CYBERWEERBAARHEID

Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime.

Eindrapport - *Werkpakket 5*

COLOFON

Dit onderzoek is uitgevoerd door het consortium bij het project
'Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime':
Dr. Remco Spithoven[1]
Dr. Rutger Leukfeldt[2,3]
Dr. Ellen Misana-ter Huurne[1]
Dr. Susanne van 't Hoff – de Goede[2]
Dr. Ynze van Houten[1]
Luuk Bekkers MSc.[2,1]
Elsa Foppen MSc.[1]
Joyce te Bos MSc.[1]
[1] Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion.
[2] Lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool.
[3] Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR).

Het consortium is een samenwerking van:

Hogeschool Saxion
Veiligheidsalliantie Regio Rotterdam
Regionale Veiligheidsstrategie Midden Nederland
Noord-Holland Samen Veilig
Veiligheidsnetwerk Oost-Nederland
Gemeente Almere
Gemeente Amersfoort
Gemeente Apeldoorn
Gemeente Capelle a/d IJssel
Flavour
De FraudeHelpdesk
De Haagse Hogeschool
Gemeente Den Helder
Gemeente Dordrecht
Gemeente Ede
Gemeente Enschede
Gemeente Haarlem
Gemeente Rotterdam
Gemeente Utrecht
Gemeente Zoetermeer
Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)
Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

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

SAMENVATTING

In dit rapport ronden de lectoraten Maatschappelijke Veiligheid van Hogeschool Saxion en Cybercrime & Cybersecurity van de Haagse Hogeschool het RAAK-publiek project 'Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime' af. Samen met onze consortiumpartners richtten de lectoraten zich in dit twee jaar durende project op de hoofdvraag 'Met welke interventies kunnen ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten?'.

Duidelijk was dat cybercriminaliteit voor alle doelgroepen in de samenleving een actuele en urgente dreiging vormt. Allereerst werden daarom door het consortium de doelgroepen en specifieke delicten geselecteerd waarop – op basis van literatuur en interviews met experts die met de doelgroepen werken – met voorrang moest worden geïnvesteerd op de cyberweerbaarheid Dit heeft geresulteerd in de keuze voor drie doelgroepen: jongeren voor phishing, misbruik van seksueel beeldmateriaal en geldezelen; ouderen voor digitale oplichting (waaronder phishing) en mkb'ers voor phishing en ransomware. Voor elk van deze doelgroepen is verdiepend onderzoek naar de weerbaarheid tegen de geselecteerde delicten uitgevoerd op basis van representatief vragenlijstonderzoek en verdiepende interviews onder leden van de gekozen doelgroepen. Tevens is daarbij onderzocht wat de verklarende variabelen zijn voor zelfbeschermend gedrag.

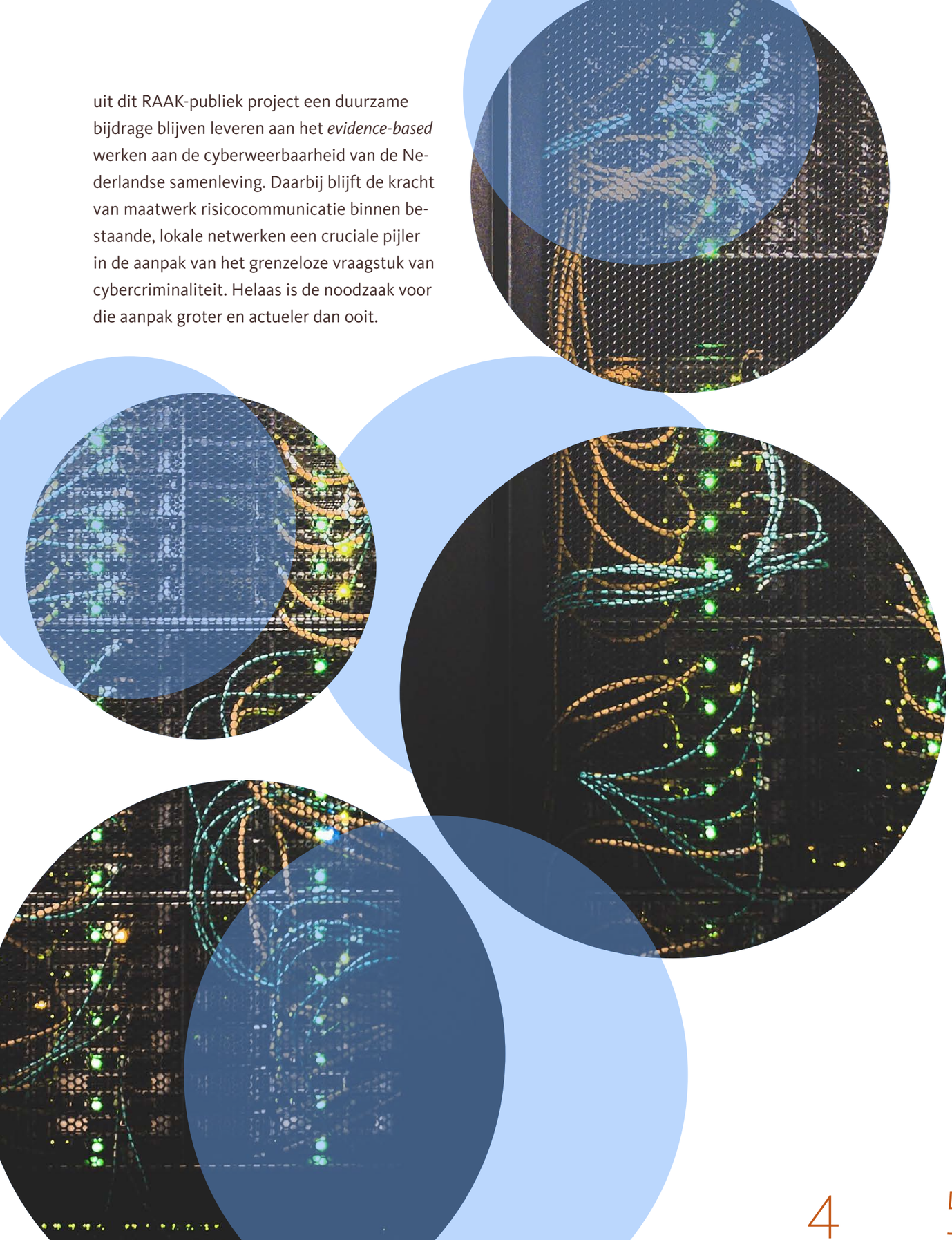
Aan de hand van deze brede kennisbasis zijn door de onderzoekers van de hogescholen, in nauwe samenwerking met de consortiumpartners uit de praktijk, vier interventies ontwikkeld en geëvalueerd:

1. 'Doorsturen doe je niet!' om jongeren weerbaarder te maken tegen misbruik van seksueel beeldmateriaal;
2. Instagram-campagne om jongeren weerbaarder te maken tegen geldezelen;
3. Laat je geen h@ck zetten! om ouderen weerbaarder te maken tegen digitale oplichting;
4. MKB Cyber Buddy's om mkb'ers weerbaarder te maken tegen ransomware.

De interventies ter preventie van slachtofferschap van phishing konden, met het oog op de beschikbare tijd en capaciteit, helaas niet binnen de spanne van dit project worden ontwikkeld. In overleg met het consortium is besloten deze vier interventies te ontwikkelen en na implementatie te evalueren.

De interventies die ontwikkeld zijn binnen dit project onderscheiden zich van bestaande interventies omdat de door ons ontwikkelde interventies *evidence-based* zijn. Daarmee vormen deze interventies een belangrijke bouwsteen in de landelijke beweging naar een *evidence-based* aanpak van cyberweerbaarheid. Inmiddels zijn de samenwerkende lectoraten van dit project door de Citydeal Lokale Cyberweerbaarheid gevraagd om te helpen met het verder uitrollen van deze *evidence-based* aanpak door alle beschikbare interventies buiten dit project van een procesevaluatie en effectevaluatie te voorzien. Dit wordt opgepakt vanuit het consortium bij de recent toegekende SPRONG-subsidie, waarmee de samenwerkende lectoraten met hun praktijkpartners

uit dit RAAK-publiek project een duurzame bijdrage blijven leveren aan het *evidence-based* werken aan de cyberweerbaarheid van de Nederlandse samenleving. Daarbij blijft de kracht van maatwerk risicocommunicatie binnen bestaande, lokale netwerken een cruciale pijler in de aanpak van het grenzeloze vraagstuk van cybercriminaliteit. Helaas is de noodzaak voor die aanpak groter en actueler dan ooit.



VOORWOORD

Cybercriminaliteit is een groot, wereldwijd probleem. Inmiddels wordt de mondiale impact daarvan gelijkgeschaard aan of zelfs groter ingeschat dan de impact van de georganiseerde handel in drugs (Naidoo, 2021). Cybercriminaliteit is dus big business. Ook in Nederland vallen er veel slachtoffers. Alleen in het jaar 2021 werden bijna 2,5 miljoen mensen slachtoffer van cybercriminelen (CBS, 2022). Al bij de aanvraag van het RAAK-project *Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime* in juni 2019 was voor een aantal gemeenten duidelijk dat cybercriminaliteit een urgent probleem betreft. Intussen is de bewustwording over de omvang en impact van cybercriminaliteit breed om zich heen gaan grijpen. Maar de vraag blijft hoe we slachtofferschap van cybercriminaliteit onder inwoners en bedrijven effectief en onderbouwd in kunnen perken. Dat is waar dit project om ging: *evidence-based* werken aan de preventie van slachtofferschap van cybercriminaliteit. Vandaag de dag bestaan er een flink aantal interventies gericht op het voorkomen van slachtofferschap van cybercriminaliteit. Vaak zijn deze interventies met de beste intenties gemaakt. Er leeft een diep besef: 'We moeten wat doen...'. Maar werkt het ook echt? Waarop is de interventie gebaseerd? En komt je boodschap überhaupt wel bij de doelgroep aan? Dit project vormt een belangrijke bouwsteen in de beweging naar een evidence-based aanpak om slachtofferschap van cybercriminaliteit tegen te gaan. Daar is al voor de afronding van dit project een mooi vervolg op gekomen: binnen het SPRONG-consortium werken we met nieuwe partner NHL Stenden Hogeschool aan meer samenhangende projecten rond cyberweerbaarheid.Voor de ministeries van VenJ, EZK en BZK evalueren we met elkaar alle interventies uit de Citydeal Lokale Cyberweerbaarheid en brengen we er een aantal via experimenteel onderzoek naar de volgende stap. Ook zijn er verschillende, nieuwe interventies met nieuwe partners in het vooruitzicht.Met de resultaten in de vorm van maar liefst tien wetenschappelijke en negen praktijkgerichte publicaties, tientallen bijdragen aan onderwijs in de vorm van inbreng in minoren, gastcolleges, onderzoeksopdrachten en afstudeerscripties en de vele lezingen die wij in de praktijk over dit project hebben mogen verzorgen, kunnen wij terugkijken op een succesvol RAAK-Publiek project. Als klap op de vuurpijl was ons project genomineerd voor de RAAK-award 2022. Hoewel we niet in de prijzen zijn gevallen, zien wij deze nominatie als duidelijke blijk van waardering voor de resultaten van de samenwerking tussen onze lectoraten onderling en de mooie samenwerking met de praktijk. We zien er als samenwerkende lectoraten dan ook naar uit om met onze partners de volgende stappen naar meer cyberweerbaarheid te zetten. Daarbij levert het praktijkgericht onderzoek een onmisbare bijdrage als motor achter kennis en innovatie.

