Naar een cyberweerbaar Amersfoort

Aanzetten voor gerichte risicocommunicatie ter bevordering van de cyberweerbaarheid op basis van een onderzoek onder het Amersfoortse Burgerpanel.

Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion
dr. Remco Spithoven, Elsa Foppen BSc., dr. Ynze van Houten & dr. Ellen Misana – ter Huurne

i.s.m. Anthonie Drenth MSc., gemeente Amersfoort
& Haagse Hogeschool, Lectoraat cybersecurity in het mkb

December 2020

Een verkennend onderzoek naar aanzetten voor gerichte risicocommunicatie ter bevordering van de cyberweerbaarheid, op basis van een onderzoek onder het Amersfoortse Burgerpanel. Uitgevoerd door Hogeschool Saxion, lectoraat Maatschappelijke Veiligheid in samenwerking met de gemeente Amersfoort en het lectoraat Cybersecurity in het mkb van de Haagse Hogeschool.

December 2020

Inhoud

1. Inleiding **5**

2. Theoretisch kader **7**

3. Onderzoeksmethode en steekproef **9**

4. Slachtofferschap van cybercriminaliteit **11**

5. Risicoperceptie en - bewustzijn **13**

6. Zelfbeschermend gedrag **15**

6.1 Effectiviteitsverwachtingen 15

6.2 Huidig zelfbeschermend gedrag 16

6.3 Toekomstig zelfbeschermend gedrag 16

7. Informatiebehoefte **19**

8. Conclusies ten aanzien van beschrijvende statistieken **21**

9. Verklarende statistieken **23**

9.1 Vrouwelijke inwoners 23

9.2 Mannelijke inwoners 24

9.3 21 tot 30 jarige inwoners 24

9.4 65+ jarige inwoners 25

9.5 Lager opgeleide inwoners 25

10. Aanzetten voor gerichte risico-communicatie **27**

10.1 Richtlijnen voor algemene risico-communicatie 27

10.2 Vrouwelijke inwoners 28

10.3 Mannelijke inwoners 29

10.4 21 tot 30 jarige inwoners 29

10.6 65+ jarige inwoners 30

10.5 Lager opgeleide inwoners 31

Geraadpleegde literatuur **33**

Bijlage 1 – Overzicht van gerapporteerd zelfbeschermend gedrag **35**

1. Inleiding

De gemeente Amersfoort heeft vanuit haar publieke taak om haar inwoners en ondernemers te ondersteunen in hun cyberweerbaarheid behoefte aan inzicht in de mate van risicobewustzijn, het zelfbeschermend gedrag en de beïnvloedende factoren hiervan. Dit rapport beschrijft het onderzoek dat is uitgevoerd om hier inzicht in te krijgen met behulp van data verzameld uit het Amersfoortse burgerpanel. Op basis van de resultaten van dit onderzoek worden adviezen en aanbevelingen gegeven waarmee gemeente Amersfoort gerichte risicocommunicatie activiteiten kan ontwikkelen met als doel om de cyberweerbaarheid onder inwoners en ondernemers in de gemeente te bevorderen (Leukfeldt, Spithoven & Misana-ter Huurne, 2020; Spithoven, 2020). Het doel van de gemeente Amersfoort is daarbij om de inwoners en ondernemers te ondersteunen op hun weg naar cyberweerbaarheid.

Cyberweerbaarheid wordt in dit rapport opgevat als het samenvallen van risicobewustzijn en zelfbeschermend gedrag tegen cybercriminaliteit (Misana-ter Huurne, et al., 2019; Spithoven, 2020). Daarbij is het uitgangspunt dat – om effect te sorteren – risicocommunicatie inspeelt op de specifieke beleving van een doelgroep en de specifieke verklaringen voor de afwezigheid van zelfbeschermend gedrag onder deze doelgroep. Er is in de risicocommunicatie over cybercriminaliteit simpelweg geen *one size fits all* aanpak. De hoofdvraag van dit onderzoek luidt daarom:

Hoe is het gesteld met de cyberweerbaarheid van de Amersfoortse bevolking en hoe kan deze door de gemeente Amersfoort worden vergroot?

Om de hoofdvraag te beantwoorden, zijn de volgende deelvragen geformuleerd:

Deelvraag 1: Hoe is het gesteld met de risicoperceptie en het risicobewustzijn rondom cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?

Deelvraag 2: Hoe is het gesteld met het zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?

Deelvraag 3: Wat zijn de verklaringen voor het huidige zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?

Deelvraag 4: Hoe kan de gemeente Amersfoort het zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking vergroten?

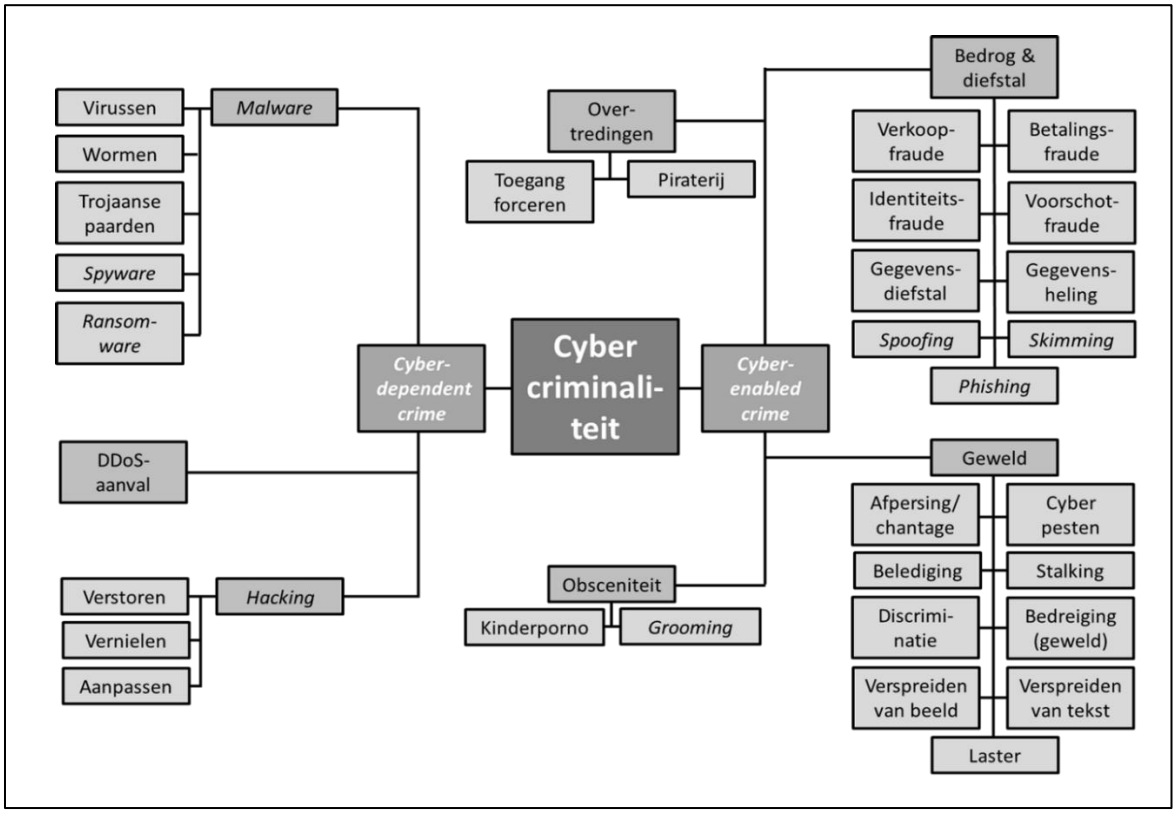
Een eerder ontwikkelde vragenlijst (Misana-ter Huurne et al., 2019) is uitgezet onder de respondenten van het Amersfoortse burgerpanel. Daarmee maken wij in dit rapport een beeld op van het huidige risicobewustzijn en zelfbeschermende gedrag van de respondenten en zoeken wij per doelgroep naar de specifieke verklaringen voor zelfbeschermend gedrag tegen de risico's van de volgende vormen van cybercriminaliteit: (I) phishing; (II) hacken; (III) gijzelsoftware; (IV) online koop- en verkoopfraude; (V) online psychisch geweld en (VI) cybercriminaliteit in het algemeen.

In het vervolg van dit rapport gaan we allereerst in op de theoretische achtergronden van dit onderzoek. Vervolgens bespreken we de steekproef van dit onderzoek en gaan we in op de vraag voor welke groepen binnen de Amersfoortse samenleving het onderzoek representatief is. In het opvolgende onderdeel beschrijven we het onder de respondenten aanwezige slachtofferschap van cybercriminaliteit waarna we overgaan tot een behandeling van de onder hen aanwezige risicoperceptie en het risicobewustzijn, de mate van zelfbeschermend gedrag en de informatiebehoefte van de respondenten. Bij de verklarende statistieken gaan we in op verklaringen voor het huidige zelfbeschermend gedrag voor cybercriminaliteit onder de doelgroepen die uit de exploratieve verkenning naar voren komen en bijzondere aandacht van de gemeente Amersfoort hadden (ouderen). Afsluitend brengen we algemeen advies uit voor risicocommunicatie rondom cybercriminaliteit en een specifiek advies per doelgroep in de Amersfoortse bevolking.

