermende maatregelen uit. In Bijlage 3 is een overzicht opgenomen van alle zelfbeschermende maatregelen. De meest voorkomende zijn:

1. Vergrendelingscodes en wachtwoorden gebruiken voor devices (75%)
2. Inloggegevens niet delen (74%)
3. Vergrendelen devices wanneer deze niet in gebruik zijn (73%)
4. Verschillende wachtwoorden voor verschillende toepassingen gebruiken (71%)
5. Controleren van afzenders van berichten op betrouwbaarheid (70%)

Uit aanvullende analyses blijkt dat mannen significant[16] meer zelfbeschermend gedrag vertonen dan vrouwen ((zeer) hoog respectievelijk 50% en 39%). Daarnaast vertonen 'jongere' jongeren significant[17] minder zelfbeschermend gedrag dan 'oudere jongeren'. Van de jongste groep (tot 18 jaar) vertoont 66% een lage mate van zelfbeschermend gedrag, van de middelste leeftijdsgroep (18-21 jaar) is dat 55% en bij de oudste groep (22-25 jaar) is dat 45%. Er zijn geen significante effecten van opleidingsniveau op zelfbeschermend gedrag gevonden.

Wanneer we respondenten indelen op leeftijd, geslacht en opleidingsniveau, dan springen de jonge (<18 jaar), lager opgeleide vrouwen eruit; hiervan vertoont maar liefst 94% een lage mate van zelfbeschermend gedrag. 'Oudere' jongeren en mannen vertonen daarmee meer zelfbeschermend gedrag dan de 'jonge' jongeren en vrouwen (Figuur 4).

[14] $t=6.94$; $p<.001$
[15] $r=.10$; $p<.001$
[16] $t=4.48$; $p<.001$
[17] $X^2 = 45.67$; $p<.001$



Figuur 4. Zelfbeschermend gedrag naar geslacht, leeftijd en opleidingsniveau

Uit de verklarende statistiek blijkt dat lager opgeleide, jonge vrouwen een significant lagere mate van zelfbeschermend gedrag rapporteren dan de rest van de populatie[18].

Om inzicht te krijgen in de mogelijk achterliggende redenen van het lagere zelfbeschermend gedrag onder deze specifieke doelgroep, is getoetst op welke variabelen deze specifieke doelgroep afwijkt van de rest van de populatie. Hieruit blijkt, dat deze doelgroep significant lager scoort op effectiviteitsverwachtingen (beoordeeld nut[19] en uitvoerbaarheid[20] van zelfbeschermende maatregelen) en significant hoger op sociale invloed[21]. Dit impliceert dat zij zichzelf minder goed in staat achten te beschermen tegen cybercriminaliteit en ook het nut van zelfbeschermende maatregelen ook lager beoordelen. Daarnaast zijn zij gemotiveerder om te voldoen aan een sociale norm (de 'motivation to comply'); dat wil zeggen, dat zij sneller geneigd zijn hun gedrag aan te passen, wanneer zij het idee hebben dat dat vanuit de sociale omgeving van hen wordt verwacht.

Over hun zelfbeschermende gedrag zeggen de geïnterviewde jongeren onder andere het volgende:

[18] t=3.34; p<.001
[19] t=3.15; p<.01
[20] t=1.92; p<.10
[21] t=-2.34; p<.05

"Als je geen vrienden met mij bent op Facebook kan je niet veel zien. Instagram hetzelfde. Mijn locatie kan je ook niet zien. Ik post ook bijna niets. Ik post sowieso niet dat ik met vakantie ben i.v.m. inbreken. Stuur gewoon naderhand: ''leuke vakantie gehad en nu weer lekker thuis.'' (jongere1)

"Ik heb ook thuis een speciaal boekje met wachtwoorden die ik nooit ergens mee naartoe neem." (jongere3)

"Ik ben er nu wel panisch mee dat als ik een laptop koop, het eerste wat ik doe is een virusscan installeren. Zonder virusscanner ga ik niet het internet op."(jongere4)

"Goed opletten bij mailtjes en niet goedgelovig zijn" (jongere7)

[Heb je een virusscanner?] "Weet ik niet." [Je hebt geen maatregelen genomen om jezelf te beschermen?] "Nee, ik heb er geen verstand van. Ik zou echt niet weten wat ik zou moeten doen." (jongere8)

"Een antivirusprogramma, maar die is al heel lang verlopen en die doe ik niet updaten. Dat is het eigenlijk. Verder niet." (jongere9)

"Ik doe wel als ik zo'n mailtje krijg die ik niet vertrouw, dan blokkeer ik 'm gelijk. Dan blokkeer je het adres in principe. En voor de rest, ja, gewoon op de e-mails letten. That's it." (jongere16)

"Ik heb verschillende wachtwoorden voor verschillende accounts. Tenminste, dat probeer ik." (jongere19)

"Ik gebruik dus altijd virusscanners. Ik gebruik zo weinig mogelijk social media. Ik heb mijn GPS bijna altijd uitstaan. Ik bankier nooit op willekeurige wifi. Ik verander mijn wachtwoord regelmatig." (jongere20)

"Ik heb een pleister op mijn webcam" (jongere21)

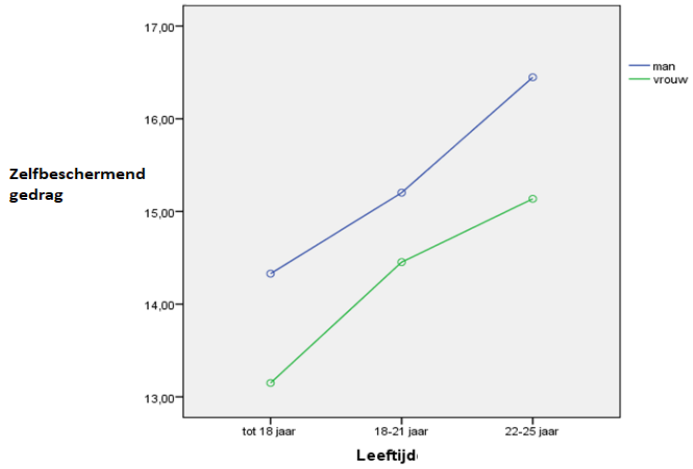
"Ook bij de virusscanner heb ik vragen van: 'ik heb 'm wel, maar is het nodig om een betaalde versie te hebben of is de gratis versie ook genoeg?'"' (jongere23)

"Volgens mij kan je ook zo'n antivirus op je laptop zetten, antimaatregelen.[Doe je dat zelf ook?] Nee. [Waarom niet?] Weet ik niet." (jongere24)

4.5. Deelvraag 4: Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren bij cybercriminaliteit?

4.5.1. Huidig zelfbeschermend gedrag

Er is getoetst in welke mate leeftijd, geslacht en opleidingsniveau van invloed zijn op het uitvoeren van zelfbeschermend gedrag. Hierbij is een direct effect gevonden van leeftijd en geslacht op zelfbeschermend gedrag, waarbij jongeren (tot 18 jaar)[22] en vrouwen[23] significant minder zelfbeschermend gedrag vertonen (Figuur 5). Daarnaast blijkt, dat lager opgeleide jongeren[24] significant minder zelfbeschermend gedrag vertonen dan de middelbare en hoger opgeleide jongeren.



Figuur 5. Zelfbeschermend gedrag naar geslacht en leeftijd

4.5.2. Toekomstig zelfbeschermend gedrag

Op de vraag of respondenten voornemens zijn om in de toekomst aanvullende of voorbereidende maatregelen te treffen tegen cybercriminaliteit, geeft een ruime meerderheid van de respondenten aan dit waarschijnlijk of zeker wel te gaan doen (62%).

Persoonlijke factoren

Uit aanvullende analyses blijkt, dat de intenties tot zelfbeschermend gedrag onder vrouwen hoger[25] is dan die onder mannen, en dat leeftijd positief samenhangt[26] met gedragsintenties. Dit impliceert dat

[22] F=19,90; p<.001
[23] F=18.12; p<.001
[24] P<.05
[25] t=3.28; p<.001
[26] r=.12; p<.001

'oudere' jongeren en vrouwen meer geneigd zijn om in de toekomst aanvullende zelfbeschermende maatregelen te gaan treffen, dan de jongere en mannelijke respondenten.

Daarnaast hangt ervaring met cybercriminaliteit (slachtofferschap) ook samen met het hebben van grotere intenties tot zelfbeschermend gedrag, waarbij jongeren die al slachtoffer zijn geworden de grootste intentie[27] hebben om in de toekomst zelfbeschermend gedrag te gaan uitvoeren (71%, tegen 61% van de jongeren die geen ervaring hebben met slachtofferschap). Er is geen significante samenhang tussen opleidingsniveau en gedragsintenties aangetroffen.

Verder blijkt, dat wanneer men het persoonlijke risico als groter inschat[28] en zelfbeschermend gedrag als uitvoerbaar[29] en nuttig[30] beschouwt, men eerder geneigd is zelfbeschermende maatregelen te treffen. Ook zien we dat hoe groter het huidige zelfbeschermende gedrag is, hoe groter de intenties zijn om zichzelf in de toekomst ook te (blijven) beschermen[31].

Sociale invloed

Op de vraag of mensen in hun omgeving het belangrijk vinden dat zij zichzelf beschermen tegen cybercriminaliteit, zijn de meningen verdeeld: 44% geeft aan het hier (volledig) mee eens te zijn, 23% is het hier (volledig) mee oneens en 33% is het hier niet mee eens/niet mee oneens. Wel geeft bijna de helft van de respondenten aan (47%) dat mensen in hun omgeving verwachten dat zij zich beschermen tegen cybercriminaliteit. Hier zien we verschillen tussen mannen en vrouwen; vrouwen scoren significant hoger op subjectieve normen dan mannen[32].

Bij sociale invloed kijken we naast de waargenomen subjectieve normen naar de motivatie van respondenten om aan deze normen te voldoen (de zogenoemde 'motivation to comply'). Deze is iets onder het gemiddelde (2.92). Ook hier zien we dat vrouwen hoger scoren; zij zijn eerder geneigd te voldoen aan waargenomen subjectieve normen om zich te beschermen tegen cybercriminaliteit[33]. Zowel opleidingsniveau als leeftijd hangt niet samen met de motivation to comply.

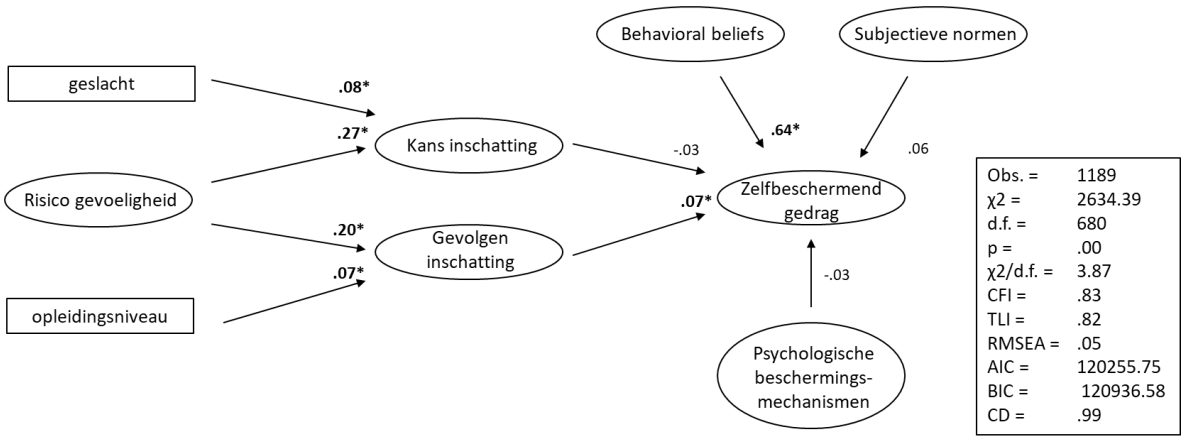
[27] $t=1.88$; $p<.10$
[28] $r=.17$; $p<.001$
[29] $r=.09$; $p<.001$
[30] $r=.14$; $p<.001$
[31] $r=.21$; $p<.001$
[32] $t=3.77$; $p<.001$
[33] $t=4.46p$; $p<.001$

Eigen verantwoordelijkheid

Het overgrote deel van de respondenten (81%) geeft aan dat hij/zij het een eigen verantwoordelijkheid vindt om zichzelf te beschermen tegen cybercriminaliteit. Hierbij zien we dat eigen verantwoordelijkheid ook samenhangt met zelfbeschermend gedrag. Van de personen die op dit moment zeer laag scoren op zelfbeschermend gedrag vindt 73% het de eigen verantwoordelijkheid, terwijl van de respondenten die zeer hoog scoren op zelfbeschermend gedrag 86% vindt dat het de eigen verantwoordelijkheid is om jezelf te beschermen tegen de risico's van cybercriminaliteit.