Dr. Remco Spithoven

Lector Maatschappelijke Veiligheid, Hogeschool Saxion

Dr. Rutger Leukfeldt

Lector Cybercrime & Cybersecurity, De Haagse Hogeschool

INHOUD

1. AANLEIDING EN OPZET VAN HET RAAK-PUBLIEK PROJECT CYBERWEERBAARHEID

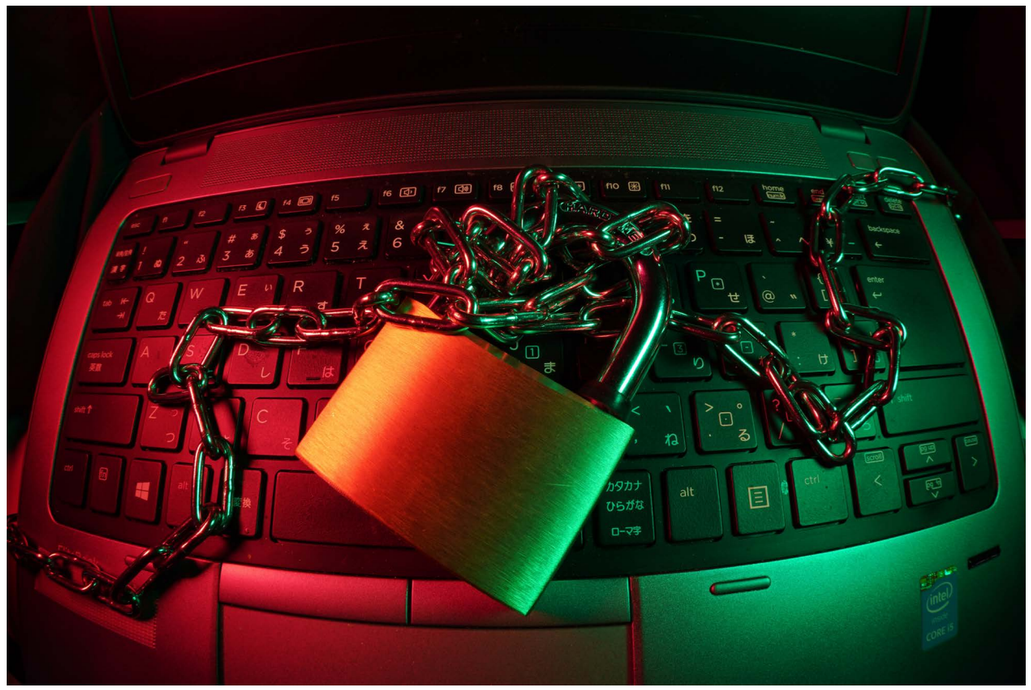
Ambtenaren openbare orde en veiligheid-spelen een centrale rol in de zorg voor maatschappelijke veiligheid. Hun focus ligt van oudsher op de preventie van slachtofferschap van veelvoorkomende criminaliteit (zoals diefstal, vernielingen en vandalisme) en high impact crime (zoals woninginbraak, overvallen en straatroven) binnen hun verzorgingsgebied. Intussen heeft de digitalisering van de samenleving een ongeëvenaarde gelegenheid voor criminaliteit gecreëerd.

Nederlandse gemeenten hebben cybercrime in de afgelopen jaren dan ook breed als beleidsprioriteit omarmd. Maar in de vertaling van deze beleidsprioriteit naar concrete acties ging hetmis. Duidelijk was dat de ambtenaren openbare orde en veiligheid een taak voor zichzelf zagen in de preventie van cybercrime, maar waar te beginnen in de aanpak van dit mondiale, abstracte probleem? In dit project bundelden professionals uit twaalf gemeenten en vier regionale veiligheidsnetwerken hun slagkracht met onderzoekers van twee hogescholen en het NSCR voor de cyberweerbaarheid van de samenleving. Na verloop van tijd is het consortium uitgebreid met Flavour, de FraudeHelpdesk en het Centrum voor Criminaliteitspreventie en Veiligheid.

De hoofdvraag van dit project luidde: *Met welke interventies kunnen ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten?* Middels actieonderzoek werkten professionals samen met onderzoekers aan het ontwikkelen van nieuwe interventies. Daarbij verscherpten zij hun beeld van de omvang en achtergronden van slachtofferschap van cybercrime. Ook onderzochten zij achtergronden en verklaringen voor het risicobewustzijn en preventief gedrag onder doelgroepen. Deze inzichten zijn in verschillende iteraties aangevuld met effectstudies, om tot een set van vier beproefde interventies te komen waarmee de cyberweerbaarheid van burgers en bedrijven zal toenemen.

Het project omvatte een viertal deelvragen:
1. Voor welke doelgroepen zijn interventies om het risicobewustzijn en het preventieve gedrag ten aanzien van cybercriminaliteit te vergroten het meest noodzakelijk?
2. Voor welke typen cybercrime zijn interventies om het risicobewustzijn en het preventievegedrag van deze doelgroepen te vergroten het meest noodzakelijk?
3. Hoe is het gesteld met het risicobewustzijn en het preventieve gedrag van deze doelgroepen voor de geselecteerde typen cybercrime en wat zijn de verklaringen voor het risicobewustzijn
en het preventieve gedrag?
4. Welke interventies kunnen Nederlandse gemeenten inzetten om het risicobewustzijn en het preventieve gedrag rondom deze typen cybercrime onder deze doelgroepen te bevorderen?

In dit afsluitende rapport maken we de balans van het project op. Met vier *evidence-based* interventies leveren we – ondanks de turbu-



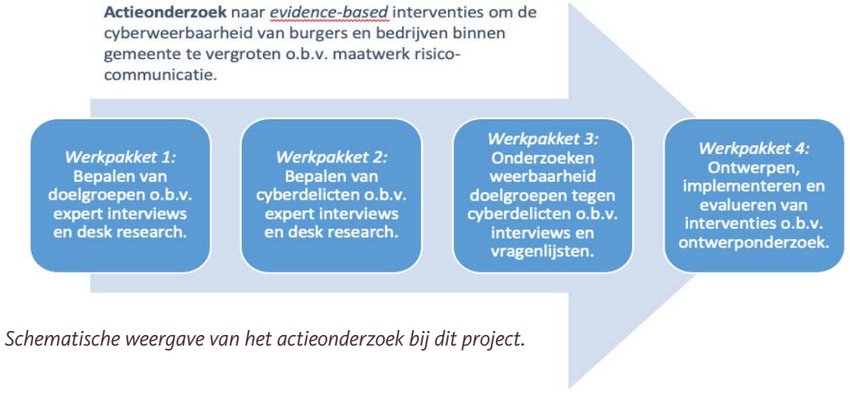
lentie onderweg – vier voorbeelden af voor de gemeentelijke praktijk. In opvolgende projecten, waaronder de evaluatie en doorontwikkeling van interventies in de Citydeal Lokale Cyberweerbaarheid, zal deze werkwijze de lokale aanpak van cyberweerbaarheid blijven versterken om tot een onderbouwde en bewezen effectieve preventie van slachtofferschap van cybercriminaliteit te komen. Op 16 februari 2023 zal er een afsluitende conferentie voor alle consortiumpartners plaatvinden die wordt opengesteld voor belangstellenden. Hiervoor zullen gemeenten en hun lokale partners worden uitgenodigd door het Centrum voor Criminaliteitpreventie en Veiligheid (het CCV), de Vereniging Nederlandse Gemeenten en de Citydeal Lokale Cyberweerbaarheid waar het consortium bij dit project vanaf de start bij betrokken is. Tevens wordt hier de start van het inmiddels toegekende SPONG-project gevierd.

In de opvolgende hoofdstukken leest u de chronologische uitkomsten van het project. In Hoofdstuk 2 kunt u meer lezen over de opbouw en het verloop van het actieonderzoek dat in het kader van dit project is uitgevoerd. In Hoofdstuk 3 gaan we in op de resultaten van de deelvraag rondom de doelgroepen om in Hoofdstuk 4 de delicten waarop de interventies gericht moeten zijn te bespreken. Vervolgens brengen we in Hoofdstuk 5 verslag uit van de uitkomsten van het kwalitatieve en kwantitatieve onderzoek naar risicobewustzijn en zelfbeschermend gedrag onder de gekozen doelgroepen voor de gekozen delicten. In Hoofdstuk 6 beschrijven we de vier ontworpen interventies en wat de resultaten van de effectevaluaties waren. In Hoofdstuk 7 maken we de balans op van het totale project en geven we een overzicht van wat het project heeft opgeleverd en wat de vervolgstappen zijn.

2. OPBOUW EN VERLOOP VAN HET ACTIEONDERZOEK BIJ DIT PROJECT

Het project bestond uit een actieonderzoek. Onder actieonderzoek verstaan wij het streven om geëvalueerde interventies te ontwikkelen om een aspect van een huidige beroepspraktijk te verbeteren en vernieuwen (de Lange e.a., 2011). Het project kwam immers voort uit een breed ervaren omissie in de beroepspraktijk (Migchielbrink, 2013) van ambtenaren openbare orde en veiligheid van Nederlandse gemeenten. Het project van dit consortium is gebaseerd op een concrete hulpvraag om de huidige situatie rondom het nieuwe fenomeen cybercrime te 'beschrijven, begrijpen en op te lossen' (de Lange e.a, 2011, p. 109). Het project was dan ook volledig gericht op verandering en innovatie (Berding & Witte, 2013). Het praktijkprobleem – het ontbreken van handvatten voor gemeenten om burgers en bedrijven weerbaarder te maken tegen cybercrime – werd door de deelnemers aan het consortium breed onderschreven. De eerste drie deelvragen betroffen de verkenningsvragen: Wat speelt er precies? Wanneer komt het voor en hoe vaak? De vierde deelvraag betrof het ontwerpen, implementeren en evalueren van de interventies.

In de kern was dit project een interdisciplinair actieonderzoek waarin de onderzoekers en ambtenaren openbare orde en veiligheid uit de gemeentelijk en regionale praktijk op gelijke voet en met inbreng van ieders expertise, werkten aan de verbetering en vernieuwing van de beroepspraktijk (de Lange et al, 2011; Migchielbrink, 2013) om de bij de start van het project heersende handelingsverlegenheid (Migchielbrink, 2013) ten aanzien van het bestendigen van de cyberweerbaarheid van de lokale samenleving, te doorbreken. Onderzoekers van de hogescholen en professionals van gemeenten en regionale veiligheidsnetwerken werkten gezamenlijk aan het verbeteren van het praktisch handelen (ibidem). De uitwerking van dit onderzoeksproject is - zoals veel actieonderzoek - multi-methodisch: Het consortium combineerde in dit actieonderzoek de kracht van de volgende onderzoeksmethoden: (I) deskresearch; (II) interviews; (III) vragenlijsten en (IV) ontwerponderzoek. Dit zullen wij onderstaand per werkpakket onderbouwen. Het project was in vier werkpakketten opgebouwd, langs de vier deelvragen van het onderzoek zoals in de onderstaande figuur schematisch is weergegeven (Figuur 1)



Figuur 1 - Schematische weergave van het actieonderzoek bij dit project.

In het vijfde en laatste werkpakket zijn alle bevindingen samengevoegd. Daarvan is het voorliggende rapport de uitkomst. Tevens zal er in het kader van dat werkpakket op 16 februari 2023 een afsluitende conferentie plaatsvinden. Het project startte officieel pas op 1 april 2020, maar met de bekendwording van de positieve uitslag op de aanvraag is het consortium al op 11 februari 2020 van start gegaan met de eerste consortiumbijeenkomst in Utrecht. Een goed begin is immers het halve werk.

Figuur 1 - Startbijeenkomst van het RAAK-consortium op 11 februari 2020.

Het proces dat met dit project werd ingegaan kon op voorhand niet volledig in detail worden uitgewerkt. Actieonderzoek betreft immers *'(...) een dynamisch, complex en soms chaotisch verlopend proces waarin verschillende fasen door elkaar lopen, parallel aan elkaar zich ontwikkelen en/of in elkaar overgaan'* (de Lange e.a. 2011, p. 114). En dat hebben we geweten met dit actieonderzoek. Na de start - waarbij we naast een kennismaking ook een inventarisatie maakten van de stand van zaken in de gemeenten ten aanzien van cyberweerbaarheid en de vervolgstappen binnen het consortium - deed al snel de coronapandemie zijn intrede. De eerste Nederlandse lockdown was daarmee nog voordat het project officieel van start zou gaan een feit.

Onze consortiumpartners waren als ambtenaren Openbare Orde en Veiligheid veelal lokaal belast met de noodmaatregelen die getroffen moesten worden. Toen de druk vanuit corona afnam, kregen zij al vrij snel te maken met de grote stroom aan vluchtelingen uit Oekraïne die moesten worden opgevangen. Ook bleken er bij de start van het project, ondanks de voorgenomen inspanningen op dit front, nog maar weinig interventies door de deelnemende gemeenten te zijn geïmplementeerd. Dit liep door de opvolgende crises verdere vertraging op, waardoor de inhoud van werkpakket 4 is teruggebracht naar het ontwerpen van nieuwe interventies, in plaats van het door-ontwikkelen van bestaande, reeds geïmplementeerde interventies. Gedurende het project heeft het consortium haar eigen wendbaarheid bewezen door steeds improviserend te werk te gaan. De onderzoekers sprongen bij waar de professionals te druk waren met de crises die hun dagelijks werk domineerden.