2. Theoretisch kader

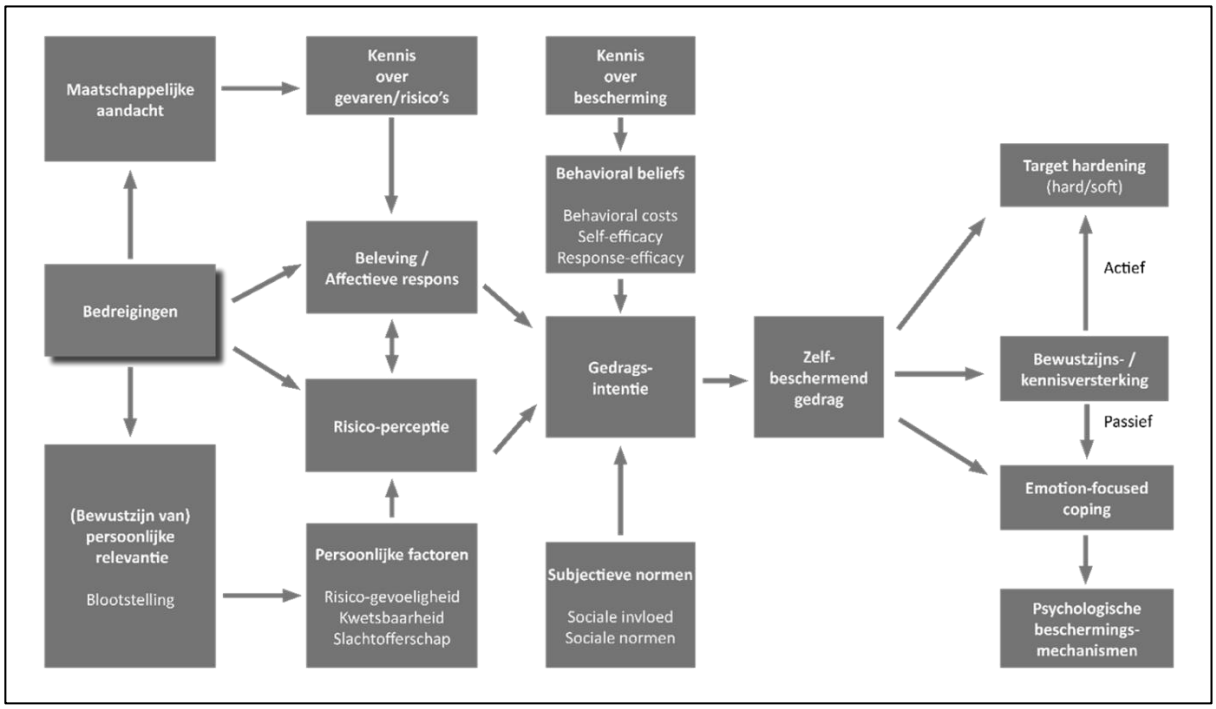
In de Westerse offline, fysieke wereld is de criminaliteit de afgelopen decennia onmiskenbaar gedaald. Dat is niet *out of the blue* gebeurd maar is het gevolg van een toegenomen mate van beveiliging, zo concluderen criminologen (De Jong, 2018; Farrell et al., 2011; 2014; Van Dijk, Tseloni & Farrell, 2012).De drijvende krachten achter de toegenomen beveiliging zijn logischerwijs: (I) een toegenomen maatschappelijk bewustzijn, (II) de overtuiging dat het eigen gedrag en de eigen maatregelen effect hebben op de kans op slachtofferschap, (III) een bereidheid in maatregelen te investeren of eigen gedrag aan te passen, en (IV) de mogelijkheid om maatregelen te treffen of het eigen gedrag aan te passen. Deze ontwikkeling van meer bescherming tegen slachtofferschap van criminaliteit in de offline wereld nemen we als basis voor aanzetten naar het vergoten van de cyberweerbaarheid in de gedigitaliseerde samenleving. Als neveneffect van de digitalisering hebben veel verschillende vormen van criminaliteit over de jaren ook een digitale variant gekregen.

Cybercriminaliteit omvat veel verschillende typen delicten. De literatuur onderscheidt doorgaans twee categorieën. Onder (I) cyber-enabled criminaliteit worden meer klassieke vormen van criminaliteit verstaan die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en phishing. Naast gedigitaliseerde, klassieke criminaliteit is er ook sprake van compleet nieuwe vormen van criminaliteit die zonder de nieuwe ICT onmogelijk zou zijn. Onder deze nieuwe vormen van (II) cyber-dependent crime wordt criminaliteit verstaan die wordt gepleegd door middel van ICT met ICT als doelwit, zoals bijvoorbeeld hacken, DDoS-aanvallen, virussen, ransomware en andere malware. Inmiddels is cybercriminaliteit een veelkoppig monster, elke categorie kent inmiddel vele verschijningsvormen zoals in de taxonomie van Spithoven in Figuur 1 goed is te zien.



Figuur 1 - Taxonomie van cybercriminaliteit (Spithoven 2020, p. 49).

Elke vorm van cybercriminaliteit kent zijn eigen wegen waarlangs het ontstaat, maar duidelijk is dat voor het gros van de cybercriminaliteit de mens en zijn omgang met technologie de zwakste schakel vormt. We moeten dus naast een focus op specifieke cyberdelicten ook oog hebben voor het feit dat iedere doelgroep uniek is en daarom risico's anders zal beleven, en het gedrag niet zomaar aan zal passen. In Figuur 2 is het theoretisch model opgenomen dat onderzoekers van het lectoraat Maatschappelijke Veiligheid ontwikkelden om inzicht te geven in de factoren en processen die zelfbeschermend gedrag beïnvloeden.



Figuur 2. Conceptueel model voor de verklaring van risicobeleving en zelfbeschermend gedrag rondom cybercriminaliteit (Spithoven 2020, p. 65, op basis van Misana – ter Huurne et al. 2019).

We leggen dit theoretische model nu op hoofdlijnen uit[1]. De individuele doelstelling om zelfbeschermend gedrag te vertonen in het nemen van maatregelen of het aanpassen van het eigen gedrag ontstaat onder invloed van verschillende factoren. Ten eerste is er de beleving van de risico-perceptie en de beleving (of de affectieve respons) die deze dreiging teweeg brengt. Deze twee factoren staan op hun beurt onder invloed van de kennis die het individu van het risico heeft en de maatschappelijke aandacht die het risico heeft ontvangen. Gezamenlijk leiden deze factoren tot een inschatting hoe relevant het risico voor het individu is. Dit wordt medebepaald door persoonlijke kenmerken zoals de risicogevoeligheid en de ingeschatte kwetsbaarheid van het individu.

Dit theoretisch model lag aan de basis van de vragenlijst die in dit onderzoek is gebruikt om de onderzoeksvraag 'Hoe is het gesteld met de cyberweerbaarheid van de Amersfoortse bevolking en hoe kan deze door de gemeente Amersfoort worden vergroot?' te beantwoorden. Aan de hand van de beschrijvende statistieken kijken we in dit rapport naar verschillen tussen doelgroepen en geven we aanzetten voor risico-communicatie op basis van de verklarende statistieken voor het zelfbeschermend gedrag van de doelgroepen (I) mannen, (II) vrouwen, (III) 21-30 jarigen; (IV) 65+ jarigen en (V) lager opgeleiden.

[1] Voor een meer gedetailleerde uitleg verwijzen wij u graag naar eerdere publicaties van Misana-ter Huurne et al. (2019), Spithoven (2020) en Leukfeldt, Spithoven & Misana (2020).

3. Onderzoeksmethode en steekproef

De kennisvraag van de gemeente Amersfoort rondom de cyberweerbaarheid van de inwoners heeft betrekking op een grote groep mensen: Amersfoort telde in 2020 157.279 inwoners. Daarmee is de onderzoeksmethode automatisch op een gestandaardiseerde vragenlijst uitgekomen (Babbie, 1998). Voor de afname van de vragenlijst is het bestaande burgerpanel van Amersfoort ingezet. Dit panel bestond op het moment van de afname van deze vragenlijst uit 6109 personen die woonachtig zijn in Amersfoort. Daarvan hebben 3003 respondenten de vragenlijst ingevuld en ligt de respons op afgerond 49 %. Omdat jongeren zijn ondervertegenwoordigd in het burgerpanel, heeft de gemeente Amersfoort aanvullend via sociale media geworven. Daar via deze oproep hebben nog eens 248 van de 664 benaderde personen de vragenlijst ingevuld. Dat maakt de respons via sociale media 37%. De verdeling van alle over de leeftijdscategorieën als volgt (Tabel 1).

Tabel 1 – Leeftijdsopbouw van de respondenten afgezet tegen de methode van dataverzameling.

		Onbekend	15 tot 20 jaar	21 tot 30 jaar	31 tot 45 jaar	46 tot 65 jaar	65+ jaar	Totaal
Burgerpanel *Respons 49%*	Aantal	43	39	140	550	1404	827	3002
	Procent	1%	1%	5%	18%	47%	28%	92%
Social Media *Respons 37%*	Aantal	171	1	10	9	34	23	248
	Procent	69%	0%	4%	4%	14%	9%	8%
Totaal	Aantal	214	40	150	559	1438	850	3251
	Procent	7%	1%	5%	17%	44%	26%	100%

In totaal hebben 3251 respondenten de vragenlijst ingevuld. De categorisering van de leeftijdscategorieën heeft plaatsgevonden aan de hand van de digitaliseringscohorten aan de hand van het werk van Kayser (2020). Vergeleken met de totale Amersfoortse populatie (15,3% is 65+ jaar oud en 8,1% is 18 tot 24 jaar oud; O&S Amersfoort, 2020), blijkt dat de steekproef niet volledig representatief is; jongeren zijn ondervertegenwoordigd en ouderen zijn oververtegenwoordigd.