Toetsing Cyber Resilience Model

Om inzicht te krijgen in welke factoren daadwerkelijk bijdragen aan het uitvoeren van zelfbeschermend gedrag, is het Cyber Resilience Model getoetst. In Figuur 6 is het resultaat van het paddiagram weergegeven; een grafische weergave van de veronderstelde verbanden tussen de factoren in het model, getoetst op de empirische gegevens van de jongeren. Bij de pijlen tussen de factoren zijn de sterktes van de verbanden weergegeven in coëfficiënten. Wanneer deze coëfficiënten significant zijn (dus niet op toeval berust), is dit met een asterisk (*) aangegeven. De RMSEA - Root Mean Square Error of Approximation - is voor dit model geschat op .05. Ook de overige fit-indices gaven een redelijk goede tot goede uitslag. Dit betekent dat het pad diagram goed op de aangetroffen structuren in de data past.



Figuur 6. Cyber Resilience Model bij jongeren

Uit de modeltoetsing blijkt dat het zelfbeschermend gedrag het sterkst wordt beïnvloed door de effectiviteitsverwachtingen ('behavioral beliefs'). Deze hebben een sterke positieve invloed op het zelfbeschermende gedrag. Dat betekent, dat wanneer jongeren meer het nut inzien van zelfbeschermende

maatregelen en zichzelf in staat achten deze ook uit te voeren, ze meer zelfbeschermende maatregelen nemen. Daarnaast zijn ook percepties van de ernst van de gevolgen direct van invloed op het uitvoeren van zelfbeschermend gedrag; wanneer de mogelijke gevolgen als ernstiger worden ingeschat, vertonen ze meer zelfbeschermend gedrag. Deze inschatting van de gevolgen wordt beïnvloed door zowel het opleidingsniveau (hoger opgeleiden schatten deze gevolgen hoger in dan lager opgeleiden) en de risicogevoeligheid (jongeren die gevoeliger zijn voor risico's, schatten deze gevolgen ook hoger in).

Geslacht en risicogevoeligheid hebben beiden invloed op de kansinschatting, maar deze laatste is niet significant van invloed op het zelfbeschermend gedrag bij jongeren. Datzelfde geldt voor de subjectieve normen; de perceptie dat de sociale omgeving verwacht dat men zichzelf voorbereidt op cybercriminaliteit, heeft geen significante invloed op de mate van zelfbeschermend gedrag.

4.6. Deelvraag 5: Op welke factoren ten aanzien van cybercriminaliteit moeten campagnes zich richten om gedragsverandering bij jongeren te stimuleren?

Uit deelvraag 4 blijkt dat de volgende factoren een rol spelen bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren bij cybercriminaliteit:

1. Persoonlijke kenmerken:
    a. Opleidingsniveau
    b. Leeftijd
    c. Geslacht
    d. Risicogevoeligheid
2. Effectiviteitsverwachtingen:
    a. Zelfeffectiviteit (uitvoerbaarheid zelfbeschermende maatregelen)
    b. Responseffectiviteit (beoordeeld nut van zelfbeschermende maatregelen)
3. Ervaring met slachtofferschap
4. Perceptie van eigen verantwoordelijkheid om jezelf te beschermen

Daarnaast is gevonden dat de intenties om in de toekomst aanvullende zelfbeschermende maatregelen samenhangen met leeftijd en geslacht, waarbij jongere vrouwen de laagste intenties hebben om zichzelf (beter) te gaan beschermen tegen cybercriminaliteit.

Opvallend is, dat de lager opgeleide, jonge (jonger dan 18 jaar) vrouwen het laagst scoren op zelfbeschermend gedrag.

Daarnaast geeft bijna de helft van de geënquêteerden (44%) aan behoefte te hebben aan meer informatie over hoe men zichzelf beter kan beschermen tegen de risico's van cybercriminaliteit. Opvallend is dat de meerderheid van de vrouwen (56%) behoefte heeft aan meer informatie, terwijl dat bij de mannen slechts ongeveer een derde (37%) is. Ook zien we hier een verschil tussen opleidingsniveau en informatiebehoefte, waarbij lager opgeleiden significant[34] minder behoefte hebben aan informatie dan hoger opgeleiden (geen behoefte: (v)mbo 64%, havo/hbo 55%, (v)wo 46%).

Op de vraag aan welke informatie men dan behoefte heeft geven de vragenlijstrespondenten aan vooral informatie te willen over cybercriminaliteit in zijn algemeenheid en over handelingsperspectieven (zelfbeschermende maatregelen). Behoefte aan informatie het grootst over:

1. **Handelingsperspectieven**
    a. *Hoe kan ik cybercriminaliteit herkennen?*
    b. *Hoe kan ik slachtofferschap voorkomen?*
    c. *Wat kan ik doen om mezelf te beschermen?*
    d. *Wat moet ik doen wanneer ik slachtoffer ben geworden?*
2. **Algemene informatie cybercriminaliteit**
    a. *Wat is cybercriminaliteit?*
    b. *Wat zijn de risico's en voor wie?*
    c. *Welke ontwikkelingen zijn er?*

Dit patroon wordt bevestigd in de interviews. Respondenten wil deze informatie het liefst ontvangen van onafhankelijke en betrouwbare bronnen. Hieronder volgen de meest genoemde:

1. Overheid in de vorm van gemeenten, politie, rijksoverheid;
2. Onafhankelijk experts in de vorm van IT professionals en adviseurs;
3. School door middel van lesprogramma's van reguliere docenten.

Van de respondenten die aangeven behoefte te hebben aan meer informatie geeft bijna de helft (48%) aan voornemens te zijn om zelf actief op zoek te gaan naar informatie over hoe men zich tegen cybercriminaliteit kan beschermen. Hierbinnen zien we geen significante verschillen wanneer we kijken naar opleidingsniveau, geslacht en leeftijd.

[34] $X^2 = 11.28$; $p<.05$

Bij de ontwikkeling van risicocommunicatie campagnes zou daarom (vooral) ingezet moeten worden op de jongere, lager opgeleide vrouwen. Bij deze doelgroep is veel winst te behalen wanneer het gaat om zelfbeschermend gedrag. Als in campagnes of interventies rekening wordt gehouden met de invloed van deze factoren, kan dit het zelfbeschermende gedrag onder jongeren positief beïnvloeden.

Daarnaast is het relevant om in campagnes aandacht te hebben voor de verschillen in beleving en gedrag tussen jongens en meisjes; jongens vertonen een wat hogere mate van zelfvertrouwen in hun eigen zelfbeschermend gedrag, de beoordeling van hun eigen kunnen hierin en daarnaast een lagere inschatting van het risico. Wanneer hieraan voorbij wordt gegaan, zullen jongens ook minder ontvankelijk zijn voor risico-informatie. Het doorbreken van de optimistic bias kan hierbij essentieel zijn; als de focus ligt op de bewustwording dat het iedereen kan overkomen (en dus niet alleen 'anderen') en de persoonlijke kwetsbaarheid wordt vergroot, kan dit een trigger zijn voor het zelfbeschermende gedrag.

Daarnaast is het opvallend, dat leeftijd een sterke invloed heeft op het zelfbeschermende gedrag; de jongere doelgroep (tot 18 jaar) lijkt een kwetsbaardere groep te zijn; hun risicopercepties en gedrag is significant lager dan van oudere jongeren. Hier zal een stuk bewustzijn en kennis een rol spelen.

5. Cyberweerbaarheid bij mkb'ers

In dit hoofdstuk worden de onderzoeksvragen beantwoord die betrekking hebben op de doelgroep mkb'ers. Allereerst staat in paragraaf 5.1 de steekproef en respondenten beschreven. Voor meer details verwijzen we naar de methodische verantwoording van dit rapport. Vervolgens worden de deelvragen die betrekking hebben op het mkb beantwoord. In paragraaf 5.2 staat de vraag centraal hoe mkb'ers risico's en mogelijke schade van cybercriminaliteit ervaren. Paragraaf 5.3 gaat dieper in op hoeverre mkb'ers wetens hoe zij zichzelf kunnen beschermen tegen of voorbereiden op de risico's van cybercriminaliteit. Vervolgens komen het zelfbeschermende gedrag van mkb'ers en de factoren die daarop van invloed zijn aan bod in respectievelijk paragraaf 5.4 en 5.5. Tenslotte geeft paragraaf 5.6 meer inzicht in de factoren waarop campagnes zich moeten richten om zelfbeschermend gedrag bij mkb'ers te stimuleren.

5.1. Steekproef en respondenten

In totaal hebben 631 mkb-ondernemers de vragenlijst bij dit onderzoek ingevuld. Van de respondenten was 59% man. De gemiddelde leeftijd is 57 jaar, met een minimum van 16 jaar en een maximum van 85 jaar. De meeste respondenten (71%) hebben een hoog opleidingsniveau, 22% heeft een middelbaar opleidingsniveau en 7% is laag opgeleid.

De respondenten zijn gemiddeld veel online: 97% is minimaal dagelijks online. Een deel is minstens ieder wakker uur online (19%) of zelfs (bijna) continu online tijdens de uren dat men wakker is (18%). De belangrijkste redenen om online te zijn, zijn: werk (89%), bankieren (86%) en ontspanning (66%).

Daarnaast zijn 25 interviews gehouden met mkb'ers. De groep bestond voor 80% uit mannen en 20% uit vrouwen. De gemiddelde leeftijd was 42 jaar (range 22-64). Het hoogste genoten opleidingsniveau van de deelnemers was als volgt verdeeld: 4% mavo, 8% havo/vwo/gymnasium, 20% mbo, 28% hbo, 40% universiteit. De voornaamste dagbesteding van de groep was werken (92%).

5.2. Deelvraag 1. Hoe beleven mkb'ers de risico's en mogelijke schade van cybercriminaliteit?

Bij de beleving van de risico's en mogelijke schade van cybercriminaliteit voor mkb'ers, behandelen we achtereenvolgens slachtofferschap, risicobewustzijn en risicoperceptie.

5.2.1. Slachtofferschap

Uit het vragenlijstonderzoek blijkt dat een klein deel van de respondenten (8%) het afgelopen jaar slachtoffer is geworden van cybercriminaliteit. Hierbij worden met name het hacken van accounts en websites genoemd.

De personen die slachtoffer zijn geworden, noemen vooral de emotionele schade: men is geschrokken, wordt onzeker en heeft minder vertrouwen in de medemens. Ook schaamte en een gevoel van machteloosheid wordt door sommige respondenten genoemd. Financieel bleef de schade veelal beperkt tot een klein bedrag, of er was helemaal geen financiële schade. Op de vraag of respondenten naar aanleiding van het slachtofferschap het eigen gedrag heeft aangepast, antwoordt een deel dat zij voorzichtiger zijn, hun wachtwoorden hebben veranderd of alerter zijn, bijvoorbeeld door de afzender van e-mails grondiger te controleren. Opvallend is, dat een groot deel ook aangeeft zijn of haar gedrag niet te hebben aangepast. De redenen die hierbij genoemd werden, waren dat ze vinden dat ze voldoende beschermd zijn, of dat ze zichzelf niet in staat achten zich goed te beschermen tegen slachtofferschap van cybercriminaliteit.

Uit de interviews komt een grotere prevalentie van slachtofferschap onder mkb'ers naar voren, waarbij 16 van de 25 geïnterviewden aangeven slachtoffer te zijn geworden van een vorm van cybercriminaliteit[35]. Sommige mkb'ers zijn al meerdere keren slachtoffer geworden. De helft van de slachtoffers (8) heeft schade geleden door dit incident. Een mkb'er (1) heeft directe financiële schade ondervonden, de oorzaken hiervan was fraude via berichtendienst Whatsapp waarbij het slachtoffer 7,5 duizend euro overmaakte naar een dader. Zes slachtoffers geven aan schade te hebben geleden in tijdsverlies, voorbeelden van tijdsverlies zijn om via skimming verloren geld terug te krijgen van de bank, het herstellen van schade aan websites en/of computers na een hack of de tijd die is verloren doordat een ondernemer terug moest naar een drie maanden oude back-up na een ransomware aanval. Alle administratieve werkzaamheden in de verloren drie maanden moesten opnieuw uitgevoerd worden:

> *"Heel veel tijd, voornamelijk mijn tijd. Financieel ook wel (I: Waar zat hem dat in?) omdat ik niet goed kon zien wie er wel en niet had betaald. Er zullen best een aantal facturen tussendoor zijn geglipt waarvan ik niet meer weet of ze betaald hebben. Een sluitende administratieve controle? Nee! Ik heb met de accountant overlegd wat moet ik daar mee want ik moet ook btw aangifte*

[35] De gegevens uit de interviews zijn gebaseerd op een selecte groep respondenten, die niet representatief is voor de doelgroep. De aantallen zijn door deze 'selectie bias' derhalve indicatief.

doen [..]. Ik was uiteindelijk blij dat het jaar afgelopen was, want daar kloppen dingen niet." (mkb11)

Drie ondernemers geven aan imagoschade te hebben geleden, de schade hiervan is natuurlijk niet te kwantificeren maar kan voor een mkb'er groot zijn:

"Het kost wat tijd, het is vervelend en klanten hebben het gezien, dat is eigenlijk onbetaalbaar" (mkb25)

De meerderheid van de slachtoffers (10) heeft naar aanleiding van het ondervonden slachtofferschap zijn of haar gedrag aangepast om toekomstig slachtofferschap te voorkomen. Hierbij wordt vooral gesproken over voorzichtig(er) omgaan met wachtwoorden, de IT leverancier te vragen meer of betere maatregelen te nemen of in te kopen zoals malwarescanners of in de cloud te gaan werken. Slachtoffers kampen met gevoelens van schaamte en eigen verantwoordelijkheid naar aanleiding van het incident:

"Schaamte, ik dacht wat ben ik dom geweest." (mkb20)

"Ik vind het nog steeds wel heel erg dom van mezelf dat ik niet geconstateerd heb dat die beveiliging onvoldoende was want eigenlijk kletst die computer elke dag tegen je maar ik heb niet voldoende beseft." (mkb11)

Desondanks heeft de meerderheid van de mkb'ers (11) met zijn of haar omgeving gesproken over het slachtofferschap, opvallend is dat slachtoffers naast mededogen en ondersteuning vanuit de omgeving ook bevestigd worden in de overtuiging dat slachtofferschap vaak verwijtbaar is:

''Lief en steun, ze begrepen het ook wel omdat ik zo moe was. Ze vonden mij ook wel een beetje naïef, en ze zeiden dat ze het zelf nooit zouden doen'' (mkb23)

Slechts één slachtoffer heeft aangifte gedaan van politie, in een zaak van cyberstalking en identiteitsfraude. De overige slachtoffers hebben geen aangifte gedaan omdat ze weinig vertrouwen hebben in het nut ervan of niet stil staan bij de mogelijkheid van een aangifte.

