MASTER THESIS

# WHATSAPP FRAUDE

*Een kwalitatieve studie naar risicobewust handelen door ouderen bij WhatsApp fraude*


SANNE DE JONG 6878164

## Voorwoord

Het schrijven van een masterscriptie kent voor iedere student zijn ups & downs. Naast de moeilijkheden die de coronapandemie met zich bracht, had ik ook gezondheidsproblemen die ervoor zorgde dat het niet het makkelijkste half jaar zou worden in mijn studententijd. Desondanks ben ik zeer trots dat ik hierbij mijn masterscriptie presenteer voor de opleiding Sociology: Contemporary Social Problems aan de Universiteit Utrecht. Ik heb met een hoop enthousiasme en toewijding gewerkt aan dit onderzoek en heb veel geleerd in de afgelopen periode. Dit heb ik aan een aantal mensen te danken.

Allereerst wil ik graag Susanne van ’t Hoff – de Goede & Luuk Bekkers, mijn stagebegeleiders, bedanken. Ongeacht het online plaatsvinden van al onze meetings, stonden zij altijd klaar om mij te voorzien van advies en begeleiding en heb ik tevens veel van ze kunnen leren. Naast mijn stagebegeleiders wil ik ook het hele lectoraat Cybersecurity in het MKB ontzettend bedanken. Ondanks dat alle meetings online plaatsvonden, hebben zij er ten alle tijden voor gezorgd dat ik mij als een volwaardige collega voelde en wat ik inbreng werd serieus gennomen.

Tevens wil ik mijn scriptie supervisor, Amy Nivette, bedanken voor de fijne begeleiding die zij heeft gegeven. Zij heeft mij voorzien van duidelijke feedback & fijne begeleiding in het scriptie proces, waardoor deze scriptie nu in deze huidige vorm voor u ligt. Haar positiviteit en toegankelijkheid hebben er voor gezorgd dat ik altijd gemotiveerd ben gebleven de deadlines te halen. Tevens wil ik Tali Spiegel, onze mastercoordinator, bedanken voor al haar steun in de moeilijke periodes die ik in mijn scirptieperiode heb doorlopen. Dat heeft mij enorm gerustgesteld op belangrijke momenten.

Als laaste wil ik een blijk van dank aan mijn familie en vrienden geven, omdat die mij voorzien hebebn van nodige afleiding of om mijn ei bij kwijt te kunnen. In het speciaal wil ik graag mijn opa bedanken die voor mij mijn scriptie heeft doorgelezen en van feedback heeft voorzien, dat waardeer ik enorm.

Ik wens u veel leesplezier!

Sanne de Jong
Tuk, 25 juni 2021

## Abstract

WhatsApp fraude is een onderwerp dat de afgelopen 2 jaar met regelmaat verschijnt in de media. Hierbij komt tevens naar voren dat de meeste slachtoffers van dit type cybercrime voornamelijk ouderen zijn (Politie Nederland, 2020). Onderzoek van Leukfeldt & van 't Hoff – de Goede (2021) en de cijfers van de politie laten zien dat WhatsApp fraude een nieuw en groeiend fenomeen is waar veel Nederlandse ouderen mee te maken krijgen. Om deze redenen is het verkrijgen van inzicht over ouderen en WhatsApp fraude, omtrent de intentie tot wel of niet risicobewust handelen, door middel van onderzoek belangrijk. Ook om zo de eerste stappen te zetten richting effectieve interventies om ouderen weerbaar te maken tegen WhatsApp fraude. De onderzoeksvragen van dit onderzoek zijn dan ook:

- Beschrijvende vraag: *Wat weten ouderen van risicobewust handelen bij WhatsApp fraude?*
- Verklarende vraag: *Waarom hebben ouderen wel of geen intentie om risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten?*
- Beleidsvraag: *Welke invalshoeken geven deze inzichten op eventuele interventies die zich richten op het verminderen van slachtofferschap van ouderen bij WhatsApp fraude?*

De resultaten laten zien dat de kennis omtrent WhatsApp fraude bij ouderen aanwezig is, echter niet volledig is, omdat het bijvoorbeeld verward wordt met phishing. Wat betreft de kennis over risicobewust handelen bij WhatsApp fraude door ouderen, valt het meest op dat ze deze kennis onbewust hebben. Wanneer ze moeten handelen doen ze dat, echter wanneer gevraagd wordt naar dit soort handelingen komen zij daar niet direct op. Kijkend naar waarom ouderen wel of niet risicobewust handelen bij WhatsApp fraude zijn de factoren herkenning van de red flags, response effectiviteit en response kosten van belang. De ouderen handelen niet risicobewust als ze de 'red flags' niet herkennen. Tevens wordt afgezien van een risicobewuste handeling als deze als niet effectief (response effectiviteit) is of als de kosten daarvoor een drempel vormen (response kosten). Kosten kunnen ook gezien worden als het gevoel hebben iemand lastig te vallen met een risicobewuste handeling, zoals het bellen van hun zoon of dochter. Hiermee kan worden geconcludeerd dat (intentie tot) gedrag van ouderen bij WhatsApp fraude afhankelijk is van de kennis, en hiermee het kunnen herkennen van de 'red flags' en de interne afwegingen die zij maken op basis van de Protection Motivation Theory (Floyd, et al., 2000). De inzichten van dit onderzoek maakt dat er gekeken zal moeten worden naar interventies die zijn gefocust op het verbreden van kennis over, het waarschuwen voor, en het laten ervaren van WhatsApp fraude.

**Kernwoorden:** risicoperceptie; risicobewustzijn; risicobewust handelen; WhatsApp fraude; vriend-in-nood fraude; gedragsintentie; ouderen.

**Master thesis**
**WhatsApp fraude**
*Een verdiepend onderzoek in het risicobewust handelen door ouderen bij WhatsApp fraude*

Sanne de Jong (6878164)
s.dejong13@students.uu.nl
Master thesis, Sociology: Contemporary Social Problems
Universiteit Utrecht

Universiteit Utrecht Begeleider: Amy Nivette
Stagebegeleiders: dr. Susanne van ’t Hoff-de Goede & Luuk Bekkers

Woordenaantal: 10.381 (incl. tabellen)
25 juni 2021

# Inhoudsopgave

# 1. Introductie

Op 12 oktober 2020 kopte NU.nl: *"Bijna vier keer zo vaak WhatsApp fraude gemeld als in 2019. Het aantal gemelde gevallen van WhatsApp fraude is ten opzichte van 2019 flink gestegen. Er kwamen tot 1 oktober dit jaar vier keer zoveel meldingen binnen als in heel 2019, laat de Fraudeheldesk aan NU.nl weten."*. WhatsApp fraude is een onderwerp dat de afgelopen 2 jaar met regelmaat verschijnt in de media. Hierbij komt tevens naar voren dat de meeste slachtoffers van dit type cybercrime voornamelijk ouderen zijn (Politie Nederland, 2020). Echter: Wat maakt het dat juist deze doelgroep het vaakst slachtoffer wordt van dit type cybercrime? In hoeverre is deze doelgroep zich bewust van het risico van WhatsApp fraude en weet deze doelgroep hoe zij risicobewust kunnen handelen bij vermoedelijke WhatsApp fraude? Allemaal vragen waar onderzoek voor nodig is om meer duidelijkheid te krijgen in het slachtofferschap van ouderen bij WhatsApp fraude.

## 1.1 Achtergrond

Deze studie is onderdeel van een grotere studie, het project Cyberweerbaarheid. Dit is een project dat wordt uitgevoerd door onderzoekers van de Haagse Hogeschool, Hogeschool Saxion en het Nederlandse Studiecentrum voor Criminaliteit en Rechtshandhaving (NSCR) in samenwerking met verschillende gemeenten en regionale veiligheidsnetwerken. Dit project heeft als doel de inwoners van de gemeenten weerbaar te maken tegen cybercrime door middel van (beproefde) effectieve interventies gericht op specifieke doelgroepen & specifieke cybercrime delicten (Misana-ter Huurne, Leukfedlt, Spithoven, van 't Hoff-de Goede, van Houten, Bekkers & Walther, 2021).
Dit onderzoek richt zich specifiek op de doelgroep ouderen, 55 jaar of ouder, in combinatie met het delict vriend-in-nood fraude, ook wel WhatsApp fraude genoemd. Het doel van de thesis is om een bijdrage te leveren aan de te ontwikkelen interventies gericht op het weerbaar maken van ouderen tegen WhatsApp fraude. Aan de hand van gesprekken ment de gemeenten en experts op dit gebied, is vastgesteld dat de doelgroep ouderen een kwetsbare groep is met betrekking tot cybercrime. De gemeenten vinden het belangrijk dat er interventies ontwikkeld worden om ouderen weerbaar te maken tegen cybercrime (Misana-ter Huurne, et al., 2021). Om dit effectief te kunnen doen is eerst onderzoek nodig naar deze doelgroep. Op basis van de genoemde gesprekken met gemeenten en experts is ervoor gekozen te kijken naar de combinatie ouderen en WhatsApp fraude. Volgens de gemeenten kan iedereen slachtoffer worden van WhatsApp fraude, maar op basis van politiecijfers is te zien dat dit type fraude voornamelijk voorkomt bij ouderen. Volgens expert is dit delict onder de doelgroep ouderen het afgelopen jaar sterk toegenomen. Om deze redenen vinden de gemeenten het belangrijk dat voor deze delict en doelgroep combinatie een interventie wordt ontwikkeld om de weerbaarheid te verbeteren (Misana-ter Huurne, et al., 2021).

## 1.2 Maatschappelijke relevantie

Momenteel leven wij in een steeds meer digitaliserende wereld, waarin geacht wordt dat wij als maatschappij meebewegen in deze digitale wereld. Denk bijvoorbeeld aan internetbankieren of het doen van belastingaangifte. Er wordt van iedereen verwacht dat dit digitaal gedaan wordt, ook van de ouderen. Hiermee gaat de groei van cybercrime gepaard. In 2019 is ten opzichte van 2017 het percentage van de Nederlanders die slachtoffer zijn geweest van cybercrimedelicten gestegen van 11% naar 13%. De meest voorkomende delicten zijn hacken, cyberpesten, koop- en verkoopfraude en identiteitsfraude (Centraal Bureau voor de Statistiek, 2019). Inmiddels wordt cybercrime dan ook bestempeld als een groot maatschappelijk probleem (Beerthuizen, Sipma, Van der Laan, 2020).
De studie van Das en Nayak (2013) laat zien wat voor impact het heeft slachtoffer te worden van cybercrime. De slachtoffers geven aan dat het een grote emotionele last geeft. Naast dat ze sterke emoties als boos, geïrriteerd en gevoel van bedrog ervaren, geven de slachtoffers zichzelf vaak de schuld. Deze impact op slachtoffers heeft veel invloed op hun leven.

Het CCV geeft aan dat ouderen momenteel misschien niet de grootste groep slachtoffers zijn, maar dat dit zeker een groeiende groep is doordat ouderen steeds meer tijd doorbrengen online (Lenssink & van der Meer, 2019). Hierbij geeft Politie Nederland (2020) aan dat ouderen (55 jaar en ouder) momenteel het meest slachtoffer worden van WhatsApp fraude. WhatsApp fraude is een groeiende type cybercrime in Nederland. Onderzoekers van 't Hoff – de Goede en Leukfeldt van de Haagse Hogeschool hebben in 2021 voor het eerst in Nederland een representatieve studie uitgevoerd onder 20.000 Nederlanders over dit type fraude. Hierin werd duidelijk dat maar liefst 15% van de Nederlanders een poging van WhatsApp fraude hebben meegemaakt. Dit onderzoek en de cijfers van de politie laten zien dat WhatsApp fraude een nieuw en groeiend fenomeen is waar veel Nederlandse ouderen mee te maken krijgen. Om deze redenen is het verkrijgen van inzicht over ouderen en WhatsApp fraude door middel van onderzoek belangrijk om zo de eerste stappen te zetten richting effectieve interventies om ouderen weerbaar te maken tegen WhatsApp fraude.

## 1.3 Wetenschappelijke relevantie

Cybercrime en cybercrime slachtofferschap wordt steeds frequenter onderzocht (van 't Hoff-de Goede, van der Kleij, Leukfeldt & van der Weijer, 2019: Beerthuizen, Sipma & van der Laan, 2020: van Wilsem, 2010: Dodel & Mesch, 2017: Das & Nayak, 2013: Leukfeldt & Yar, 2016), maar is nog altijd een vrij nieuw en onduidelijk onderwerp. De kwantitatieve onderzoeken naar cybercrime zijn al beperkt, maar kwalitatief onderzoek naar cybercrime is nog beperkter aanwezig. Het is een type criminaliteit die met de jaren groeit, maar door de technologische ontwikkelingen ook veranderd van aard. Hierbij is WhatsApp fraude een nieuw opkomende cybercrime delict waar, zeker in combinatie met ouderen, nog geen onderzoek naar is gedaan.
Hoewel er naar de combinatie ouderen en WhatsApp fraude nog geen onderzoek gedaan is, heeft er wel verkennend onderzoek plaatsgevonden naar dit delict (van 't Hoff – de Goede & Leukfeldt, 2021). Doordat dit onderzoek een verkennend onderzoek was, is er enkel gekeken naar belangrijke, algemene informatie omtrent dit delict en zijn er verder geen analyses gedaan omtrent de combinatie van dit delict met de leeftijdscategorie 55+. Dit kwalitatieve onderzoek dient daarom als een verdieping op het delict WhatsApp fraude in combinatie met de doelgroep ouderen (55+) door te onderzoeken wat de kennis van ouderen is over het risico van WhatsApp fraude en hoe ouderen denken en handelen bij vermoedelijke WhatsApp fraude kan dit inzichten dit geven voor de eerste stappen richting interventies die ouderen weerbaarder maken tegen WhatsApp fraude.