Van de respondenten heeft 1,9% (n = 57) aangegeven geen opleiding te hebben afgerond op het moment van dit onderzoek, 8,3% (n = 257) gaf aan een middelbaar opleidingsniveau te hebben (vmbo, mulo of ulo) en 89,8% (n = 2766) een hoger opleidingsniveau of wo-niveau (havo, vwo, hbo of universiteit). Daarmee is duidelijk dat deze vragenlijst vooral is ingevuld door **hoogopgeleide respondenten van middelbare leeftijd.**

Van de respondenten is 94,8% (n = 2347) minimaal dagelijks online. Van deze groep is, 44,1% (n = 1093) meerdere keren per dag, 13,2% (n = 327) minimaal ieder uur tijdens de wakkere uren en 7,8% (n = 192) continu tijdens de wakkere uren, online. Interessant om te vermelden is dat er statistisch significante[2] verschillen zijn tussen leeftijdscategorieën in de mate van online zijn. Hierbij valt op dat de **21 tot 30 jarigen verhoudingsgewijs het meest online zijn** (minstens ieder wakker uur en haast continu).

[2] $X^2(35)= 261.39$, p.05.

4. Slachtofferschap van cybercriminaliteit

Van de respondenten is 7,8% (n = 221) het afgelopen jaar naar eigen zeggen slachtoffer geworden van cybercriminaliteit. Daarbij zijn er ***geen* statistisch significante verschillen tussen leeftijdscategorieën, geslacht of opleidingsniveau gevonden**. Het merendeel van de respondenten (89,6%, n = 2532) geeft aan dat zij het afgelopen jaar geen slachtoffer zijn geworden van cybercriminaliteit en 2,6% (n = 74) weet niet zeker of zij wel of geen slachtoffer zijn geworden. Middels het coderen van de open antwoorden is het volgende overzicht ontstaan (Tabel 2). **De slachtoffers van cybercriminaliteit hebben voornamelijk te maken gehad met diefstal en bedrog**[3], waarbij vooral slachtofferschap van respectievelijk verkoopfraude (o.a. via marktplaats); Microsoft oplichting; Neppe BitCoin-advertenties; Phishing en Identiteitsfraude zijn genoemd.

Tabel 2 – Verdeling van slachtofferschap over de totale steekproef en de subpopulatie van slachtoffers.

	Slachtofferschap in totale steekproef		Slachtofferschap in populatie slachtoffers	
	%	**n**	**%**	**n**
Diefstal en bedrog	5	144	63	144
Hacking	1,5	43	19	43
Online geweld	1	28	12	28
Malware	0,5	13	6	13
Totaal	7,8	2827	100	221

De financiële schade ten gevolge van slachtofferschap varieert tussen de 20 en 3500 euro. Naast de financiële schade geven veel respondenten aan dat zij emotionele schade ervaren ten gevolge van het incident: **Men is geschrokken, ervaart wantrouwen tegenover de medemens en is gefrustreerd.** Een respondent geeft hier bijvoorbeeld de volgende toelichting: “37 euro kwijt en mijn vertrouwen is geschaad. Ik heb er nog steeds een rot gevoel over” (R_{878}).

Daarnaast geven respondenten aan dat het slachtofferschap hen veel tijd heeft gekost omdat slachtofferschap veel rompslomp oplevert. Men moet een melding maken van het slachtofferschap, het kost tijd om de schade te herstellen en te verhalen. Respondenten geven hier bijvoorbeeld de volgende toelichtingen:
“Heel vervelend, niet persoonlijk maar weer werk om te herstellen en schade te verhalen” (R_{2891}).
“Administratieve rompslomp. Melding maken bij de bank en een nieuwe creditkaart ontvangen. Dit heeft ervoor gezorgd dat ik minder snel aankopen doe met de creditcard” (R_{1778}).
“Gedoe en een nieuw telefoonnummer voor mijn dochter” (R_{224}).

Iets meer dan de helft van de slachtoffers (52,8%, n = 114) heeft naar eigen zeggen ook melding gemaakt van het incident. **Van de mensen die hun slachtofferschap meldden, deed 39,1% (n = 45) dat bij de politie en 60,9% (n = 70) ging hiervoor naar de betrokken partij** (bijvoorbeeld een webwinkel) **of een landelijk meldpunt** (bijvoorbeeld fraudehelpdesk.nl).

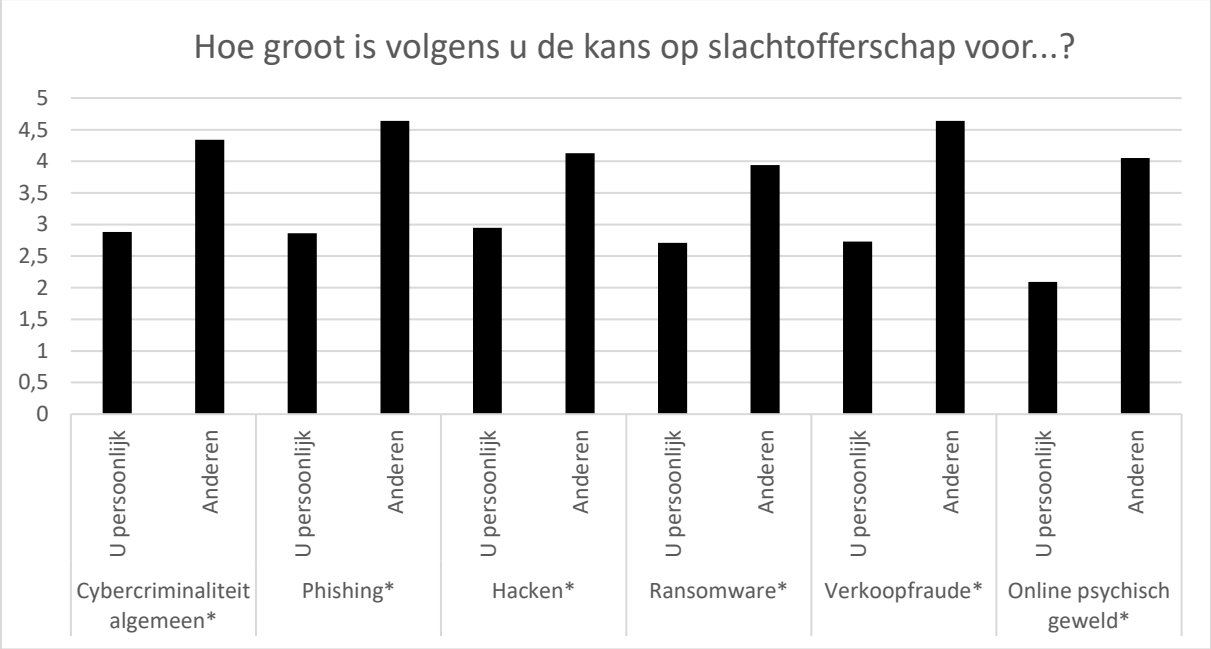
De slachtoffers die geen melding maakten gaven hiervoor als reden dat zij geen schade hebben geleden en de verwachting te hebben dat er niks met de melding wordt gedaan. Op de vraag of respondenten naar aanleiding van het slachtofferschap het eigen gedrag hebben aangepast antwoordt het merendeel bevestigend (74,6%, n = 126). **Respondenten die hun gedrag hebben aangepast na hun slachtofferschap geven vooral aan dat zij alerter zijn geworden** (71,4%, n = 90);

[3] In de categorie ‘diefstal en bedrog’ komt volgens Spithoven (2020) onder andere verkoop-; betalings-; identiteits- en voorschotfraude voor evenals gegevensdiefstal en –heling; *spoofing*, *skimming* en *phishing*.

wachtwoorden hebben gewijzigd (19%, n = 24) en extra beveiligingsmaatregelen zoals een virusscanner hebben aangeschaft (9,5%, n = 12). De reden dat andere slachtoffers hun gedrag niet aanpasten is dat zij naar eigen zeggen voor het slachtofferschap al alert waren en dit na het incident nog steeds zijn.

5. Risicoperceptie en - bewustzijn

De kansinschatting van respondenten om zelf het slachtoffer van cybercriminaliteit te worden is net onder gemiddeld: 2,88 (op een 6-puntsschaal). De modus (32,9 %) ligt dan ook op de keuze voor "kleine kans". De respondenten schatten de kans dat een gemiddelde Nederlander slachtoffer wordt van cybercriminaliteit significant[4] hoger in op 4,34 (op dezelfde 6-puntsschaal) en daarmee ligt de modus (39,7 %) op "grote kans". Er is onder de respondenten met andere woorden sprake van een *'optimistic bias',* waarbij men cybercriminaliteit als een risico beschouwt, maar zichzelf minder kwetsbaar acht dan anderen. **Deze *optimistic bias* is voor elk onderzocht type cybercriminaliteit statistisch significant** (met * in het overzicht gemarkeerd) **en met andere woorden van toepassing op alle in deze vragenlijst onderzochte vormen van cybercriminaliteit** (Figuur 3).



Figuur 3 – Illustratie van de consequent significante (gemarkeerd met *) optimistic bias onder respondenten.