5.2.2. Bewustzijn

Een ruime meerderheid (63%) van de ondervraagde mkb'ers denkt grotendeels of volledig te weten welke risico's hij/zij loopt om slachtoffer te worden van cybercriminaliteit. Ongeveer een gelijk deel van de respondenten (60%) zegt grotendeels of volledig te weten hoe hij/zij (een poging tot) cybercriminaliteit kan herkennen. Slechts één procent geeft aan het helemaal niet te weten. Over wat men moet doen

wanneer men denkt slachtoffer te zijn geworden, is men wat minder zelfverzekerd: 45% geeft aan dit grotendeels of volledig te weten, ruim de helft geeft aan dit 'een beetje' te weten.

Tabel 1 Kennis en bewustzijn risico's en maatregelen

Ik weet:…	**Helemaal niet**	**Een beetje/ enigszins**	**Grotendeels/ volledig**
…welke risico's ik loop om slachtoffer te worden van cyber-criminaliteit.	1%	36%	63%
…hoe ik (een poging tot) cybercriminaliteit kan herkennen.	2%	38%	60%
…wat ik moet doen wanneer ik slachtoffer word van cyber-criminaliteit.	2%	52%	45%

Uit de interviews is naar voren gekomen dat alle mkb'ers (25) phishing e-mails ontvangen en zeggen op de hoogte zijn van de dreiging van deze berichten, zij geven aan deze te herkennen en te verwijderen. Desgevraagd geven mkb'ers aan bij de herkenning van phishing e-mails vooral te letten op de afzender/ het e-mailadres (21), de strekking van de e-mail (15), de link (7), de spelling en opmaak van de e-mail (11) en of zij de e-mail verwachten (8). Opvallend is dat de helft van de geïnterviewde mkb'ers zich moeilijk een voorstelling kan maken van de schade die slachtofferschap van phishing bij hen zou kunnen berokkenen, zes geven expliciet aan geen idee te hebben. Respondenten die een inschatting maken van mogelijke gevolgen noemen vooral identiteitsfraude (12) onbekende financiële gevolgen (10), meer spam (3), malware (3) of ransomware (2). Daarnaast geven drie mkb'ers aan dat een datalek een gevolg kan zijn van slachtofferschap.

> *"Klantgegevens komen op straat te liggen, dan heb je een datalek. Dat geeft je imago een klap. Het kan daarnaast je klanten geld kosten. Misschien kan je er ook een boete voor krijgen".* (mkb3)

De meerderheid van de geïnterviewde mkb'ers (15) weet niet exact wat te doen bij slachtofferschap en zou een derde persoon zoals een IT'er of een goede bekende voor hulp inschakelen. Ondanks dat mkb'ers aangeven zich voor slachtofferschap te schamen en verwachten dat zij mogelijk uitgelachen zouden worden, geeft veruit de grootste groep (19) aan over slachtofferschap met de omgeving te zullen praten:

> *"Ze zouden normaal reageren: 'Wat klote voor je'. Ze zouden ook wel een beetje lachen, maar alleen als het niet te ernstig is."* (mkb3)

In de interviews gaven de meeste mkb'ers (24) aan nooit persoonlijk geconfronteerd te zijn met ransomware, maar herkennen deze vorm van cybercriminaliteit wel uit het nieuws. De meesten (15) hebben niet direct een idee wat ze zouden moeten doen bij slachtofferschap en geven aan hier een externe expert of (indien aanwezig) de IT-afdeling inschakelen:

> *"(I: Heb je enige idee wat je zou moeten doen?) Nee, ik zou in blinde paniek mijn IT'er bellen. "* (mkb6)

De meerderheid (18) geeft aan nooit te zullen betalen, omdat je geen eigen garantie hebt dat je hiermee daadwerkelijk geholpen bent en uit het principe dat je niet moet onderhandelen met criminelen:

> *"Ze kunnen je blijven chanteren. Als je beveiliging niet op orde is. Je hebt geen garantie dat je je bestanden terug krijgt. Daarnaast wil je niet dat zij geld krijgen, daarmee hou je het in stand."* (mkb20)
>
> *''Daar (betalen) geloof ik niet in, dan zit je enkel in een portaal naar nog meer ellende.''* (mkb7)

Over mogelijk slachtofferschap van ransomware geven mkb'ers aan dat zij dit – in tegenstelling tot phishing - meer als echte criminaliteit zien en zich hiervoor minder zouden schamen en eerder geneigd zijn naar de politie (14). Desondanks hebben de respondenten weinig vertrouwen in de mogelijkheden die politie heeft:

> *"Ik verwacht van de politie dat ze opsporen en oppakken. Maar dat gebeurt nooit. De politie is niet slim genoeg, ze geven het te weinig prioriteit en ze hebben de internationale samenwerking niet op orde."* (mkb22)

5.2.3. Risicoperceptie

Mkb'ers zijn in de vragenlijst gevraagd hoe groot zij de kans achten om zelf het slachtoffer van cybercriminaliteit te worden. Deze kans is iets beneden gemiddeld onder de respondenten: gemiddeld 2.96 (op een 6-puntsschaal). Hierin is geen significant verschil tussen mannen en vrouwen aangetroffen.

Tabel 2 Kansinschatting persoonlijk slachtofferschap

Hoe groot schat u de kans in om de komende 12 maanden *zelf* slachtoffer te worden van …				
	Geen kans	*(heel) klein*	*Niet klein/ niet groot*	*(heel) groot*
Cybercriminaliteit?	5%	63%	25%	6%
Phishing?	11%	56%	19%	10%
Ransomware?	8%	61%	26%	5%

Uit de interviews komt een soortgelijk beeld naar voren, waarbij de grootste groep (16) respondenten aangeeft dat de kans dat zij zelf slachtoffer zullen worden klein of zelf niet aanwezig is. Zij geven wel aan dat dit voor anderen in het bedrijf mogelijk anders is, waardoor de kans voor het bedrijf an sich groter zou kunnen zijn:

> *"Ik ben heel moeilijk op te lichten, maar mijn personeel weet al minder, en hoe meer personeel je hebt…Die denken dan misschien wel: 'Sjors zal dat wel geregeld hebben'."* (mkb7)

De vragenlijstrespondenten schatten in dat een gemiddelde Nederlander een significant grotere kans heeft dan zijzelf om slachtoffer te worden van cybercriminaliteit: 4.28[36] (op een 6-puntsschaal). Dit betekent, dat de 'optimistic bias' van toepassing is op het thema, waarbij men cybercriminaliteit als risico beschouwt, maar zichzelf minder kwetsbaar acht dan anderen.

We zien dit beeld ook terug in de antwoordcategorieën, wanneer we deze vergelijken tussen de kans op persoonlijk slachtofferschap en de kans op slachtofferschap voor een gemiddelde Nederlander: de persoonlijke kans wordt door het grootste deel van de mkb-ondernemers als '(heel) kleine kans' of zelfs 'geen kans' ingeschat, terwijl voor een gemiddelde Nederlander de meeste respondenten dit als '(heel) groot' inschatten.

Tabel 3 Kansinschatting slachtofferschap algemeen

Hoe groot schat u de kans in dat *een gemiddelde Nederlander* de komende 12 maanden slachtoffer wordt van …				
	Geen kans	*(heel) klein*	*Niet klein/ niet groot*	*(heel) groot*
Cybercriminaliteit?	1%	21%	31%	47%
Phishing?	1%	17%	27%	56%
Ransomware?	0%	29%	31%	40%

[36] t=37.8; p<.001

Uit de interviews komt eveneens naar voren dat cybercriminaliteit door respondenten als een groot risico wordt gezien. Het merendeel van de mkb'ers (16) denken dat de afgelopen jaren het risico om slachtoffer te worden is toegenomen, 20 respondenten vinden cybercriminaliteit daarmee een maatschappelijk probleem. Mkb'ers hebben een redelijk duidelijk beeld voor ogen over de groepen in de samenleving die een grotere kans hebben om slachtoffer te worden of kwetsbaarder zijn. Volgens respondenten lopen met name ouderen (19) een vergroot risico door gebrek aan ervaring en kennis:

> *'En de ouderen, dat is een hele kwetsbare groep. Die kunnen het verschil tussen betrouwbaar en onbetrouwbaar niet zien. Dat zijn nog echt de mensen van het touwtje uit de voordeur van Jan Terlouw.'* (mkb7)

Daarnaast worden mensen met een lage opleiding of weinig intelligentie (10) als een risicogroep gezien. Ten slotte worden ook jongeren benoemd als risicogroep, dit wordt met name zo ingeschat door het risicovol of impulsief gedrag dat jongeren vertonen: *"jongeren zijn ook een kwetsbare groep, toen ik 12 was klikte ik echt overal op!"* (mkb23) De negatieve gevolgen van slachtofferschap worden relatief hoog ingeschat: gemiddeld 4.0 (op een 6-puntsschaal). Opvallend is, dat vrouwen de effecten van slachtofferschap negatiever inschatten dan mannen (gemiddeld 4.10 versus 3.93[37]). Er is geen significant verschil aangetroffen tussen de inschatting van negatieve gevolgen en de verschillende opleidingsniveaus of leeftijd van de mkb'ers.

5.2.4. Deelconclusie risicobeleving

Geconcludeerd kan worden dat mkb'ers zich allemaal bewust zijn van de risico's van cybercriminaliteit. Een klein deel is het afgelopen jaar zelf slachtoffer geworden van cybercriminaliteit, maar de schade bleef in veel gevallen beperkt. Wellicht dat dit verklaart waarom slechts een deel van de mkb'ers die slachtoffer zijn geworden zijn of haar gedrag na slachtofferschap heeft aangepast.

Mkb'ers schatten de mogelijk negatieve gevolgen van slachtofferschap relatief hoog in. Echter, de kans op slachtofferschap wordt redelijk laag ingeschat. Opvallend is dat er opnieuw sprake is van een sterke optimistic bias, waarbij men zichzelf significant minder vatbaar acht voor cybercriminaliteit dan andere mensen.

[37] $t=2.44$; $p<.05$

5.3. Deelvraag 2: In hoeverre weten mkb'ers hoe zij zichzelf kunnen beschermen tegen of voorbereiden op de risico's van cybercriminaliteit?

Om antwoord op deelvraag 2 te geven gaat deze paragraaf in op de effectiviteitsverwachtingen van beschermende maatregelen en de kennisbehoefte over mogelijkheden om slachtofferschap van cybercriminaliteit tegen te gaan.

Alle geïnterviewde mkb'ers zijn alert op phishingmails. Zoals in paragraaf 5.2 vermeld, letten zij bij de beoordeling hiervan met name op afzender/ het e-mailadres (21), de strekking van de e-mail (15), de link (7), de spelling en opmaak van de e-mail (11) en of zij de e-mail verwachten (8). Met uitsluiting van 'één respondent - "Niemand zegt wat ik moet doen." (mkb5) - hebben alle geïnterviewde mkb'ers maatregelen genomen tegen cybercriminaliteit. De maatregelen variëren van basismaatregelen als virusscanners, het maken van back-ups, het gebruiken van verschillende en sterke wachtwoorden tot meer geavanceerde maatregelen als tweefactor authenticatie en encryptie. Door verschillende mkb'ers wordt aangegeven dat zij uit gemak en beveiliging in de cloud zijn gaan werken. De meeste mkb'ers vertrouwen voor de maatregelen die zij nemen op een IT leverancier of een persoon in het netwerk.