Uit de tussentijdse evaluatie die (online) werd gehouden op 1 juli 2021 kwam naar voren dat de consortiumleden ondanks de nodige aanpassingen tevreden waren over de resultaten en gang van zaken. De onderzoeksvragen en resultaten tot dan toe werden beoordeeld als relevant voor de beroepsgroep; de professionals werkten actief mee; de maatschappelijk urgentie was onverminderd groot omdat het slachtofferschap van cybercriminaliteit tijdens de lockdowns een vlucht nam. Kortom, dit project werd landelijk gezien als een koploper binnen het werken aan de cyberweerbaarheid van ouderen, jongeren en mkb'ers. De informatie die tot dan toe uit het onderzoek naar voren was gekomen kwam al tegemoet aan de behoefte die leefde onder ambtenaren openbare orde en veiligheid. Over het noodgedwongen online werken werd opgemerkt dat iedereen wel aangehaakt bleef, omdat er online regelmatig contact was. Er zijn niet al te lange stiltes gebleven over wie aan zet was en wat de vervolgstappen waren. Zodoende wist iedereen wat er van hem of haar werd verwacht.

Wel waren tot op dat punt vooral de onderzoekers actief geweest. Daarom is afgesproken dat de praktijkpartners in het vierde werkpakket, in de subgroepen per doelgroep-delict combinatie de volle bijdrage zouden geven. Duidelijk was dat er een gedeelde verantwoordelijkheid werd ervaren voor het complete project door de praktijkpartners en de onderzoekers van de hogescholen. Ook werd de kans gesignaleerd om het consortium verder uit te breiden met het CCV en door te groeien naar een SPRONG-consortium. Het CCV is daarop aangesloten als consortiumpartner bij dit RAAK-project en een SPRONG-aanvraag is ingediend en recent toegekend.

3. WERKPAKKET 1: BEPALEN VAN DOELGROEPEN

Bij de beantwoording van de eerste deelvraag is gebleken dat er op basis van de literatuurstudie geen eenduidig risicoprofiel voor de meest kwetsbare groepen slachtoffers van cybercriminaliteit kan worden gedefinieerd. Studies zijn gericht op de samenhang tussen verschillende kenmerken en slachtofferschap, maar concludeerden dat er zeer beperkte samenhang tussen de afzonderlijke kenmerken als geslacht, opleidingsniveau en sociaaleconomische status en het risico op slachtofferschap van cybercriminaliteit bestaat. Cybercriminaliteit raakt daarmee dus alle doelgroepen.

Toch zijn uit de literatuurstudie wel twee groepen naar voren gekomen die een verhoogd risico op slachtofferschap van cybercriminaliteit lijken te hebben: jongeren en mkb'ers. Jongeren lijken vooral een verhoogd risico te lopen op interpersoonlijke cyberdelicten (delicten waarbij de persoonlijke levenssfeer wordt aangetast). Mkb'ers lijken een verhoogd risico te hebben op financiële cyberdelicten (delicten waarbij geld en persoonlijke informatie het doelwit zijn) en op technische cyberdelicten (delicten waarbij IT niet alleen het middel is om het delict te plegen, maar ook het doelwit). Op basis van interviews met de gemeenten uit het consortium kwam een vrij gemixt beeld van de doelgroepen naar voren met in de top drie jongeren (10 keer genoemd); mkb'ers (8 keer genoemd) en senioren (5 keer genoemd).

Daarnaast is er op basis van interviews met zestien experts - van de politie, de reclassering, banken, de fraudehelpdesk, cybersecurity bedrijven, NCSC, slachtofferhulp, MKB Nederland, VNO-NCW, Mediawijsheid, HelpWanted, KBO_PCON en de consumentenbond – geconcludeerd dat jongeren, ouderen en mkb'ers met voorrang in hun risicobewustzijn en preventief gedrag moeten worden ondersteund.


- Beantwoording eerste deelvraag -

Q1: VOOR WELKE DOELGROEPEN ZIJN INTERVENTIES OM HET RISICOBEWUSTZIJN EN HET PREVENTIEVE GEDRAG TE VERGROTEN HET MEEST NOODZAKELIJK?

A1: IN PRINCIPE LOOPT IEDEREEN RISICO OM SLACHTOFFER TE WORDEN VAN CYBERCRIME, MAAR OP BASIS VAN GESPREKKEN MET EXPERTS VERDIENEN JONGEREN, OUDEREN EN MKB'ERS VOORRANG.

4. WERKPAKKET 2: BEPALEN VAN DELICTEN

Bij de beantwoording van de tweede deelvraag is op basis van de literatuur een aantal delicten aangewezen als meest voorkomend. Daarmee ontstond er zicht op de delicten waarvoor het vergroten van cyberweerbaarheid bij potentiële slachtoffers het meest noodzakelijk is. Binnen de *technische cyberdelicten* zijn dit hacking en malware (zoals ransomware); in de categorie *financiële cyberdelicten* betreft het geldezelen, Vriend-in-noodfraude, aankoopfraude, phishing en identiteitsfraude; en binnen de *interpersoonlijke delicten* gaat het om laster, chantage, stalking en bedreiging met geweld (al dan niet met een seksuele bijbedoeling zoals misbruik van seksueel beeldmateriaal).

Tijdens interviews met de deelnemende gemeenten en in werkpakket 1 geraadpleegde experts, zijn er verschillende prominente delicten aangewezen die een verhoging van de cyberweerbaarheid onder potentiële slachtoffers verlangen, zijnde:
1. Phishing;
2. Misbruik van seksueel beeldmateriaal;
3. Malware/ransomware;
4. Vriend-in-noodfraude;
5. Geldezelen.

Op basis van de keuze van de meest prominente doelgroepen en cyberdelicten is vervolgens op basis van de literatuur een inventarisatie gemaakt van de meest relevante typen cyberdelicten binnen elke doelgroep.

Voor de doelgroep *jongeren* komt de categorie interpersoonlijke cyberdelicten het meest prominent naar voren. Bij de doelgroep *mkb'ers* komt met name de categorie technische cyberdelicten naar voren. Op basis van de resultaten uit de interviews komt een koppeling naar voren tussen ouderen en financiële cyberdelicten. Vervolgens is bekeken of er een koppeling kon worden gemaakt tussen specifieke cyberdelicten en doelgroepen. De doelgroep *jongeren* werd vooral misbruik van seksueel beeldmateriaal en geldezelen gekoppeld. Mkb'ers lopen volgens gemeenten en experts het meeste risico op slachtofferschap van *ransomware.* Binnen de doelgroep *ouderen* kwam vooral vriend-in-nood fraude (Whatsapp-fraude) naar voren.

Naast de koppelingen tussen cyberdelicten en doelgroepen, hebben diverse experts ook gewezen op prominente cyberdelicten die niet aan een specifieke doelgroep te koppelen zijn. Iedereen kan slachtoffer worden van dergelijke cyberdelicten. De experts benadrukken dan ook het belang van het verbeteren van algemene cyberweerbaarheid onder internetgebruikers. Daarbij kan niet voorbijgegaan worden aan het meest prominente cyberdelict: *phishing*. De resultaten tonen dat voor phishing geen specifieke doelgroep aangewezen kan worden, omdat slachtofferschap van dit delict prominent onder alle drie de doelgroepen voorkomt.

- Beantwoording tweede deelvraag -

Q2: VOOR WELKE TYPEN CYBERCRIME ZIJN INTERVENTIES OM HET RISICOBEWUSTZIJN EN HET PREVENTIEVE GEDRAG VAN DEZE DOELGROEPEN TE VERGROTEN HET MEEST NOODZAKELIJK?

A2: PHISHING, MISBRUIK VAN SEKSUEEL BEELDMATERIAAL EN GELDEZELEN VOOR JONGEREN; PHISHING EN WHATSAPPFRAUDE VOOR OUDEREN EN PHISHING EN RANSOMWARE VOOR MKB'ERS.

5. WERKPAKKET 3: WEERBAARHEID VAN DE DOELGROEPEN

Toen de doelgroep-delict combinaties waarop de rest van het project zou worden gericht duidelijk waren, is er in werkpakket 3 verdiepend kwalitatief en kwantitatief onderzoek gedaan naar de weerbaarheid van de gekozen doelgroepen tegen de gekozen cyberdelicten. In samenwerking met I&O Research is er een representatieve steekproef genomen voor zowel jongeren, ouderen als mkb'ers. Op basis van deze data is de derde deelvraag van het project beantwoord. Deze luidde: *'Hoe is het gesteld met het risicobewustzijn en het preventieve gedrag van deze doelgroepen voor de geselecteerde typen cybercrime en wat zijn de verklaringen voor het risicobewustzijn en het preventieve gedrag?'* Bij de interviews hebben zes studenten van de opleiding Integrale Veiligheidskunde van de Hogeschool Saxion in het kader van hun afstudeerscriptie bijgedragen aan de dataverzameling en analyse.
In de doelgroep-delict combinatie jongeren en phishing zijn 1179 vragenlijsten ingevuld en 14 interviews afgenomen. In de doelgroep-delict combinatie jongeren en misbruik van seksueel beeldmateriaal zijn 1179 vragenlijsten ingevuld en 15 interviews afgenomen. In de doelgroep-delict combinatie mkb'ers en phishing zijn er 1020 vragenlijsten ingevuld en 15 interviews afgenomen. En dit was ook het geval voor de doelgroep-delict combinatie mkb'ers en ransomware. In de doelgroep-delict combinatie ouderen en phishing zijn er 1191 vragenlijsten ingevuld en 15 interviews afgenomen. In de doelgroep-delict combinatie ouderen en vriend-in-noodfraude zijn er 1078 vragenlijsten ingevuld en 15 interviews afgenomen. Voor de vragenlijsten naar geldezelen onder jongeren is er samengewerkt met 200 eerstejaars studenten van de opleiding Integrale Veiligheidskunde-Security Management van de Hogeschool Saxion. In totaal hebben 3225 jongeren deze vragenlijst ingevuld.
De derde deelvraag is verder gespecificeerd naar de vragen: (I) Hoe het is gesteld met de risicoperceptie van de doelgroep ten aanzien van het delict?; (II) In hoeverre weet de doelgroep hoe zij zichzelf kunnen beschermen tegen of voorbereiden op het delict?; (III) In welke mate vertoont de doelgroep zelfbeschermend gedrag ten aanzien van het delict ?; (IV) Welke factoren een rol spelen bij het zelfbeschermend gedrag van de doelgroep ten aanzien van het delict? Middels de vragenlijsten is inzicht verkregen in risicobewustzijn, zelfbeschermend gedrag en verklarende factoren. Achterliggende overtuigingen en aanvullende verklaringen zijn via de interviews in beeld gebracht.De vragenlijsten en topiclists voor de interviews zijn gebaseerd op het cyberweerbaarheidsmodel dat aan de basis van dit onderzoek lag.

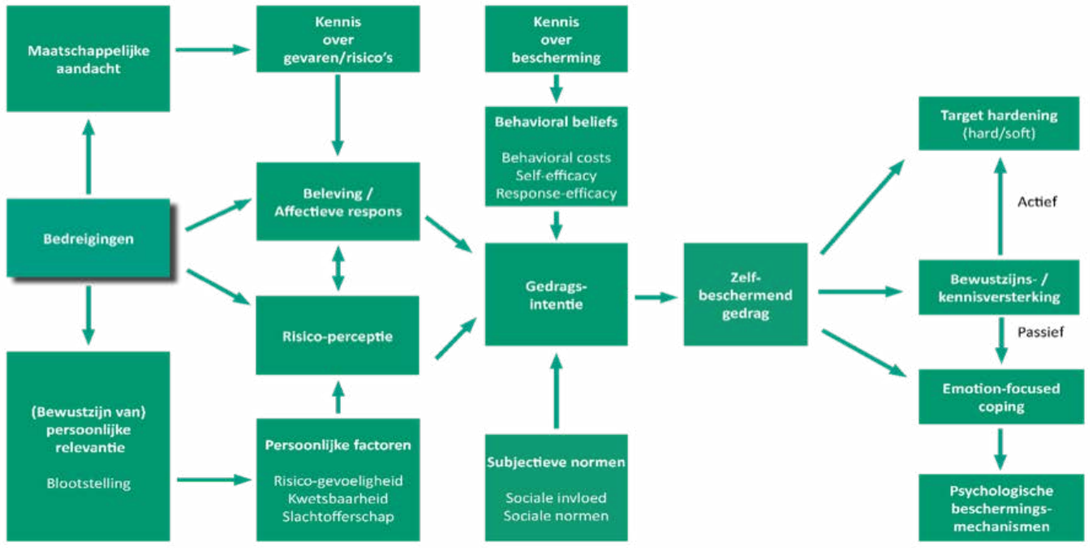
5.1 Het Cyberweerbaarheidsmodel

Voordat ambtenaren openbare orde en veiligheid met hun lokale partners het preventieve gedrag van potentiële slachtoffers van cybercrime kunnen versterken, is het nodig te weten hoe en waarom zij (geen) zelfbeschermende maatregelen nemen. Uit eerder onderzoek is gebleken, dat effectieve risico-

communicatie 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 cybercrime. Risicocommunicatie in essentie is bedoeld om individuen te ondersteunen om geïnformeerde beslissingen te nemen ten aanzien van de risico's waarmee zij worden geconfronteerd. Risicocommunicatie is maatwerk. Om optimaal effect te sorteren, wordt de communicatie gebaseerd op de beleving en percepties van de doelgroep. 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 de risicocommunicatie zijn aanvullende inzichten opgedaan over hoe gedragsverandering ten aanzien van risico's tot stand komt. In de basis kunnen mensen op twee manieren reageren op informatie over mogelijke risico's: problem-focused coping of emotion-focused coping. Bij problem-focused coping is het doel om het 'probleem' – in dit geval het risico of de dreiging van cybercrime – te minimaliseren. In het Exended Parallel Processing model (EPPM) en de Protectie Motivatie Theorie (PMT) 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 beleving 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. Juist om deze redenen is het belangrijk om de communicatie over cybercrime 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, makkelijk uitvoerbare en nuttig ervaren, gedragsadviezen. 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. Het risicobewustzijn en het preventieve gedrag worden vervolgens, met inbegrip van de verklarende aspecten, middels specifieke interventies aangepast. 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. Figuur 3 presenteert een samenvattend conceptueel model voor de verklaring van risicobeleving en preventief gedrag rondom cybercrime.