## 1.4 Onderzoeksvragen

Met deze masterthesis wordt de kennis van ouderen over risicobewust handelen bij WhatsApp fraude inzichtelijk gemaakt. Tevens wordt er gekeken naar het gedachteproces die ouderen hebben bij het beslissen om wel of niet risicobewust te handelen bij WhatsApp fraude. Met deze inzichten kunnen de eerste stappen gezet worden richting interventies om ouderen weerbaar te maken tegen WhatsApp fraude.
Allereerst zal de mate van kennis van ouderen over risicobewust handelen bij WhatsApp fraude in kaart worden gebracht met behulp van de volgende beschrijvende vraag:

> *"Wat weten ouderen van risicobewust handelen bij WhatsApp fraude?"*

Vervolgens zal worden gekeken wat de afwegingen zijn van ouderen om juist wel of juist niet (de intentie te hebben om) risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten. Dit wordt gedaan aan de hand van de volgende verdiepende vraag:

> *"Waarom hebben ouderen wel of geen intentie om risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten?"*

Met deze inzichten worden er een kijk gegeven in het gedachteproces van ouderen bij WhatsApp fraude, wat mogelijkheden biedt voor interventies die zich richten op het verminderen van slachtofferschap van ouderen bij WhatsApp fraude. Gepoogd wordt de volgende beleidsvraag te beantwoorden:

> *"Welke invalshoeken geven deze inzichten op eventuele interventies die zich richten op het verminderen van slachtofferschap van ouderen bij WhatsApp fraude?"*

# 2. Theoretisch kader

## 2.1 Cyberweerbaarheid

Experts schatten dat ongeveer 95% van het succes van alle cyberdelicten komt door menselijk handelen. Hiermee wordt bedoeld dat het slachtofferschap vrijwel altijd het gevolg is van het menselijk onveilig handelen van slachtoffers. Hierbij kan men denken aan onveilig gedrag, het niet naleven van (gedrags)regels of het ontbreken van richtlijnen (Roelofs, de Koning, van Vliet, Wijn, Rijk & Young, 2018). Er valt daarom dan ook veel winst te behalen bij het vergroten van de weerbaarheid van potentiele slachtoffers van cyberdelicten om zo het slagen van deze delicten in de kiem te smoren (Misana-ter Huurne, et al., 2021).

Cyberweerbaarheid heeft een breed spectrum aan definities. Een veel gebruikte definitie is die van Hausken (2020): *"Cyberweerbaarheid is het vermogen van een actor om cyberincidenten te weerstaan, erop te reageren en te herstellen, om zo de operationele continuïteit van de actor te waarborgen".* Anders gezegd, zoals wordt gesteld in het rapport van Misana-ter Huurne, van Houten, Spithoven, Notté en Leukfeldt (2020), is cyberweerbaarheid *"de mate waarin iemand in staat is tegenstand te bieden tegen cybercrime ofwel de mate waarin iemand zelfbeschermend gedrag vertoont met betrekking tot cybercrime"*. Hierbij wordt zelfbeschermend gedrag gezien als acties of gedragingen die men uitvoert om zichzelf te beschermen tegen gevaren, risico's of het gevolg daarvan (inclusief (negatieve) emoties) (Misana-ter Huurne, et al., 2020). Toegepast op de huidige studie, wordt met cyberweerbaarheid gefocust op de gedragingen of acties die iemand neemt om zichzelf te beschermen tegen cyberrisico's of de gevolgen daarvan.

In de literatuur zijn verschillende factoren beschreven die verklaren waarom mensen wel of niet zelf-beschermend gedrag vertonen. Hierbij staat de beleving van risico's centraal. Voordat iemand zelfbeschermend gedrag ten opzichte van een risico vertoont, moet hij of zij dit risico als persoonlijk relevant beleven (Misana-ter Huurne, 2020). Om de cyberweerbaarheid van mensen te kunnen vergroten, moet er onder andere voor gezorgd worden dat hun risicobewustzijn omtrent het cyberrisco verhoogd wordt om zo zelfbeschermend gedrag te stimuleren.

## 2.2 Ouderen en WhatsApp fraude

Meerdere studies (Holtfreter, Reisig, Mears & Wolfe, 2014: Carcach, Graycar & Muscat, 2001: Burnes, Henderson, Sheppard, Zhao, Pillemer & Lachs, 2017) hebben aangetoond dat ouderen over het algemeen vaker doelwit zijn van pogingen tot financiële fraude en dat deze fraude de meest significante en frequente vorm van criminaliteit is die ouderen kunnen ervaren (Zhang, Ren, Li & Lin, 2019). Met de voorspelde vergrijzing van de samenleving (Stoeldraijer, van Duin & Huisman, 2017), is de verwachting dat financiële fraude enkel maar zal toenemen (Zhang, et al., 2019).

Een voorbeeld van financiële fraude, is WhatsApp fraude. In 2020 is er door onderzoekers van het Centre of Expertise Cybersecurity van De Haagse Hogeschool voor het eerst in Nederland een grootschalig onderzoek gedaan naar deze vorm van fraude. Dit onderzoek laat zien dat Whatsapp fraude een variant is van financiële fraude die steeds 'populairder' wordt. Zo toont die studie onder andere aan dat 15% van de Nederlanders in het afgelopen jaar een poging tot WhatsApp fraude hebben meegemaakt. Hiervan maakte 5% ook daadwerkelijk geld over (van 't Hoff-de Goede, et al., 2021).

Daarbij gaat het om bedragen van minder dan 750 euro tot bedragen van meer dan 2500 euro. De slachtoffers rapporteren echter dat de psychische gevolgen ernstiger zijn dan de financiële gevolgen (van 't Hoff-de Goede & Leukfeldt, 2021).

Dat dit type fraude voornamelijk voor komt onder ouderen is duidelijk terug te zien in de cijfers van Politie Nederland (2021). Zij geven aan dat er in 2020 een toename in aangiftes van dit type fraude is vastgesteld. Hierbij vormde de 55-plussers de grootste groep slachtoffers.
Ondanks dat het bekend is dat ouderen vaker slachtoffer zijn van dit type fraude, is het nog onduidelijk waarom zij hier vaker slachtoffer van zijn. Zhang, et al. (2019) verwachten dat een aantal factoren hier een rol in spelen: psychologische kwetsbaarheid, sociale isolatie, het natuurlijke vertrouwen dat ouderen hebben, het nemen van risico's en basiskennis. Zij stellen dat deze factoren van invloed zijn op hoe zij keuzes maken in gedrag.

*Psychologische kwetsbaarheid* & sociale isolatie
Psychologische kwetsbaarheid en sociale isolatie zijn nauw met elkaar verbonden. Het een versterkt het ander of het een veroorzaakt het andere. Ouderen met lage volbrenging van sociale behoeftes, depressie en/of sociale isolatie, oftewel psychologische kwetsbaarheid, vertonen een sterkere psychische behoefte om te verbinden met anderen, inclusief vreemden, waardoor ze makkelijke doelwitten worden voor fraudeurs. Dit wordt benadrukt door de studie van Lichtenberg, Stickney & Paulson (2013) die vonden dat ouderen met psychologische kwetsbaarheid waarschijnlijk drie keer meer kans hadden op slachtoffer te worden van fraude. Sociale isolatie is dus van invloed op de (psychologische) kwetsbaarheid van een persoon. Daarmee is die persoon tevens kwetsbaar voor fraude. Dit omdat geïsoleerde ouderen mogelijk in contact komen met daders die doen alsof zij een sociale connectie willen ontwikkelen. Ouderen kunnen ideale slachtoffers zijn voor zogenoemde 'hunters' omdat veel van hen alleen wonen, door bijvoorbeeld het overlijden van hun partner, wat resulteert in isolatie. Hierdoor zijn ze misschien gewilliger om in contact te komen met onbekenden. Hunters zijn opzoek naar dit soort mensen, om zich dan vervolgens bijvoorbeeld voor te doen als een liefdesinteresse of vertrouwenspersoon. Een andere factor die van belang is bij sociale isolatie, is de invloed van familieleden. Wanneer een ouder iemand alleen leeft is er vaak geen directe supervisie van eventuele familieleden, wat ze een makkelijk doelwit maakt voor fraudeurs. Een voorbeeld van fraude die hierop in speelt is telemarketing fraude.

*Het 'natuurlijke' vertrouwen*
Het feit dat ouderen goed van vertrouwen zijn, is al lange tijd geïmpliceerd als een primaire factor bij de kwetsbaarheid van ouderen voor fraude. Veel studies hebben ook aangetoond dat ouderen inderdaad over het algemeen goed van vertrouwen zijn als het wordt vergekejeb met jongere mensen. (Li & Fung, 2012; Kirchheimer, 2011). Doordat ouderen dus over het algemeen anderen, ook onbekenden, snel vertrouwen, worden ze kwetsbaar voor slachtofferschap van fraude.

*Het nemen van risico's*
Het financieel risico-nemend gedrag van een persoon, beïnvloed mogelijk de kans om slachtoffer van fraude te worden. Studies (Holtfreter, Reisig & Blomberg, 2006: Samanez-Larking, Gibbs, Khanna, Nielsen, Cartsen & Knutson, 2007) hebben namelijk aangetoond dat slachtoffers van fraude vaak risico-nemers zijn. Tevens wordt gesuggereerd dat de houding ten opzichte van risicovolle vooruitzichten van invloed zijn op de gepercipieerde kans van oplichting. Er is groeiend bewijs dat ouderen een verminderde 'negatieve opwinding' vertonen voor verwacht verlies (Samanez-Larking, et al., 2007) waardoor ze mogelijk risicovollere financiële besluiten nemen. Dit maakt dat ouderen mogelijk een grotere kans hebben om slachtoffer te worden van fraude als gevolg van een afname van de impact (verlies van geld, e.d.) die verwacht wordt als gevolg van het gesignaleerde risico.

*Basiskennis*
De kwetsbaarheid van ouderen voor fraude, als resultaat van een beperkt fraude bewustzijn, kan komen van een beperkte, of zelfs geen kennis in deze zaken. Dit varieert van het niet kunnen herkennen van fraude, de zogenoemde 'red flags', maar ook in het niet weten wat men moet doen met deze zaken. Dit maakt ouderen een makkelijk doelwit voor fraude, omdat zij soms simpel weg niet eens weten dat zij te maken hebben met fraude.

Echter, ondanks dat er veel onderzoek is gedaan naar factoren die ouderen gevoelig maken voor fraude, zijn theorieën over de kwetsbaarheid van ouderen bij fraude schaars en is het van belang dat dit ontwikkeld gaat worden (Zhang, et al., 2019).

## 2.3 Risicoperceptie en risicobewust handelen

Risicoperceptie wordt in de criminologie literatuur gedefinieerd als een cognitieve, op eigen inschatting beoordeling (beleving) van de kans op (crimineel) slachtofferschap (Liem, Kuipers & Sciarone, 2018). Wanneer de risicoperceptie van iemand realistisch is, kan het een nuttige aanpassingsfunctie hebben om hem te helpen het risico van slachtofferschap te ontlopen. Echter, criminologische en psychologische onderzoeken hebben aangetoond dat mensen de neiging hebben overmoedig te zijn in de inschatting van hun risico om slachtoffer te worden wanneer dit vergeleken wordt met het daadwerkelijke risico (Russo, Roccato & Vieno, 2012) Onderzoek toont aan dat de kloof tussen statistische waarschijnlijkheid van risico's en de individuele beleving van risico met name groot is op het gebied van veiligheid en gezondheid (Liem, et al., 2018). De afgelopen jaren is een van de opmerkelijke bevindingen in onderzoek naar risicoperceptie de 'optimistic bias' geweest (Helweg-Larsen & Shepperd, 2001). De 'optimistic bias' is de neiging van mensen om te melden dat ze minder dan anderen geneigd zijn om negatieve gebeurtenissen te ervaren (Cho, Lee & Chung, 2010). Zij schatten hun eigen risico lager in ten opzichte van anderen. Dit fenomeen beïnvloed zowel de percepties als de gedragingen, bijvoorbeeld risicobewust handelen, met betrekking tot verscheidenheid aan risico's, zoals cybercriminaliteit slachtofferschap (Cho, et al., 2010). De studie van Cho et al. (2010) bevestigde opnieuw het fenomeen van de 'optimistic bias' nu ten opzichte van online privacy risico's. Het liet zien dat individuen de kans voor zichzelf significant minder inschatten dan anderen met betrekking tot het ervaren van online privacy risico's. Dit toont aan dat ook online de 'optimistic bias' aanwezig is.