> *"Via [bedrijf x] is dat gegaan. Wij vertrouwen eigenlijk altijd op [bedrijf x], zij leveren alles. Wij hadden ook hun reviews bekeken. Wij gaan ervan uit dat het goed werkt dan, het is ook een grote partij [..] Nu is dus het goed genoeg beveiligd (I: hoe weet je dat?) Er is al zo lang niets gebeurd.. Wij hebben nooit geïnvesteerd in veiligheid, we hebben gewoon pakketten aangeschaft en daar zit het (beveiliging) bij in."* (mkb21)
>
> *"Als het nodig is doe je het. Dus onze website is nu ook dubbel beveiligd. Hij is gebackupt dus hij draait 2x en we hebben een internetbureau en die doet alle updates en die regelt alle veiligheid."* (mkb23)

Enkele bedrijven (3) hebben een certificering voor informatiebeveiliging of zijn bezig deze te behalen, vanuit deze certificering zitten zij volgens eigen zeggen in een continu proces waarbij zij via een analyse van alle risico's passende maatregelen nemen. Daarnaast zijn het internet en kennissen/collega's bronnen van informatie voor mkb'ers om maatregelen te nemen.

> *"We hebben een on/offboarding procedure, we maken back ups, we houden awareness trainingen, we doen maandelijks een risico analyse, we hebben een firewall, we gebruiken vpn, we gebruiken 2 factor authenticatie en we hebben malwarescanners. (I: en waarom heb je die maat-*

regelen genomen?) Meerdere redenen, de normen (ISO27001 & NEN7510) schrijven het voor. Maar we zien ook het nut omdat het daarmee veiliger wordt". (mkb25)

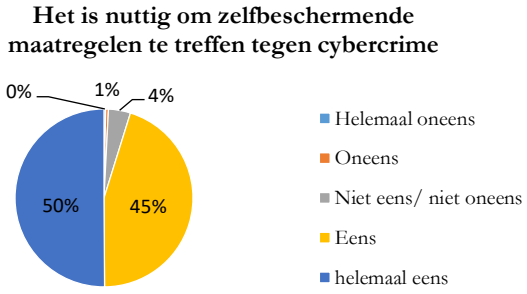
5.3.1. Effectiviteitsverwachtingen

Zelfeffectiviteit

De mate waarin mkb'ers zichzelf in staat achten te beschermen tegen cybercriminaliteit is boven gemiddeld; 3.54 (op een vijfpuntsschaal). Hier zien we dat mannen gemiddeld significant meer vertrouwen hebben in eigen kunnen om zichzelf te beschermen dan vrouwen (3.59 versus 3.46[38]). Uit de verklarende statistiek blijkt, dat vrouwen vooral het idee hebben minder goed te weten welke risico's zij lopen om slachtoffer te worden van cybercriminaliteit (vrouwen: gemiddeld 3.53 versus mannen: gemiddeld 3.71[39]). Zij vinden het echter niet lastiger om zichzelf te beschermen tegen cybercriminaliteit dan mannen. Er is geen samenhang gevonden tussen leeftijd en zelfeffectiviteit.

Responseffectiviteit

De mkb'ers zien het nut in van het nemen van maatregelen of het uitvoeren van zelfbeschermend gedrag met een gemiddelde van 4.43 op een vijfpuntsschaal. Maar liefst 95% geeft aan het (helemaal) eens te zijn met de stelling: "Het is nuttig om maatregelen te treffen om jezelf te beschermen tegen cybercriminaliteit". Geslacht en leeftijd hangen niet significant samen met deze responseffectiviteit.



Figuur 7. Responseffectiviteit

[38] t=2.18; p<.05
[39] T=2.58; p<.01

Uit de interviews komt eenzelfde beeld naar voren. Twaalf geïnterviewde mkb'ers geven expliciet aan het nuttig te vinden maatregelen te nemen. De redenen om dit te doen variëren waarbij de leveranciers of de opvatting van medewerkers, familie of vrienden vaak aanleiding zijn om tot actie over te gaan. Deze personen zijn met name leidend in de maatregelen die worden genomen, de meeste respondenten geven aan zelf op de hoogte te zijn van de risico's en nemen maatregelen.

> *"om gewoon een hele hoop ellende te voorkomen."* (mkb10): *"Ik wil er gewoon alles aan doen om veilig te zijn."* (mkb14)

Hierbij wordt door enkele respondenten wel aangegeven dat de maatregelen in het kostenplaatje van de organisatie moet passen.

5.3.2. Kennisbehoefte

Het merendeel van de respondenten (70%) geeft aan het een eigen verantwoordelijkheid te vinden om beschermd te zijn tegen cybercriminaliteit. Ruim de helft van de respondenten heeft dan ook behoefte aan meer informatie over hoe men zichzelf beter kan beschermen tegen de risico's van cybercriminaliteit. Opvallend is, dat de behoefte aan informatie onder mannen hoger (55%) is dan onder vrouwen (47%). Verder blijkt, dat leeftijd negatief samenhangt met informatiebehoefte[40], wat impliceert dat hoe jonger men is, hoe groter de behoefte aan informatie over het voorkomen van slachtofferschap van cybercriminaliteit is.

Op de vraag aan welke informatie de respondenten dan behoefte heeft, geven respondenten aan vooral informatie te willen over cybercriminaliteit in zijn algemeenheid, de risico's ervan en over handelingsperspectieven (zelfbeschermende maatregelen en gedragsadviezen). De behoefte aan informatie onder mkb'ers is het grootst over:

1. Handelingsperspectieven:
    a. Hoe kan ik (een poging tot) cybercriminaliteit herkennen?
    b. Hoe kan ik slachtofferschap voorkomen; Wat kan ik doen om mezelf te beschermen?
    c. Wat moet ik doen wanneer ik slachtoffer ben geworden?
2. Algemene informatie cybercriminaliteit:
    a. Wat is cybercriminaliteit; welke vormen zijn er?
    b. Wat zijn de risico's en voor wie? Welke effecten?

[40] Correlatie r=-.15; p<.001

c. Wat zijn de ontwikkelingen op het gebied van cybercriminaliteit; nieuwe vormen van cybercriminaliteit?

Men wil deze informatie het liefst ontvangen van onafhankelijke en als betrouwbaar bestempelde bronnen. De meest genoemde zijn: (I) overheden (rijk, gemeente of politie); (II) onafhankelijk experts (IT-professionals en adviseurs)en (III) internet providers. Van de respondenten die aangeven behoefte te hebben aan meer informatie is een meerderheid (67%) voornemens om ook zelf actief op zoek te gaan naar deze informatie.

Uit interviews komt een vergelijkbaar beeld naar voren, waarbij meer dan de helft (13) van de mkb'ers aangeeft behoefte te hebben aan extra informatie over cybercriminaliteit. Hierbij wordt met name aangegeven dat men behoefte heeft aan informatie over nieuwe risico's en ontwikkelingen (8), hierbij is het van belang dat deze informatie is toegespitst op het mkb zelf:

> *"Ik wil kennis van 'normale' cases over hoe het kan gaan. Met bedrijven zoals dat van mij. Wat komt er in de toekomst aan? Zijn wij nu voldoende voorbereid? Dat weet ik niet."* (mkb2)

In het verlengde hiervan hebben bedrijven (7) behoefte aan informatie die input geeft aan het handelingsperspectief van de mkb'er: *"Een soort van checklist wat te doen of maatregelen die je kan nemen."* (mkb22)

5.3.3. Deelconclusie kennis zelfbeschermend gedrag

Mkb'ers zijn verdeeld over hun kennis van zelfbeschermend gedrag ten aanzien van cybercriminaliteit. Een meerderheid zegt redelijk tot goed in staat te zijn zichzelf te beschermen tegen cybercriminaliteit, (een poging tot) cybercriminaliteit te herkennen en te weten welke risico's hij/zij loopt. Maar de andere helft geeft aan dit slechts een beetje of enigszins te weten. Men lijkt, met andere woorden, geen unaniem vertrouwen in het eigen kunnen te hebben voor wat betreft het tegengaan van slachtofferschap van cybercriminaliteit. Vooral over wat men moet doen wanneer men slachtoffer is geworden, is men wat onzekerder. Ruim de helft is ook niet (volledig) overtuigd dat hij/zij zichzelf momenteel voldoende beschermt tegen cybercriminaliteit.

Respondenten zien wel het nut in van zelfbeschermende maatregelen en veel mkb'ers willen hierover ook extra informatie ontvangen. Dit is onder te verdelen in twee categorieën: informatie over cybercriminaliteit in zijn algemeenheid en specifieke informatie over zelfbeschermende maatregelen. Daarnaast

is men welwillend zelf actief naar informatie op zoek te gaan, waarbij er behoefte onder mkb'ers is aan het (snel) kunnen vinden van actuele, betrouwbare en praktisch toepasbare informatie.

5.4. Deelvraag 3: *In welke mate vertonen mkb'ers zelfbeschermend gedrag ten aanzien van cybercriminaliteit?*

5.4.1. Huidig zelfbeschermend gedrag

Respondenten is gevraagd welke zelfbeschermende maatregelen zij reeds uitvoeren. Zij konden van 24 maatregelen aangeven of zij deze hanteren en daarnaast of er andere, niet in de vragenlijst aangedragen maatregelen zijn die zij uitvoeren. De respondenten voeren gemiddeld 18 van de 24 zelfbeschermende maatregelen uit. De meest voorkomende maatregelen onder mkb'ers staan hieronder weergegeven. Het volledige overzicht van zelfbeschermende maatregelen onder mkb'ers staat in Bijlage 3.

1. E-mails die men niet vertrouwt direct verwijderen (99%);
2. Controleren of de afzender van een e-mail betrouwbaar is (98%);
3. Voorzichtig zijn met het openen van bijlagen (96%);
4. Inloggegevens niet aan onbekenden geven (94%);
5. Voorzichtig zijn met het aanklikken van links (93%).

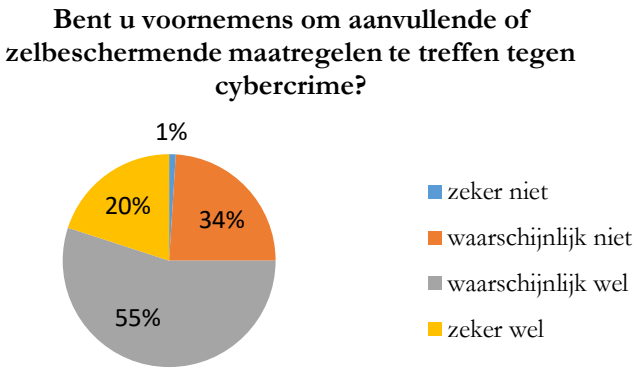
De minst gebruikte zelfbeschermende maatregelen onder de respondenten zijn:

1. Het versleutelen van bestanden met wachtwoorden (28%);
2. Een VPN-verbinding gebruiken (32%);
3. Een browser-extensie (bijv. Adblocker) gebruiken (48%);
4. Een wachtwoord niet voor verschillende toepassingen gebruiken (53%);
5. Vermijden van openbare WiFi-netwerken (58%).

Hierbij zijn geen verschillen gevonden tussen mannen en vrouwen. Ook opleidingsniveau en leeftijd hangen niet samen met het huidige zelfbeschermend gedrag onder mkb'ers.

De meeste mkb'ers (71%) gaven aan voornemens te zijn om in de toekomst waarschijnlijk of zeker aanvullende zelfbeschermende maatregelen te nemen. Hierbij valt op, dat leeftijd positief met deze gedragsintenties samenhangt. Hoe ouder de respondent, hoe meer hij/zij aangeeft geneigd te zijn om in

de toekomst zelfbeschermende maatregelen te gaan treffen[41]. Opvallend is echter dat leeftijd niet samenhangt met het huidige zelfbeschermende gedrag. Ook het hebben van persoonlijke ervaring met slachtofferschap van cyberslachtofferschap hangt niet samen met deze gedragsintenties.



Figuur 8. Gedragsintenties

Onder de mkb'ers hangen de persoonlijke risicoperceptie[42] en het beoordeelde nut van zelfbeschermend[43] gedrag beiden positief samen met de intentie om in de toekomst aanvullende zelfbeschermende maatregelen te treffen. Dit houdt in dat hoe groter men het persoonlijke risico inschat en hoe nuttiger men zelfbeschermende maatregelen beoordeelt, hoe sterker de voornemens om zelfbeschermend gedrag te gaan uitvoeren. Daarnaast blijkt ook, dat hoe meer zelfbeschermende maatregelen[44] men reeds heeft getroffen, hoe groter de neiging is om dit in de toekomst uit te breiden.

Gedragseffectiviteit

Aan mkb'ers is gevraagd in hoeverre zij vinden dat hun huidige gedrag hen beschermt tegen de risico's van cybercriminaliteit (zie tabel 4). Dit wordt als relatief hoog beoordeeld met een gemiddelde van 3.64 op een vijfpuntsschaal. Een grote meerderheid (69%) vindt dat de eigen genomen maatregelen de kans op slachtofferschap verminderen, maar men is iets minder overtuigd of men ook daadwerkelijk voldoende is beschermd (56%). Hierbij is een sterke positieve samenhang te zien tussen gedragseffectiviteit en zelfbeschermende maatregelen[45], wat impliceert dat mkb'ers die meer zelfbeschermende maatregelen hebben genomen, vinden dat zij beter beschermd zijn tegen cybercriminaliteit en dat deze maatre-

[41] Correlatie r=.15; p<.001
[42] Correlatie r=.18; p<.001
[43] Correlatie r=.12; p<.001
[44] Correlatie r=.26; p<.001
[45] Correlatie r=.40; p<.001

gelen ervoor zorgen dat zij minder kans hebben om slachtoffer te worden. Geslacht en leeftijd hangen niet significant samen met deze ervaren gedragseffectiviteit.