Figuur 3 - Het cyberweerbaarheidsmodel.

De gedragsintentie om preventief gedrag ten aanzien van cybercrime te nemen komt tot stand langs verschillende factoren: (I) de perceptie van het risico; (II) de beleving van/ affectieve respons op het risico. Deze worden op hun beurt beïnvloed door (III) de kennis van risico's op basis van (IV) de maatschappelijke aandacht voor de risico's en (V) de persoonlijke relevantie van de risico's die wordt gefilterd door (VI) persoonlijke factoren. Daarnaast wordt de gedragsintentie beïnvloed door (VII) subjectieve normen en (VIII) behavioral beliefs. Het is zaak om per doelgroep, op maat, in te spelen op deze samenhangende concepten om effect te sorteren en doelgroepen - in plaats van naar (A) emotion-focused coping onder invloed van psychologische beschermingsmechanismen – naar (B) target hardening te brengen en zo de cyberweerbaarheid te vergroten.

5.2 Jongeren en phishing

Van de jongeren is 1,3% afgelopen jaar slachtoffer geworden van phishing. Van deze groep heeft 27% op een link geklikt en/of gegevens verstrekt, is 40% geld en 27% gegevens verloren en heeft 27% last van schaamte en 20% last van angst als gevolg van het slachtofferschap. Daarnaast heeft 32% behoefte aan meer informatie over hoe zij zichzelf kunnen beschermen tegen slachtofferschap van phishing. Jongeren geven aan te weten wat phishing is en wat de risico's zijn. Het risicobewustzijn is dan ook relatief hoog. De meeste van hen hebben al eens een phishing bericht ontvangen. Hoewel zij de kans om slachtoffer te worden klein inschatten, ervaren zij de impact van slachtofferschap wel als groot. Ook denken zij zelf minder snel slachtoffer te worden dan hun leeftijdsgenoten. Er is dus sprake van een zogenaamde 'optimistic bias'. Zij maken zich weinig zorgen over hun eigen veiligheid. Zij vinden dat ze zichzelf goed (kunnen) beschermen en denken ook dat dit nuttig is. Zij zijn wel onzeker over de effectiviteit van hun huidige zelfbeschermend gedrag. De gedragsintentie is gemiddeld, waarbij de grootste belemmeringen tijd, ingewikkeldheid en effectiviteit zijn. Verder hebben lager opgeleiden jongeren minder kennis van het fenomeen en beschermen zij zich minder goed. Jongeren zijn meer geneigd om zichzelf te beschermen als ze zich meer zorgen maken, denken dat anderen dit van hen verwachten en zich minder goed in staat achten zichzelf te beschermen.

5.3 Jongeren en misbruik van seksueel beeldmateriaal

Van de respondenten bij de vragenlijst heeft 38% seksuele beelden ontvangen, 25% eigen seksuele beelden verstuurd, 3% seksuele beelden van anderen doorgestuurd, is 0,5% afgelopen jaar zelf slachtoffer geworden. Verder heeft 14% behoefte aan meer informatie over sexting. In tegenstelling tot de respondenten van de vragenlijst gaven bijna alle respondenten bij de interviews aan tot nu toe (nog) niet aan sexting te hebben gedaan. Ervaring neemt toe met leeftijd en opleidingsniveau. Het risicobewustzijn onder jongeren is relatief hoog, zij maken zich ook weinig zorgen over hun eigen veiligheid. Zij denken dat anderen eerder slachtoffer worden dan zij zelf, er is dus sprake van een optimistic bias. Een verklaring hiervoor kan worden gevonden in de strategie : voorkomen is beter dan genezen. Zij voorkomen dat er seksueel beeldmateriaal van hen bestaat, vermijden opslag in de cloud als zij wel seksueel beeldmateriaal van zichzelf maken en houden het voor zichzelf. Bij het eventuele versturen van seksueel beeldmateriaal speelt vertrouwen in de ontvanger een cruciale rol. Verder zijn jongeren meer geneigd zichzelf te beschermen wanneer zij zich meer zorgen maken, denken dat anderen van hen verwachten dat zij zich goed beschermen en zij zich minder goed in staat achten zichzelf te beschermen. De impact van slachtofferschap wordt wel als zeer groot ervaren. Zij denken dat zij zichzelf goed (kunnen) beschermen. Omdat weinig respondenten aangeven zelf aan sexting te doen, is hun risicoperceptie relatief laag en maken ze zich daarom ook weinig zorgen over hun veiligheid. Hun gedragsintenties zijn daarmee ook relatief laag. De belemmeringen die zij ervaren met betrekking tot zelfbeschermend gedrag zijn tijd, ingewikkeldheid en effectiviteit.

5.4 Jongeren en geldezelen

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

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

5.5 Mkb'ers en phishing

Op basis van bedrijfskenmerken kan geen risicogroep worden aangewezen die zich onveiliger gedraagt dan andere mkb'ers. Bedrijfskenmerken, zoals aantal medewerkers, hangen niet samen met het nemen van maatregelen. Voor de 25% van de mbk'ers die de minste beschermende maatregelen nemen, geldt dat de intentie om maatregelen te nemen tegen phishing in hun bedrijf vooral samenhangt met hun risicoperceptie en affectieve respons. 33% geeft aan behoefte te hebben aan meer informatie over phishing. Mkb'ers zijn zich bewust van de risico's en de impact van phishing. Ze schatten de kans op slachtofferschap voor hun eigen bedrijf zeer laag in en schatten de kans dat vergelijkbare mkb'ers slachtoffer worden hoger in. Er is dus wederom sprake van een

optimistic bias. Eventuele schade en emotionele impact als gevolg van phishing wordt hoger ingeschat, maar nog steeds relatief laag. Mkb'ers nemen 'soms' tot 'vaak' maatregelen tegen phishing. Hierbij zijn de grootste belemmeringen tijd en moeite.

Mkb'ers hebben een sterkere intentie om maatregelen te nemen tegen phishing als ze de risico's van phishing hoger inschatten (risicoperceptie), ze zich zorgen maken over de risico's van phishing voor hun bedrijf (affectieve respons), mbk-bedrijven in de omgeving zichzelf beschermen tegen phishing (sociale norm) en ze meer weten over phishing (risicobewustzijn).

5.6 Mkb'ers en ransomware

Voor de 25% van de mkb'ers die de minste beschermende maatregelen nemen, geldt dat de intentie om maatregelen te nemen tegen ransomware in hun bedrijf vooral samenhangt met hun risicoperceptie en affectieve respons. 41% geeft aan behoefte te hebben aan meer informatie over ransomware.
Mkb'ers zijn zich bewust van de risico's en de impact van ransomware. Zij schatten de kans op slachtofferschap voor hun eigen bedrijf zeer laag in en schatten de kans dat vergelijkbare mkb'ers slachtoffer worden hoger in. Er is dus sprake van een optimistic bias. Eventuele schade en emotionele impact worden hoger ingeschat. Mkb'ers nemen 'soms' tot 'vaak' maatregelen tegen ransomware. De grootste belemmeringen hierbij zijn tijd en moeite.

Mkb'ers hebben een hogere intentie om maatregelen tegen ransomware in hun bedrijf te nemen als ze de risico's van ransomware hoger inschatten (risicoperceptie), ze zich zorgen maken over de risico's van ransomware voor hun bedrijf (affectieve respons), MKB-bedrijven in de omgeving zichzelf beschermen tegen ransomware (sociale invloed) en ze meer weten over ransomware (risicobewustzijn).

5.7 Ouderen en phishing

Van de ouderen heeft 77% het afgelopen jaar een phishing-bericht ontvangen en is 1,2% daadwerkelijk slachtoffer geworden van phishing. Verder heeft 46% behoefte aan meer informatie over hoe zij zichzelf kunnen beschermen tegen phishing, hoe ze (een poging tot) phishing kunnen herkennen, wat ze moeten doen bij slachtofferschap en welke vormen van phishing er bestaan. Ouderen zijn zich redelijk bewust van de risico's en de impact van phishing. Zij schatten de kans om slachtoffer te worden laag in en schatten de kans dat vergelijkbare ouderen slachtoffer worden hoger in. Er is dus ook hier weer sprake van een optimistic bias. De mogelijke schade en emotionele impact worden wel hoog ingeschat. Ouderen rapporteren dat ze vaak maatregelen tegen phishing nemen. Zij die het minst aan zelfbeschermend gedrag doen zijn vaak laagopgeleid. De grootste belemmeringen bij het nemen van (aanvullende) maatregelen zijn dat het te ingewikkeld is en vanwege de veronderstelling dat aanvullende maatregelen niet beter zouden beschermen.

Ouderen zijn meer geneigd zich te beschermen tegen phishing als ze zich zorgen maken over de risico's van phishing (affectieve respons), anderen vinden dat ze zich zouden moeten beschermen en ze geneigd zijn aan deze subjectieve norm te voldoen (sociale norm) en als ze zichzelf momenteel minder goed in staat achten om zich te beschermen tegen phishing (zelfeffectiviteit).

5.8 Ouderen en vriend-in-noodfraude

Van de respondenten is 15% het afgelopen jaar benaderd door een oplichter via een chat-app, zoals WhatsApp. 5% daarvan heeft daadwerkelijk geld overgemaakt (0,7% van alle oudere smartphonebezitters). Een op de vijf ouderen heeft behoefte aan meer informatie over vriend-in-noodfraude. Voornamelijk over hoe zij zichzelf kunnen beschermen en welke (nieuwe) fraudevormen er zijn. Ouderen zijn zich gemiddeld redelijk bewust van de risico's met betrekking tot vriend-in-noodfraude, nemen relatief veel zelfbeschermende maatregelen en achten zich in staat zichzelf te beschermen. Zij maken zich niet heel veel zorgen en vinden dat vooral anderen veel risico lopen. Er is sprake van een grote optimistic bias. De mogelijke schade bij slachtofferschap wordt als hoog gezien. Slachtoffers van vriend-in-noodfraude melden financiële schade, een gevoel van schaamte en verlies van vertrouwen, en passen hun onlinegedrag aan. Ouderen maken nog relatief weinig afspraken met vrienden/familie over hoe om te gaan met betaalverzoeken. Het treffen van zelfbeschermende maatregelen wordt wel als nuttig en effectief gezien. Ouderen worden vooral tegengehouden bij het nemen van maatregelen tegen cybercrime (in het algemeen) omdat het te ingewikkeld is.