Risicobewust handelen, offline of online, kan ook gedefinieerd worden als veilig gedrag. In het geval van onlinegedrag, wordt dit in de literatuur ook wel cyber hygiënisch gedrag genoemd (van 't Hoff-de Goede, et al., 2019). Als iemand zich risicobewust gedraagt, risicobewust handelt, houdt dit in dat hij of zij bewust bezig is met de risico's die hij of zij loopt en daar naar handelt. Wanneer gekeken wordt naar WhatsApp fraude, is er op basis van literatuur en expertise instanties (Politie Nederland, 2021: Fraudehelpdesk, 2021: Fraudehelpdesk, 2020: Kamp, 2020: NU.nl 2021) een lijst vast te stellen van gedragingen, ofwel gedragsintenties, die als risicobewust handelen kunnen worden bestempeld. In tabel 1 is een overzicht van de gedragingen weergegeven met daarachter een toelichting daarvan. Het gaat bij deze gedragingen of gedragsintenties dus om risicobewust handelen bij (mogelijke) WhatsApp fraude.

*Tabel 1 Overzicht risicobewuste handelingen bij (mogelijke) WhatsApp fraude*

| Risicobewuste handeling WhatsApp fraude | Toelichting |
|---|---|
| **Profielfoto controleren** | Is er een profielfoto aanwezig, en klopt deze foto? |
| **Telefoonnummer controleren** | Staat het nummer in de contactenlijst. Maar ook: wanneer het nummer wordt ingetoetst op Google, wordt dit nummer dan aan verdachte zaken gelinkt? |
| **Niet op linkjes klikken** | Denk hierbij aan bijvoorbeeld tikkie verzoek linkjes |
| **Verifiëren** | Bel het jou bekende nummer van de persoon die je (schijbaar) contact via een onbekend nummer. Wanneer de persoon niet bereikbaar is, laat dan een bericht achter en maak geen geld over tot je die persoon gesproken hebt |
| **Bewijsmateriaal verzamelen** | Noteer het nummer, maak screenshots van het gesprek en noteer eventueel het rekeningnummer waar geld naar overgemaakt moet worden. Dit kan gebruikt worden bij het doen van aangifte |
| **Nummer rapporteren aan WhatsApp** | In WhatsApp kan een nummer gerapporteerd worden. Dit nummer wordt dan doorgestuurd naar WhatsApp als zijnde ongewenste praktijken en zal voor jou niet meer zichtbaar zijn in WhatsApp |
| **Aangifte politie en/of fraude helpdesk** | Maak melding bij de politie of de fraude helpdesk, deze instanties bundelen de meldingen omtrent deze praktijken. Indien ook daadwerkelijk slachtoffer geworden, doe dan aangifte. |

## 2.4 PMT (Protection motivation theory)

De protection motivation theory (PMT) is oorspronkelijk opgesteld in 1975 door Rogers, maar heeft sinds dien een aantal revisies ondergaan (Floyd, Prentice-Dunn & Rogers, 2000: Milne, Orbell & Sheeran, 2002). PMT is een sociaal cognitieve theorie die gedrag probeert te voorspellen en richt zich op de motivatie die men heeft om zichzelf te beschermen. Het concept 'protection motivation' kan gezien worden als het hebben van een intentie (Floyd, et al., 2000) die van invloed is op het daadwerkelijke gedrag (van 't Hoff-de Goede, et al., 2019). De theorie bestaat uit een breed spectrum van factoren, die samen voorspellen en verklaren in welke mate mensen gemotiveerd zijn om voorzorgsmaatregelen te nemen, risicobewust te handelen, en preventief gedrag te vertonen (Floyd, et al., 2000: van 't Hoff-de Goede, et al., 2019). Het PMT stelt dat mensen gemotiveerd raken om zichzelf te beschermen tegen een dreiging na een evaluatie van de dreiging en het nemen van maatregelen tegen deze dreiging.

Bij de dreiging-evaluatie gaat het om twee onderdelen:

- *De gepercipieerde kwetsbaarheid:* hiermee wordt bedoeld de inschatting van eigen kwetsbaarheid voor de dreiging
- *De gepercipieerde impact:* hiermee wordt bedoeld de inschatting van de ernst van de dreiging en de gevolgen daarvan.

Vervolgens doet iemand dan de maatregel-evaluatie, deze bestaat uit drie onderdelen:

- *Response effectiviteit:* een besluit, afweging, over de effectiviteit van de maatregel tegen de dreiging
- *Zelfeffectiviteit:* hiermee wordt bedoeld of de persoon zich instaat acht om effectief maatregelen te nemen
- *Responsekosten:* dit is de afweging of de te nemen moeite of te verwachten kosten het waard zijn de maatregel te nemen

Deze twee evaluaties beïnvloeden de motivatie van mensen om door te gaan met hun gedrag, of juist om af te zien van een gedraging (Floyd et al., 2000). Dat het PMT een nuttig theoretisch raamwerk is om het innerlijke proces van mensen te begrijpen wanneer zij moeten kiezen hoe zich, online, te gedragen, is gebleken door eerdere studies waarin PMT is toegepast op cybergedrag (Jansen, 2018: Sommerstad, Karlzén & Hallberg, 2015: van 't Hoff-de Goede, et al., 2019: Crossler & Bélanger, 2014).

Een ander onderdeel van PMT zijn de twee intra-persoonlijke factoren die samenhangen met (cyber)gedrag. Deze zijn persoonlijkheidskenmerken, die weer bestaat uit twee onderdelen, zelfcontrole en persoonlijkheidsdimensies, en eerdere ervaringen (Floyd, et al., 2000). Zelfcontrole wordt in meerdere onderzoeken als relevant bestempeld voor cybergedrag (van Wilsem, 2013, van de Weijer & Leukfeldt, 2017). Tevens kan op basis van literatuur een aantal persoonlijkheidskenmerken vastgesteld worden die risicofactoren zouden kunnen vormen voor onveilig (cyber)gedrag. Deze kenmerken worden ook wel de 'Big 5' genoemd: extraversie, emotionele stabiliteit, openheid voor nieuwe ervaringen, servicegerichtheid en zorgvuldigheid. Een onderzoek van Van de Weijer en Leukfeldt (2017) richtte zich op het onderzoeken van de samenhang van de 'Big 5'en slachtofferschap van online criminaliteit. Uit dit onderzoek kwam naar voren dat personen die een hoge score hadden op zorgvuldigheid en emotionele stabiliteit, een lager risico hebben om slachtoffer te worden van een cyberdelict. Dit risico is dan juist weer hoger voor personen die grote openheid voor nieuwe ervaringen hebben. Voornamelijk emotionele stabiliteit lijkt meer samenhang te hebben met online criminaliteit dan met andere criminaliteit. Dit houdt in dat personen die hoog scoren op dit persoonlijkheidskenmerk, minder vaak slachtoffer lijken te worden van online criminaliteit dan van traditionele criminaliteit (van de Weijer & Leukfeldt, 2017). Het andere onderdeel van de intra-persoonlijke factoren van PMT, zijn de eerdere ervaringen van mensen, bijvoorbeeld eerder slachtofferschap van online criminaliteit. Deze eerdere ervaringen zouden een belangrijke voorspeller voor toekomstig gedrag kunnen zijn (Van 't Hoff-de Goede, et al., 2019). In PMT wordt gesteld dat wanneer mensen slachtoffer zijn geweest van een cyberaanval zij hun gedrag aanpassen en daarom zich (online) veiliger zouden gedragen dan mensen die (nog) geen slachtoffer zijn geworden (van 't Hoff- de Goede, 2019). Dit wordt echter niet door alles studies ondersteund. Zo vonden Cain, Edwards & Still (2018) geen verband tussen veilig cybergedrag (in de literatuur ook wel cyber hygiënisch gedrag genoemd) en eerdere aanvallen. Mogelijk lijden eerdere ervaringen zelfs tot minder veilig gedrag door slachtoffer ten opzichte van niet-slachtoffers. (Cain et al., 2018).

## 2.5 Huidige studie

Op basis van de literatuur kunnen een aantal verwachtingen gesteld worden voor deze studie. Deze studie is gefocust op het verklaren waarom ouderen wel of juist niet risicobewust handelen bij vermoedelijke WhatsApp fraude. De verwachting is dan ook dat dit verklaard kan worden aan de hand van de motivatie die zij hebben voor het vertonen van dit gedrag of het hebben van de intentie voor dit gedrag aan de hand van PMT. Aan de hand van het PMT zal zichtbaar worden wat de afwegingen zijn die ouderen maken omtrent een verdacht WhatsApp berichtje en daarom de gedragsintenties hebben die zij aangeven. Op basis van het theoretisch kader van de studie van Zhang, et al. (2019) zal de factor kennis, de herkenning van de zogenoemde 'red flags' worden

meegenomen. En van de Protection Motivation Theory (Floyd, et al., 2000) zal enkel de twee interne evaluatieprocessen die iemand door maakt die van invloed zijn op (intentie tot) gedrag worden meegenomen in dit onderzoek.

# 3. Methode

## 3.1 Onderzoeksmethode

Er is gekozen voor een kwalitatieve onderzoeksstrategie bedoeld om te kunnen evalueren wat de kennis van ouderen is over risicobewust handelen bij WhatsApp fraude, waarom ouderen wel of niet risicobewust handelen bij (mogelijke) WhatsApp fraude en welke eventuele invalshoeken dit geeft voor interventies. Een kwalitatieve methode kan helpen bij een beter begrip van de doelgroep omdat respondenten hun gedachtenproces kunnen vertellen en nieuwe informatie kunnen leveren (Verhoeven, 2014). De data is verzameld door middel van semigestructureerde interviews met ouderen van 55 jaar of ouder, waarbij gebruik gemaakt is van een topiclijst. Deze topiclijst is opgesteld in samenwerking met de onderzoekers van het project cyberweerbaarheid van de Haagse Hogeschool en Saxion Hogeschool. Er is gekozen voor een semigestructureerd interview om dat dit de mogelijkheid biedt om door te vragen op de antwoorden die de respondent geeft. Het zorgt ervoor dat het gesprek natuurlijk verloopt (Morling, Carr, Heger Boyle, Cornwell, Correll, Crosnoe, Waters & Freese. 2018). Tegelijkertijd geeft een semigestructureerd interview de mogelijkheid om aan de hand van vooraf geformuleerde vragen er zeker van te zijn dat alle specifieke elementen die van belang zijn voor het onderzoek bevraagd worden (Verhoeven, 2014).

## 3.2 Respondenten

Het werven van respondenten was een moeizaam proces. Een groot deel van potentiele respondenten van deze studie was (in verband met de coronapandemie) terughoudend in het doen van interviews offline. Daarbij had men vaak niet de mogelijkheid het interview online te doen (niet de kennis en/of middelen om gebruik te maken van online videobel media). Tevens zijn veel interviews gecanceld door de respondenten omdat ze op het moment van de geplande interviewdatum verschijnselen (o.a. verkouden) van corona vertoonden en binnen het geplande tijdsbestek het niet mogelijk was het interview op een later tijdstip of online te laten plaatsvinden. Hierdoor zijn er uiteindelijk in totaal slechts 15 gesprekken gevoerd met ouderen van 55 jaar of ouder. Deze respondenten zijn op verschillende manieren geworven. De enige eisen die gesteld zijn aan het deelnemen van het interview waren dat de respondenten 55 jaar of ouder moesten zijn en dat zij in ieder geval gebruik maakten van WhatsApp. Het merendeel van de respondenten (tien respondenten) hebben gereageerd op de vraag gericht aan 55+ers om mee te doen aan de interviews via een lokale buurt Facebookpagina (Facebook Buurtpagina Tuk). Dit bericht is weergegeven in bijlage I De overige 5 respondenten zijn geworven via het netwerk van de onderzoeker. Naar alle respondenten is een informatie brief (bijlage II) en een toestemmingsformulier (bijlage III) gestuurd. In tabel 2 is een overzicht van de eigenschappen van de respondenten weergegeven. Hierin is te zien dat er in totaal 8 mannen en 7 vrouwen hebben deelgenomen aan de interviews. Verder is de verdeling in de leeftijdscategorieën als volgt: 5 respondenten waren tussen de 55 en 65 jaar, 5 respondenten waren tussen de 65 en 75 jaar en 5 respondenten waren 75 jaar of ouder.