Tabel 4 Gedragseffectiviteit

	(helemaal) oneens	Niet oneens / niet eens	(helemaal) Eens
Ik vind dat ik mij voldoende bescherm tegen cybercriminaliteit.	9%	35%	56%
De door mij genomen maatregelen zorgen er voor dat ik minder kans heb om slachtoffer te worden van cybercriminaliteit.	8%	23%	69%

5.4.2. Sociale invloed

Bij sociale invloed kijken we naar de subjectieve normen en de 'motivation to comply'.

Subjectieve normen

Mkb'ers rapporteren relatief hoge waargenomen subjectieve normen; gemiddeld 3.58 op een vijfpuntsschaal. Op de vraag of mensen in hun omgeving het belangrijk vinden dat zij zichzelf beschermen tegen cybercriminaliteit, zijn de meningen verdeeld. Iets meer dan de helft van de respondenten (52%) geeft aan het hier (volledig) mee eens te zijn, 13% is het hier (volledig) mee oneens en 35% is het hier niet mee eens/niet mee oneens.

Op de vraag of mensen in hun omgeving verwachten dat zij zichzelf beschermen tegen cybercriminaliteit, geeft een ruime meerderheid aan dat zij dit zo ervaren (62%). Slechts 9% geeft aan dat dit niet het geval is en bijna een derde weet het niet (30%).

Er zijn geen significante verschillen tussen mannen en vrouwen in de waargenomen subjectieve normen. Leeftijd hangt echter positief samen met subjectieve normen[46]. Dit impliceert, dat hoe ouder de respondent is, hoe groter de waargenomen subjectieve normen.

Motivation to comply

Bij sociale invloed kijken we naast de waargenomen subjectieve normen naar de motivatie van respondenten om aan deze normen te voldoen ('motivation to comply'). Deze is iets onder het gemiddelde; 2.72 op een vijfpuntsschaal. Ook hier zien we dat er geen significante verschillen zijn tussen mannen en

[46] Correlatie r=.14; p<.001

vrouwen, maar wel weer dat leeftijd positief samenhangt met de motivation to comply[47]. Dit impliceert dat hoe ouder de respondent, hoe meer men geneigd is te voldoen aan de subjectieve normen.

5.4.3. Deelconclusie zelfbeschermend gedrag

De meeste mkb'ers vertonen een relatief hoge mate van zelfbeschermend gedrag. Dat wil zeggen, dat zij momenteel reeds veel zelfbeschermende maatregelen hebben getroffen. Toch is een meerderheid voornemens om in de toekomst aanvullende zelfbeschermende maatregelen te treffen. We zien dat deze gedragsintenties onder ouderen hoger zijn dan onder jongeren. Deze voornemens worden vooral ingegeven door een hogere persoonlijke risicoperceptie en een groter beoordeeld nut van zelfbeschermende maatregelen. Daarnaast lijkt onzekerheid over toekomstige ontwikkelingen op het gebied van cybercriminaliteit een rol te spelen: ondanks dat een grote meerderheid vindt dat het huidige zelfbeschermend gedrag de kans op slachtofferschap verkleint, vraagt ongeveer de helft zich af of dit voldoende is om in de toekomst ook goed tegen cybercriminaliteit beschermd te zijn.

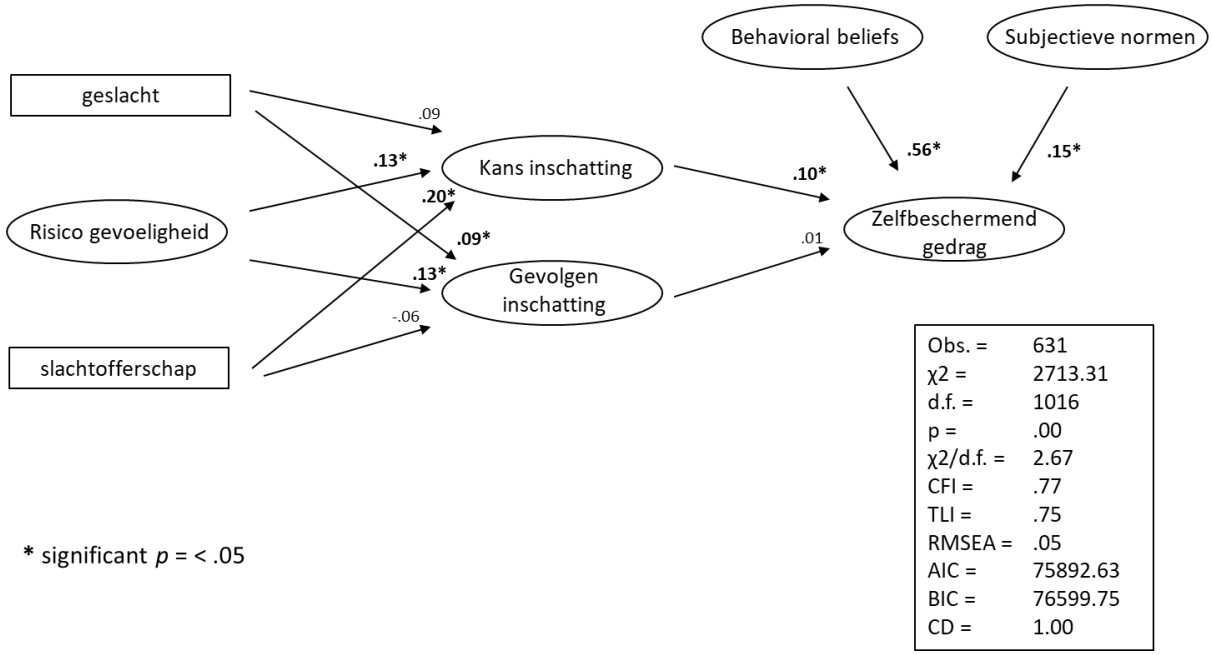
5.5 Deelvraag 4: *Welke factoren spelen een rol bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb'ers bij cybercriminaliteit?*

Op basis van het conceptueel model is getoetst of en in welke mate de voorspellende variabelen van invloed zijn op het zelfbeschermend gedrag van mkb'ers. Hieruit blijkt dat zelfbeschermend gedrag vooral wordt ingegeven door behavioral beliefs (beoordeeld nut en uitvoerbaarheid van zelfbeschermende maatregelen), de kansinschatting van persoonlijk risico en subjectieve normen.

Toetsing Cyber Resilience Model

Om inzicht te krijgen in welke factoren daadwerkelijk bijdragen aan het uitvoeren van zelfbeschermend gedrag onder mkb'ers, is het Cyber Resilience Model getoetst. In Figuur 9 is het resultaat van het pad diagram weergegeven; een grafische weergave van de veronderstelde verbanden tussen de factoren in het model, getoetst op de empirische gegevens van de mkb'ers. Bij de pijlen tussen de factoren zijn de sterktes van de verbanden weergegeven in coëfficiënten. Wanneer deze coëfficiënten significant zijn (dus niet op toeval berust), is dit met een asterisk (*) aangegeven. De RMSEA - Root Mean Square Error of Approximation - is voor dit model geschat op .05. Ook de overige fit-indices gaven een redelijk goede tot goede uitslag. Dit betekent dat het paddiagram goed op de aangetroffen structuren in de data past.

[47] Correlatie r=.12; p<.001



Figuur 9. Cyber Resilience Model bij mkb'ers

Uit de modeltoetsing blijkt dat het zelfbeschermend gedrag vooral wordt ingegeven door de effectiviteitsverwachtingen ('behavioral beliefs'). Deze hebben een sterke positieve invloed op het zelfbeschermende gedrag. Dat betekent, dat wanneer mkb'ers meer het nut inzien van zelfbeschermende maatregelen en zichzelf beter in staat achten deze ook uit te voeren, ze meer zelfbeschermende maatregelen nemen. Daarnaast speelt ook risicoperceptie een belangrijke rol; zowel de kansinschatting om persoonlijk slachtoffer te worden van cybercriminaliteit als de inschatting van de ernst van de gevolgen beïnvloeden direct het zelfbeschermend gedrag; wanneer mkb'ers de kans om persoonlijk slachtoffer te worden hoger inschatten en de mogelijke gevolgen als ernstiger worden ingeschat, vertonen ze meer zelfbeschermend gedrag. Deze risicoperceptie wordt beïnvloed door geslacht, risicogevoeligheid en slachtofferschap; vrouwen schatten de gevolgen van cybercriminaliteit hoger in, mkb'ers die al eens slachtoffer zijn geworden schatten de kans op slachtofferschap hoger in en wanneer men gevoeliger is voor risico's, schat men de kans op slachtofferschap en de schadelijke effecten daarvan als groter in.

Daarnaast wordt zelfbeschermend gedrag direct beïnvloed door subjectieve normen; mkb'ers die het beeld hebben dat hun sociale omgeving verwacht dat zij zelfbeschermend gedrag vertonen, nemen ook daadwerkelijk meer zelfbeschermende maatregelen. Waarschijnlijk speelt hier de verantwoordelijkheid

die zij hebben voor (het voortbestaan van en schade aan) hun bedrijf en de medewerkers daarin een belangrijke rol.

5.6 Deelvraag 5: *Op welke factoren moeten campagnes zich richten om zelfbeschermend gedrag bij mkb'ers te stimuleren?*

Uit deelvraag 4 blijkt dat de volgende factoren een rol spelen bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb'ers:

1. Persoonlijke kenmerken:
    a. Geslacht
    b. Slachtofferschap
    c. Risicogevoeligheid
2. Effectiviteitsverwachtingen:
    a. Zelfeffectiviteit (uitvoerbaarheid zelfbeschermende maatregelen)
    b. Responseffectiviteit (beoordeeld nut van zelfbeschermende maatregelen)
3. Risicoperceptie (inschatting kans op slachtofferschap en ernst van de gevolgen bij slachtofferschap)
4. Subjectieve normen

Daarnaast is gevonden dat de intenties om in de toekomst aanvullende zelfbeschermende maatregelen te nemen positief samenhangen met leeftijd, wat impliceert dat hoe ouder de respondent, hoe meer hij/zij geneigd is in de toekomst aanvullende zelfbeschermende maatregelen te gaan treffen tegen cybercriminaliteit. Ook hangen de gedragsintenties sterk samen met de behoefte aan aanvullende informatie over cybercriminaliteit en zelfbeschermende maatregelen[48], wat impliceert dat mkb'ers die meer geneigd zijn aanvullende zelfbeschermende maatregelen te treffen in de toekomst, meer behoefte hebben aan informatie.

Bij de ontwikkeling van risicocommunicatie campagnes zou daarom (in eerste instantie) ingezet moeten worden op de risicoperceptie, waarbij het doorbreken van de 'optimistic bias' essentieel is. Wanneer de perceptie toeneemt dat men persoonlijk slachtoffer kan worden van cybercriminaliteit en dat dit ernstige gevolgen kan hebben, ontstaat een gevoel van urgentie en persoonlijke relevantie. Dan is men meer ontvankelijk voor (informatie over) het uitvoeren van zelfbeschermende maatregelen. Als in campagnes

[48] Correlatie r=.19; p<.001

of interventies een duidelijk appél wordt gedaan op de persoonlijke relevantie van cybercriminaliteit, kan dit het zelfbeschermende gedrag onder mkb'ers positief beïnvloeden.

Daarnaast is het relevant om aandacht te hebben voor de effectiviteitsverwachtingen. Hierbij staan het beoordeeld nut en de uitvoerbaarheid van zelfbeschermende maatregelen centraal. Als mkb'ers inzien dat het nuttig én relatief makkelijk is om zelfbeschermende maatregelen uit te voeren, komt dit ten goede aan de mate van zelfbescherming.

Daarnaast kan een beroep worden gedaan op de sociale invloed. Hierbij is het beïnvloeden van de subjectieve norm om zelfbeschermend gedrag te vertonen relevant. Dit is, naast de risicoperceptie en effectiviteitsverwachtingen, een belangrijke directe voorspeller van zelfbeschermend gedrag onder mkb'ers. Het aanstippen van de verantwoordelijkheid voor en de verwachtingen uit de sociale omgeving van de onderneming kan hierbij een belangrijke rol spelen.

6. Conclusies

6.1 Jongeren

Jongeren geven zichzelf een gemiddelde kans om slachtoffer te worden van cybercriminaliteit. Hier is sprake van een *optimistic bias*, want volgens de jongeren hebben "anderen" een *grote* kans slachtoffer te worden. Cybercriminaliteit wordt gezien als een groot risico, maar jongeren - met name mannen - vinden zichzelf minder kwetsbaar dan anderen. Een deel ziet zichzelf ook niet als een interessant doelwit voor criminelen. Ze achten zichzelf vaardig in het herkennen van cybercriminaliteit (bijvoorbeeld een phishingmail), maar zijn daarnaast wel onzeker over nieuwe technieken die door cybercriminelen worden ingezet.