Er zijn bij de inschatting van de eigen kans en de gevolgen van slachtofferschap de volgende significante verschillen zichtbaar voor:

- Leeftijdscategorieën[5]: **respondenten van 21 tot 30 jaar - nota bene de categorie die naar eigen zeggen het meest online is en daarmee volgens de wetenschappelijke literatuur** (Spithoven, 2020; Leukfeldt, 2016; Jansen et al., 2017) **meer risico loopt- gaf vaker aan 'geen kans' of een 'hele kleine kans' te ervaren om zelf het slachtoffer van cybercriminaliteit te worden.** Deze groep is overigens wel de groep die significant[6] sterker instemt met de stelling dat slachtofferschap van cybercriminaliteit hen ernstige schade op zou leveren;
- Geslacht[7]: mannen kozen opvallend vaker de uiterste categorieën van 'hele kleine kans' voor zichzelf en 'hele grote kans' voor anderen dan vrouwen in hun ervaren kans op

[4] T(2337)=55,80; p.001.
[5] $X^2(30)$= 80.47, p.05.
[6] $X^2(25)$= 53.01, p.05.
[7] $X^2(12)$= 58.00, p.05.

slachtofferschap van cybercriminaliteit. Vrouwen schatten schade ten gevolge van cybercriminaliteit significant[8] hoger in dan mannen;

- Opleidingsniveau[9]: **hoe lager opgeleid de respondenten waren, hoe vaker zij een (hele) kleine kans voor en hoe hoger opgeleid de respondenten waren, hoe vaker zij een (hele) grote kans op slachtofferschap van cybercriminaliteit voor zichzelf ervaren**. **Dus: hoe hoger het opleidingsniveau, hoe kleiner de aangetroffen optimistic bias.** Lager opgeleide respondenten stemden ook significant[10] minder vaak in met de stelling dat slachtofferschap van cybercriminaliteit hen ernstige schade op zou leveren.

De potentiële negatieve gevolgen van slachtofferschap worden door de respondenten relatief hoog ingeschat: 3,96 (op een 6-puntsschaal). Respondenten schatten de schade ten gevolge van gijzelsoftware het hoogst in: 4,11 en van online psychisch geweld het laagst in: 3,85 (op een 6-puntsschaal).

Het merendeel van de respondenten, 53% (n = 1474), geeft aan grotendeels of volledig te weten welke risico's zij lopen om slachtoffer te worden van cybercriminaliteit. Slechts 3,5% (n = 97) geeft aan helemaal niet te weten welke risico's zij lopen en 42,2% (n = 1174) zegt een beetje of enigszins een beeld hebben van zijn/haar persoonlijke risico's. Hierbij was een significant[11] verschil tussen mannen en vrouwen zichtbaar: **mannen zijn naar eigen zeggen beter op de hoogte van de risico's van cybercriminaliteit dan vrouwen**.

[8] $X^2(10)= 28,09$, p.05.
[9] $X^2(18)= 77.46$, p.05.
[10] $X^2(15)= 78.51$, p.05.
[11] Fisher exact = p.01.

6. Zelfbeschermend gedrag

6.1 Effectiviteitsverwachtingen

Ruim de helft van de respondenten (58,9%, n = 1642) geeft aan grotendeels of volledig te weten hoe zij zichzelf kunnen beschermen tegen cybercriminaliteit. De overige deelnemers weten niet (3,7%, n = 103), een beetje (11,4%, n = 317) of enigszins (25,1%, n = 698) hoe zij zich kunnen beschermen. **Ruim 40% van de respondenten, voornamelijk vrouwen[12], heeft duidelijke twijfels over hoe zij zich kunnen beschermen tegen cybercriminaliteit**. Voor leeftijd en opleidingsniveau waren er geen statistisch significante verschillen zichtbaar.

De respondenten zijn nog iets onzekerder over hun eigen kunnen om een poging tot cybercriminaliteit te herkennen. Van de respondenten geeft 4,7% (n = 129) aan helemaal niet te weten hoe zij cybercriminaliteit kunnen herkennen en denkt 39,1% (n = 1084) een beetje of enigszins te weten hoe een poging tot cybercriminaliteit herkend kan worden. Wel geeft meer dan de helft van de respondenten aan (55,2%, n = 1528) grotendeels of volledig te weten hoe zij een poging tot cybercriminaliteit kunnen herkennen. **Hierbij zijn vrouwen wederom significant[13] onzekerder dan mannen.** Voor leeftijd en opleidingsniveau waren er geen statistisch significante verschillen zichtbaar.

Wanneer men slachtoffer is geworden, dan weet 38,5 % (n= 1068) van de respondenten naar eigen zeggen hoe zij moeten handelen. Een deel van de respondenten (12,8%, n = 356) weet helemaal niet wat zij moeten doen en 46,5% (n = 1290) geeft aan een beetje of enigszins te weten wat zij moeten doen na slachtofferschap. **Ook hier bestaat een significant[14] verschil waarbij vrouwen naar eigen zeggen minder goed weten hoe te handelen na slachtofferschap dan mannen.** Voor leeftijd en opleidingsniveau waren er geen statistisch significante verschillen zichtbaar.

Effectiviteitsverwachtingen betreffen verder:
(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 net boven gemiddeld (3.32 op de 6-puntsschaal). **Mannen hebben hierbij significant[15] meer vertrouwen in hun eigen kunnen om zichzelf te beschermen tegen cybercriminaliteit, dan vrouwen.**

Responseffectiviteit
De respondenten vinden het over het algemeen nuttig om maatregelen te nemen om je tegen cybercriminaliteit te beschermen. Maar liefst 95,6% (n = 2559) is het (volledig) eens met de stelling: "*het is nuttig om maatregelen te treffen om je te tegen cybercriminaliteit te beschermen".* 76,6% (n = 1963) van de respondenten is het (volledig) oneens met de stelling: "*Maatregelen nemen heeft weinig zin; het verkleint de kans om slachtoffer van cybercriminaliteit te worden niet of nauwelijks".* Opvallend hierbij is dat er een significant verschil bestaat tussen mannen en vrouwen: **mannen**

[12] Fisher exact = p.01.
[13] Fisher exact = p.01.
[14] Fisher exact = p.01.
[15] Fisher exact = p.01.

vinden het nuttiger om maatregelen te treffen om je tegen cybercriminaliteit te beschermen dan vrouwen.[16]

Gedragseffectiviteit
Aan respondenten is gevraagd in hoeverre zij zelf vinden dat zij zichzelf voldoende beschermen tegen cybercriminaliteit. Dit wordt net boven gemiddeld beoordeeld (3.65 op een 5-puntsschaal). Bijna driekwart van de respondenten (73,3%, n = 1897) vindt dat de door hem/haar genomen maatregelen ervoor zorgen dat de kans om slachtoffer te worden van cybercriminaliteit afneemt.

6.2 Huidig zelfbeschermend gedrag

Een lijst van 25 zelfbeschermende maatregelen is aan de respondenten voorgelegd. Zij konden aangeven of zij de maatregelen reeds uitvoeren en daarnaast of er andere, niet in de vragenlijst aangedragen maatregelen zijn die zij uitvoeren. In Bijlage 1 is een overzicht opgenomen van deze zelfbeschermende maatregelen en hoe de respondenten zichzelf hierop scoorden. De meest voorkomende antwoorden zijn:

1. Controleren van afzenders van berichten op betrouwbaarheid (98%);
2. E-mails verwijderen die men niet vertrouwt (97,9%);
3. Updates direct na beschikbaarheid installeren (96,6%);
4. Gebruiken van sterke wachtwoorden met meerdere cijfers en tekens (96,3%);
5. Voorzichtig met openen van bijlagen (96,3%).

Van alle 25 antwoorden is een schaalscore geconstrueerd. Daarbij werd door de respondenten gemiddeld aangegeven dat zij 19 van de 25 maatregelen namen (minimum 1, maximum 25, S.D.=5,23). Daarbij zijn echter *geen* significante verschillen gevonden voor leeftijd, geslacht, opleidingsniveau, eerder slachtofferschap en de ingeschatte gevolgen van slachtofferschap van cybercriminaliteit. Wel significant[17] was het verschil tussen respondenten die hun kans op slachtofferschap van cybercriminaliteit hoog inschatten en respondenten die deze lager inschatten: hoe meer genomen maatregelen, hoe kleiner de kans werd ingeschat om zelf het slachtoffer van cybercriminaliteit te worden. In bijlage 1 zijn alle antwoordopties en de mate waarin respondenten ermee instemden terug te vinden.

6.3 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 (86,2%, n = 2036). Maar bij doorvragen *welke* maatregelen respondenten in de toekomst willen treffen, bleek dit streven minder concreet. De respondenten noemden daarbij overwegend de volgende maatregelen:

1. Beveiligingssoftware installeren en regelmatig updaten (25%);
2. Alert zijn wanneer met online is (mail, sites) (20%);
3. Verschillende, moeilijke wachtwoorden gebruiken en regelmatig wijzigen (17%);
4. Updates voor de pc installeren (9%);
5. Ontwikkelingen op het gebied van cybercriminaliteit volgen om kennis te vergaren (8%);
6. Regelmatig een back-up maken (6%).

---

[16] Fisher exact = p.01.
[17] $X^2(80)= 146,67$, p.05.

Sociale invloed
Meer dan de helft van de respondenten geeft aan dat mensen in hun omgeving het belangrijk vinden dat de respondenten zichzelf tegen cybercriminaliteit beschermen (62,1%) en zelfs van hen verwachten dat zij zelfbeschermende maatregelen treffen (70,2%). Verder geeft 9,7% aan het (volledig) oneens te zijn met de stelling "Mensen in mijn omgeving vinden het belangrijk dat ik mezelf tegen cybercriminaliteit bescherm" en 28,1% is het er niet mee eens en niet mee oneens. Wanneer het gaat om de stelling "Mensen in mijn omgeving verwachten dat ik mezelf tegen cybercriminaliteit bescherm" dan is 6,7% van de respondenten het er (volledig) mee oneens en is 23% het er niet mee eens en niet mee oneens.