*Tabel 2 Eigenschappen respondenten*

| Eigenschap | | Aantal respondenten |
|---|---|---|
| Leeftijd | 55-65 jaar | 5 |
| | 65-75 jaar | 5 |
| | 75+ jaar | 5 |
| Geslacht | Man | 8 |
| | Vrouw | 7 |
| Manier van interviewen | Offline | 9 |
| | WhatsApp videobellen | 3 |
| | Zoom | 1 |
| | Teams | 2 |

## 3.3 Dataverzameling en verwerking

De interviews vonden plaats tussen 1 april en 30 april 2021. Interviews duurden een half uur tot maximaal een uur. De interviews hebben op verschillende manieren plaatsgevonden. Om ervoor te zorgen dat de respondent zoveel mogelijk op zijn of haar gemak zou zijn tijdens het interview, lag de keuze omtrent de manier van interviewen bij de respondent. De keuze hierin was in eerste instantie of de respondent graag het interview online wilde doen of offline bij de respondent thuis. Wanneer de respondent voor de online-mogelijkheid koos, is daarbij gevraagd via welk online kanaal voor de respondent de beste optie was. Uiteindelijk hebben 6 respondenten ervoor gekozen de interviews online te laten plaatsvinden, waarvan 3 via WhatsApp videobellen, 1 via het medium Zoom en 2 via Microsoft Teams. Met de overige 9 respondenten hebben de interviews offline bij de respondent thuis plaats gevonden. Bij de offline interviews zijn de coronamaatregelen die op dat moment golden in acht genomen. In april 2020 hield dit in: de interviewer ging op de dag van het interview bij geen enkel ander huishouden op bezoek dan die van de respondent, er werd minimaal 1.5 meter afstand gehouden en indien iemand symptomen van corona vertoonde is het interview uitgesteld. Alle interviews zijn opgenomen met toestemming van de respondent voorafgaand aan het interview. Daarnaast is er informatie gegeven over het doel van het onderzoek, de vrijheid van de respondent om te kunnen stoppen met het interview op elk moment, anonimiteit, de mogelijkheid om vragen te kunnen stellen en wat er met het interview wordt gedaan. Naast dat deze informatie is gegeven aan het begin van het interview, is er tevens van tevoren een informatiebrief (bijlage II) en een informed consent formulier (bijlage III) gestuurd naar de respondent waar dezelfde informatie in stond. De respondenten hebben het informed consentformulier ondertekend retour gestuurd. Om de anonimiteit van de respondent te waarborgen zijn namen en andere te traceren persoonsgegevens weggelaten in de transcripties van de interviews en niet verwerkt in het verslag. De transcripten zijn dus volledig geanonimiseerd. De namen van de respondenten zijn bekend bij de onderzoeker. In het verslag wordt verwezen naar de respondenten als *'Respondent [nummer]*'. Deze nummers zijn willekeurig gegeven aan de respondenten. Op deze manier zullen quotes niet kunnen worden herleid naar specifiek respondenten en blijft de anonimiteit gewaarborgd. De opnames van de interviews zijn na het maken van de transcripten vernietigd. Verder is alle data is opgeslagen in een speciale database van de Universiteit Utrecht om veiligheid van de data te garanderen.

*Topiclijst*

Omdat de interviews die werden afgenomen, ook gebruikt worden voor het project Cyberweerbaarheid is de topiclijst (bijlage IV) opgesteld in samenwerking met de onderzoekers van de Haagse Hogeschool en Saxion Hogeschool. De interviewvragen zijn geformuleerd met de intentie beter inzicht te krijgen van de kennis van de respondenten over het risico van WhatsApp fraude, wat de respondenten doen met mogelijke WhatsApp fraude berichten en hoe zij zich beschermen tegen WhatsApp fraude. Tevens is gevraagd naar welke hulpmiddelen respondenten eventueel nodig hebben om zich nog beter te beschermen tegen dit delict. De definitie van WhatsApp fraude is in het

interview gegeven nadat de respondent een rollenspel heeft gedaan en heeft verteld over wat zijn of haar kennis is over WhatsApp fraude. Dit om de antwoorden op die vragen niet te beïnvloeden en om vervolgens bij de andere vragen omtrent de definitie op één lijn te zitten met de respondent. In tabel 3 is te zien hoe de vragen uit de topiclijst relateren aan de onderzoeksvragen en welke concepten van het theoretisch kader daaraan gerelateerd zijn.

*Tabel 3 Onderzoeksvragen en bijbehorende topiclijst vragen en concepten*

| **Onderzoeksvragen** | **Corresponderende topiclijst vragen** | **Bij behorende concepten** |
|---|---|---|
| "Wat weten ouderen van risicobewust handelen bij WhatsApp fraude?" | Topic 2: vragen 1,2,3<br>Topic 3: alle vragen | Risicoperceptie<br>Risico bewustzijn<br>Risico bewust handelen |
| "Waarom hebben ouderen wel of geen intentie om risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten?" | Volledig topic 1<br><br>Topic 4 & 5 alle vragen | Gedragsintentie<br>PMT-model<br>Risicobewust handelen<br>Optimistic bias |
| "Welke invalshoeken geven deze inzichten op eventuele interventies die zich richten op het verminderen van slachtofferschap van ouderen bij WhatsApp fraude?" | Topic 5: Vraag 4<br>Topic 6: Vraag 1 & 2 | n.v.t |

Het rollenspel is opgenomen in de topiclijst om te proberen het gedachtenproces en afwegingen van de ouderen te achterhalen bij het ontvangen van verschillende 'verdachte' WhatsApp berichten. Hierin zijn 3 verschillende stappen in een WhatsApp bericht voorgelegd aan de respondent. De respondent is verteld dat hij of zij zich voor moeten stellen dat men een moeder of vader is van een uit huis wonend kind Mieke. In het rollenspel krijgt de respondent 3 verschillende momenten in een Whatsapp gesprek zien. Bij elke situatie wordt de respondent gevraagd wat de eerste gedachte is bij het WhatsApp bericht en waarom, en wat de respondent voor actie(s) zou ondernemen bij dit bericht en waarom. De 3$^{e}$ situatie is weergegeven in figuur 1, de overige situaties zijn te vinden in bijlage IV


*Figuur 1 WhatsApp rollenspel situatie 3*

Onderzoeker Luuk Bekkers heeft deelgenomen aan het eerste interview en heeft de transcripten van de eerste twee interviews gelezen om hiermee te evalueren of de topiclist, zowel de vragen zelf als de volgorde, van goede kwaliteit waren. Hierna zijn een aantal vragen anders verwoord, omdat bleek dat hier meer verduidelijking nodig was. Verder is het WhatsApp rollenspel naar voren verplaatst in het interview. In eerste instantie werd dit aan het einde van het interview geplaatst, echter kon hier mogelijk mee gezegd worden dat door eerdere vragen die al gesteld zijn, de respondent mogelijk sneller het verwachte gewenste gedrag vertoond in het rollenspel.

### 3.4 Betrouwbaarheid en validiteit

Om de betrouwbaarheid van het onderzoek te waarborgen is er gebruik gemaakt van een topiclijst. Wanneer er gebruik wordt gemaakt van een topiclist, waarbij van tevoren topics en bijbehorende vragen zijn geformuleerd, kunnen interviews beter met elkaar worden vergeleken (Verhoeven, 2014). De interne validiteit is zoveel mogelijk gewaarborgd door de respondenten continu om toelichting te vragen bij hun antwoorden en hierbij concrete voorbeelden te geven, de topiclijst tussentijds te evalueren en, door middel van terugkoppelingen van de onderzoeker, te controleren of de onderzoeker de respondent goed begrepen heeft (Verhoeven, 2014). De objectiviteit van de onderzoeker werd ook zoveel mogelijk ingedekt: er zijn geen sturende vragen gesteld en de vragen zijn zo open als mogelijk gesteld (Morling, et al., 2018). Ook over de volgorde van de vragen is nagedacht. Het rollenspel is direct aan het begin geplaatst om een nog niet beïnvloed antwoord te krijgen van de respondent. Dit omdat de kans bestaat dat als het rollenspel pas na de vragen plaatsvindt, de respondent de factoren die in de vragen besproken worden, benoemd terwijl dit mogelijk niet zijn of haar gebruikelijke antwoord zou zijn.

### 3.5 Analyse

Door middel van het theoretisch kader en de topiclijst zijn de eerste codes geformuleerd, dit betrof kernbegrippen die worden onderzocht en bijdragen aan het beantwoorden van de onderzoeksvragen. Vervolgens zijn de transcripten aandachtig doorgenomen waarna relevante fragmenten zijn gekoppeld aan de geformuleerde codes. Indien er andere relevante fragmenten waren die van belang waren voor het onderzoek, zijn er middels open coderen nieuwe codes geformuleerd, die hieraan zijn gekoppeld. Vervolgens is het proces van axiaal coderen gestart, hierbij zijn codes met elkaar vergeleken. Codes die veel overlap hadden zijn samengevoegd, overbodige codes zijn verwijderd en sommige codes zijn hernoemd. De laatste fase was het selectief coderen, hierbij is gekeken hoe vaak bepaalde codes waren genoemd, de relevantie van de codes zijn heroverwogen en de samenhang tussen codes is bekeken. Uiteindelijk zijn er 45 hoofd- en subcodes gebruikt, deze zijn te vinden in de codeboom in bijlage V. Het coderen is gebeurd in ATLAS.ti. Ook het analyseren van de transcripten is gedaan aan de hand van het programma ATLAS.ti. Dit is een software die gericht is op de analyse van kwalitatieve onderzoeksgegevens. De interviews zijn geanalyseerd door de codes die van belang zijn voor het beantwoorden van de onderzoeksvragen geselecteerd en gezamenlijk geanalyseerd. Door deze codes over te zetten in een Excel bestand die onder andere weergeeft hoe vaak een bepaalde code is benoemd en in hoeveel interviews, is het mogelijk patronen en verbanden te destilleren.

## 4. Resultaten

In dit hoofdstuk zullen de belangrijkste bevindingen uit de interviews worden besproken. Dit gebeurt aan de hand van de onderzoeksvragen die vervolgens in thema's zijn opgesplitst.

### 4.1 Resultaten onderzoeksvraag 1

Bij onderzoeksvraag 1 staat de kennis van ouderen over risicobewust handelen bij WhatsApp fraude centraal. Hiernaast gekeken naar wat de kennis is van ouderen over WhatsApp fraude in het

algemeen en op welke manier de ouderen deze kennis verkrijgen. De resultaten op deze thema's worden hieronder besproken.

*Kennis WhatsApp fraude*
Het merendeel van de respondenten, dertien van de vijftien, geven aan bekend te zijn met WhatsApp fraude. Echter wanneer gevraagd wordt naar wat het inhoudt, worden er niet altijd correcte omschrijvingen gegeven: acht van de respondenten gaven een omschrijving die meer aansluit bij het cyberdelict 'phishing'.

*"Nouja, dat criminelen proberen te vissen naar jouw rekeningnummer en jouw geld afhandig proberen te maken. "* – Respondent 11

*"Ja ik denk misschien hetzelfde als bij mail, dat ze toch gegevens van je proberen los te pulken, daar zal het wel op neer komen."* – Respondent 9

Twee respondenten gaven aan niet bekend te zijn met WhatsApp fraude. Zij gaven aan dat het eigenlijk een voor hun onbekende variant van fraude is. Anders dan bijvoorbeeld phishing via de email of verkoopfraude, wat voor hen bekender is.

*"Nee eigenlijk niet. Ik realiseer me dat nu. Dat wat ik dan weet komt meestal via de mail en andere dingen."* – Respondent 9

*"Ik weet te weinig hoe dat allemaal precies werkt. Ik bedoel ik kan dr mee uit de voeten met internet en internetbankieren en WhatsApp, maar hoe het allemaal precies werkt weet ik niet. En dat roept wel bij mij onzekerheid op."* – Respondent 12

*(Basis) Kennis risicobewust handelen bij WhatsApp fraude*
Ondanks dat acht van de respondenten niet de juiste omschrijving van WhatsApp fraude gaven, hebben alle vijftien respondenten aangetoond kennis te hebben van risicobewust handelen in het algemeen en bij (vermoedelijke) WhatsApp fraude. Alle respondenten hebben ofwel in het rollenspel, ofwel bij de vragen, ofwel bij allebei, bewust of onbewust aangetoond zichtbaar kennis te hebben van risicobewust handelen. Dan wel omdat ze zelf duidelijk aangeven te weten dat de handelingen die zij aangeven te zullen doen ervoor zorgen dat zij geen slachtoffer worden, of omdat zij risicobewust handelen in het rollenspel. Termen die veel van de respondenten laten vallen zijn dat het gaat om 'nuchter' of 'logisch' nadenken om zo de juiste keuzes te maken.