Jongeren schatten de negatieve gevolgen van slachtofferschap relatief hoog in, waarbij vrouwen dat meer doen dan mannen, en hoger opgeleiden meer dan lager opgeleiden. Een meerderheid heeft maar gedeeltelijk een beeld bij de risico's die ze lopen.

Over wat je moet doen als je slachtoffer van cybercriminaliteit bent geworden, zijn jongeren weinig zelfverzekerd. Een kwart van de jongeren (met name vrouwen) heeft zelfs geen idee. Een relatief klein deel van de jongeren is daadwerkelijk slachtoffer geweest van cybercriminaliteit, wat voor deze groep een duidelijke impact heeft gehad. Naast schade door verlies van geld en bestanden, is er een emotionele component: men is geschrokken en voelt zich minder veilig online, en past ook het online gedrag aan.

Bijna alle jongeren – maar met name hoger opgeleiden - zien het nut in van jezelf beschermen tegen cybercriminaliteit (hoge responseffectiviteit). De kennis over hoe je je kunt beschermen tegen cybercriminaliteit is echter beperkt: twee derde geeft aan dat in beperkte mate te weten. Met name vrouwen en jongere jongeren achten zichzelf minder goed in staat om zich tegen cybercriminaliteit te beschermen (lagere zelfeffectiviteit). Een meerderheid van de jongeren - maar met name vrouwen en oudere jongeren - geeft aan voornemens te zijn in de toekomst aanvullende maatregelen te treffen tegen cybercriminaliteit. Dit geldt nog des te meer voor jongeren die ervaring hebben met slachtofferschap.

Zelfbeschermend gedrag komt meer voor bij mannen en bij oudere jongeren (zij vinden ook dat zij zich beter beschermen dan vrouwen en jongere jongeren. Met name lager opgeleide vrouwen onder de 18 jaar vertonen een lage mate van zelfbeschermend gedrag[49]. Dit komt omdat zij zichzelf minder goed in

[49] Een kanttekening hierbij is echter, dat de resultaten gebaseerd zijn op zelfgerapporteerd gedrag. Dat wil zeggen: dat we jongeren hebben gevraagd hoe ze zich gedragen en wat ze doen om zichzelf te beschermen tegen cybercrime. We hebben hier geen daadwerkelijk gedrag onderzocht. Uit recent onderzoek (Van 't Hoff- de Goede et al.,

staat achten zich te beschermen, en ook minder het nut daarvan inzien. Zij worden hierbij sterk beïnvloed vanuit hun sociale omgeving. Dit biedt aanknopingspunten om online zelfbeschermend gedrag bespreekbaar te maken en een gezamenlijke norm te stellen. Ook voor risicocommunicatie-activiteiten en voorlichting kan dit richting bepalen om voor deze specifieke doelgroep gerichte interventies te ontwikkelen op scholen of bijvoorbeeld voor thuis.

Uit de resultaten blijkt dat de volgende factoren een rol spelen bij het wel of niet uitvoeren van zelfbeschermend gedrag van jongeren bij cybercriminaliteit:

1. Persoonlijke kenmerken:
    a. Opleidingsniveau
    b. Leeftijd
    c. Geslacht
    d. Risicogevoeligheid
2. Effectiviteitsverwachtingen:
    a. Zelfeffectiviteit (uitvoerbaarheid zelfbeschermende maatregelen)
    b. Responseffectiviteit (beoordeeld nut van zelfbeschermende maatregelen)
3. Ervaring met slachtofferschap
4. Perceptie van eigen verantwoordelijkheid om jezelf te beschermen

Daarnaast is gevonden dat de intenties om in de toekomst aanvullende zelfbeschermende maatregelen samenhangen met leeftijd en geslacht, waarbij jongere vrouwen de laagste intenties hebben om zichzelf (beter) te gaan beschermen tegen cybercriminaliteit.

Opvallend is, dat de lager opgeleide, jonge (jonger dan 18 jaar) meiden het laagst scoren op zelfbeschermend gedrag.

6.2 Mkb'ers

Geconcludeerd kan worden, dat mkb'ers zich terdege bewust zijn van de risico's van cybercriminaliteit. Een klein deel is afgelopen jaar slachtoffer geworden van cybercriminaliteit, maar de schade bleef in veel gevallen beperkt. Wellicht dat dit verklaart waarom slechts een deel van de personen die slachtoffer zijn geworden zijn of haar gedrag na slachtofferschap heeft aangepast.

2019) is gebleken, dat daadwerkelijk online gedrag kan afwijken van zelfgerapporteerd online gedrag. Toekomstig onderzoek moet uitwijzen of deze verschillen blijven bestaan bij daadwerkelijk zelfbeschermend gedrag.

Men schat de mogelijk negatieve gevolgen van slachtofferschap relatief hoog in. Echter, de kans op slachtofferschap wordt redelijk laag ingeschat. Opvallend is dat er sprake is van een sterke optimistic bias, waarbij men zichzelf significant minder vatbaar acht voor cybercriminaliteit dan andere mensen.

Mkb'ers zijn verdeeld over hun kennis van zelfbeschermend gedrag ten aanzien van cybercriminaliteit. Een meerderheid zegt redelijk tot goed in staat te zijn zichzelf te beschermen tegen cybercriminaliteit, (een poging tot) cybercriminaliteit te herkennen en te weten welke risico's hij/zij loopt. Maar ook bijna de helft geeft aan dit slechts een beetje of enigszins te weten. Mkb'ers lijken niet unaniem te vertrouwen in eigen kunnen te hebben. Vooral over wat men moet doen wanneer men slachtoffer is geworden, is men wat onzekerder. Ruim de helft is ook niet (volledig) overtuigd of hij/zij zichzelf momenteel voldoende beschermt tegen cybercriminaliteit.

Men ziet wel het nut in van zelfbeschermende maatregelen en veel mkb'ers wil hierover ook extra informatie ontvangen. Dit is onder te verdelen in twee categorieën: informatie over cybercriminaliteit in zijn algemeenheid en specifieke informatie over zelfbeschermende maatregelen. Daarnaast is men welwillend zelf actief naar informatie op zoek te gaan, waarbij de behoefte is aan actuele en praktisch toepasbare informatie.

De meeste mkb'ers vertonen een relatief hoge mate van zelfbeschermend gedrag. Dat wil zeggen dat zij momenteel reeds veel zelfbeschermende maatregelen hebben getroffen. Toch is een meerderheid voornemens om in de toekomst aanvullende zelfbeschermende maatregelen te treffen. We zien dat deze gedragsintenties onder ouderen hoger zijn dan onder jongeren. Deze voornemens worden vooral ingegeven door een hogere persoonlijke risicoperceptie en een groter beoordeeld nut van zelfbeschermende maatregelen. Daarnaast lijkt onzekerheid over toekomstige ontwikkelingen op het gebied van cybercriminaliteit een rol te spelen: ondanks dat een grote meerderheid vindt dat het huidige zelfbeschermend gedrag de kans op slachtofferschap verkleinen, vraagt ongeveer de helft zich af of dit voldoende is om goed beschermd te zijn tegen cybercriminaliteit.

Uit de resultaten blijkt dat de volgende factoren een rol spelen bij het wel of niet uitvoeren van zelfbeschermend gedrag van mkb'ers:

1. Persoonlijke kenmerken:
    a. Geslacht
    b. Slachtofferschap
    c. Risicogevoeligheid

2. Effectiviteitsverwachtingen:
    a. Zelfeffectiviteit (uitvoerbaarheid zelfbeschermende maatregelen)
    b. Responseffectiviteit (beoordeeld nut van zelfbeschermende maatregelen)
3. Risicoperceptie (inschatting kans op slachtofferschap en ernst van de gevolgen bij slachtofferschap)
4. Subjectieve normen

Daarnaast is gevonden dat de intenties om in de toekomst aanvullende zelfbeschermende maatregelen positief samenhangen met leeftijd, wat impliceert dat hoe ouder de respondent, hoe meer hij/zij geneigd is in de toekomst aanvullende zelfbeschermende maatregelen te gaan treffen tegen cybercriminaliteit. Ook hangen de gedragsintenties sterk samen met de behoefte aan aanvullende informatie over cybercriminaliteit en zelfbeschermende maatregelen[50], wat impliceert dat mkb'ers die meer geneigd zijn aanvullende zelfbeschermende maatregelen te treffen in de toekomst, meer behoefte hebben aan informatie.

7. Aanbevelingen

Op basis van de resultaten en conclusies uit dit onderzoek worden de volgende aanbevelingen gedaan om de cyberweerbaarheid onder de doelgroepen jongeren en mkb'ers te vergroten:

7.1 Jongeren

1. Richt de campagne op het doorbreken van de aangetroffen, stevige optimistic bias. Besteed hierbij specifieke aandacht aan de persoonlijke kansinschatting om slachtoffer te worden ("het kan ook jóu overkomen").
2. Met name vrouwen en 'jongere' jongeren zijn kwetsbaarder voor slachtofferschap; richt een algemene campagne op deze doelgroepen.
3. Een belangrijke doelgroep zijn de lager opgeleide, jonge (tot 18 jaar) vrouwen. Zij vertonen significant minder zelfbeschermend gedrag. In de voorlichting kunnen sociale invloed en subjectieve normen van belang zijn; deze groep is vatbaarder voor deze factoren en kan – los van de kennis en risicoperceptie – via sociale beïnvloeding worden gemotiveerd om zelfbeschermend gedrag te gaan uitvoeren.
4. Daarnaast hebben jonge, lager opgeleide vrouwen een lagere perceptie van het nut en de uitvoerbaarheid van zelfbeschermende maatregelen. Concrete, makkelijk uitvoerbare ge-

[50] Correlatie r=.19; p<.001

dragsadviezen in combinatie met het benadrukken van het nut van de maatregelen kan hen stimuleren hun zelfbeschermend gedrag te vergroten.

5. Zorg voor een herkenbare stijl en betrouwbaar afzender, bijvoorbeeld vanuit een overheidspartij of via scholen. Een combinatie van deze afzenders is het meest optimale om de belangrijkste doelgroep te stimuleren.

7.2 Mkb'ers

1. Richt ook de campagne voor mkb'ers op het doorbreken van de aangetroffen, stevige optimistic bias. Besteed hierbij specifieke aandacht aan de persoonlijke kansinschatting (het kan ook jóu overkomen).
2. Besteed aandacht aan de effectiviteitsverwachting binnen de behavioral beliefs: geef concreet aan wat men zelf (makkelijk!) kan doen om zichzelf beter te beschermen (zelfeffectiviteit) en daarnaast waarom dit nuttig is of hoe dit helpt je te beschermen (responseffectiviteit).
3. Richt de campagne ook op het vergroten van de sociale norm: subjectieve normen blijken ook een voorspeller te zijn van zelfbeschermend gedrag. Met andere woorden: mkb'ers zijn geneigd meer zelfbeschermende maatregelen te treffen, wanneer zij het idee hebben dat dit van hen verwacht wordt in de (sociale) omgeving.
4. Zorg voor gelaagdheid in informatie: de behoefte aan informatie is groot, maar dynamisch; iedere mkb'er heeft weer zijn eigen informatiebehoefte. Sommige mkb'ers zullen alleen willen weten wat ze moeten doen en hoe, terwijl anderen ook verdiepende informatie willen over de risico's van cybercriminaliteit, de ontwikkelingen en wat dit betekent voor de eigen onderneming, en wie welke verantwoordelijkheden heeft in de bescherming tegen cybercriminaliteit. Zorg daarom voor een koppeling tussen de campagne en een (online) platform waarop mkb'ers onafhankelijke en betrouwbare informatie kunnen vinden over algemene informatie en actuele trends op het gebied van cybercriminaliteit.

Geraadpleegde literatuur

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50, pp. 179-211.

Alcatara, P., & Riglietti, G. (2015). *Emergency Communications Report 2015, Busi-ness Continuity Institute, Coversham*, available at http://www.thebci.org/index.php/resources/bci-research-reports

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3(1)*, 400-420

Brands, J., & van Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*. https://doi.org/10.1177/1477370819839619

Brunton-Smith, I. (2018). Fear 2.0. Worry about cybercrime in England and Wales. *The Routledge International Handbook on Fear of Crime*, pp. 93-105

CBS (2019). Leerlingen, deelnemers en studenten; onderwijssoort, vanaf 1900. Geraadpleegd op https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37220/table?ts=1580807485329

Domenie, M. M. L., Leukfeldt, E. R., van Wilsem, J. A., Jansen, J., & Stol, W. P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving*. Den Haag : Boom Lemma.

Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The Affect Heuristic in Judgments of Risks and Benefits. *Journal of Behavioral Decision Making*, 13, pp. 1-17.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). *Social Phishing*. Indiana University, Bloomington: School of Informatics.

Heij, R. de (2019). ICT, kennis en Economie. *Centraal Bureau voor de Statistiek.*

Hoff, S. van ,t, Van der Kleij, R., Van de Weijer, S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online?* Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC); Ministerie van Justitie en Veiligheid.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40.

Jansen, J., Kop, N. en Stol, W. (2017) Internetbankieren: Veiligheidspercepties van gebruikers. *Tijdschrift voor Veiligheid,* 16, 1, 36–51.