Ondanks dat het merendeel van de respondenten aangeeft dat hun sociale omgeving het belangrijk vindt dat zij zichzelf beschermen tegen cybercriminaliteit en verwachten dat zij zelfbeschermende maatregelen nemen, is minder dan de helft van de respondenten door deze sociale invloed naar eigen zeggen ook daadwerkelijk geneigd om zichzelf te beschermen tegen cybercriminaliteit. Op de stelling "Ik ben geneigd om mezelf te beschermen, omdat anderen dat ook doen" wordt door respondenten dan ook verschillend gereageerd: 48,3% is het hier (volledig) mee oneens, 23,7% is het er (volledig) mee eens en 28,1% is het niet eens maar ook niet oneens met de stelling. De resultaten van de stelling "Ik ben geneigd om mezelf te beschermen, omdat mensen om mij heen dat van mij verwachten" geven een zelfde beeld: 48,3% is het hier (volledig) mee oneens, 25,2% is het er (volledig) mee eens en 26,5% is het niet eens maar ook niet oneens met de stelling.

7. Informatiebehoefte

Bijna de helft van de geënquêteerden (43,2%) geeft aan behoefte te hebben aan meer informatie over hoe men zichzelf beter kan beschermen tegen de risico's van cybercriminaliteit. Daarbij was het verschil tussen mannen en vrouwen significant[18]: 39% (n=552) van de mannen gaf aan behoefte te hebben aan meer informatie tegen 50% (n=1006) van de vrouwen. Ook het verschil in leeftijdscategorieën bleek significant[19]: hoe ouder de respondenten zijn, hoe minder behoefte zij aan deze informatie zeggen te hebben. Tenslotte was ook het verschil tussen opleidingsniveaus significant[20] voor deze vraag: verhoudingsgewijs geven de lager opgeleiden en hoger opgeleiden aan de meeste behoefte aan deze informatie te hebben, waar de middelbaar opgeleiden daar minder behoefte aan zeggen te hebben.

Het merendeel (81,9%) van de respondenten die aangaven behoefte te hebben aan meer informatie is ook bereid om zelf actief op zoek te gaan naar deze informatie. **Deelnemers hebben behoefte aan duidelijke en concrete informatie, die ook door "digibeten" te begrijpen is.** Het overgrote deel van de respondenten heeft naar eigen zeggen behoefte aan tips om zichzelf te beschermen tegen cybercriminaliteit. **Daarnaast willen mensen graag informatie ontvangen over de laatste ontwikkelingen en trends in cybercriminaliteit, hoe zij deze vormen van cybercriminaliteit kunnen herkennen en wat zij moeten doen als ze toch slachtoffer zijn geworden van cybercriminaliteit.** Respondenten vinden het belangrijk om deze informatie te ontvangen van een onafhankelijke en betrouwbare instantie. Uit de open vraag uit de desgevraagde toelichting hierop, blijkt respondenten dan denken aan de volgende instanties: de overheid in het algemeen (34%, n = 229), de gemeente (17%, n = 115), deskundigen op het gebied van beveiliging (9%, n = 57) en de politie (6%, n = 41). Ten slotte vinden mensen dat de bedrijven die online diensten aanbieden (o.a. internetprovider) ook een verantwoordelijkheid hebben om hun klanten te informeren over de risico's ten aanzien van cybercriminaliteit en hoe deze risico's te beperken (13%, n = 89).

[18] $X^2(1)= 29,05$, p.05.
[19] $X^2(5)= 13,40$, p.05.
[20] $X^2(3)= 14,43$, p.05.

8. Conclusies ten aanzien van beschrijvende statistieken

In dit onderdeel trekken we op basis van de resultaten van de beschrijvende statistieken de conclusies voor de eerste twee deelvragen van dit onderzoek:

Deelvraag 1: Hoe is het gesteld met de risicoperceptie en het risicobewustzijn rondom cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?

Deelvraag 2: Hoe is het gesteld met het zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?

Slachtofferschap van cybercriminaliteit is gelijkmatig over de respondenten verdeeld: er zijn geen statistisch significante verschillen tussen leeftijdscategorieën en geslacht aangetroffen. De slachtoffers van cybercriminaliteit hebben voornamelijk te maken gehad met diefstal en bedrog. Het slachtofferschap van cybercriminaliteit heeft grote impact op de slachtoffers: Men is geschrokken, ervaart wantrouwen tegenover de medemens en is gefrustreerd. Daarnaast geven respondenten aan dat het slachtofferschap hen veel tijd heeft gekost. Van de mensen die hun slachtofferschap meldden, deed men dat vooral bij de betrokken partij als een bank of een landelijk meldpunt als de Fraudehelpdesk en veel minder bij de politie. De slachtoffers die geen melding maakten gaven hiervoor als reden dat zij geen schade hebben geleden of de verwachting te hebben dat er niks met de melding wordt gedaan. Respondenten die hun gedrag hebben aangepast na hun slachtofferschap geven vooral aan dat zij alerter zijn geworden.

Er is een consequente *optimistic bias* zichtbaar onder de respondenten: Voor alle in deze vragenlijst onderzochte vormen van cybercriminaliteit schatten de respondenten de kans op eigen slachtofferschap significant lager in dan voor anderen. De **leeftijdscategorie 21 tot 30 jaar** - nota bene de categorie die naar eigen zeggen het meest online is - gaf vaker aan ‘geen kans’ of een ‘hele kleine kans’ te ervaren om zelf het slachtoffer van cybercriminaliteit te worden. Hoe **lager opgeleid** de respondenten waren, hoe vaker zij een (hele) kleine kans en hoe hoger opgeleid de respondenten waren, hoe vaker zij een (hele) grote kans op slachtofferschap van cybercriminaliteit ervaren.

De potentiële negatieve gevolgen van slachtofferschap worden door de respondenten relatief hoog ingeschat. Het merendeel van de respondenten, 53% (n = 1474), geeft aan grotendeels of volledig te weten welke risico’s zij lopen om slachtoffer te worden van cybercriminaliteit. Mannen zijn naar eigen zeggen beter op de hoogte van de risico’s van cybercriminaliteit dan vrouwen. Voornamelijk **vrouwen** hebben duidelijke twijfels over hoe zij zich kunnen beschermen tegen cybercriminaliteit. Ook zijn vrouwen onzekerder over hoe zij een poging tot cybercriminaliteit kunnen herkennen. Ook twijfelen vrouwen meer aan het nut van het nemen van maatregelen tegen cybercriminaliteit.

Ondanks dat het merendeel van de respondenten aangeeft dat hun sociale omgeving het belangrijk vindt dat zij zichzelf beschermen tegen cybercriminaliteit en verwachten dat zij zelfbeschermende maatregelen nemen, is minder dan de helft van de respondenten door deze sociale invloed naar eigen zeggen ook daadwerkelijk geneigd om zichzelf te beschermen tegen cybercriminaliteit.

Respondenten hebben behoefte aan duidelijke en concrete informatie die ook door “digibeten” te begrijpen is. Daarnaast willen mensen graag informatie ontvangen over de laatste ontwikkelingen en trends in cybercriminaliteit, hoe zij deze vormen van cybercriminaliteit kunnen herkennen en wat zij moeten doen als ze toch slachtoffer zijn geworden van cybercriminaliteit.

Op basis van de beschrijvende statistieken komen de volgende doelgroepen voor risicocommunicatie in Amersfoort in beeld: (I) vrouwelijke inwoners; (II) 21 tot 30 jarige inwoners en (III) lager opgeleide

inwoners. Daarnaast gaf de gemeente Amersfoort te kennen ook interesse te hebben in de doelgroepen (IV) mannen en (V) 65+ jarige inwoners.

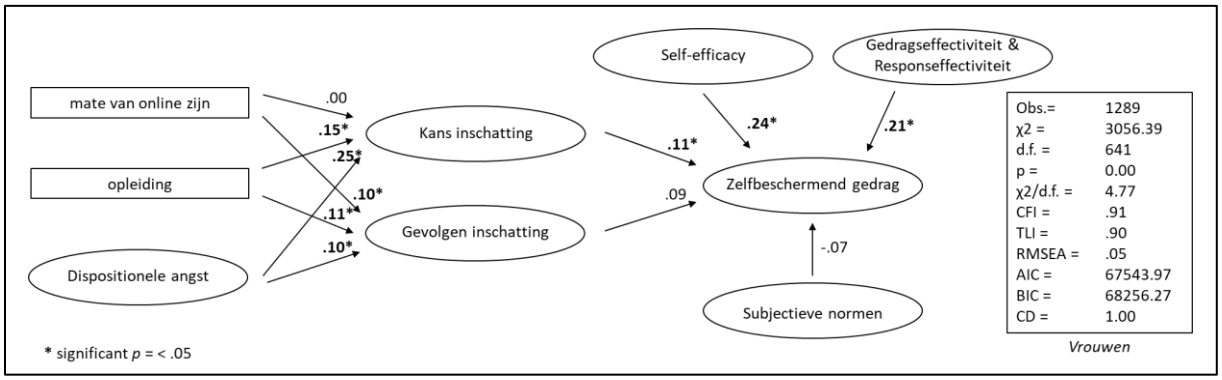
Deze vijf doelgroepen zullen dan ook middels *Structural Equation Modelling*[21] verder worden onderzocht om verklaringen voor het zelfbeschermend gedrag te vinden waar met risicocommunicatie op kan worden ingespeeld.

[21] Structural Equation Modelling is het beste samen te vatten als een integratie van verschillende statistische technieken als regressieanalyse, factoranalyse en schaalconstructies. Hiermee kunnen onderlinge verbanden tussen concepten op een gedetailleerde manier worden berekend, waarbij expliciet rekening wordt gehouden met onderlinge afhankelijkheid en de onderlinge samenhang van meerdere variabelen.

9. Verklarende statistieken

In dit onderdeel beantwoorden we deelvraag 3 van dit onderzoek '*Wat zijn de verklaringen voor het huidige zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking?'* door de antwoorden op de vragenlijst voor de theoretische concepten uit het theoretisch model (Figuur 4) op elkaars verklaringskracht door te rekenen. Hierbij ontbreken de concepten responseffectiviteit en de kennis van risico's en gevolgen van slachtofferschap van cybercriminaliteit omdat deze omwille van de omvang niet in de vragenlijst waren opgenomen. We behandelen achtereenvolgend de doelgroepen (I) vrouwelijke inwoners; (II) mannelijke inwoners; (III) 21 tot 30 jarige inwoners; (IV) 65+ jarige inwoners en (V) lager opgeleide inwoners.