*"Dat is gewoon logisch nadenken. Kijk als je een naam terugstuurt, dan, okal, ja, als je een naam terugstuurt dan maak je bekend dat je een klein kind of vriend hebt met die naam en dat moet je niet doen, dat geeft hun de macht. Het is niet dat ik dit door mijn omgeving of via bijvoorbeeld mijn tijdschriften heb geleerd, maar dat is gewoon logisch nadenken vanuit mijzelf. "* – Respondent 1

Ondanks dat alle respondenten hebben aangetoond kennis te beschikken over risicobewust handelen, tonen zeven respondenten ook aan soms geen kennis te hebben van risicobewust handelen. Dit valt vooral op bij het rollenspel.
Zes van de respondenten herkennen niet direct de 'red flags' die maken dat fraude vermoed kan worden. De reactie die ze dan ook gaven op de situaties waren geen risicobewuste handelingen, omdat ze er van uit gingen dat het bericht 'gewoon' van hun zoon of dochter kwam.

*"Ik ben thuis dus..ja.. niets geks aan. Dus ik denk dan dat het 1 van mijn kinderen moet zijn die mij dus een appjes stuurt.. Ja ik zou antwoorden van "ik ben thuis". En wil je komen."* – Respondent 13

Vanaf situatie 1 herkende twaalf van de respondenten de 'red flags' direct al. Vanaf situatie 2 waren dat twee respondenten en de laatste respondent herkende de 'red flags' pas bij situatie 3. Het merendeel van de respondenten, tien van de vijftien, toonde de intentie tot, en hiermee ook de kennis van, risicobewust handelen zodra de 'red flags' waren herkend. Vijf respondenten handelden, ondanks het herkennen van de 'red flags', niet direct risicobewust. Dit was zoals ze zelf aangaven uit nieuwsgierigheid wat er achterweg zou komen. In een later stadium (situatie 2 of 3) handelden zij wel risicobewust.

*"Ja ik ben ook een beetje nieuwsgierig aangelegd natuurlijk dus ik denk dat ik de vraag denk ik wel ga beantwoorden om verder informatie te krijgen, dus zou reageren met ja"* – Respondent 1

*Bron van kennis (risicobewust handelen) WhatsApp fraude*
De respondenten gaven meerdere opties aan als de bron waar zij de informatie over WhatsApp fraude vandaan hebben: eigen ervaring, ervaring van anderen, de krant, het nieuws, sociale media, actualiteitenprogramma's, de ouderenbond en de gids van de consumentenbond. Van deze opties is het vaakst, acht respondenten, aangegeven dat de informatie via een actualiteitenprogramma is vergaard. De programma's die daarbij waren genoemd zijn Radar (twee keer), Opsporing verzocht (één keer), Opgelicht (vier keer) en BAIT (één keer). Hierbij gaat het zowel om informatie over WhatsApp fraude in het algemeen, als informatie over risicobewust handelen bij WhatsApp fraude.

*"Ja, nouja, dit is altijd wel iets in televisieprogramma's zoals Opgelicht. Dat komt er wel heel vaak in, van, ga er vooral niet op in!"* – Respondent 3

## 4.2 Resultaten onderzoeksvraag 2

Bij onderzoeksvraag 2 staat centraal een verklaring te vinden waarom ouderen wel of niet de intentie hebben om risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten. In het theoretisch kader zijn factoren genoemd die hierbij van invloed op (kunnen) zijn en die het gedrag zouden kunnen verklaren. Aan de hand van deze factoren worden de resultaten besproken. Maar eerst wordt vastgesteld of de respondenten wel of niet risicobewust handelen.

*Wel of niet risicobewust handelen*
Dit is in de interviews op twee manieren bevraagd: aan de hand van een rollenspel met drie situaties en aan de hand van de vraag hoe zij zich beschermen tegen WhatsApp fraude wanneer zij een verdacht bericht zouden ontvangen. Vastgesteld is dat tien respondenten niet altijd risicobewust handelden, voornamelijk in het rollenspel. Zoals eerder aangegeven kwam dit mede door het niet direct herkennen van de 'red flags' ofwel omdat zij nieuwsgierig waren wat achter het bericht weg zou komen. Uiteindelijk hebben alle vijftien respondenten risicobewuste handelingen aangegeven in het interview. Van de handelingen die van tevoren in het theoretisch kader zijn vastgesteld als risicobewuste handelingen bij WhatsApp fraude, is "verifiëren" het meest genoemd (11 respondenten).

*"ja dan zou ik op hun oude nummer wat ik nog heb van klopt het dat je een nieuw telefoonnummer hebt weet je wel. Ik verifieer op hun oude nummer. Op het nummer wat bij mij bekend is laat ik het zo zeggen. Ik verifieer op het nummer wat mij bekend is."* – Respondent 12

De handelingen die het minst zijn genoemd zijn handelingen die met elkaar in verbinding staan: bewijsmateriaal verzamelen (1 respondent) en aangifte doen bij de politie (4 respondenten). De overige respondenten noemden soms deze opties wel, maar gaven aan dat zij het nut niet inzagen, omdat ze verwachten niet serieus te worden genomen of omdat het geen effect zal hebben. De respondenten zelf kwamen ook met andere handelingen. Zie tabel 4 voor een overzicht van alle type risicobewuste handelingen, die bestempeld kunnen worden als risicobewust handelen, ondanks dat

dit niet van tevoren is vastgesteld in het theoretisch kader. Deze extra (eventueel nieuwe) handelingen worden ook bestempeld als risicobewust handelen omdat het gaat om acties die er direct of indirect voor kunnen zorgen dat de respondent geen slachtoffer wordt van WhatsApp fraude. De handelingen die het meest zijn genoemd zijn: Negeren (9 respondenten) en controleren taalgebruik (9 respondenten). Met de laatste handeling wordt naast controleren op spelling en grammatica met betrekking tot de Nederlandse taal, ook bedoeld dat men kijkt naar of het 'buiten karakter' is: Past het taalgebruik, en op WhatsApp hiermee ook het gebruik van emoticons, bij hoe de communicatie gebruikelijk gaat met deze persoon.

*"Ja kijk het is maar net hoe je gewend bent om met je kinderen te praten. Dus ja dat zou ook wel opvallen ja. We zeggen nooit 'hey pap' eigenlijk altijd hoi, of heit. "* – Respondent 14

*Tabel 4* Lijst van handelingen respondenten (Codes)

| **Codes** | **Interviews** | **Aantal referenties** |
|---|---|---|
| **Risicobewust handelen** | 15 | 15 |
| Wel risicobewust handelen | 15 | 83 |
| *Telefoonnummer controleren* | 9 | 14 |
| *Profielfoto controleren* | 2 | 2 |
| *Niet klikken op link* | 1 | 1 |
| *Niet geld overmaken* | 5 | 8 |
| *Verifiëren* | 11 | 38 |
| *Bewijsmateriaal verzamelen* | 1 | 1 |
| *Nummer rapporteren* | 2 | 3 |
| *Aangifte politie* | 4 | 5 |
| *Aangifte fraudehelpdesk* | 2 | 2 |
| *Geen informatie geven** | 1 | 1 |
| *Controleren taalgebruik (spelling/grammatica, maar ook past deze manier van communiceren)** | 9 | 13 |
| *Negeren** | 9 | 19 |
| *Advies naasten vragen** | 6 | 11 |
| *Advies instantie vragen** | 4 | 6 |
| *Nummer blokkeren** | 4 | 8 |
| *Gesprek verwijderen** | 5 | 8 |
| Niet risicobewust handelen | 10 | 17 |
| *Ziet 'red flags' niet* | 3 | 5 |
| *Ziet 'red flags' handelt niet naar* | 6 | 7 |

*Noot.* De kolom interviews omschrijft het aantal personen dat een code genoemd heeft. Aantal referenties beschrijft hoe vaak een fragment is geplaatst onder deze code.
**Niet vooropgestelde code, opgesteld aan de hand van fragment in de interviews*

*Gepercipieerde kwetsbaarheid (dreiging-evaluatie PMT)*
Twaalf van de vijftien geïnterviewde ouderen zien WhatsApp fraude niet direct als een risico voor zichzelf. Volgens de respondenten is de belangrijkste reden hiervoor is dat ze kennis van en ervaring met (WhatsApp) fraude hebben. Dat maakt dat ze ervan overtuigd zijn dat ze er niet zomaar intrappen. De respondenten die het wel als een risico voor zichzelf zagen, gaven aan dat het risico niet per definitie groot was, maar dat het iets is waar je altijd rekening mee moet houden.
Wel zijn negen van de respondenten van mening dat het risico dat zij lopen lager is dan het risico van leeftijdsgenoten, want, zo wordt gesteld, over het algemeen is de kennis van ouderen omtrent de technologie en dit soort fraudezaken mogelijk wat minder of hebben hier geen ervaring mee. Dat ze

volgens de respondenten kwetsbaarder maakt dan henzelf voor WhatsApp fraude. Opvallend is dat de respondenten waarvan werd aangegeven dat deze de 'red flags' wel herkenden, maar hierna niet handelden, ook onder de respondenten vielen die hun eigen risico voor WhatsApp fraude lager inschatte ten opzichte van leeftijdsgenoten.

*"Ja..nou..Ik denk dat dat te maken heeft met bepaalde levenservaring, hoe je er in staat, hoe scherp of je bent, ja. Allemaal factoren. En hoeveel ervaring heb je al. Kijk als je helemaal 0 ervaring hebt dan en ben je eerder misschien, eerder, in de situatie dat je zegt van, nou ja ik kan dat wel doen. En dan heb je een ervaring en dat maakt je scherper weet je wel."* – Respondent 15

*Gepercipieerde impact (dreiging-evaluatie PMT)*
De meeste respondenten achten de financiële impact die slachtofferschap van WhatsApp fraude met zich brengt, niet als een zware impact. Volgens hen gaat het vaak over bedragen tussen de honderd en duizend euro wat volgens hen vervelend is, maar niet het einde van de wereld. Wel geven de respondenten aan dat de vraag naar geld en de hoogte van het geldbedrag hen direct wantrouwend maakt. Wat volgens hen een grotere impact zal hebben wanneer zij slachtoffer zouden worden van WhatsApp fraude, is de emotionele impact. De meeste respondenten vinden dat voornamelijk de emotionele impact veel zwaarder meeweegt dan de financiële impact. Daar kom je lastiger overheen. Onder de emotionele impact scharen de respondenten het schaamtegevoel dat je er ingetrapt bent, de boosheid en een soort van machteloosheidsgevoel wat het teweeg brengt.

*"Je mist wat geld, maar op mijn oude dag doet dat mij geen pijn meer hoor haha. Meer dat je gewoon je stom voelt dat je er ingetrapt bent"* – Respondent 13

*Zelfeffectiviteit (Maatregel-evaluatie PMT)*
Van de vijftien respondenten, zijn twaalf respondenten ervan overtuigd dat zij in staat zijn zichzelf te beschermen tegen WhatsApp fraude. De overige drie respondenten geven aan dat ze de kennis niet hebben om zelfverzekerd te zeggen: dit kan ik of dat ze hier onzeker over zijn dus niet goed weten of ze instaat zullen zijn zichzelf te beschermen. De respondenten die hier wel van overtuigd zijn geven als voornaamste reden dat ze bekend zijn met (WhatsApp) fraude, wat maakt dat ze weten hoe ze moeten handelen in zulke situaties en daarmee zichzelf kunnen beschermen.

*Response effectiviteit (Maatregel-evaluatie PMT)*
De maatregelen die respondenten nemen, de risicobewuste handelingen, zijn benoemd in tabel 4. Alle respondenten vinden de maatregelen die zij ondernemen een effectieve maatregel om te voorkomen dat zij slachtoffer worden van zowel WhatsApp fraude, als fraude in het algemeen. De respondenten geven als voornaamste reden waarom ze deze maatregelen als effectief achten, het feit dat ze nog nooit slachtoffer zijn geworden van (WhatsApp) fraude. De respondenten geven tevens aan dat de effectiviteit van de maatregel voor hen de belangrijkste reden is om de maatregel uit te voeren.

*Responsekosten (Maatregel-evaluatie PMT)*
Volgens de respondenten zijn de kosten en moeite die zij voor de maatregelen moeten maken, dan wel in geld, dan wel in tijd of andere zaken, minimaal en is het "een kleine moeite" de maatregelen in kwestie uit te voeren.
Alle vijftien respondenten geven aan dat de kosten die gemaakt moeten worden om de maatregelen in kwestie uit te voeren, voor hen van geen enkele invloed zijn voor op het wel of niet doen. Desondanks gaven twee respondenten bij drie type maatregelen (risicobewuste handelingen) wel beperkingen aan in de kosten waardoor zij mogelijk af zouden zien van die maatregelen. Een respondent gaf aan dat met name het doen van aangifte bij de politie veel tijd en moeite kost door de hoeveelheid papierwerk wat je dan moet invullen. Dit maakt dat deze respondent in het vervolg

niet zo snel aangifte zou doen bij de politie, hooguit een melding ervan maken en dan al het papierwerk achterwege laten. Een andere respondent gaf aan haar kinderen niet te willen lastigvallen met dit soort zaken omdat zij vaak ook druk zijn met hun werk en niet altijd de tijd hebben een telefoontje van haar over dit soort zaken aan te nemen. Dit ging om de maatregel met betrekking tot verifiëren, het bellen van de persoon in kwestie op het voor de respondent bekende nummer om te bevestigen dat het wel of niet om die persoon gaat, en advies vragen aan naasten. Deze respondent gaf wel aan advies te willen vragen aan bijvoorbeeld haar kinderen, maar door het mogelijk storen van haar kind zou zij wellicht hiervan afzien en dan de politie of de bank om advies zou vragen.