Jansen, J., Leukfeldt, R., Wilsem, J. V., & Stol, W. (2013). Onlinegedragingen: een risico voor hacken en persoonsgerichte cyberdelicten. *Tijdschrift voor Criminologie, 55(4)*, 394-408.

Kievik, M., Misana-ter Huurne, E.F.J., Gutteling, J.M., & Giebels, E. (2018). Making it stick: Exploring the effects of information and behavioral training on self-protectiveness of citizens in a real-life safety setting. *Safety Science*, 101, 1-10.

Kleij, van der R. & Leukfeldt, E.R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In: Ahram T., Karwowski W. (eds) Advances in Human Factors in Cybersecurity. AHFE 2019*. Advances in Intelligent Systems and Computing*, vol 960. Springer, Cham.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3(1)*, 9.

Leukfeldt, E.R. (2018) *De 'Human' factor in Cybersecurity.* Den Haag : Haagse Hogeschool.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37(3)*, 263-280.

Lindell, M.K. & Perry, R.W. (2012). The Protective Action Decision Model: Theoretical Modifications and Additional Evidence. *Risk Analysis*, 32 (4), 616-632.

Ngo, F. T., & Paternoster, R. (2011). CybercrimeCybercriminaliteit Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5(1)*.

Notté, R.J., Slot, L., van 't Hoff-de Goede, S. & Leukfeldt, E.R**.** (2019). *Cybersecurity in het mkb. Nulmeting.* Den Haag: De Haagse Hogeschool.

Paulissen, L., & van Wilsem, J. A. (2015). *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*. Apeldoorn : Politie & Wetenschap.

Rhee, Hyeun-Suk; Ryu, Young; and Kim, Cheong-Tag, "I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security" (2005). *ICIS 2005 Proceedings.* Paper 32.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (p. 113–132). Plenum Press.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.), *Social Psychophysiology: a source book,* 153-176. New York: Guilford Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91, 93-114.

Rubin, H.J. & Rubin, R.S. (1995) *Qualitative interviewing: the art of hearing data*. Thousand Oaks : Sage.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. *CHI 2010: Privacy Behaviors.* April 10–15, 2010, Atlanta, GA, USA.

Slovic, P., Finucane, M.L., Peters, E., & MacGregor, D. (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality. *Risk Analysis*, 24 (2), pp. 311-322.

Sun, Y., Pan, Z., & Shen, L. (2008), Understanding the Third-Person Perception: Evidence From a Meta-Analysis, *Journal of Communication*, 58 (2), 280–300.

Ter Huurne, E.F.J. (2008). *Information Seeking in a Risky World. The Empirical and Theoretical Development of FRIS: A Framework of Risk Information Seeking*. Enschede: University of Twente.

Trendmicro(z.d), via: https://www.trendmicro.com/vinfo/in/security/definition/Ransomware (laatst binnengehaald op 16-12-2019).

Van Noije, L. & K. Wittebrood (2010) What is fear of crime and how is it determined? A review of the literature. In: *CPSI: Changing perceptions of security and interventions* (7th EU framework programme), via www.tno.nl/.

an de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453.

Vos, M. (2017). *Communication in Turbulent Times: Exploring Issue Arenas and Crisis Communication to Enhance Organisational Resilience*. Jyväskylä University: School of Business and Economics.

Weinstein, N. D. (1989). Optimistic biases about personal risks. *Science*, *246*(4935), 1232+.

Weiss, R.S. (1995) *Learning from strangers. The art and methods of qualitative interview studies*. New York : Free Press.

Witte, K. (1992). Putting the Fear back in Fear Appeals: The Extended Parallel Process Model. *Communication Monographs*, 59, pp. 329–349.

WODC(2011). *Monitor Criminaliteit Bedrijfsleven 2010: Feiten en trends inzake aard en omvang van criminaliteit in het bedrijfsleven*. Den Haag: WODC.

Bijlage 1 – Gebruikte vragenlijst

- OVER DEZE VRAGENLIJST -

Hartelijk dank dat u de tijd wilt nemen om deze vragenlijst in te vullen!

De vragenlijst gaat over uw mening over criminaliteit via het internet (cybercriminaliteit) en hoe u het risico van cybercriminaliteit beleeft. Het invullen van deze vragenlijst duurt ongeveer 10 minuten.

Bij de meeste vragen kunt u antwoorden door een hokje bij een antwoord aan te kruisen. Bij enkele andere vragen wordt u gevraagd om zelf een antwoord op te schrijven. Mocht u op een vraag niet willen antwoorden, dan kruist u het hokje bij 'geen antwoord' aan.

Er zijn geen goede of foute antwoorden in de vragenlijst; uw mening en beleving staan centraal. Vul daarom de vragenlijst s.v.p. zo eerlijk mogelijk in.

Deelname aan deze vragenlijst is volledig anoniem; uw antwoorden op de vragen kunnen op geen enkele wijze naar u worden herleid.

De resultaten van deze vragenlijst worden gebruikt voor wetenschappelijke en praktijkgerichte publicaties en een advies hoe cybercriminaliteit het beste kan worden tegengegaan.

- OVER CYBERCRIMINALITEIT -

In deze vragenlijst gaat het over cybercriminaliteit en vormen van cybercriminaliteit. Hierbij worden in dit onderzoek de volgende beschrijvingen gebruikt voor (I) cybercriminaliteit, (II) phishing en (III) ransomware:

I - Onder *cybercriminaliteit* (algemeen) verstaan we alle vormen van criminaliteit die met behulp van internet worden gepleegd; denk aan oplichting, diefstal, identiteitsfraude, etc.
II - *Phishing* is een vorm van cybercriminaliteit en is online oplichting, waarbij criminelen e-mails of websites namaken om slachtoffers te misleiden, om hun inloggegevens te achterhalen en toegang te krijgen tot hun online accounts;
III - *Ransomware* is ook een vorm van cybercriminaliteit, waarbij daders via internet programma's op apparaten van hun slachtoffers installeren die alle bestanden op de apparaten vergrendelen. Deze worden pas weer ontgrendeld wanneer slachtoffers op tijd geld overmaken naar de criminelen. Als dat niet gebeurt, dan gaan de bestanden verloren.

1. Hoe groot schat u uw kans om de komende 12 maanden *zelf* het slachtoffer te worden van …

	geen kans	hele kleine kans	kleine kans	geen kleine / geen grote kans	grote kans	hele grote kans	geen antwoord
cybercriminaliteit?	☐	☐	☐	☐	☐	☐	☐
phishing?	☐	☐	☐	☐	☐	☐	☐
ransomware?	☐	☐	☐	☐	☐	☐	☐

2. In hoeverre bent u het eens met de volgende stelling:

"Als ik slachtoffer zou worden van … , dan levert dat ernstige schade voor mij op."

(Bijvoorbeeld het verlies van geld, tijd of bestanden of emotionele schade; schaamte en wantrouwen).

	helemaal mee oneens	mee oneens	niet mee oneens / niet mee eens	mee eens	helemaal mee eens	geen ant-woord
…cybercriminaliteit…	□	□	□	□	□	□
… phishing …	□	□	□	□	□	□
… ransomware…	□	□	□	□	□	□

3a) Bent u in de afgelopen twaalf maanden <u>zelf</u> slachtoffer van cybercriminaliteit geworden?

ja	nee	weet ik niet	geen ant-woord
□	□	□	□

Indien u 'nee' antwoordde, ga door naar vraag 4.

b) Wat was de schade en/of impact voor u persoonlijk?

_____ s.v.p. omschrijven

□ weet ik niet □ geen antwoord

c) Heeft uw slachtofferschap ervoor gezorgd dat u uw online gedrag heeft aangepast?

***Zo ja*, hoe? *Zo nee*, waarom niet?**

_____ s.v.p. omschrijven

□ weet ik niet □ geen antwoord

4. In hoeverre bent u het eens met onderstaande stellingen?

Ik weet:…	helemaal niet	een beetje	enigszins	grotendeels	volledig	geen antwoord
… hoe ik mij kan beschermen tegen cybercriminaliteit.	□	□	□	□	□	□
…welke risico's ik loop om slachtoffer te worden van cybercriminaliteit.	□	□	□	□	□	□
…hoe ik (een poging tot) cybercriminaliteit kan herkennen.	□	□	□	□	□	□
…wat ik moet doen wanneer ik slachtoffer word van cybercriminaliteit.	□	□	□	□	□	□

5. In hoeverre bent u het eens met de volgende stellingen over uw eigen bescherming tegen cybercriminaliteit?

	volledig oneens	oneens	niet oneens / niet eens	eens	volledig eens	geen antwoord
Ik vind dat ik mij voldoende tegen cybercriminaliteit bescherm.	□	□	□	□	□	□
De door mij genomen maatregelen zorgen er voor dat ik minder kans heb om slachtoffer van cybercriminaliteit te worden.	□	□	□	□	□	□
Het is nuttig om maatregelen te treffen om je tegen cybercriminaliteit te beschermen.	□	□	□	□	□	□
Ik vind het lastig om me goed tegen cybercriminaliteit te beschermen.	□	□	□	□	□	□
Maatregelen treffen heeft weinig nut; het verkleint de kans om slachtoffer van cybercriminaliteit te worden niet of nauwelijks.	□	□	□	□	□	□

6. In hoeverre bent u het eens met de onderstaande stellingen?

Mensen in mijn omgeving …	volledig mee oneens	oneens	niet mee eens/ niet mee oneens	eens	volledig mee eens	geen antwoord
…vinden het belangrijk dat ik mezelf tegen cybercriminaliteit bescherm.	□	□	□	□	□	□
…verwachten dat ik mezelf tegen cybercriminaliteit bescherm.	□	□	□	□	□	□
Ik ben geneigd om mezelf te beschermen, omdat…						
…anderen dat ook doen.	□	□	□	□	□	□
…mensen om mij heen dat van mij verwachten.	□	□	□	□	□	□

7 a) Bent u voornemens om in de toekomst aanvullende voorbereidende of zelfbeschermende maatregelen te treffen tegen cybercriminaliteit?

zeker niet	waarschijnlijk niet	waarschijnlijk wel	zeker wel	geen antwoord
□	□	□	□	□

b) *Zo ja*, welke aanvullende voorbereidende of zelfbeschermende maatregelen bent u voornemens tegen cybercriminaliteit te treffen? *Zo nee*, waarom niet?

_____ s.v.p. omschrijven

□ weet ik niet □ geen antwoord

8. Hieronder volgen een aantal mogelijkheden om de risico's of mogelijk slachtofferschap van cyber-criminaliteit tegen te gaan. Kruis hieronder aan wat u momenteel zelf al doet om u te beschermen.

	ja	nee	geen antwoord
Ik installeer updates zodra deze beschikbaar zijn.	□	□	□
Ik controleer of de afzender van een e-mail betrouwbaar is.	□	□	□
Ik let bij online betalen op de aanwezigheid van het slotje in de browser.	□	□	□
Ik gebruik sterke wachtwoorden met meerdere cijfers en tekens.	□	□	□
Ik download *geen* films, muziek en/of games op illegale wijze.	□	□	□
Ik heb mijn profielsites (zoals Facebook, Instagram) niet openbaar staan.	□	□	□
Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media.	□	□	□
Ik gebruik een virusscanner.	□	□	□
Ik gebruik een firewall.	□	□	□
Ik gebruik een VPN-verbinding (Virtual Private Network).	□	□	□
Ik geef mijn inloggegevens niet aan onbekenden.	□	□	□
Ik verwijder e-mails die ik niet vertrouw direct.	□	□	□
Ik gebruik dubbele verificatie op mijn accounts.	□	□	□
Ik gebruik een vergrendelingscode of wachtwoord op al mijn apparaten.	□	□	□
Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen.	□	□	□
Ik maak een back-up (reservekopie) van mijn waardevolle bestanden.	□	□	□
Ik vermijd het gebruik van openbare wifi.	□	□	□
Ik vermijd onveilige websites.	□	□	□
Ik ben voorzichtig met het openen van bijlagen.	□	□	□
Ik kijk naar het bestandstype voordat ik bijlagen open.	□	□	□
Ik ben voorzichtig met het aanklikken van links.	□	□	□
Ik vergrendel mijn apparaten als ik deze niet gebruik.	□	□	□
Ik versleutel bestanden met een wachtwoord of andere beveiliging.	□	□	□
Ik gebruik een browser extensie, zoals een adblocker	□	□	□
□ Anders namelijk _____ s.v.p. beschrijven			

De vragenlijst gaat verder op de volgende pagina.

9. Hoe groot schat u de kans dat *een gemiddelde inwoner van Nederland* slachtoffer wordt van …. in de komende twaalf maanden?

	geen kans	hele kleine kans	kleine kans	geen kleine / geen grote kans	grote kans	hele grote kans	geen ant-woord
…cybercriminaliteit	□	□	□	□	□	□	□
… phishing	□	□	□	□	□	□	□
…ransomware	□	□	□	□	□	□	□

10 a) Heeft u behoefte aan meer informatie over de risico's van cybercriminaliteit en hoe u zich daartegen kunt beschermen?

ja	nee	geen antwoord
□	□	□

b) Aan wat voor informatie heeft u behoefte? *Indien u met 'nee' antwoordde, ga naar vraag 11.*

_____ s.v.p. omschrijven

□ weet ik niet □ geen antwoord

c) Hoe en van wie zou u deze informatie willen krijgen?