9.1 Vrouwelijke inwoners



Figuur 4 – SEM voor het zelfbeschermend gedrag van vrouwelijke inwoners.

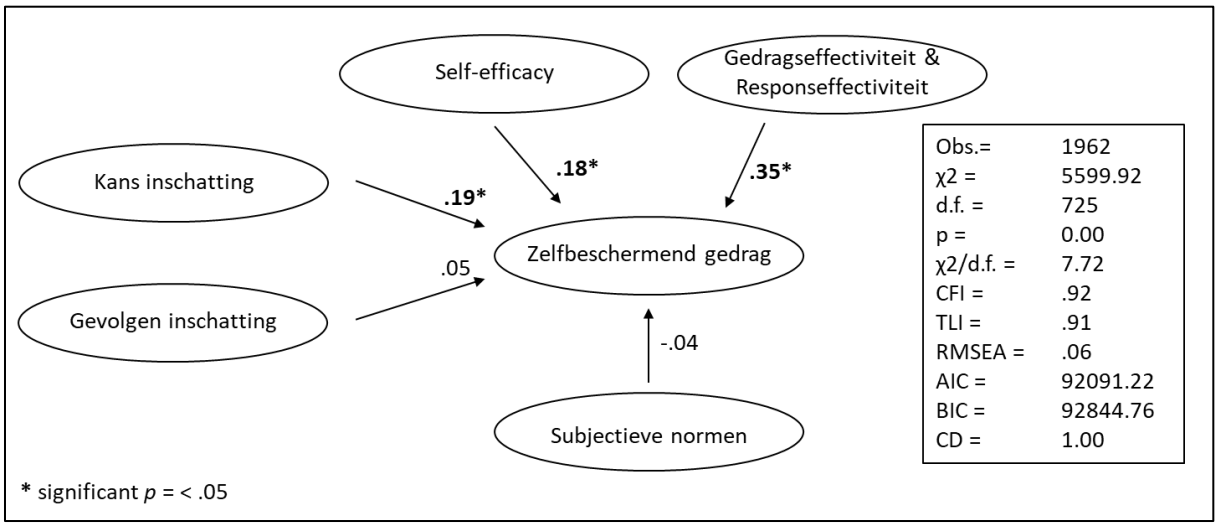
Het huidige zelfbeschermend gedrag van de vrouwelijke respondenten (Figuur 4) wordt vooral verklaard door *self-efficacy*: de overtuiging om in staat te zijn zichzelf te beschermen tegen of adequaat te handelen bij dreigend slachtofferschap van cybercriminaliteit.

Ook is de ervaren *gedragseffectiviteit en effectiviteitsverwachtingen* bij deze doelgroep van belang. Dit zijn de overtuigingen dat (I) men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt; (II) dat de genomen maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden en (III) het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen.

Tevens is de kans inschatting van invloed op het zelfbeschermend gedrag onder deze doelgroep. Dat betekent dat hoe hoger men de kans inschat om slachtoffer van cybercriminaliteit te worden, hoe sterker men zelfbeschermend gedrag rapporteert. Deze kans inschatting wordt overigens indirect verklaard door:

I. opleidingsniveau – hoger opgeleiden rapporteren een hogere kans inschatting;
II. mate van online zijn – meer online actieven rapporteren een hogere kans inschatting;
III. dispositionele angst – angstigere respondenten rapporteren een hogere kans inschatting.

9.2 Mannelijke inwoners

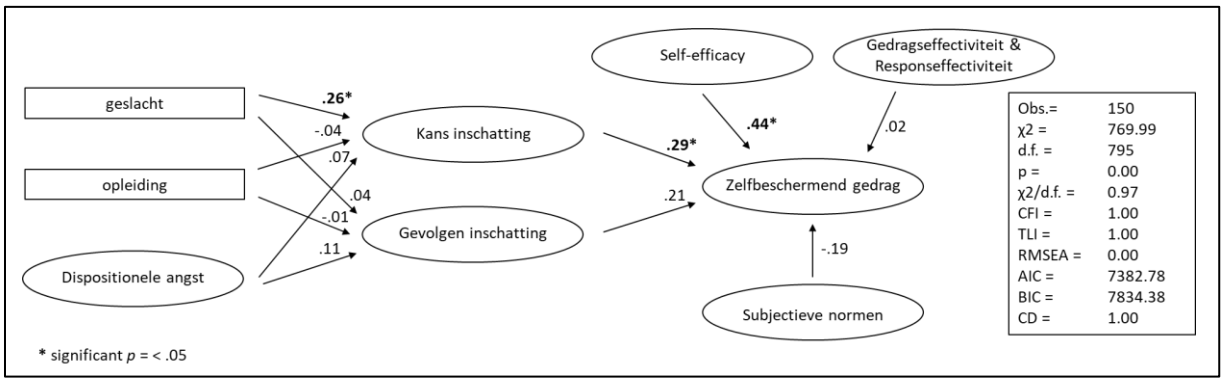


Figuur 5 – SEM voor het zelfbeschermend gedrag van mannelijke inwoners.

Het huidige zelfbeschermend gedrag van de mannelijke respondenten (Figuur 5) wordt vooral verklaard door de *gedragseffectiviteit en de responseffectiviteit*: Dit zijn de overtuigingen dat (I) men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt; (II) dat de genomen maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden en (III) het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen.

Ook is de *kansinschatting* voor het slachtofferschap van cybercriminaliteit voor deze doelgroep van invloed.

9.3 21 tot 30 jarige inwoners



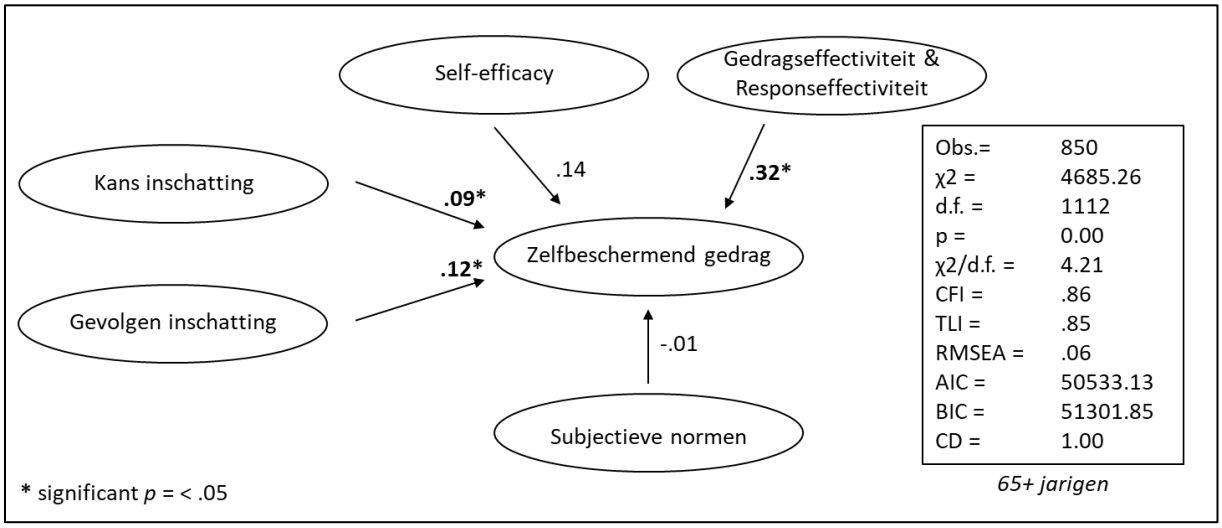
Figuur 6 – SEM voor het zelfbeschermend gedrag van 21 tot 30 jarige inwoners.

Het huidige zelfbeschermend gedrag van 21 tot 30 jarige inwoners (Figuur 6) wordt vooral verklaard door *self-efficacy*: de overtuigingen te weten (I) hoe zich tegen cybercriminaliteit te beschermen; (II) welke risico's men loopt om slachtoffer van cybercriminaliteit te worden; (III) hoe een poging tot cybercriminaliteit kan worden herkent en (IV) wat men moet doen als men slachtoffer wordt van cybercriminaliteit.

Ook is de kans inschatting om slachtoffer te worden van cybercriminaliteit – in de vorm van (I) algemene dreiging; (II) phishing; (III) hacking; (IV) gijzelsoftware; (V) online koop- en verkoopfraude en (VI) online psychisch geweld - van invloed op het zelfbeschermend gedrag onder 21 tot 30 jarige

Amersfoortse respondenten. De invloed van de kans inschatting op het zelfbeschermend gedrag wordt voor een goed deel indirect verklaard door de invloed van geslacht onder deze respondenten: vrouwen schatten hun kans om slachtoffer te worden van cybercriminaliteit hoger in dan mannen.