# 5. Conclusie & Discussie

In dit hoofdstuk worden de onderzoeksvragen beantwoord en de resultaten geïnterpreteerd en bediscussieerd. De sterke punten en tekortkomingen van dit onderzoek worden benoemd en suggesties voor vervolgonderzoek zullen worden gedaan.

De eerste onderzoeksvraag luidt: *"Wat weten ouderen van risicobewust handelen bij WhatsApp fraude?"* Hierbij wordt de algemene kennis over het delict in acht genomen, om daarna ook te bezien wat de kennis is over risicobewust handelen bij een dergelijk delict.
Er kan geconcludeerd worden dat over het cyberdelict WhatsApp fraude de kennis onder ouderen zeker wel aanwezig is, echter vaak niet volledig. Wat betreft de kennis over het delict wordt herhaaldelijk verward met andere cyberdelicten, zoals phishing. Wat betreft kennis over risicobewust handelen in het algemeen en bij (mogelijke) WhatsApp fraude in het bijzonder zijn er wisselende bevindingen. Er kan geconcludeerd worden dat de kennis aanwezig is. De handelingen die vanuit het theoretisch kader zijn opgesteld zijn in ieder geval allemaal een keer teruggekomen in de interviews. Daarbij kwamen de respondenten tevens zelf nog met enige andere handelingen die ook bestempeld kunnen worden als risicobewust handelen. Toch wordt de kennis niet altijd direct toegepast: de 'red flags' worden niet altijd direct herkend waardoor toepassing van de kennis vaak niet volgt. Dit is passend bij wat het onderzoek van Zhang, et al. (2019) aangeeft over de invloed van herkenning van 'red flags' op gedrag.

De tweede onderzoeksvraag luidt: *"Waarom hebben ouderen wel of geen intentie om risicobewust te handelen bij het ontvangen van vermoedelijk WhatsApp fraude berichten?"* Uit de interviews blijkt dat het hebben van kennis wel degelijk een belangrijke factor is als het gaat om risicobewust handelen daarbij. Zoals Zhang, et al. (2019) stellen: kennis maakt dat 'red flags' worden herkend waardoor het gedrag daarop kan worden aangepast. Deze theorie wordt door de interviews bevestigd. Wanneer de respondenten de 'red flags' niet herkenden, werd er ook niet risicobewust gehandeld.
Een andere conclusie die kan worden getrokken is dat respondenten, misschien niet zo zwart-wit als gesteld in de protection motivation theory (Floyd, et al., 2000), inderdaad de twee type evaluaties doorlopen voor ze daadwerkelijk handelen of de intentie tot handelen tonen. De dreigings-evaluatie doorlopen ze vooral in het stukje vorming van argwaan wanneer er om geld wordt gevraagd. Als het tevens gaat om vrij hoge bedragen gaat, gaat er een alarmbel rinkelen, omdat ze mogelijk geld kunnen verliezen (gepercipieerde impact). Echter de gepercipieerde kwetsbaarheid daarbij lijkt weinig van invloed om wel of niet risicobewust te handelen. Daarbij is geen verschil in reactie te zien tussen respondenten die WhatsApp fraude niet als risico zagen voor zichzelf ten opzichte van de respondenten die het wel als een risico voor zichzelf zagen. Dit is anders dan verwacht zou worden op basis van de Protection Motivation Theory, (Floyd, et al., 2000) waarin verwacht zou worden dat wanneer men het risico hoog voor zichzelf in schatten, sneller risicobewust handelen en andersom. De maatregel-evaluatie wordt ook doorlopen waarbij voor de meeste respondenten vooral de response effectiviteit van belang is om een maatregel te nemen. De response kosten zijn van

beperkte invloed op het handelen. Slechts een enkeling onderneemt een bepaalde handeling niet omdat de response kosten worden gezien als een drempel voor de respondent.

Een sterk punt van dit onderzoek is dat aan het begin van het interview gebruik is gemaakt van het rollenspel. De interviews laten een duidelijk verschil zien tussen de reacties van de respondenten op het rollenspel ten opzichte van de antwoorden op de vraag over wat de respondenten doen om zichzelf te beschermen tegen WhatsApp fraude. In het rollenspel gaan de respondenten veel meer in op de acties die zij zouden ondernemen per situatie terwijl wanneer ze gevraagd wordt welke maatregelen ze zouden nemen, komen de respondenten op veel minder maatregelen en vergeten de maatregelen die ze zelf hebben gebruikt in het rollenspel. Op deze manier heb je op verschillende wijze de respondent bevraagd naar het risicobewust handelen en zo meer inzicht gekregen in wat de respondent nu precies doet in bepaalde situaties.

Kijkend naar de resultaten moet men in acht nemen dat, uitgaande van onder andere de protection motivation theory, niet alle aspecten (de intra-persoonlijke factoren) zijn meegenomen in dit onderzoek. Dit houdt in dat er mogelijk nog andere verklaringen zijn voor het gedrag dat de ouderen in dit onderzoek hebben getoond. Zeker als er gekeken wordt naar de resultaten, is te zien dat sommige intra-persoonlijke factoren mogelijk aanwezig zijn (zelfcontrole, eerdere ervaringen, kenmerken van de ‘big 5’). Door de kwalitatieve aard van dit onderzoek kan niet op statistische basis gezegd worden of dit van invloed is op het gedrag. Voor verder onderzoek zou het dan ook goed zijn om de intra-persoonlijke factoren die nu niet meegenomen zijn, wel mee te nemen. Dit zou kunnen aan de hand van zowel een kwalitatieve als een kwantitatieve studie. Het kwantitatieve om zo duidelijkheid te verschaffen over de kenmerken en de invloed daarvan op gedrag, zoals onder andere is gedaan in het onderzoek naar online veilig gedrag van van der Hoff-de Goede, et al. (2019). En het kwalitatieve om diepgang te geven aan deze resultaten en daardoor het gedachtenproces hierachter beter te begrijpen. Tevens moet bij de interpretatie van de resultaten, rekening worden gehouden met het feit dat het een onderzoek is op een kleine schaal (15 respondenten) wat betekent dat de patronen en verklaringen die in dit onderzoek zijn ontdekt, mogelijk slechts op kleine schaal zichtbaar zijn. Voor verder onderzoek is het dan ook van belang een onderzoek op grotere schaal te ondernemen om zo duidelijk te krijgen of de verklaringen en patronen die nu zijn gevonden, dan nog steeds zichtbaar zijn.

# 6. Beleidsadvies

Een andere vraag die in dit onderzoek centraal stond was de beleidsvraag: "*Welke invalshoeken geven deze inzichten op eventuele interventies die zich richten op het verminderen van slachtofferschap van ouderen bij WhatsApp fraude?"* Aan de hand van de kennis die is opgedaan met de conclusies uit de eerste twee onderzoeksvragen, wordt op deze vraag in dit hoofdstuk antwoord gegeven.
De inzichten van het onderzoek geven de volgende aanbevelingen over de invalshoeken op eventuele interventies: kennis verbreding, 'on the spot' interventies en 'rollenspel' interventies.

*Kennis verbreding*
De interviews met de ouderen, maar ook gesprekken met experts[1] laten zien dat (sommige) ouderen toch een kennisachterstand hebben op het gebied van WhatsApp fraude. Er is sprake van te weinig herkenning van 'red flags', en te weinig risicobewust handelen bij dit type fraude. Als je kijkt naar het rapport van Emm (2010), wordt ook gesteld dat de maatschappij een soort 'common sense' mist in de online wereld die wij wel hebben in de 'echte' wereld. Om die common sense te creëren is volgens Emm veel onderwijzing nodig. De eerste aanbeveling is dan ook om met de interventies te focussen op het faciliteren van kennisverbreding op dit gebied voor ouderen om hen weerbaarder te maken tegen dit type cyberdelict. Dit wordt ondersteund door Zhang, et al. (2019) die aangeven dat kennis voor ouderen van belang is om 'red flags' te kunnen herkennen en zo niet slachtoffer te worden. Dit wordt ook ondersteund door het onderzoek van Alsharnouby, Alaca en Chiasson (2015) die aantoont dat bij phishing kennis een belangrijke factor is van slachtofferschap. Ali (2019) stelt dan ook dat het creëren van awareness belangrijk is voor het tegenhouden van slachtofferschap van phishing. Dit zou dus mogelijk ook effectief kunnen zijn voor WhatsApp fraude.
Er zijn een aantal richtingen waaraan gedacht kan worden in de trant van interventies om deze kennisverbreding te faciliteren. Zo kan er gedacht worden aan het publiekelijk toegankelijk maken van een soort stappenplan: "Hoe herken je WhatsApp fraude?" en vooral ook: "Wat doe je er mee?" Van belang hierbij is dat een dergelijk stappenplan breed uitgerold wordt over verschillende kanalen omdat, onder andere uit dit onderzoek, blijkt dat ouderen op gevarieerde manieren hun kennis vergaren. Voor het opstellen van zo'n stappenplan kan er gekeken worden naar het stappenplan dat al is gemaakt door IT4senioren (zie bijlage VI) samen met de tips die zijn geformuleerd door de Fraudehelpdesk (2020).

Meerdere studies (Schilder, Brusselaers & Bogaerts, 2015: Valcke, Schellens & van Keer, 2007) laten echter zien dat verbreden van de kennis niet per se leidt tot veilig (online) gedrag en risicobewust handelen (op de lange termijn). Daarom moet men ook kijken naar 'op het moment' interventies die puur focussen op het voorkomen dat men slachtoffer wordt als het bijna staat te gebeuren.

*'On the spot' interventies*
Omdat in de interviews naar voren is gekomen dat ouderen niet altijd de 'red flags' bij WhatsApp fraude herkennen, is de tweede aanbeveling om middels de invalshoeken van interventies te focussen op het moment dat iemand bijna slachtoffer wordt. Onderzoek van Petelka, Zou en Schaub (2019) toont aan dat waarschuwen voor phishing een effectieve manier is om men niet op phishing links te laten klikken. Hierin was vooral het geforceerd waarschuwen (een waarschuwing die hoe dan ook in beeld kwam) het meest effectief bleek. Participanten die de geforceerde waarschuwing kregen hadden was het significant waarschijnlijker dat zij niet op de link zouden drukken ten opzichte van de groep die deze waarschuwing niet kreeg (Petelka, et al., 2019).
Een bedrijf dat al met dit type interventies werkt is Marktplaats (z.d.). Marktplaats geeft een melding wanneer een gebruiker in contact staat met een andere gebruiker die wordt verdacht van of waarvan

[1] Zoals naar voren is gekomen tijdens expert bijeenkomst (donderdag 1 april 2021, georganiseerd door het consortium van het project cyberweerbaarheid)

het bewezen is dat hij of zij fraude pleegt (op welke manier dan ook). Op deze manier wordt de gebruiker gewaarschuwd dat het mogelijk verstandig is niet met hem of haar in zee te gaan. Deze interventie is tevens door een respondent in de interviews genoemd als iets wat haar heeft behoed van zaken doen met iemand die door marktplaats verdacht werd van fraude. Dit zou iets kunnen zijn om te implementeren bij zowel banken als WhatsApp (indien technisch mogelijk). Wanneer een bankrekening of telefoonnummer gerapporteerd staat als dat het gelinkt wordt met (mogelijk) fraude, krijgt de persoon die geld wil over maken naar dit rekeningnummer dan een bericht c.q. krijgt bij zo'n telefoonnummer een melding met daarin aangegeven dat dit nummer gerelateerd is aan (mogelijke) fraude. Op deze manier waarschuw je ouderen 'on the spot' voor dat ze op het punt staan om slachtoffer te worden van (WhatsApp) fraude.
Er is nog wel een belangrijke factor waar rekening mee moet worden gehouden. In de interviews met de ouderen is duidelijk naar voren gekomen dat ze niet snel melding zouden maken bij de politie, omdat zij het gevoel hebben dat dit toch niet serieus wordt genomen of omdat er toch niets mee wordt gedaan. Om dit type interventies te kunnen laten werken is dus wel de stap van de ouderen nodig om dit te melden bij de politie of WhatsApp (rapporteren). Ook is een goede samenwerking tussen de politie en WhatsApp en de politie en de banken hierin van belang.