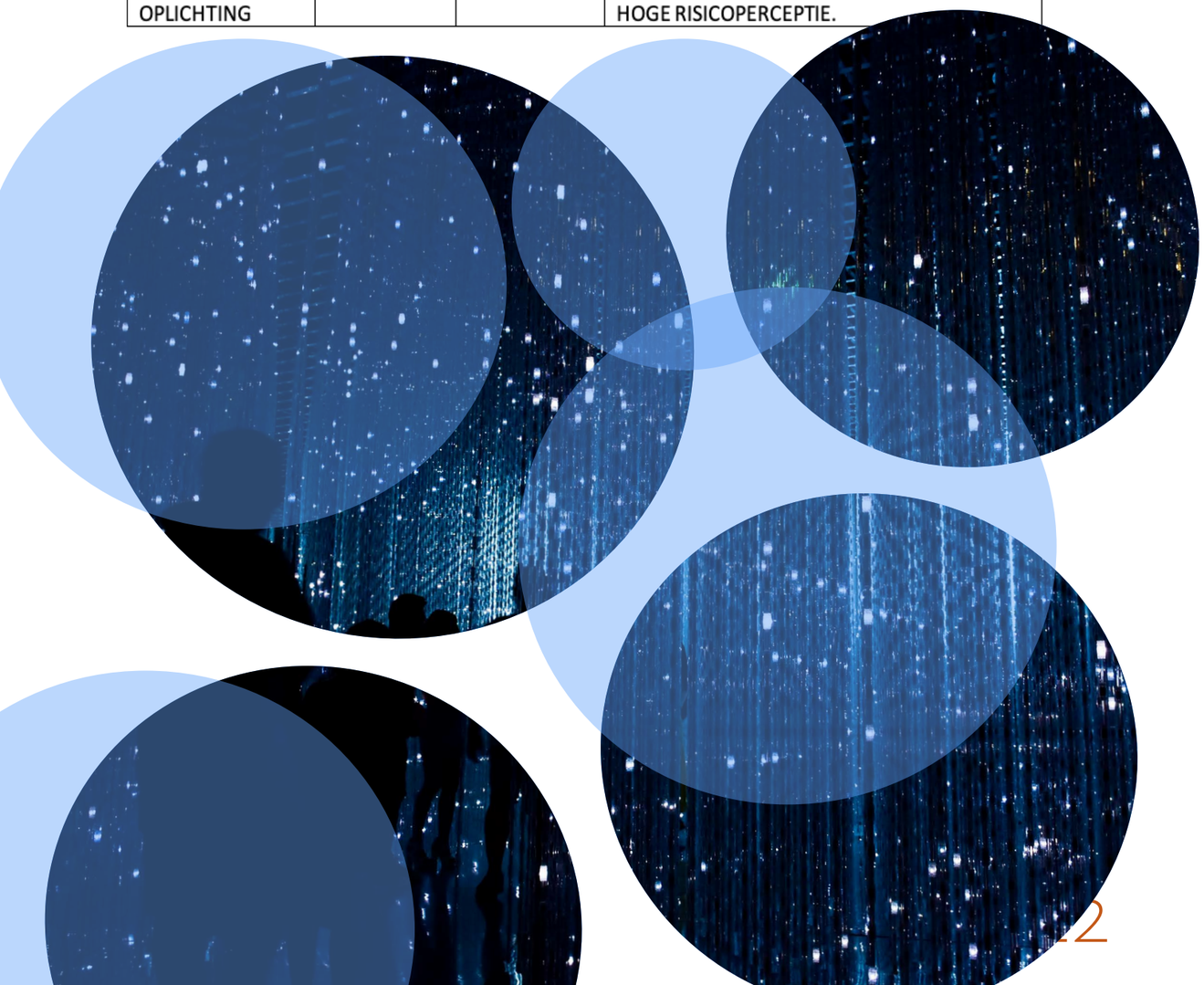
Ouderen zijn meer geneigd om zich te beschermen tegen vriend-in-noodfraude als zij zichzelf minder goed in staat achten zich te beschermen tegen vriend-in-noodfraude (zelfeffectiviteit), zij zich meer zorgen maken over vriend-in-noodfraude (affectieve respons) en als anderen vinden dat ze zichzelf zouden moeten beschermen, en ze geneigd zijn aan deze subjectieve norm te voldoen (sociale norm). Verder is de affectieve respons hoger bij een hoge risicoperceptie; die wordt weer hoger door respectievelijk een lage zelfeffectiviteit en een hoog risicobewustzijn.

- Beantwoording derde deelvraag -

Q3: HOE IS HET GESTELD MET HET RISICOBEWUSTZIJN EN HET PREVENTIEVE GEDRAG VAN DEZE DOELGROEPEN VOOR DE GESELECTEERDE TYPEN CYBERCRIME EN WAT ZIJN DE VERKLARINGEN VOOR HET RISICOBEWUSTZIJN EN HET PREVENTIEVE GEDRAG?

A3: OP BASIS VAN HET ONTWIKKELDE CYBERWEERBAARHEIDSMODEL ZIJN VRAGENLIJSTEN ONDER REPRESENTATIEVE STEEKPROEVEN VOOR DE DOELGROEPEN AFGENOMEN, DEZE ZIJN AANGEVULD MET KWALITATIEVE INTERVIEWS. HIERUIT ZIJN PER DOELGROEP DE VOLGENDE, BEKNOPTE BEVINDINGEN OPGEDAAN:

	NIVEAU VAN BEWUSTZIJN	KANS-INSCHATTING	ACHTERLIGGENDE VERKLARINGEN ZELFBESCHERMEND GEDRAG
JONGEREN, PHISHING	RELATIEF HOOG	LAAG	OPTIMISTIC BIAS, AFFECTIEVE RESPONS, SOCIALE NORM & ZELFEFFECITIVITEIT.
JONGEREN, SHAMESEXTING /SEXTORTION	RELATIEF HOOG	LAAG	LAGE RISICOPERCEPTIE, OPTIMISTIC BIAS & ZELFEFFECTIVITEIT.
JONGEREN, GELDEZELEN	RELATIEF LAAG	LAAG	LAGE RISICOPERCEPTIE, OPTIMISTIC BIAS & LAGE INSCHATTING GEVOLGEN.
MKB'ERS, PHISHING	RELATIEF HOOG	LAAG	LAGE RISICOPERCEPTIE, OPTIMISTIC BIAS, AFFECTIEVE RESPONS & SOCIALE NORM.
MKB'ERS, RANSOMWARE	RELATIEF HOOG	LAAG	LAGE RISICOPERCEPTIE, OPTIMISTIC BIAS, AFFECTIEVE RESPONS.
OUDEREN, PHISHING	REDELIJK	LAAG	OPTIMISTIC BIAS, OPLEIDINGSNIVEAU & ZELFEFFECTIVITEIT.
OUDEREN, DIGITALE OPLICHTING	REDELIJK	LAAG	OPTIMISTIC BIAS, ZELFEFFECTIVITEIT, AFFECTIEVE RESPONS, SOCIALE INVLOED & HOGE RISICOPERCEPTIE.



6. WERKPAKKET 4: NAAR VIER *EVIDENCE BASED* INTERVENTIES

In dit onderdeel beschrijven we de vier interventies die de praktijkpartners samen met de onderzoekers van de hogescholen hebben ontwikkeld op basis van de bevindingen uit de voorgaande werkpakketten.
Daarbij is in het consortium besloten om *geen* interventie voor phishing te ontwikkelen, omdat dit in de beschikbare capaciteit en tijd niet realistisch werd geacht. Door de praktijkpartners en onderzoekers is gezamenlijk voorrang gegeven aan de ontwikkeling van interventies voor misbruik van seksueel beeldmateriaal en geldezelen voor jongeren, digitale oplichting voor ouderen en ransomware voor mkb'ers.
Op basis van de resultaten van werkpakket 3 kunnen in vervolgprojecten voor de specifieke doelgroepen nog interventies worden ontworpen om hen weerbaarder te maken tegen phishing.

De ontwikkelde interventies zijn evidence-based en wel om twee redenen. Allereerst zijn zij ontwikkeld op basis van de resultaten van onderzoek naar hoe de doelgroep het specifieke risico beleeft en wat daarbij voorspellend bleek voor het zelfbeschermend gedrag (werkpakket 3, zie onderdeel 5). Daarnaast zijn alle interventies na de implementatie voorzien van een effectevaluatie. In de onderstaande onderdelen brengen wij verslag uit van het doel van de ontwikkelde interventies, geven we een beschrijving van de ontwikkelde interventies, behandelen we de resultaten van de effectmetingen en trekken we per ontwikkelde interventie een conclusie.

6.1 Jongeren en misbruik van seksueel beeldmateriaal

Praktijkpartners van Flavour, gemeente Ede, Rotterdam en Zoetermeer, regionaal veiligheidsnetwerk Oost-Nederland ontwikkelden samen met onderzoekers van Hogeschool Saxion en Malkander Jongerenwerk en Helpwanted.nl op basis van de uitkomsten van werkpakketten 1, 2 en 3 een interventie om jongeren weerbaarder te maken tegen misbruik van seksueel beeldmateriaal op basis van een *serious game*.

6.1.1 Doel en beschrijving van de ontwikkelde interventie

Sexting – een samenvoeging van seks en texting – is een moderne uiting van het klassieke, seksuele experimenteergedrag van jongeren. Helaas levert het jongeren ook risico's op: het zonder toestemming opslaan, doorsturen of ongericht verspreiden van seksuele beelden. De impact voor slachtoffers kan groot zijn. Jongeren lopen in hun experimenteergedrag ook het risico om bewust of onbewust dader te worden: een foto of video is tegenwoordig immers in een oogwenk gemaakt en doorgestuurd. Shame sexting (het zonder toestemming doorsturen van andermans seksueel beeldmateriaal) en sextortion (afpersing met gebruik van seksueel beeldmateriaal, vaak in ruil voor geld of seks) betreft een nog ernstigere categorie en kan leiden tot jeugddetentie.
Veel jongeren nemen zelfbeschermende

maatregelen, bijvoorbeeld door te voorkomen dat er seksueel beeldmateriaal van ze bestaat. Jongeren die wel seksueel beeldmateriaal van zichzelf verzenden, leunen vooral op vertrouwen in de ontvanger van de beelden. De mate van zelfbeschermend gedrag is wel leeftijdsafhankelijk: hoe jonger ze zijn, hoe minder zelfbeschermend gedrag jongeren vertonen (wat in nog sterkere mate geldt voor meisjes). Blootstelling aan risico's start al op jonge leeftijd, en in de groep van 12-14 jaar zijn al slachtoffers te betreuren.

Uit het onderzoek in werkpakket 3 bleek dat de sociale omgeving – in de vorm van subjectieve normen bij misbruik van seksueel beeldmateriaal – grote invloed heeft op het voornemen voor toekomstig zelfbeschermend gedrag. Met deze uitgangspunten is gewerkt aan een interventie.

De *serious game* die is ontwikkeld richt zich op de subjectieve norm onder jongeren met betrekking tot het doorsturen van seksueel beeldmateriaal, met als centrale boodschap *"Doorsturen doe je niet!"*. De interventie heeft de eerste twee klassen van het middelbaar onderwijs (leeftijd 12-14 jaar) als doelgroep en richt zich zowel op het voorkomen van slachtofferschap als daderschap. De interventie bestaat uit een serious game en een groepsbespreking, die samen passen in een schoolles. De game biedt een veilige plek om te experimenteren met gedrag zonder dat het leidt tot consequenties.

Spelers ervaren via realistische scenario's hoe ze – bedoeld of onbedoeld - slachtoffer of dader kunnen worden van misbruik van seksuele beelden. De mate van realisme wordt vergroot door het gebruik van video's van jonge acteurs. Zij krijgen in een schoolse context te maken met diverse scenario's waarbij het volgen van verschillende paden (aangegeven door de speler) leidt tot verschillende uitkomsten. Elke uitkomst (variërend van het volledig vermijden van het maken/uitwisselen van seksuele beelden tot het dader zijn van sextortion) wordt begeleid door een toelichting van de consequenties, biedt handelingsperspectieven om negatieve uitkomsten te voorkomen, en bronnen voor informatie en hulp bij onverhoopt slachtofferschap of daderschap (Figuur 4).

Figuur 4 – Print screens van de ontwikkelde interventie 'Doorsturen doe je niet!' om jongeren weerbaarder te maken tegen misbruik van seksueel beeldmateriaal.

De interventie is technisch ontwikkeld door Flavour, een game-ontwikkelaar bekend van Hackshield. Voor de inhoudelijke verantwoording is onder anderen gezorgd door HelpWanted.nl, Jongerenwerk Malkander, Hogeschool Saxion en de praktijkpartners van gemeente Ede, Rotterdam en Zoetermeer, regionaal veiligheidsnetwerk Oost-Nederland. De serious game wordt begeleid door een docenteninstructie, met onder meer. informatie over hoe de nabespreking te voeren. Deze groepsbespreking is mede gericht op de sociale norm met betrekking tot. het doorsturen van seksuele beelden. Voor de school is tevens een informatiebrief voor ouders gemaakt.

6.1.2 Effectmeting

De interventie is geëvalueerd op twee middelbare scholen. De interventie leidt tot een toename van het risicobewustzijn, de risicoperceptie, de ingeschatte kans op (bewust of onbewust) daderschap, zorgen over slachtofferschap, zelfeffectiviteit bij mogelijk slachtofferschap, de intentie om zich meer te gaan verdiepen in de materie, en het zelfbeschermende gedrag (met name door te voorkomen dat er überhaupt seksuele beelden bestaan).