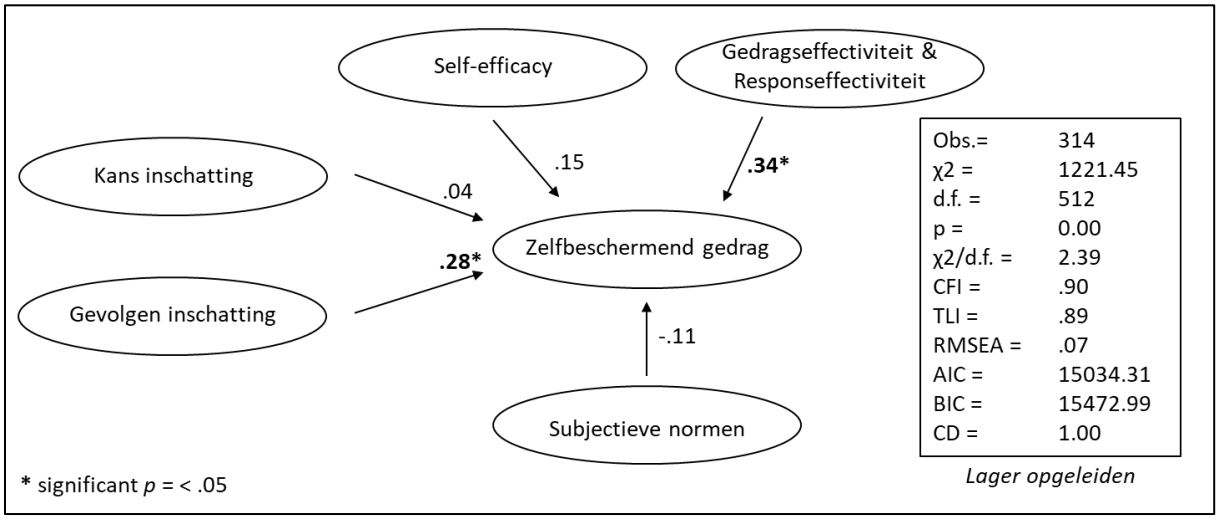
9.4 65+ jarige inwoners



Figuur 7 – SEM voor het zelfbeschermend gedrag van 65+ jarige inwoners.

Het huidige zelfbeschermend gedrag onder 65+ jarige inwoners (Figuur 7) wordt vooral verklaard door de *gedragseffectiviteit* en responseffectiviteit. Dit zijn de overtuigingen dat (I) men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt; (II) dat de genomen maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden en (III) het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen. Daarnaast is ook de inschatting van de *gevolgen* maar ook de inschatting van de *kans* op slachtofferschap van cybercriminaliteit van invloed op het zelfbeschermend gedrag: hoe zwaarder men de gevolgen en hoe groter men de kans inschat, hoe meer men aangeeft zelfbeschermend gedrag te vertonen.

9.5 Lager opgeleide inwoners



Figuur 8 – SEM voor het zelfbeschermend gedrag van lager opgeleide inwoners.

Het huidge zelfbeschermend gedrag van lager opgeleide respondenten (Figuur 8) wordt vooral verklaard door de ervaren gedragseffectiviteit en de responseffectiviteit. Dit zijn de overtuigingen dat (I) men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt; (II) dat de genomen maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden en (III) het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen. Ook wordt het zelfbeschermend gedrag van deze doelgroep verklaard door de gevolgen inschatting van slachtofferschap van cybercriminaliteit.

10. Aanzetten voor gerichte risico-communicatie

In dit laatste onderdeel van het onderzoeksrapport zullen we de laatste deelvraag van dit onderzoek beantwoorden: *'Hoe kan de gemeente Amersfoort het zelfbeschermend gedrag tegen slachtofferschap van cybercriminaliteit onder doelgroepen binnen de Amersfoortse bevolking vergroten?'*. Achtereenvolgend bespreken we (I) aanzetten voor algemene risico-communicatie rondom cybercriminaliteit en richtlijnen voor de risico-communicatie aan de specifieke doelgroepen: (II) vrouwelijke inwoners; (III) mannelijke inwoners; (IV) 21 tot 30 jarige inwoners; (V) 65+ jarige inwoners en (VI) lager opgeleide inwoners.

10.1 Richtlijnen voor algemene risico-communicatie

- ➔ Gedragsverandering gaat niet over één nacht ijs, daar is tijd voor nodig. Laat daarom de risicocommunicatie ten aanzien van cybercriminaliteit structureel op natuurlijke momenten/plekken terugkomen voor de specifieke doelgroepen. Risicocommunicatie is *nooit* een eenmalige interventie, want pas bij enkele herhalingen van de boodschap wordt deze door de doelgroepen opgepakt.

- ➔ Zorg voor gelaagdheid in informatie: de behoefte aan informatie is groot, maar dynamisch; deze varieert van persoon tot persoon: sommige inwoners 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 risico's. Zorg daarom voor een koppeling tussen (doelgroep)gerichte communicatie activiteiten en een (online) platform waarop men onafhankelijke en betrouwbare informatie kan vinden over algemene informatie en actuele trends op het gebied van cybercriminaliteit.

- ➔ Richt algemene risico-communicatie over cybercriminaliteit in Amersfoort op het doorbreken van de *optimistic bias* met de volgende basisboodschap:

  Het kan jou WEL overkomen, slachtofferschap van cybercriminaliteit komt even vaak voor onder alle Amersfoorters!

- ➔ Besteed daarbij extra aandacht aan de specifieke risico's van gijzelsoftware omdat de kans op slachtofferschap van deze vorm van cybercriminaliteit als relatief laag door de respondenten werd ingeschat terwijl bijna één op de tien respondenten de afgelopen twaalf maanden slachtoffer is geworden.

- ➔ Geef elk van de onderstaande, specifiekere doelgroepen in begrijpelijke taal informatie over de laatste ontwikkelingen en trends in cybercriminaliteit, hoe zij deze vormen van cybercriminaliteit kunnen herkennen en voorkomen en wat zij in algemene zin moeten doen als ze toch slachtoffer zijn geworden van cybercriminaliteit.

- ➔ Voor nagenoeg elke, nader onderzochte doelgroep (met uitzondering van de 21 tot 30 jarige inwoners) bleek dat de gedragseffectiviteit en responseffectiviteit van significante invloed op het huidige zelfbeschermende gedrag te zijn. Besteed aandacht aan 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).

➔ Richt daarmee de algemene risicocommunicatie op de volgende componenten:
- de vraag of men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermd voelt en of dat wel echt zo is;
- de vraag of alle maatregelen die men neemt tegen slachtofferschap van cybercriminaliteit wel alle actuele risico's afdekt;
- het onderbouwen van het nut van aanvullende maatregelen, concreet kunnen de volgende maatregelen meer worden gestimuleerd:
(I) openbare Wi-Fi niet gebruiken;
(II) zoveel mogelijk dubbele verificatie aanzetten;
(III) geen films, muziek en/of games downloaden i.v.m. malware;
(IV) profielsites (zoals Facebook, Instagram) niet langer openbaar houden;
(V) belangrijke bestanden met een wachtwoord versleutelen;
(VI) browser extensies ten behoeve van cybersecurity installeren, zoals adblockers;
(VII) wachtwoorden opslaan in een password manager, met voor elk account een ander sterk wachtwoord;
(VIII) een VPN-verbinding gaan gebruiken.

10.2Vrouwelijke inwoners

Vrouwen hebben in vergelijking tot mannen duidelijke twijfels over hoe zij zich kunnen beschermen tegen cybercriminaliteit. Ook zijn vrouwen onzekerder over hoe zij een poging tot cybercriminaliteit kunnen herkennen en twijfelen zij meer aan het nut van het nemen van maatregelen tegen cybercriminaliteit. Opvallend is echter wel dat er onder de respondenten geen verschil is aangetroffen in de omvang van het slachtofferschap van mannen en vrouwen.

➔ Speel allereerst in op de beleefde kans op slachtofferschap van cybercriminaliteit.
Hoe groot is jouw kans om slachtoffer van cybercriminaliteit te worden?
Doorbreek daarbij het gevoel van onzekerheid onder deze doelgroep met de boodschap:
Jij kunt zelf simpele maatregelen treffen, die je goed tegen slachtofferschap van cybercriminaliteit beschermen, zoals…

➔ Ondersteun deze doelgroep met toegankelijke informatie over hoe zij pogingen tot cybercriminaliteit kunnen herkennen. Dit draagt bij aan het vergroten van de *self efficacy* en daarmee het vertrouwen in eigen kunnen om zichzelf te beschermen. Richt je hierbij op:
- Hoe zij zich tegen verschillende vormen van cybercriminaliteit kunnen wapenen;
- Hoe zij pogingen tot cybercriminaliteit kunnen herkennen;
- Wat zij moeten doen als zij slachtoffer worden van cybercriminaliteit;
- Waar ze aanvullende informatie kunnen vinden.

➔ Vergroot, in aanvulling op het verhogen van de self-efficacy, de responseffectiviteit van aanbevolen maatregelen of gedragingen. Wanneer vrouwen een hoger vertrouwen hebben in eigen kunnen om zichzelf te beschermen èn het nut inzien van de gedragsadviezen, dan zijn zij eerder geneigd deze op te volgen. Geef daarom duidelijk aan waarom het nuttig en effectief is om maatregelen te treffen.
- Bestendig onder deze doelgroep de opvatting dat maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden;
- Bestendig ook de opvatting dat het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen.

- ➔ Zorg dat in eerste instantie eenvoudige en effectieve adviezen worden gegeven, waardoor de drempel zo laag mogelijk is om ze uit te voeren. Koppel dit aan 'storytelling': ervaringsverhalen van vrouwen die slachtoffer zijn geworden en laten zien wat de impact is (geweest), in combinatie met direct toepasbare gedragsadviezen om dit te voorkomen. Hiermee draagt deze communicatie bij aan de responseffectiviteit van de doelgroep.

10.3 Mannelijke inwoners

Bij de mannelijke inwoners is sterkere *optimistic bias* aangetroffen dan bij vrouwen. Mannen geven ook verhoudingsgewijs vaak aan dat zij meer vertrouwen hebben in eigen kunnen om zichzelf te beschermen dan vrouwen.