*'Rollenspel' interventies*
De laatste aanbeveling voor een invalshoek voor interventies is om deze interventies te focussen op ervaring. Dus de ouderen laten ervaren aan de hand van een soort rollenspel wat WhatsApp fraude nu eigenlijk inhoudt en hen zelf actie daarin laten ondernemen en daar feedback op te geven. Het onderzoek van Ali (2019), gefocust op phishing, laat zien dat als men bewust traint met situaties van phishing, dit ten goede komt met betrekking tot de kennis over het delict en de kans op slachtofferschap van het delict. Dit onderzoek laat dezelfde resultaten zien als een eerdere studie van Kumaraguru, Rhee, Acquisti, Cranor, Hong en Nunge (2007). Deze hebben een trainingsinterventie voor phishing e-mails getest en de resultaten laten zien dat er een significant verschil was tussen de groepen voor (en zonder) de training ten opzichte van de groepen met training in het herkennen van phishing e-mails. Dit laat tevens het belang van de theorie gesteld door Zhang, et al. (2019) dat de herkenning van de 'red flags' van belang is voor de kans slachtofferschap. Dit type interventie zou kunnen door bijvoorbeeld een soort centrum te creëren waarbij je jouw (groot)ouders kunt opgeven om getest te worden of zij weerbaar zijn tegen WhatsApp fraude. Hierbij wordt er dus via WhatsApp met een onbekend nummer contact opgenomen met de opgegeven (groot)ouder door iemand van het centrum die zich voor doet als het (klein)kind. Dus op dezelfde manier als zou gebeuren bij daadwerkelijke WhatsApp fraude. Echter, in plaats van een echte link voor betaling, stuurt de link het "slachtoffer" door naar een website met informatie over WhatsApp fraude. Het centrum verteld achteraf natuurlijk aan de persoon die getest is, wat er nu gebeurd is en door wie hij of zij is opgegeven. Er wordt een soort feedback document gedeeld met de (groot)ouder omtrent hoe hij of zij heeft gehandeld en wat hij of zij eventueel in de toekomst anders of beter kan doen. Dit type interventie is in de interviews ook door een respondent benoemd als een mogelijkheid voor interventies omdat zij na het rollenspel in het interview het idee had er nog meer van te begrijpen. Dit duidt op een mogelijk draagvlak aan onder de ouderen voor dit type interventies. Tevens is er draagvlak voor dit type interventie bij beleidsmakers van de gemeente die belast zijn met cybersecurity[2]. Dit zijn de groep mensen die de interventies uiteindelijk zouden moeten implementeren.

[2] Zoals naar voren is gekomen tijdens expert bijeenkomst (donderdag 1 april 2021, georganiseerd door het consortium van het project cyberweerbaarheid)

# Literatuurlijst


Ali, G. A. (2019). Protecting Users from Phishing Email through Awareness and Training. *Indian Journal of Science and Technology*, *12*(25), 1–9. https://doi.org/10.17485/ijst/2019/v12i25/145743

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Burnes, D., Henderson, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis. *American Journal of Public Health*, *107*(8), 13–21. https://doi.org/10.2105/ajph.2017.303821a

Beerthuizen, M. G. C. J., Sipma, T., & van der Laan, A. M. (2020). *Aard en omvang van dader-en slachtofferschap van cyber-en gedigitaliseerde criminaliteit in Nederland.* WODC. https://repository.wodc.nl/handle/20.500.12832/253

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Caracach, C., Graycar, A., & Muscat, G. (2001). The victimization of older Australians. Canberra, Australia: Australian Institute of Criminology.

Centraal Bureau voor de Statistiek. (2019). *Slachtofferschap criminaliteit - Veiligheidsmonitor 2019*. CBS. https://longreads.cbs.nl/veiligheidsmonitor-2019/slachtofferschap-criminaliteit/

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Das, S., & Nayak, T. (2013). Impact Of Cyber Crime: Issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *5*(2), 142–153. https://www.ijeset.com/media/0002/2N12-IJESET0602134A-v6-iss2-142-153.pdf

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367. https://doi.org/10.1016/j.chb.2016.11.044

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537–549. https://research-repository.griffith.edu.au/bitstream/handle/10072/383426/Drew170061.pdf?sequence=1

Emm, D. (2010). *Patching Human Vulnerabilities*. Kaspersky Lab. http://www.techdata.ca/techsolutions/softwareconnections/files/aug2010/KASPERSKY%20LAB_PatchingHumanVulnerabilities.pdf

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Fraudehelpdesk. (2020, 21 oktober). *Een bekende die via WhatsApp om financiële hulp vraagt? Pas op!*https://www.fraudehelpdesk.nl/alert/een-bekende-die-via-whatsapp-om-financiele-hulp-vraagt-pas-op/

Fraudehelpdesk. (2021, 11 maart). *Een nummer rapporteren aan WhatsApp*. https://www.fraudehelpdesk.nl/fraude/een-nummer-rapporteren-aan-whatsapp/

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

Helweg-Larsen, M., & Shepperd, J. A. (2001). Do Moderators of the Optimistic Bias Affect Personal or Target Risk Estimates? A Review of the Literature. *Personality and Social Psychology Review*, *5*(1), 74–95. https://doi.org/10.1207/s15327957pspr0501_5

Holtfreter, K., Reisig, M. D., & Blomberg, T. G. (2006). Consumer fraud victimization in Florida: An empirical study. *ST. Thomas Law Review*, *18*(3), 761–789.

Holtfreter, K., Reisig, M. D., Mears, D. P., & Wolfe, S. E. (2014, maart). *Financial Exploitation of the Elderly in a Consumer Context*. U.S. Department of Justice. https://ncvc.dspacedirect.org/bitstream/handle/20.500.11990/1235/Financial%20Exploitation%20of%20the%20Elderly_IR_508.pdf?sequence=8&isAllowed=y

Jansen, J., Stol, W. P., & Open Universiteit (Heerlen ; 2010-. . ..). (2018). *Do You Bend Or Break?* Amsterdam University Press.

Kamp, R. (2020, 14 december). *WhatsApp-fraude herkennen en voorkomen*. Consumentenbond.nl. https://www.consumentenbond.nl/veilig-internetten/whatsapp-fraude

Kirchheimer, S. (2011). *Scams Trap Older Adults*. Aarp.org. https://www.aarp.org/money/scams-fraud/info-02-2011/scams-trap-older-adults.html

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *CHI*, *2007*. https://dl.acm.org/doi/pdf/10.1145/1240624.1240760?casa_token=9GePW2OCcisAAAAA:C-T7xXjt5dScAa7e-EpWOa0KI0OflLaT3ID2CHS-DcoTaU5e-F_edkmmX5sbmcDJ_VJD1es-nodyWg

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology and Marketing*, *18*(7), 763–783. https://doi.org/10.1002/mar.1029

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Li, T., & Fung, H. H. (2012). Age Differences in Trust: An Investigation Across 38 Countries. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *68*(3), 347–355. https://doi.org/10.1093/geronb/gbs072

Lichtenberg, P. A., Stickney, L., & Paulson, D. (2013). Is Psychological Vulnerability Related to the Experience of Fraud in Older Adults? *Clinical Gerontologist*, *36*(2), 132–146. https://doi.org/10.1080/07317115.2012.749323

Liem, M. C. A., Kuipers, S. L., & Sciarone, J. (2018). *Terroristische dreiging in Nederland De risicoperceptie en de mogelijkheden voor risicocommunicatie*. Universiteit Leiden. https://scholarlypublications.universiteitleiden.nl/access/item%3A3145905/view

Marktplaats. (z.d.). *Oplichting & Fraude*. Marktplaats.nl. Geraadpleegd op 7 juni 2021, van https://help.marktplaats.nl/s/article/meldpunt-internetoplichting

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, *7*(2), 163–184. https://doi.org/10.1348/135910702169420

Misana-ter Huurne, E., Spitshoven, R., Leukfeldt, R., van ’t Hoff-de Goede, S., van Houten, Y., Bekkers, L., & Walther, M. (2021). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime*. Hogeschool Saxion & Haagse Hogeschool. https://www.nwo.nl/projecten/raakpub06032-0

Misana-ter Huurne, E., van Houten, Y., Spitshoven, R., Notté, R., & Leukfeldt, R. (2020, februari). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers*. Saxion.

https://www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/saxion--haagse-hogeschool---cyberweerbaarheid.-risicobewustzijn-en-zelfbeschermend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers..pdf

Morling, B., Carr, D., Heger Boyle, E., Cornwell, B., Correll, S., Crosnoe, R., Waters, M. C., & Freese, J. (2018). *Research Methods*. Universiteit Utrecht.

NU.nl. (2020, 12 oktober). *Bijna vier keer zo vaak WhatsApp-fraude gemeld als in 2019*. https://myprivacy.dpgmedia.nl/consent/?siteKey=ucf98legs1caotgh&callbackUrl=https%3A%2F%2Fwww.nu.nl%2Fprivacy-gate%2Faccept%3FredirectUri%3Dhttps%253A%252F%252Fwww.nu.nl%252Ftech%252F6083304%252Fbijna-vier-keer-zo-vaak-whatsapp-fraude-gemeld-als-in-2019.html

NU.nl. (2021, 26 april). *800 euro lichter door WhatsApp-fraude: "Hij deed zich voor als mijn dochter"*. https://www.nu.nl/geldzaken/6129163/800-euro-lichter-door-whatsapp-fraude-hij-deed-zich-voor-als-mijn-dochter.html

Petelka, J., Zou, Y., & Schaub, F. (2019). Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. *CHI*, *2019*. https://dl.acm.org/doi/pdf/10.1145/3290605.3300748?casa_token=GiiN6Opv_tIAAAAA:dd4oWEF41oIgSiLc4jddWlG-nJuo9Ww35LD5PWm8UMky8nFBa6m40iWhMGUDtFy6Ve-peIwP-qG4r8w

Politie Nederland. (2021). *WhatsApp-fraude (vriend-in-noodfraude)*. politie.nl. https://www.politie.nl/themas/whatsapp-fraude-vriend-in-noodfraude.html

Roelofs, M., de Koning, N. M., van Vliet, A. J., Wijn, R., van Rijk, R., & Young, H. J. (2018). *De menselijke kant van cybersecurity: Conceptuele ontwikkelingen en de Cyber Security Assistent.* TNO.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Russo, S., Roccato, M., & Vieno, A. (2012). Criminal Victimization and Crime Risk Perception: A Multilevel Longitudinal Study. *Social Indicators Research*, *112*(3), 535–548. https://doi.org/10.1007/s11205-012-0050-8

Samanez-Larkin, G. R., Gibbs, S. E. B., Khanna, K., Nielsen, L., Carstensen, L. L., & Knutson, B. (2007). Anticipation of monetary gain but not loss in healthy older adults. *Nature Neuroscience*, *10*(6), 787–791. https://doi.org/10.1038/nn1894

Schilder, J. D., Brusselaers, M. B. J., & Bogaerts, S. (2015). The Effectiveness of an Intervention to Promote Awareness and Reduce Online Risk Behavior in Early Adolescence. *Journal of Youth and Adolescence*, *45*(2), 286–300. https://doi.org/10.1007/s10964-015-0401-2

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46. https://doi.org/10.4018/ijisp.2015010102

Stoeldraijer, L., van Duin, C., & Huisman, C. (2017, december). *Bevolkingsprognose 2017–2060*. Centraal Bureau voor de Statistiek. https://www.cbs.nl/nl-nl/maatwerk/2017/52/bevolkingsprognose-2017-2060

Valcke, M., Schellens, T., Van Keer, H., & Gerarts, M. (2007). Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in Human Behavior*, *23*(6), 2838–2850. https://doi.org/10.1016/j.chb.2006.05.008

van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Van der Meer, P., & Lenssinck, A. (2019, juni). *Cyber Crime*. CCV. https://hetccv.nl/fileadmin/user_upload/06_onderzoek_cybercrime.pdf

van ’t Hoff de Goede, S., & Leukfeldt, R. (2021). *15 procent Nederlanders maakt poging tot WhatsApp-fraude mee in 2020*. De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/over-de-haagse/de-haagse-actueel/nieuws/details/2021/02/08/15-procent-nederlanders-maakt-poging-tot-whatsapp-fraude-mee-in-2020

Van ’t Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., & Leukfeldt, E. R. (2019). *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. WODC, Centre of Expertise Cybersecurity (Haagse Hogeschool) & NSCR. https://repository.wodc.nl/handle/20.500.12832/2433

van Wilsem, J. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437–453. https://doi.org/10.1177/1043986213507402

van Wilsem, J. A. (2010). Digitale en traditionele bedreiging vergeleken. *Tijdschrift voor Criminologie*, *52*(1), 73–87. https://scholarlypublications.universiteitleiden.nl/access/item%3A2863798/view

Verhoeven, N. (2014). *Wat is onderzoek?* (5de editie). Boom Lemma.

Zhang, Q., Shao, J., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults’ vulnerability to fraud. *Journal of Elder Abuse & Neglect*, *31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

# Bijlage I: Facebook bericht Buurtpagina

# Bijlage II: Informatie brief

Beste ,

Hierbij wil ik u uitnodigen om deel te nemen aan een interview dat wordt uitgevoerd door een student van de Universiteit Utrecht, voor een onderzoek dat onder de verantwoordelijkheid van het Centre of Expertise Cyber Security (CoECS), onderdeel van de Haages Hogeschool, valt.