6.1.3 Conclusies en vervolgonderzoek

Het richten van de interventie op de doelgroep van 12 tot 14 jaar blijkt (zeer) goed gekozen te zijn. De meeste jongeren ervaren de interventie als positief: ze vinden dat hun risicobewustzijn is toegenomen en dat ze handelingsbekwamer zijn geworden door de interventie. Docenten kunnen de les zelfstandig uitvoeren m.b.v. de gegeven instructies. Geconcludeerd kan worden dat de interventie goed inzetbaar is door gemeenten in Nederland, die de interventie bij scholen – of andere plaatsen waar jongeren uit de doelgroep 12 tot 14-jarigen samenkomen - kunnen aanbieden. Met experimenteel vervolgonderzoek onder grotere aantallen deelnemers zou onderzocht kunnen worden of er na het doorlopen van de interventie een verschil bestaat in de weerbaarheid van opleidingsniveaus tegen misbruik van seksueel beeldmateriaal van jongeren en op welke wijze de interventie inhoudelijk doorontwikkeld zou kunnen worden.

6.2 Jongeren en geldezelen

Praktijkpartners van de gemeente Haarlem, Apeldoorn, Dordrecht en regionale veiligheidsnetwerken Regionale Veiligheidsstrategie Midden-Nederland en Noord-Holland Samen Veilig ontwikkelden samen met onderzoekers van de Haagse Hogeschool op basis van de uitkomsten van werkpakketten één tot en met drie een interventie om jongeren weerbaarder te maken tegen geldezelen door een campagne op Instagram.

6.2.1 Doel en beschrijving van de ontwikkelde interventie

Het doel van deze interventie is het verhogen van het bewustzijn en de risicoperceptie van jongeren op Instagram met betrekking tot geldezels. De interventie bestaat uit twee delen: (I) nagemaakte ronseladvertenties op Instagram en (II) landingspagina's. De advertenties die zijn gebaseerd op advertenties van echte ronselaars van geldezels, stellen dat jongeren geld kunnen verdienen met hun bankpas. Als jongeren vervolgens op een advertentie klikken, komen ze terecht op één van de twee externe websites. Die bevatten informatie over het fenomeen geldezelen en hebben een sterk waarschuwend karakter. Bij de ene landings-

pagina lag het accent op afschrikken door de gevolgen van het geldezelen te benadrukken. Bij de andere pagina lag het accent op hulp bij het maken van betere keuzes, zoals het vinden van een gewone (bij)baan (Figuur 5).

Advertentie A

Advertentie B

Advertentie C

Afschrikpagina

Hulppagina

Figuur 5 – Print screens van de ontwikkelde Instagram campagne om jongeren weerbaarder te maken tegen geldezelen.

6.2.2 Effectmeting

In hoeverre bereikt de interventie de doelgroep en verhoogd de interventie het bewustzijn van jongeren omtrent geldezels? En met welke instellingen, advertenties en landingspagina lukt dat het beste? De advertenties zijn in twee campagnes meer dan een maand lang getoond aan Nederlandse Instagram gebruikers tussen de 18 en 25 jaar aan de hand van een quasi-experimenteel design.
In totaal zijn bijna 100.000 verschillende Instagram gebruikers bereikt met de advertenties. Daarvan hebben 906 personen op een advertentie geklikt. In het algemeen lijkt dus ongeveer 1% van de jongeren op Instagram geïnteresseerd in het verdienen van geld met hun bankpas. Dit komt redelijk overeen

met het vooronderzoek in werkpakket 3 waar 0,8% van de jongeren naar eigen zeggen als geldezel had opgetreden (zie onderdeel 5.4). Het klikpercentage per conditie verschilt van 0.16% tot 2.36% en is dus sterk afhankelijk van het type advertentie en de campagne-instellingen. Het klikpercentage is hoger wanneer jongeren een advertentie meerdere keren te zien krijgen. Daarnaast klikken jongeren vaker op advertenties die veel en snel geld in het voortuitzicht stellen (advertentietype A). Jongeren interacteerden vooral met de content op de hulppagina. Zo scrolde ongeveer de helft van de jongeren tot onderaan die pagina, terwijl op de afschrikpagina slechts een kwart naar beneden scrolde.
6.2.3 Conclusies en vervolgonderzoek
Instagram biedt een unieke mogelijkheid om risicovolle jongeren te bereiken voor interventiedoeleinden en voor criminologisch onderzoek. Onbekend is echter nog of de interventie daadwerkelijk voorkomt dat jongeren optreden als geldezel, maar met de juiste campagne-instellingen, advertenties en landingspagina lukt het om een groot aantal jongeren over het fenomeen te informeren. Gemeenten kunnen de interventie relatief makkelijk en goedkoop zelf toepassen via het advertentiebeheer van Instagram. Middels experimenteel vervolgonderzoek zou de ontwikkelde interventie op het preventieve effect onder jongeren onderzocht kunnen worden om daarmee de interventie inhoudelijk verder te kunnen ontwikkelen.

6.3 Ouderen en digitale oplichting

Praktijkpartners van de gemeente Amersfoort, Almere en Capelle a/d IJssel, regionaal veiligheidsnetwerken Veiligheidsalliantie Regio Rotterdam en de FraudeHelpdesk ontwikkelden samen met onderzoekers van Hogeschool Saxion op basis van de uitkomsten van werkpakketten één tot en met drie een interventie om ouderen weerbaarder te maken tegen digitale oplichting op basis van een offline training en een ondersteunende website.

6.3.1 Doel en beschrijving van de ontwikkelde interventie

De primaire focus ligt op de offline training. Daar wordt het effect op de weerbaarheid van ouderen tegen digitale oplichting nagestreefd. De website is ondersteunend aan de offline training. De doelen, op basis van werkpakket 3, waren (I) ondersteunen van het in beginsel aanwezige, risicobewustzijn; (II) doorbreken van de optimistic bias; (III) geven van handelingsperspectief bij slachtofferschap en (IV) aandacht schenken aan de sturing van zelfbeschermend gedrag op basis van sociale normen.

De offline training (Figuur 6) bestaat uit de volgende onderdelen:
1. Invullen van een nep-toestemmingsformulier en groepsgesprek;
2. Doorbreken van schaamte en delen van ervaringen;
3. Delen van tips hoe jezelf te beschermen, welke vormen van digitale oplichting er zijn en wat daarin de ontwikkelingen zijn;
4. Regietheater, live samen oefenen met aangereikte handvatten om jezelf tegen digitale oplichting te beschemen;
5. Handout mee als naslagwerk met daarin tips hoe jezelf te beschermen en wat te doen als je slachtoffer wordt.

Figuur 6 - Foto's van de offline training met links de behandeling van het nep-toestemmingsformulieren rechts het regietheater in actie.

De ondersteunende website (Figuur 7) - bedoeld als inhoudelijke voorbereiding van deelnemers op de offline bijeenkomst en digitaal naslagwerk voor deelnemers - bestaat uit de volgende onderdelen:
1. *Call to action* (video) door het hoofd cybercrime van de Nationale Politie;
2. Drie slachtoffers (video's) over de impact van slachtofferschap;
3. Tips hoe jezelf tegen digitale oplichting te beschermen;
4. Handelingsadvies bij slachtofferschap;
5. Agenda voor lokale, offline bijeenkomsten en links naar partners.

Figuur 7 – Print screens van de call to action van Theo van der Plas, de preventie tips en het verhaal van slachtoffer Juan.

6.3.2 Effectmeting

De deelnemers aan de try-out voor de offline training waren na de training significant minder bezorgd en meer zelfverzekerd ten aanzien van het risico van digitale oplichting. Het vaststellen van het effect van de offline voorlichting vergt een groter aantal deelnemers.

6.3.3 Conclusies en vervolgonderzoek

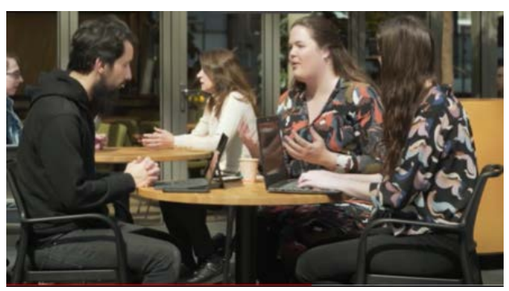
De interventie heeft daarmee slechts eerste sporen van effectiviteit vertoond onder een kleine groep deelnemers aan de offline training. Deze effectiviteit dient onder een groter aantal deelnemers nader onderzocht te worden. De bezoekers van de site hebben *geen* significante verschillen op hun cyberweerbaarheid en achterliggende factoren in vergelijking tot de controlegroep. De naslagfunctie wordt duidelijk door de bezoekers gewaardeerd en bezoekers zijn niet bezorgder dan de controlegroep.
Vooral de offline training biedt perspectief op het vergroten van de weerbaarheid van ouderen tegen digitale oplichting. De website is daaraan ondersteunend. Bezoekers waarderen de geboden informatie en de werkvormen van de training. De bezoekers van de website waren tevreden over de geboden informatie, wel is er nog een verbeterslag in het taalniveau aan te brengen omdat deze als complex wordt ervaren. Met experimenteel onderzoek onder een groter aantal deelnemers kan de effectiviteit van de offline interventie nader worden onderzocht.

6.4 Mkb-ers en ransomware

Praktijkpartners van de gemeente Utrecht, Den Helder en Enschede ontwikkelden samen met onderzoekers van de Haagse Hogeschool op basis van de uitkomsten van werkpakketten één tot en met drie een interventie om mkb-ers weerbaarder te maken tegen ransomware.

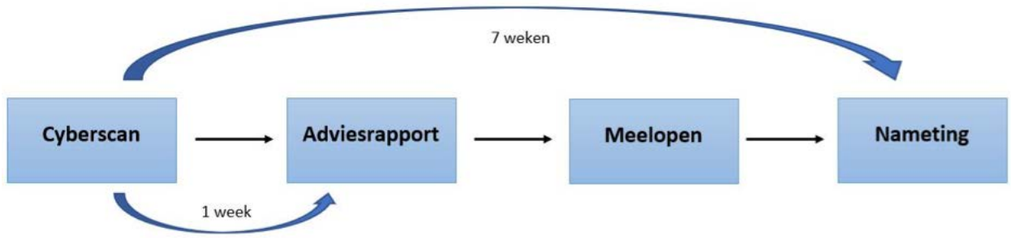
6.4.1 Doel en beschrijving van de ontwikkelde interventie

Het midden- en kleinbedrijf (mkb) wordt relatief vaak slachtoffer van cybercriminaliteit en ondervindt hiervan in hoge mate schade. In dit rapport presenteren we de ontwikkeling en evaluatie van een interventie genaamd "MKB Cyber Buddy's". Het doel van de interventie is om de weerbaarheid van mkb'ers tegen ransomware te vergroten. De hoofdvraag is: *Is de interventie "MKB cyber buddy's" een effectieve interventie voor Nederlandse gemeenten om de cyberweerbaarheid van mkb'ers in hun gemeente met betrekking tot ransomware te bevorderen?*
In het "MKB Cyber Buddy's" project worden deelnemende mkb'ers gekoppeld aan een IT student die als buddy een aantal weken het bedrijf ondersteunt op het gebied van cybersecurity (Figuur 8).



Figuur 8 – Projectleider en student in gesprek met een mkb-bedrijf.

Aan de hand van een cyberscan, een op maat gemaakt adviesrapport en werkbezoeken krijgen de ondernemers passend en toegankelijke adviezen van IT studenten (Figuur 9).



Figuur 9 – Proces van de MKB Cyber Buddy's.

Op basis van resultaten uit werkpakket 3, in het adviesrapport rapport risicocommunicatie opgenomen die inspeelt op twee wetenschappelijk onderbouwde factoren die bijdragen aan de motivatie van mkb'ers om maatregelen te nemen tegen ransomware, namelijk 'subjectieve norm' en 'affectieve respons'.

6.4.2 Effectmeting

Gemiddeld hebben de buddy's aan deelnemende mkb'ers 35.5 maatregelen geadviseerd, verdeeld over beleids-, technische- en medewerker maatregelen. Zeven weken later hebben de mkb'ers gemiddeld aangegeven 34,3% van de geadviseerde maatregelen ingevoerd te hebben. Bovendien gaf ruim 60 procent van de respondenten aan dat zij op basis van het adviesrapport op korte termijn (verdere) verbeteringen gaan doorvoeren in de cybersecurity van de onderneming. Er zijn tijdens de pilot verschillende lessen geleerd die verbeterpunten bieden voor toekomstige uitvoerders van het project. Deze verbeterpunten hebben met name betrekking op het effectiever werven van ondernemers voor het project, het uitbreiden van de training voor buddy's en het verdelen van taken en verantwoordelijkheden tussen uitvoerders.