_____ s.v.p. omschrijven

□ weet ik niet □ geen antwoord

d) Bent u voornemens zelf naar deze informatie op zoek te gaan?

ja	nee	geen antwoord
□	□	□

De vragenlijst gaat verder op de volgende pagina.

11) In hoeverre bent u het eens met de volgende stellingen?

	volledig mee on-eens	mee on-eens	mee eens	volledig mee eens	geen ant-woord
1. Ik reageer snel angstig op situaties.	□	□	□	□	□
2. Andere mensen lopen meer kans om het slachtoffer van cybercriminaliteit te worden dan ik.	□	□	□	□	□
3. Ik wil liever niet nadenken over de kans dat ik zelf het slachtoffer van cybercriminaliteit word.	□	□	□	□	□
4. Ik ben zelf verantwoordelijk om slachtofferschap van cybercriminaliteit te voorkomen.	□	□	□	□	□
5. Ik ga meestal van het ergste uit.	□	□	□	□	□
6. Het heeft geen zin om je zorgen te maken over cybercriminaliteit, als daders je slachtoffer willen maken, dan lukt hen dat toch wel.	□	□	□	□	□

ACHTERGRONDVRAGEN

A. Hoe vaak maakt u gebruik van internet voor privé doeleinden? Kies alstublieft 1 antwoord.

□ Minder dan 1 keer per maand
□ Minimaal 1 keer per maand, maar niet wekelijks
□ Minimaal 1 keer per week, maar niet dagelijks
□ Dagelijks
□ Meerdere keren per dag
□ Minstens ieder uur (tijdens de uren dat ik wakker ben)
□ Ik ben (bijna) continu online (tijdens de uren dat ik wakker ben)
□ Weet ik niet
□ Geen antwoord

B. Waarvoor bent u online? (LET OP: Meerdere antwoorden zijn mogelijk!)

Werk	studie	winkelen	bankieren	ontspanning	sociale contacten	geen ant-woord
□	□	□	□	□	□	□
□ Anders namelijk _____ s.v.p. invullen						

C. Wat is uw geslacht? □ Man □ Vrouw □ Geen antwoord

D. Wat is uw leeftijd? _____ jaar □ Geen antwoord

E. Wat is uw hoogst genoten opleiding? _____ □ Geen antwoord

Dit is het einde van de vragenlijst. Hartelijk dank voor uw medewerking!

Bijlage 2 – Gebruikte interviewhandleiding

Bedreigingen cybercriminaliteit

1. Heeft u weleens iets gehoord over criminaliteit via het internet?
   Wat verstaat u onder criminaliteit via Internet? Welke vormen van criminaliteit via internet kent u? *[stevig op doorvragen]*

2. Bent u zelf wel eens het slachtoffer geworden van criminaliteit via het internet geworden?
   [Zo nee: Is er iemand in uw omgeving weleens slachtoffer van criminaliteit via het internet geworden?]

   Checklist voor doorvragen:

   □ *Wat was er gebeurd?*
   □ *Hoe is dat gekomen?*
   □ *Wat was de schade?*
   □ *Heeft dit verhaal voor u nog tot (gedrags)verandering geleid? Zo ja, welke en waarom?*

   Eventueel nog:
   □ *Welke impact heeft dit op u (gehad)?*
   □ *Wat voelde u toen u dit ontdekte? (bezorgd, verbolgen, geïrriteerd, angstig, boos, onzeker, bedroefd)*
   □ *Hoe bent u met deze situatie omgegaan?*
   □ *Heeft u informatie opgezocht of opgevraagd?*
   □ *Heeft u uw gedrag aangepast?*
   □ *Heeft u andere software geïnstalleerd?*
   □ *Heeft u aangifte gedaan?*
   □ *Heeft u er met uw omgeving over gesproken?*
   □ *Hoe reageerde uw omgeving?*
   □ *Hoe kijkt u op deze ervaring terug?*

Inzoomen op phishing

3. Heeft u weleens e-mail berichten ontvangen die lijken op de voorbeelden die u net heeft gezien?
   □ Hoe gaat u met dergelijke e-mail berichten om? Waar let u bijvoorbeeld op?
   □ Heeft u weleens op links in dergelijke e-mail berichten geklikt? Wat gebeurde er toen?
   □ Wat denkt u dat er kan gebeuren als u op links in dergelijke berichten klikt?
   □ Hoe groot schat u de kans dat u in de toekomst op de links in dergelijke e-mail berichten klikt?
   □ Verwacht u schade wanneer u op links in dergelijke e-mail berichten klikt?
   □ Wat voor schade? Hoe groot?
   □ Stel dat u onoplettend in een dergelijke poging zou trappen weet u wat u dan moet doen?

□ Verwacht u daarbij iets van organisaties als de politie of uw internetprovider?
□ Wat verwacht u van hen?
□ Zou u hierover met uw omgeving praten? Hoe verwacht u dat zij zullen reageren?

Inzoomen om ransomware

4. Heeft u weleens situaties tijdens uw internet- of computergebruik meegemaakt die lijken op onderstaande voorbeelden?
    a. Hoe zou u met deze situatie omgaan?
    b. Wat denkt u dat er kan gebeuren als u in een dergelijke situatie beland tijdens uw internet- of computergebruik?
    c. Verwacht u schade wanneer u in een dergelijke situatie zou komen?
    d. Wat voor schade? Hoe groot?
    e. In een dergelijke situatie zou belanden, weet u wat u dan moet doen?
    f. Hoe groot schat u de kans dat u in de toekomst tot betaling over zou gaan in een dergelijke situatie? Verwacht u daarbij iets van organisaties als de politie of uw internetprovider?
    g. Wat verwacht u van hen?
    h. Zou u hierover met uw omgeving praten? Hoe verwacht u dat zij zullen reageren?

5. Wat zijn volgens u de grootste risico's of gevaren van cybercriminaliteit voor internetgebruikers in Nederland? Welke schade (en impact) levert dit op voor de slachtoffers?

6. Welke personen of groepen personen lopen volgens u de grootste kans om slachtoffer te worden? Waarom?

7. Wie zijn er volgens u wel en wie zijn er volgens u niet in staat zichzelf voldoende te beschermen tegen cybercriminaliteit? Wat zijn kwetsbare groepen?

8. In zijn algemeenheid, denkt u dat [jongeren/mkb'ers] in Nederland zich voldoende bewust zijn van de dreiging van cybercriminaliteit en de bijbehorende risico's en mogelijke effecten? Waarom wel/niet?

9. Vindt u cybercriminaliteit een maatschappelijk probleem in Nederland? Waarom wel/niet? Wat is het grootste probleem? Welke schade (en impact) levert dit op voor de maatschappij?

10. Is het risico om slachtoffer te worden van cybercriminaliteit de laatste vijf jaar volgens u toegenomen/ afgenomen/ gelijk gebleven?
    □ toegenomen
    □ afgenomen
    □ gelijk gebleven

11. Hoe groot schat u uw kans om zelf het komende jaar slachtoffer te worden van cybercriminaliteit?
    a. Waarom schat u deze kans voor uzelf zo in?
    b. Wat voor soort criminaliteit?
    c. Welke bedreigingen en gevaren levert het [voor u persoonlijk / uw bedrijf] op?
    d. Wat zullen denkt u de gevolgen zijn voor uzelf/uw bedrijf?

    Checklist voor doorvragen > in termen van:

    □ *Geld*
    □ *Privacy*
    □ *Toekomstig internetgedrag*
    □ *Veiligheidsgevoel*
    □ *Sociale contacten*
    □ *Koop en verkoop van goederen en diensten (zaken doen)*
    □ *Voorzien in levensonderhoud (bij mbk'ers)*
    □ *Gebruik van internetdiensten*
    □ *Schaamte*
    □ *Anders, namelijk:……*

12. Hoe voelt u zich wanneer u denkt aan de mogelijkheid om zelf slachtoffer te worden van cybercriminaliteit? Eventueel opties geven:
    □ *bezorgd*
    □ *verbolgen*
    □ *geïrriteerd*
    □ *angstig*
    □ *boos*
    □ *onzeker*
    □ *bedroefd*
    □ *hoopvol*
    □ *anders, namelijk: ……*

13. Wie zouden volgens u een belangrijke rol kunnen/moeten spelen bij de bewustwording van de gevaren, en het bestrijden en voorkomen van cybercriminaliteit? Doen zij nu genoeg? Wat zou men nog meer kunnen doen?

    Eerst als open vraag, dan doorvragen op de rol van:
    - *De media*
    - *Uw opleiding/werkgever*

- *Websites en applicaties die u gebruikt*
- *Uw bank (indien respondent internetbankiert)*
- *De politie*
- *De gemeente/ overheid*
- *…*

14. Wat vindt u dat we als samenleving tegen cybercriminaliteit zouden kunnen of moeten doen? Wie is verantwoordelijk?

15. Wat heeft de samenleving volgens u nodig om nog beter voorbereid te zijn op- of te kunnen reageren op cybercriminaliteit?

16. (Op welke manier) is cybercriminaliteit een onderwerp van gesprek met mensen in uw omgeving?

17. Hoe kunt u voorkomen dat u schade oploopt of slachtoffer wordt van cybercriminaliteit?
[hier kunnen meerdere vormen aan bod komen – leg focus op phishing]
    a. Heeft u zelf maatregelen genomen om u te beschermen tegen of voor te bereiden op cybercriminaliteit? Welke?
    b. Waarom heeft u deze maatregelen genomen? Hoe kwam u aan informatie of kennis over deze maatregelen? Wat vond u van deze informatie? Wat heeft u met deze informatie gedaan?

18. Wat zijn voor u redenen om wel voorbereidings- of beschermende maatregelen te nemen of uit te voeren?
        i. Hoe nuttig vindt u dat?
        ii. Heeft u het idee dat u zich zelf daarmee voldoende beschermt tegen de dreiging van cybercriminaliteit?
    b. Zo nee, wat zijn voor u redenen om voorbereidings- of beschermende maatregelen niet te nemen of uit te voeren? Wat houdt u tegen?
        i. Zo nee, wat zou u nodig hebben om dit wel te kunnen?
        ii. Zo nee, zou u daar behoefte aan hebben? En hoe dan?
    c. Heeft u het idee dat het investeren (in tijd, geld, of gedrag) in voorbereidingsmaatregelen de moeite waard is? Waarom wel/niet?
    d. Bent u bereid tijd/energie/ geld te investeren in het treffen van voorbereidingsmaatregelen om zichzelf te beschermen tegen cybercriminaliteit?
        i. Zo ja, wat gaat u dan doen?
        ii. Wat denkt u daar mee te bereiken?

19. Weet u op dit moment hoe u moet handelen als u onverhoopt slachtoffer bent geworden van cybercriminaliteit? Zo ja, hoe?

a. Zo nee, wat zou u nodig hebben om dit wel te kunnen?

20. Heeft u behoefte aan meer informatie over cybercriminaliteit?
    a. Zo ja, waarover (bijv. risico's, melding, maatregelen, etc.)?
    b. Op welke manier zou u deze informatie willen krijgen/ontvangen?
    c. Van wie zou u deze informatie willen krijgen/ ontvangen?
    d. Waarvoor zou u deze informatie vervolgens gebruiken?

Bijlage 3 - Huidig zelfbeschermend gedrag

	Percentage 'ja':	
Zelfbeschermende maatregel:	**Jongeren**	**Mkb'ers**
Ik installeer updates zodra deze beschikbaar zijn.	62	92
Ik controleer of de afzender van een e-mail betrouwbaar is.	70	98
Ik let bij online betalen op de aanwezigheid van het slotje in de browser.	55	84
Ik gebruik sterke wachtwoorden met meerdere cijfers en tekens.	68	90
Ik download *geen* films, muziek en/of games op illegale wijze.	40	85
Ik heb mijn profielsites (zoals Facebook, Instagram) niet openbaar staan.	53	66
Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media.	47	71
Ik gebruik een virusscanner.	60	91
Ik gebruik een firewall.	44	88
Ik gebruik een VPN-verbinding (Virtual Private Network).	29	32
Ik geef mijn inloggegevens niet aan onbekenden.	74	94
Ik verwijder e-mails die ik niet vertrouw direct.	58	99
Ik gebruik dubbele verificatie op mijn accounts.	38	42
Ik gebruik een vergrendelingscode of wachtwoord op al mijn apparaten.	75	75
Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen.	29	47
Ik maak een back-up (reservekopie) van mijn waardevolle bestanden.	55	87
Ik vermijd het gebruik van openbare wifi.	25	58
Ik vermijd onveilige websites.	57	87
Ik ben voorzichtig met het openen van bijlagen.	50	96
Ik kijk naar het bestandstype voordat ik bijlagen open.	47	82
Ik ben voorzichtig met het aanklikken van links.	61	93
Ik vergrendel mijn apparaten als ik deze niet gebruik.	73	73
Ik versleutel bestanden met een wachtwoord of andere beveiliging.	28	28
Ik gebruik een browser extensie, zoals een adblocker	38	48