- ➔ Speel allereerst in op de grotere optimistic bias ten aanzien van de kans op slachtofferschap van cybercrime onder mannen, waarbij het doel is om de kansinschatting om zelf slachtoffer te worden verhoogd wordt. Toon bijvoorbeeld een foto van een zelfverzekerde man met de vraag: *Alles onder controle zeker?* En geef daarbij de informatie dat ondanks het gevoel van controle ook mannen zeker slachtoffer van cybercriminaliteit worden en ook mannen zich sterker tegen slachtofferschap van cybercriminaliteit kunnen beschermen.

- ➔ Ondersteun deze doelgroep ook door hen toegankelijke informatie te geven over welke maatregelen tegen slachtofferschap van cybercriminaliteit waarom werken. Speel daarbij ook in op de ervaren *gedragseffectiviteit en responseffectiviteit* bij deze doelgroep:
  - Laat deze doelgroep reflecteren op de vraag of men zich echt voldoende tegen slachtofferschap van cybercriminaliteit beschermt;
  - Bestendig onder deze doelgroep de opvatting dat aanvullende maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden;
  - Geef ook aan dat cybercrime zich ontwikkelt en dat zelfbeschermende maatregelen ook aanpassing vereisen, waardoor men continu alert moet blijven en niet te snel en makkelijk het idee moet hebben dat men wel voldoende beschermd is.

- ➔ Ondersteun ook deze doelgroep met toegankelijke informatie hoe zij pogingen tot cybercriminaliteit kunnen herkennen. Speel daarbij in op de *self efficacy* van deze doelgroep met toegankelijke, gerichte boodschappen over:
  - Welke vormen van cybercriminaliteit zij slachtoffer van kunnen worden;
  - Hoe zij zich tegen verschillende vormen van cybercriminaliteit kunnen wapenen;
  - Hoe zij pogingen tot cybercriminaliteit kunnen herkennen;
  - Wat zij moeten doen als zij slachtoffer worden van cybercriminaliteit.

10.4 21 tot 30 jarige inwoners

Besteed ook gerichte aandacht aan de 21 tot 30 jarige inwoners: zij gaven vaker aan 'geen kans' of een 'hele kleine kans' te ervaren om zelf het slachtoffer van cybercriminaliteit te worden terwijl zij naar eigen zeggen het meest online zijn. Er is consensus in de wetenschap dat meer online zijn, de kans op slachtofferschap van cybercriminaliteit vergroot (Leukfeldt, 2016; zie ook Jansen et al., 2017).

- ➔ Doorbreek de beleefde controle onder deze doelgroep met de basisboodschap:
  Hoe vaak ben jij ieder wakker uur wel online? Dan heb jij een grote kans op slachtofferschap van cybercriminaliteit!

- ➔ Speel in op de *self efficacy* van deze doelgroep met toegankelijke, gerichte boodschappen over:
  - Welke vormen van cybercriminaliteit zij slachtoffer van kunnen worden;
  - Hoe zij zich tegen verschillende vormen van cybercriminaliteit kunnen wapenen;
  - Hoe zij pogingen tot cybercriminaliteit kunnen herkennen;
  - Wat zij moeten doen als zij slachtoffer worden van cybercriminaliteit.

- ➔ Laat deze doelgroep nadenken over hun kansen om slachtoffer te worden van verschillende vormen van cybercriminaliteit door hen een vergelijking met senioren te laten maken. Voorbeeld: Toon een foto van één 25 jarige en één 65+ jarige man, bij een andere interventie worden vrouwen getoond en stel daarbij de vraag *Wie van deze twee heeft een grotere kans om slachtoffer van phishing te worden denk je? Guess again! Senioren en jongeren worden in dezelfde mate slachtoffer van deze vorm van cybercriminaliteit!*

10.6 65+ jarige inwoners

Besteed bij de gerichte risicocommunicatie aan 65+ jarige inwoners vooral aandacht aan de volgende punten:

- ➔ Start met het risicobewustzijn en de risicoperceptie: Maak deze doelgroep meer bewust van de *gevolgen* van slachtofferschap van cybercriminaliteit aan de hand van authentieke slachtofferervaringen van personen die tot deze doelgroep behoren.
- ➔ Laat deze doelgroep reflecteren op hun *kans* om slachtoffer te worden van cybercriminaliteit, bijvoorbeeld door hen uit te leggen hoe criminelen *social engineering* toepassen.
- ➔ Zorg dat deze communicatie altijd wordt gekoppeld aan het vergroten van de *gedragseffectiviteit en de responseffectiviteit:*
  - Laat deze doelgroep reflecteren op de vraag of men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt;
  - Bestendig onder deze doelgroep de opvatting dat maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden;
  - Bestendig ook de opvatting dat het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen.
  - Geef hierbij aan dat men simpel zelf maatregelen kan treffen die heel nuttig zijn om de kans op slachtofferschap te verkleinen.

10.5 Lager opgeleide inwoners

Besteed tenslotte ook gerichte aandacht aan lager opgeleide inwoners, zij beleven een opvallend lage kans om slachtoffer van cybercriminaliteit te worden.

- ➔ Speel bij deze doelgroep allereerst in op het vergroten van de risicoperceptie met authentieke slachtofferverhalen zodat zij een grotere kans op slachtofferschap van cybercriminaliteit zullen ervaren.
- ➔ Speel daarnaast in op de gevolgen inschatting van slachtofferschap van cybercriminaliteit.
- ➔ Speel daarna vooral in op de *gedragseffectiviteit en de responseffectiviteit:*
  - Laat deze doelgroep reflecteren op de vraag of men zich voldoende tegen slachtofferschap van cybercriminaliteit beschermt;
  - Bestendig onder deze doelgroep de opvatting dat maatregelen tegen slachtofferschap van cybercriminaliteit ervoor zorgen dat men minder kans loopt hier slachtoffer van te worden;
  - Bestendig ook de opvatting dat het nuttig is om maatregelen tegen slachtofferschap van cybercriminaliteit te nemen.

Geraadpleegde literatuur

Babbie (1998) *The practice of social research*. Wadsworth Publishing Company.

De Jong, J. (2018). *Het mysterie van de verdwenen criminaliteit*. CBS.

Farrell, G., Tseloni, A., Mailley, J. & Tilley, N. (2011). The crime drop and the security hypothesis. *Journal of Research in Crime and Delinquency*, 48(2), 147-175.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. & van der Zee, S. (2017). Victims. In: E.R. Leukfeldt (Ed.), *The human factor in cybercrime and cybersecurity* (p. 45-52). Den Haag: Eleven International Publishing.

Kayser, C.S. (2020). *Cybercrime trough social engineering. The new global crisis*. Cybercrime Analytics Inc..

Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Eleven International Publishers.

Leukfeldt, E.R., Spithoven, R. & Misana - ter Huurne, E.F.J. (2020). De lokale aanpak van cybercriminaliteit. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In: C. de Poot et al. (eds.) *Politie en cybercriminaliteit.* Cahiers Politiestudies, 56, 203-222.

Misana - ter Huurne, E.F.J., van Houten, Y.A., Spithoven, R., Notté, R.J. & Leukfeldt, E.R. (2020). *Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb'ers.* Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion & Lectoraat Cybersecurity in het mkb, De Haagse Hogeschool.

O&S Amersfoort (2020). *Amersfoort in cijfers*. Via: https://amersfoortincijfers.nl/dashboard/bevolking (laatst geraadpleegd op 09-12-2020).

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Boom Criminologie.

Van Dijk, J.J.M., Tseloni, A. & Farrell, G. (Eds.). (2012). *The international crime drop: New directions in research*. Palgrave MacMillan.

Bijlage 1 – Overzicht van gerapporteerd zelfbeschermend gedrag

Zelfbeschermende maatregel	Percentage 'ja'
Ik controleer of de afzender van een e-mail betrouwbaar is.	98
Ik verwijder e-mails die ik niet vertrouw direct.	97,9
Ik installeer updates zodra deze beschikbaar zijn.	96,6
Ik gebruik sterke wachtwoorden met meerdere cijfers en tekens.	96,3
Ik ben voorzichtig met het openen van bijlagen.	96,3
Ik ben voorzichtig met het aanklikken van links.	95,1
Ik let bij het internetten of online betalen op of er sprake is van een beveiligde verbinding (HTTPS of het 'slotje' in de adresbalk).	92,6
Ik gebruik een virusscanner.	92,1
Ik vermijd onveilige websites.	90,7
Ik vergrendel mijn apparaten als ik deze niet gebruik.	86,3
Ik maak een back-up (reservekopie) van mijn waardevolle bestanden.	85,6
Ik gebruik een vergrendelingscode of wachtwoord op al mijn apparaten.	85,4
Ik gebruik een firewall (hiermee worden ongewenste verbindingen geblokkeerd).	85
Ik kijk naar het bestandstype voordat ik bijlagen open.	84,7
Ik controleer de privacy-instellingen van mijn apparaten, apps of sociale media.	83,1
Ik geef mijn inloggegevens niet aan onbekenden.	78,4
Ik vermijd het gebruik van openbare Wi-Fi.	70,6
Ik gebruik dubbele verificatie op mijn accounts.	70
Ik download geen films, muziek en/of games op illegale wijze.	69,4
Ik heb mijn profielsites (zoals Facebook, Instagram) niet openbaar staan.	64,2
Ik gebruik hetzelfde wachtwoord voor verschillende toepassingen.	59,4
Ik versleutel belangrijke bestanden met een wachtwoord of andere beveiliging.	48,1
Ik gebruik een browser extensie, zoals een adblocker.	42
Ik sla mijn wachtwoorden op in een password manager.	38,1
Ik gebruik een VPN-verbinding (Virtual Private Network, hiermee kunt u anoniem internetten).	34