6.4.3 Conclusies en vervolgonderzoek

Alles bij elkaar genomen kan gesteld worden dat de interventie een effectieve tool is voor Nederlandse gemeenten om de cyberweerbaarheid van een specifieke groep mkb'ers in hun gemeente te bevorderen. Deze groep mkb'ers bestaat uit mkb'ers die behoefte hebben aan of open staan voor een project om de cyberweerbaarheid van hun onderneming te toetsen en (indien nodig) verbeteren. Deze mkb'ers hebben bijvoorbeeld zelf de gemeente benaderd met interesse om deel te nemen aan een project rondom cybersecurity of stonden hiervoor open nadat zij benaderd werden door de buddy (6.4% van alle benaderde mkb'ers). Na deelname aan het project is er sprake van een hogere mate van cyberweerbaarheid, gezien de toename van het aantal cybersecurity maatregelen dat deelnemende bedrijven lijken te nemen door hun deelname aan "MKB Cyber buddy's". "MKB Cyber buddy's" is een geschikte interventie voor gemeenten op zoek zijn naar een effectieve tool om mkb'ers die behoefte hebben aan informatie en hulp rondom cybersecurity in deze behoefte te voorzien. Wij raden aan het project te presenteren bij ondernemings-bijeenkomsten over

"De interventie is een effectieve tool voor Nederlandse gemeenten om de cyberweerbaarheid van een specifieke groep mkb'ers in hun gemeente te bevorderen"

cybersecurity, die door vele gemeenten reeds worden georganiseerd, waarbij ondernemers de optie geboden worden om zichzelf gelijk aan te melden voor “MKB Cyber buddy’s”. Met experimenteel onderzoek onder een groter aantal deelnemers kan de effectiviteit van de interventie, en de manier waarop de afzonderlijke onderdelen van de interventie bijdragen aan de effectiviteit, worden onderzocht.

- Beantwoording vierde deelvraag -

Q4: WELKE INTERVENTIES KUNNEN NEDERLANDSE GEMEENTEN INZETTEN OM HET RISICOBEWUSTZIJN EN HET PREVENTIEVE GEDRAG RONDOM DEZE TYPEN CYBERCRIME ONDER DEZE DOELGROEPEN TE BEVORDEREN?

A4: DE IN DIT PROJECT ONTWIKKELDE EN GEËVALUEERDE INTERVENTIES KUNNEN DOOR NEDERLANDSE GEMEENTEN WORDEN INGEZET:

JONGEREN, SHAME SEXTING/SEXTORTION	‘DOORSTUREN DOE JE NIET!’
JONGEREN, GELDEZELEN	INSTAGRAM CAMPAGNE
OUDEREN, DIGITALE OPLICHTING	‘LAAT JE GEEN H@CK ZETTEN!’
MKB, RANSOMWARE	MKB CYBER BUDDY’S

N.B.: ER IS IN DE AFGELOPEN TWEE JAAR EEN GROOT AANTAL INTERVENTIES GERICHT OP HET VERGROTEN VAN DE CYBERWEERBAARHEID VAN DOELEGROEPEN BESCHIKBAAR GEKOMEN (ZIE BIJVOORBEELD HET OVERZICHT VAN HET CENTRUM VOOR CRIMINALITEITSPREVENTIE EN VEILIGHEID. ECHTER, DEZE INTERVENTIES VEELAL NIET EVIDENCE BASED EN ZIJN NIET OP HUN EFFECTIVITEIT GEËVALUEEERD. DAARTOE ZIJN INMIDDELS DE SAMENWERKENDE LECTORATEN UIT DIT PROJECT INTUSSEN WEL VERZOCHT DOOR DE CITYDEAL LOKALE CYBERWEERBAARHEID.

7. WERKPAKKET 5: OPBRENGSTEN VAN HET PROJECT EN VERVOLG

We kijken als consortiumpartners terug op een dynamisch maar succesvol project. Een mooie klap op de vuurpijl was de nominatie voor de RAAK-award 2022 bij de SIA conferentie 2022 op 17 november jongstleden in Leiden (Figuur 10). Hoewel we niet in de prijzen zijn gevallen, zien we de nominatie als duidelijke blijk van waardering voor de resultaten van de samenwerking tussen onze lectoraten onderling en de mooie samenwerking met de praktijk.

Figuur 10 – Projectpitch door Remco Spithoven en ontvangst van het nominatiecertificaat bij de RAAK-award 2022 door Susanne van ’t Hoff-de Goede en Remco Spithoven op 17 november 2022 te Leiden.

In dit onderdeel maken we meer gedetailleerd de balans van het totale project op. Allereerst staan we stil bij de vier ontwikkelde, *evidence-based* interventies als sluitstuk van dit project, we behandelen de zeven praktijkpublicaties en de – maar liefst – tien wetenschappelijke publicaties die uit dit project zijn voortgekomen. Ook staan we stil bij de bijdragen die vanuit dit project aan het onderwijs bij Hogeschool Saxion en de Haagse Hogeschool zijn gedaan en de studentprojecten die dit heeft opgeleverd. Afsluitend gaan we in op de vervolgstappen die al zijn gezet en nog gezet kunnen worden.

7.1 De vier evidence-based interventies verder uitrollen

De vier ontwikkelde, *evidence-based* interventies zijn in beginsel geïmplementeerd bij de gemeenten die aan de interventies hebben meegebouwd. Nu deze zijn geëvalueerd, is het tijd om de interventies verder uit te rollen over het consortium en andere Nederlandse gemeenten en hun lokale partners. Wanneer er na het lezen van dit eindrapport interesse is in één of meerdere ontwikkelde interventies, dan kunt u contact opnemen met de volgende contactpersonen:

Interventie	Contactpersoon
Jongeren, Misbruik van seksueel beeldmateriaal **Doorsturen doe je niet!**	dr. Ynze van Houten, senior onderzoeker Maatschappelijke Veiligheid bij Hogeschool Saxion, via y.a.vanhouten@saxion.nl
Jongeren, Geldezelen **Instagram campagne**	dr. Rutger Leukfeldt, lector Cybercrime & Cybersecurity bij de Haagse Hogeschool, via e.r.leukfeldt@hhs.nl
Ouderen, Digitale oplichting **Laat je geen h@ck zetten!**	dr. Remco Spithoven, lector Maatschappelijke Veiligheid bij Hogeschool Saxion, via r.spithoven@saxion.nl
Mkb'ers, ransomware **MKB Cyber Buddy's**	dr. Susanne van 't Hoff-de Goede, senior onderzoeker Cybercrime & Cybersecurity bij de Haagse Hogeschool, via m.s.van-thoff-degoede@hhs.nl

7.2 Praktijkgerichte publicaties

In de loop van het project zijn de volgende praktijkgerichte publicaties gepubliceerd:

1. Spithoven, R. & Leukfeldt, E.R. (2020). Cyberweerbaarheid vraagt om maatwerk. In: De Crisismanager, via: https://decrisismanager.nl/lectoren-cyberweerbaarheid-vraagt-om-maatwerk;

2. Spithoven, R., van Ee, H. & van Houten (2021). Meer oog en zorg voor kwetsbare geldezels. In: Website voor de Politie, via: https://www.websitevoordepolitie.nl/zorg-voor-kwetsbare-geldezels/;

3. Bekkers, L.M., Leukfeldt, E.R. & Spithoven, R. (2022). Sociale media als hulpmiddel in de strijd tegen cybercriminaliteit. In SECONDANT, via: https://ccv-secondant.nl/platform/article/sociale-media-als-hulpmiddel-in-de-strijd-tegen-cybercriminaliteit-1

4. Misana-ter Huurne, E.F.J., van 't Hoff-de Goede, M.S., Bekkers, L.M., Walther, M., Spithoven, R. & Leukfeldt, E.R. (2021). Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Kwetsbare doelgroepen en bijbehorende typen cyberdelicten. Geïntegreerd deelrapport werkpakketten 1 en 2. Saxion/Haagse Hogeschool, via: https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/cyberweerbaarheid_deelrapport-wp1_2.pdf

5. Misana-ter Huurne, E., Bekkers, L., van 't Hoff-de Goede, S., van Houten, Y., Hansen, S., Foppen, E., Ebrahem, S., Spithoven, R. & Leukfeldt, R. (2021). Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Risicobewustzijn, preventief gedrag en de verklaringen daarvoor (Rapport werkpakket 3). Via: https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/cyberweerbaarheid-rapport-2-v5.pdf

6. Misana-ter Huurne, E., Bekkers, L., van 't Hoff-de Goede, S., Foppen, E., Ebramhem, S., van Houten, Y., Hansen, S., Spithoven, R. & Leukfeldt, R. (2021). Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime Risicobewustzijn en preventief gedrag wat betreft misbruik van seksueel beeldmateriaal en phishing, doelgroep jongeren (Deelrapport werkpakket 3). Hogeschool Saxion/Haagse Hogeschool.

7. Van Houten, Y., Misana-ter Huurne, E., Hansen, S., van 't Hoff-de Goede, S., Bekkers, L. Foppen, E., Leukfeldt, R. & Spithoven, R. (2021). Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Risicobewustzijn en preventief gedrag wat betreft vriend-in-noodfraude en phishing, doelgroep Ouderen (Deelrapport werkpakket 3). Hogeschool Saxion/Haagse Hogeschool.

8. Bekkers, L., van 't Hoff-de Goede, S., Misana-ter Huurne, E., van Houten, Y., Spithoven, R. & Leukfeldt, R. (2021).Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Risicobewustzijn en preventief gedrag wat betreft ransomware en phisshing, doelgroep mkb (Deelrapport werkpakket 3). Hogeschool Saxion/Haagse Hogeschool.

9. Spithoven, R. & Bekkers, L. (2021). Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Geldezelen onder jongeren Een verkennend onderzoek naar de prevalentie en risicoperceptie van jongeren rondom geldezelen. (Deelrapport werkpakket 3). Hogeschool Saxion/Haagse Hogeschool.

10. Spithoven, R., Leukfeldt, R., Misana-ter Huurne, E., van 't Hoff – de Goede, S., van Houten, Y., Bekkers, L., Foppen, E., & te Bos, J. (2022). Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Eindrapport, Werkpakket 5. Hogeschool Saxion/Haagse Hogeschool.

11. Foppen, E., Spithoven, R., te Bos, J., Bekkers, L.M., Leukfeldt, E.R., van 't Hoff-de Goede, M.S., Misana-ter Huurne, E.F.J. en van Houten, Y.A. (NOG TE VERSCHIJNEN). Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Ontwikkeling en evaluatie van vier interventies ter voorkoming van slachtofferschap onder jongeren, ouderen en mkb'ers. Rapportage werkpakket 4.

Daarnaast zijn de volgende praktijkgerichte publicaties ingediend:

12. Spithoven, R., Polman, S. & van Houten, Y.A. (NOG TE VERSCHIJNEN). Dieven gaan digitaal: criminaliteit op het web.

13. Bekkers, L.M., van 't Hoff-de Goede, M.S., Leukfeldt, E.R. & Spithoven, R. (NOG TE VERSCHIJNEN). Je bedrijf beschermen tegen ransomware. Wat motiveert mkb'ers om actie te ondernemen?

14. Foppen, E., van Houten, Y.A. & Spithoven, R. (NOG TE VERSCHIJNEN). Weerbaarheid van jongeren tegen shame sexting en sextortion.

15. Spithoven, R. & Leukfeldt, E.R. (NOG TE VERSCHIJNEN). Digitale koudwatervrees. Waarom Nederlandse gemeenten verder op cybercriminaliteit verder in beweging moeten komen.

7.3 Wetenschappelijke publicaties

In de loop van het project zijn de volgende wetenschappelijke publicaties gepubliceerd:

1. Leukfeldt, E.R., Spithoven, R. & Misana-ter Huurne (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In: C. de Poot, et al. (eds.). Politie en cybercrime, Cahiers Politiestudies, jrg. 2020, nr. 56, p. 203-223.;

2. Spithoven, R., van Houten, Y.A. & Misana-ter Huurne, E.F.J. (2020). Weerbaar tegen shame sexting en sextortion. Op zoek naar aangrijpingspunten voor aangescherpte voorlichting op scholen over de risico's van sexting. In: Pedagogiek, 40, 3, p. 261-287;

3. Bekkers, L. M. J., & Leukfeldt, E. R. (2022). Recruiting money mules on instagram: a qualitative examination of the online involvement

mechanisms of cybercrime. Deviant Behavior, 1-17;
4. Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: a quasi-experiment on engagement with money mule recruitment ads on Instagram. Journal of Experimental Criminology, 1-20.
5. van 't Hoff-de Goede, M.S., Misana-ter Huurne, E.F.J., Bekkers, L.M., van Houten, Y.A., Spithoven, R. & Leukfeldt, E.R. (2021). Weerbaar tegen phishing. Een verkenning van de onderliggende factoren bij zelfbescherming tegen phishing onder jongeren, ouderen en mkb'ers.

Daarnaast zijn de volgende wetenschappelijke publicaties ingediend:
6. Spithoven, R., Misana-ter Huurne, E.F.J. & van Houten, Y.A. (In review - NOG TE VERSCHIJNEN). Towards an Integrated Cyber Resilience Model. Combining psychological dynamics underlying problem-focused and emotion-focused coping in the strive for individual end users' cyber resilience.;
7. Foppen, E., Spithoven, R., Polman, S. & Misana-ter Huurne, E.F.J. (In review - NOG TE VERSCHIJNEN). A mix of trust and risk. Using an inductive research approach to explore adolescents' decision-making processes in response to a set vignettes about requests for online sexting.;
8. Bekkers, L.M., van Houten, Y.A., Spithoven, R. & Leukfeldt, E.R. (In review - NOG TE VERSCHIJNEN). Money Mules and Cybercrime Involvement Mechanisms: Exploring Experiences and Perceptions of Juveniles in the Netherlands. ;
9. Bekkers, L. M. J., Van 't Hoff-de Goede, M.S., Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (Geaccepteerd – NOG TE VERSCHIJNEN). Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures using an extended Protection Motivation Theory model..

Ook is momenteel het volgende artikel in ontwikkeling:
10. Misana-ter Huurne, E.F.J., Spithoven, R., van Houten, Y.A. (NOG TE VERSCHIJNEN). Image-based sexual abuse. Perceived risk and self-protective behaviors among young people: an application of an augmented PMT-model.

Na de formele afronding van dit project zal er door de consortiumpartners gezamenlijk nog de nodige artikelen worden geproduceerd. Daarvoor is nog voldoende empirisch materiaal beschikbaar.

7.4 Bijdragen aan onderwijs

Door de onderzoekers is vanuit het project een ruime bijdrage geleverd aan onderwijs in de vorm van tientallen gastcolleges. Ook is er structurele bijdrage geleverd aan vakken bij Saxion als het vak onderzoeksvaardigheden in het eerste jaar van Integrale Veiligheidskunde-Security Management. Er is drie jaar op rij door 200 studenten bijgedragen aan vragenlijstonderzoek rondom de thematiek van dit project. Ook zijn de Saxion-onderzoekers nauw betrokken bij de Saxion-minor De Digitale Revolutie van de Academie Bestuur, Recht en Ruimte en wordt elke jaargang opdrachtgeverschap voor de onderzoekscomponent van deze minor verzorgd. Aan de Haagse Hogeschool is er structurele bijdrage geleverd aan het vak 'Human Behaviour in Cybersecurity' van de opleiding HBO ICT, specialisatie Information Security Management. Ook hebben diverse studenten stage gelopen bij onderzoekers van de Haagse Hogeschool.

7.5 Studentproducten

Binnen dit project zijn de volgende studentenproducten gerealiseerd:

A. Safety & Security Lab opdrachten voor 2e en 3e jaars studenten Integrale Veiligheidskunde/Security Management, Hogeschool Saxion:
1. Elise Serti, Ilse Maandag, Julia Prins, Jurre Hanstede, Mats van Beveren en Silke Janssen (2020). Prevalentie van geldezelen onder jongeren;
2. Anne Janssen, Jasmijn Smeier, Luc Veldman, Tabitha Cornelissen (2020). Kansen voor interventies over geldezelen onder jongeren;
3. Mitchell Aalten, Lente Aan, Sita Balk, Stijn Ebels, Bowien Hulleman, Siger Lodewijks, Joost Padberg en Meggy Willemsen (2021). Cyberweerbaarheid in het mkb;
4. Arnel Hagemeijer, Emma Rosendaal, Joerick Eshuis, Madée Wolberink (2022). Social Engineering en Digitale weerbaarheid bij ouderen.

B. Producten van de minor De Digitale Revolutie, Hogeschool Saxion, jaargang 2020:
1. Nienke den Nederlanden, Melanie Prins, Ramona Linschoten en Jennifer Helder (2020). Nep-vacatures.
2. Maurice Perik, Colin Puhl, Stefan Musch en Femke Goedhart (2020). Helpdeskfraude.
3. Bart Hendriks, Mark Nijhof, Robbert Poel en Stijn Huijsmans (2020). Money muling.
4. Stijn Haandrikman, Ronald Huisjes, Stan Hulsegge en Ruben van Loon (2020). Ransomware.
5. Leon van den Bedem, Emma van Berkum, Han Bleumer en Manon Frankenhuizen (2020). Smishing.
6. Justin Bos, Pip Schuiling, Laurens Flierman en Gido Huitink (2020). Tikkie-fraude.

Bovenstaande studentonderzoeken zijn samengevoegd in het rapport:
Spithoven, R., van Houten, Y.A. & Walther, M. (2020) Cyberweerbaarheid. Resultaten van studentonderzoek naar het vergroten van de weerbaarheid van diverse doelgroepen tegen verschillende vormen van cybercriminaliteit. Saxion, lectoraat Maatschappelijke Veiligheid.
C. Producten van de minor De Digitale Revolutie, Hogeschool Saxion, jaargang 2021:
1. Eva Hartman, Chiel Karkdijk, Marc Garbe en Lotte ten Hove (2021). Verkoopfraude onder jongeren.
2. Muharrem Kocabiyik, Jesse Lesscher en Fleur Kooistra (2021). Verkoopfraude onder ouderen.
3. Herm Alberts, Hidde Altena, Ellis Brouwer en Maarten Huisman (2021). Phishing onder jongeren.
4. J. Brinkman, D. Brus, J.J. van Dooremolen, S. Gopal (2021). Phishing onder ouderen.
5. Quinty Meijering, Hidde Kok, Celine Weideveld en Tommy Möller (2021). VIN-fraude onder jongeren.
6. Koen van Norel, Bram Veldhuis, Tom Weijers, Rogier Versluis & Ellen Maathuis (2021). VIN-fraude onder ouderen.

D. Producten van de minor de Digitale Revolutie, Hogeschool Saxion, Jaargang 2022:
1. Krijn Toet, Tim Assinck, Thijmen Bertelink, Jasper Haak en Sanne Arendhorst (2022). Pre-

ventie van geldezelen op het Zonecollege.
2. Brian Berns, Lisa te Brake, Laurie Bunskock, Christiaan Groeneveld en Max de Haas (2022). Preventie van geldezelen via Het Klokhuis.
3. Seferino Bouwer, Wout Drowniak, Richelle Jongejan, Inge Kroeze en Tark Moeharram (2022). Preventie van geldezelen op het Praktijkcollege.
4. Anouk Roeberding, Remy van Uffelen, Chris Verwijken en Damian Stokvisch (2022). Preventie van geldezelen op het Sprengeloo college.

Bovenstaande studentonderzoeken zijn samengevoegd in het rapport:
Foppen, E., Polman, S. van Ee, H., van Houten, Y.A. en Spithoven, R. (2022). Geldezelen. Resultaten van studentenonderzoek naar de preventie en prevalentie van geldezelen onder jongeren in Nederland. Saxion, lectoraat Maatschappelijke Veiligheid.

E. Afstudeerscripties:
1. Diann Vosmeijer (2021). Nazorg voor money muling. Sociaal Juridische Dienstverlening, Hogeschool Saxion;
2. Shannon ten Donkelaar (2021). Naar een handreiking nazorg money muling Licht verstandelijk beperkten. Sociaal Juridische Dienstverlening, Hogeschool Saxion;
3. Mireille Winters (2021). Naar een handreiking nazorg money mules. Sociaal Juridische Dienstverlening, Hogeschool Saxion;
4. Hidde Melles (2021). Ransomware in het mkb. Integrale veiligheidskunde, Hogeschool Saxion;
5. Jeff Gaarlandt (2021). Sextortion onder jongeren. Integrale veiligheidskunde, Hogeschool Saxion;
6. Marc Garbe (2021). Phishing in het mkb. Integrale veiligheidskunde, Hogeschool Saxion;
7. Niels Rem (2021). Phishing onder senioren. Integrale veiligheidskunde, Hogeschool Saxion;
8. Paul Wu (2021). Het gebruik van wachtwoorden en -managers onder jongeren. Integrale Veiligheidskunde, Hogeschool Saxion;
9. Sanne de Jong (2021). WhatsApp-fraude onder senioren. Sociologie, Universiteit Utrecht;
10. Nikki van Mook (2021). Sexting onder jongeren. HBO Rechten, Hogeschool Saxion;
11. Jens Meuleman (2022). Effectiviteit meten van interventies over het vergroten van cyberweerbaarheid. Integrale veiligheidskunde, Hogeschool Saxion;
12. Eline Brasker (2022). Cyberweerbaarheid in het mkb. De evaluatie van het MKB Cyber Buddy's project. Sociologie, Universiteit Utrecht.

7.6 Vervolgstappen

De samenwerking tussen de lectoraten Maatschappelijke Veiligheid van de Hogeschool Saxion en Cybercrime & Cybersecurity van de Haagse Hogeschool is aan weerszijde goed bevallen. Daarom is besloten om, nog voor de afronding van dit RAAK-publiek project, een gezamenlijke aanvraag voor een SPRONG-consortium te doen. Daarvoor is de huidige samenwerking uitgebreid met het lectoraat Cybersafety van de NHL Stenden Hogeschool en is de bestaande samenwerking met de publieke partners uit dit RAAK-publiek project uitgebreid. Deze subsidie is recent toegekend en de ambitie is om in de toekomst meerdere, gezamenlijke onderzoekprojecten op een gezamenlijke onderzoeksprogrammering te gaan uitvoeren om gezamenlijk meer impact op de cyberweerbaarheid van de Nederlandse samenleving te organiseren.

Hierbij zien wij, naar aanleiding van dit RAAK-publiek project de volgende, concrete onderzoeksprojecten voor ons:
1. Uitwerking van verdere, wetenschappelijke en praktijkgerichte publicaties op basis van dit project;
2. Ontwikkeling van interventies ter preventie van slachtofferschap van phishing onder jongeren, ouderen en mkb'ers;
3. De interventie ter preventie van slachtofferschap van misbruik van seksueel beeldmateriaal onder jongeren kan met experimenteel vervolgonderzoek onder grotere aantallen deelnemers nader worden onderzocht worden op het effect van de interventie op de weerbaarheid. Hierop kan de interventie inhoudelijk worden doorontwikkeld;
4. De interventie ter preventie van geldezelen onder jongeren zou middels experimenteel onderzoek op het preventieve effect onder jongeren kunnen worden onderzocht om daarmee ook deze interventie inhoudelijk verder te ontwikkelen;
5. De effectiviteit van de interventie ter preventie van slachtofferschap van digitale oplichting onder ouderen dient nader op de effectiviteit te worden onderzocht. Er zijn de eerste sporen van effectiviteit aangetroffen, maar dit is op een klein aantal respondenten gebaseerd. Met experimenteel onderzoek onder een groter aantal deelnemers kan dit nader worden vastgesteld.
6. De effectiviteit van de interventie in het verhogen van de cyberweerbaarheid van mkb'ers tegen ransomware zou nader onderzocht kunnen worden onder een grotere groep mkb'ers. Bovendien kan de manier waarop de afzonderlijke onderdelen van de interventie bijdragen aan de effectiviteit worden onderzocht en kan de interventie daarmee verder ontwikkeld worden.
7. Evaluatie van andere, beschikbare interventies rondom de cyberweerbaarheid van doelgroepen voor Nederlandse gemeenten zoals de samenwerkende lectoraten inmiddels door de Citydeal Lokale Cyberweerbaarheid zijn verzocht te doen.

GERAADPLEEGDE LITERATUUR

Berding, J. & Witte, T. (2013) *Praktijkonderzoek op niveau. Inspelen op onderzoeksdilemma's bij sociale studies*. Bussum : Coutinho.

CBS (2022). *Nearly 2.5 million people victims of cybercrime in 2021.* Via: https://www.cbs.nl/en-gb/news/2022/09/nearly-2-5-million-people-victims-of-cybercrime-in-2021

De Lange, R., Schuman, H. & Montesano Montessiori, N.(2011). *Praktijkgericht onderzoek voor reflectieve professionals.* Garant

Migchelbrink, F. (2013). *Handboek praktijkgericht onderzoek*. SWP.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercriminaliteit. *European Journal of Information Systems*, 29(3), 306-321. https://doi.org/10.1080/0960085X.2020.1771222.