Het onderzoek waar ik uw medewerking voor wil vragen is getiteld “Cyberweerbaarheid”. In het interview zal een reeks aan onderwerpen aanbod komen waar vragen over gesteld worden omtrent uw kennis van de online wereld en gedrag(ingen) online. Het doel van het onderzoek is om uiteindelijk door middel van de inzichten, van onder andere deze interviews, interventies te ontwikkelen waardoor minder mensen slachtoffer worden van online criminaliteit (cybercriminaliteit). Het interview duurt ongeveer 45 minuten.

Omdat dit interview wordt uitgevoerd door een student van Universiteit Utrecht, heeft u de garantie dat:

1) Uw anonimiteit is gewaarborgd en dat uw antwoorden of gegevens onder geen enkele voorwaarde aan derden worden verstrekt, tenzij u hiervoor van tevoren uitdrukkelijke toestemming hebt verleend.

2) U zonder opgaaf van redenen kunt weigeren mee te doen aan het onderzoek of uw deelname voortijdig kunt afbreken. Ook kunt u achteraf uw toestemming intrekken voor het gebruik van uw antwoorden of gegevens voor het onderzoek.

3) Deelname aan het onderzoek geen noemenswaardige risico’s of ongemakken met zich meebrengt, geen moedwillige misleiding plaatsvindt, en u niet met expliciet aanstootgevend materiaal zult worden geconfronteerd.

Voor meer informatie over dit onderzoek en de uitnodiging tot deelname kunt u te allen tijde contact opnemen met de student, Sanne de Jong (huikjong@live.nl). Mochten er naar aanleiding van uw deelname aan dit onderzoek klachten of opmerkingen zijn, dan kunt u contact opnemen met dr. Susanne van ’t Hoff- de Goede (m.s.vanthoff-degoede@hhs.nl). Een vertrouwelijke behandeling van uw klacht of opmerking is daarbij gewaarborgd.

Ik hoop u hiermee voldoende te hebben geïnformeerd en dat u wilt deelnemen aan het onderzoek.

Met vriendelijke groet,

Sanne de Jong

# Bijlage III: Toestemmingsformulier

**Informed consent formulier – Onderzoek Cyberweerbaarheid**

Ik verklaar hierbij op voor mij duidelijke wijze te zijn ingelicht over de aard en methode van het onderzoek, zoals uiteengezet in de uitnodiging voor dit onderzoek.

Ik stem geheel vrijwillig in met deelname aan dit onderzoek. Ik behoud daarbij het recht deze instemming weer in te trekken zonder dat ik daarvoor een reden hoef op te geven. Ik besef dat ik op elk moment mag stoppen met het onderzoek.

Als mijn onderzoeksresultaten worden gebruikt in wetenschappelijke publicaties, of op een andere manier openbaar worden gemaakt, dan zal dit volledig geanonimiseerd gebeuren. Mijn persoonsgegevens worden niet door derden ingezien zonder mijn uitdrukkelijke toestemming.

Als ik meer informatie wil, nu of in de toekomst, dan kan ik me wenden tot Sanne de Jong, huikjong@live.nl. Voor eventuele klachten over dit onderzoek kan ik me wenden tot onderzoeker van het project Cyberweerbaarheid, dr. Susanne van ’t Hoff-de Goede, m.s.vanthoff-degoede@hhs.nl.

√ ik begrijp de bovenstaande tekst en ga akkoord met deelname aan het onderzoek

# Bijlage IV: Topiclist

*Allereerst hartelijk dank dat je wilt meewerken aan dit onderzoek.*

*Introduceer jezelf, vraag ook aan de respondent zich kort voor te stellen*

*Een steeds groter deel van ons leven speelt zich online af. Veel mensen brengen een aantal uren per dag door op internet. Sociale media, winkelen, het nieuws bekijken, e-mailen, informatie zoeken en ga zo maar door. Online kunnen we snel en veel informatie vinden en delen. Naast dat internet ons veel oplevert, kan het gebruik ervan ook risico's met zich meebrengen. Net zoals in de echte wereld, kun je ook op internet slachtoffer worden van diefstal, oplichting of fraude. Dit noemen we online criminaliteit.*

*Dit interview gaat over online criminaliteit en ik voer dit gesprek in het kader van mijn afstudeeronderzoek. Daarnaast is dit interview ook onderdeel van een groot project waar meerdere onderzoekers van Hogeschool Saxion en de Haagse Hogeschool aan werken. Dit grote project wordt uitgevoerd in samenwerking met gemeenten en regionale veiligheidsnetwerken en heeft als doel om gemeenten te helpen effectieve voorlichting over online criminaliteit aan hun inwoners en ondernemers te geven. Hiermee willen gemeenten hun inwoners en ondernemers helpen zich beter te kunnen beschermen tegen de risico's van online criminaliteit.*

*Om tot die effectieve voorlichting te komen, willen gemeenten weten hoe mensen zich gedragen online en waarom, hoe ze omgaan met de kans om slachtoffer te worden van online criminaliteit, of ze de gevaren en risico's kennen en of ze weten hoe ze kunnen voorkomen dat ze slachtoffer worden van online criminaliteit. Omdat mensen online van veel verschillende typen delicten slachtoffer kunnen worden, net als in de fysieke wereld, gaan we specifiek in op één vorm van online criminaliteit: vriend in nood fraude. Daar gaat dit interview over.*

*Omdat wij meerdere personen interviewen, worden geluidsopnames gemaakt van dit gesprek. Deze opnames worden alleen gebruikt voor de analyse van uw interview. Alles wat u zegt of vindt, zal geanonimiseerd worden verwerkt en uw antwoorden zullen op geen enkele wijze met u als persoon in verband kunnen worden gebracht. Na analyse worden deze opnames vernietigd. Uw anonimiteit is volledig gewaarborgd. Vind u het goed dat ik het interview opneem?*

*Er zijn geen goede of foute antwoorden, uw mening en ideeën staan centraal.*
*Als u verder geen vragen heeft, dan stel ik voor dat we gaan beginnen.*
*Eerst zou ik graag wat algemene vragen willen stellen.*
*Als het nog niet aan bod is gekomen:*

- Wat is uw leeftijd?
- Wat doet u in het dagelijks leven?
- *Noteren:* geslacht van respondent.

**Topic 1: Rollenspel**

*In het eerste deel van het interview zou ik graag een rollenspel met u willen doen. In dit rollenspel bent u een moeder/vader van een uit huis wonend kind: Mieke. In dit rollenspel ga ik u zo een aantal WhatsApp berichten laten zien. Het is de bedoeling dat u zich voorstelt dat u deze berichten zelf*

*ontvangt. Vervolgens stel ik u een aantal vragen over wat u zou doen en waarom. Heeft u hier verder nog vragen over voor dat we beginnen?*

***Whatsapp bericht 1 (Eerste contact bericht onbekend nummer 'hoi mam/pap, ben je thuis')***

- Wat is uw eerste gedachte bij het zien van dit bericht?
    - En waarom?
- Wat zou u doen met dit bericht?
    - En waarom?

De afbeelding die aan de respondent wordt getoond (versie vader, versie moeder):


***Whatsapp bericht 2 (opbouw naar geldvraag, 'ja nieuw nummer want ben gewisseld van provider maar ik heb een probleem')***

- Wat is uw eerste gedachte bij het zien van dit bericht?
    - En waarom?
- Wat zou u doen met dit bericht?
    - En waarom?

De afbeelding die aan de respondent wordt getoond (versie vader, versie moeder):


***Whatsapp bericht 3 (vraag om geld, 'kan momenteel niet internetbankieren en ik moet voor 17 uur een betaling doen')***

- Wat is uw eerste gedachte bij het zien van dit bericht?
    - En waarom?
- Wat zou u doen met dit bericht?
    - En waarom?

De afbeelding die aan de respondent wordt getoond (versie vader, versie moeder):


Dat was het rollenspel. Dan zou ik het nu met u willen hebben over het risico van vriend-in-nood fraude.

**Topic 2: Kennis**

1. Bent u bekend met vriend-in-nood fraude?
2. Wat houdt dat volgens u in?
3. Hoe komt u aan die kennis?

*Ik zal nu even bespreken wat de definitie is van vriend-in-nood-fraude. Bij vriend-in-nood fraude krijgt u via WhatsApp zogenaamd een dringend verzoek van een vriend(in), familielid of bekende om snel geld over te maken. In werkelijkheid komt het appje van een oplichter die zich voordoet als een bekende die u op slinkse wijze geld wil aftroggelen.*

**Topic 3: Risicoperceptie**
*Dan nu nog weer even kijkend naar risicoperceptie*

1. Ziet u vriend-in-nood fraude als een risico voor uzelf?
    - Kunt u dat toelichten?
2. Hoe schat u de kans dat u hiervan slachtoffer te worden in?
    - Waarom?
3. Hoe schat u de ernst van de gevolgen hiervan in?
    - Waarom
4. Waar baseert u dat op? *(vraag in ieder geval door op: wat speelt een rol: kans, ernst van de gevolgen, eerder slachtoffer geworden etc.)*
5. *Indien meerdere spelen een rol:* welke reden is het belangrijkste?
6. Waarom zou dit risico voor uzelf verschillen ten opzichte van andere mensen?

Ik zou het nu graag willen hebben over het beschermen van uzelf tegen vriend-in-nood fraude.

***Topic 4: Jezelf beschermen***

1. Vind u het nodig om uzelf te beschermen tegen vriend-in-nood fraude?
    - Kunt u dat toelichten?
    - Waar baseert u dat op? *(doorvragen!)*
2. Denkt u dat u in staat bent uzelf te beschermen tegen vriend-in-nood fraude?
    - Kunt u dat toelichten?
    - Waar baseert u dat op? *(doorvragen!)*

**Topic 5: Het nemen van maatregelen**

1. Op welke manieren probeert u, als u een verdacht bericht krijgt, te voorkomen om slachtoffer te worden van vriend-in-nood fraude? *(bespreek in ieder geval: voorzichtig gedrag, hulp vragen)*
2. Waarom heeft u ervoor gekozen om dat te doen? (*bespreek in ieder geval: hoe effectief is het, kosten, moeite, omdat anderen het doen)*
    - Ziet u het gedrag als effectief? Hoe effectief? Waarom
    - Kost het u veel tijd, moeite of geld?
    - Andere in de omgeving die dit ook doen?
    - *Indien meerdere spelen een rol:* welke reden in het belangrijkste?
    - Hoe bent u erop gekomen om dat te doen?
3. Is dit voldoende om u tegen slachtofferschap van vriend-in-nood fraude te beschermen?
    - Waarom?
4. Hoe zou u zichzelf nog meer kunnen beschermen tegen vriend-in-nood fraude?
    - Waarom doet u dat nog niet? *(bespreek in ieder geval: hoe effectief is het, toegankelijkheid, kosten, moeite, informatievoorziening)*
        - *Indien meerdere spelen een rol:* welke reden in het belangrijkste?

**Topic 6: Ondersteuning**

1. Stel dat u uzelf graag beter wil beschermen tegen vriend-in-nood fraude. Wat hebt u daarvoor nodig?
    - Waarom?
2. Ziet u hierin een rol voor de gemeente?
    - Zo ja, hoe ziet die er volgens u uit?
    - Zo nee, waarom niet en welke partij is dan volgens u wel geschikt om u hierin te ondersteunen/helpen?

Afsluiting

- Hebben wij in dit interview nog iets gemist dat u wilt meegeven?

# Bijlage V: Codeboom

| Codes | Interviews | Aantal referenties |
|---|---|---|
| **Kennis/Ervaring** | 15 | 18 |
| Kennis Risicobewust handelen | 15 | 47 |
| Kennis WhatsApp fraude | 15 | 32 |
| Geen kennis Risicobewust handelen | 7 | 11 |
| Geen kennis WhatsApp fraude | 9 | 14 |
| Kennis via actualiteiten programma's* | 8 | 11 |
| Kennis via gids consumentenbond* | 1 | 1 |
| Kennis via krant* | 6 | 6 |
| Kennis via naasten* | 3 | 3 |
| Kennis via nieuws* | 1 | 1 |
| Kennis via ouderenbond* | 1 | 1 |
| Kennis via social media* | 3 | 3 |
| Kennis door eigen ervaring* | 2 | 2 |
| Kennis door ervaring van anderen* | 2 | 4 |
| **Risicobewust handelen** | 15 | 15 |
| Wel risicobewust handelen | 15 | 83 |
| *Telefoonnummer controleren* | 9 | 14 |
| *Profielfoto controleren* | 2 | 2 |
| *Niet klikken op link* | 1 | 1 |
| *Niet geld overmaken* | 5 | 8 |
| *Verifiëren* | 11 | 38 |
| *Bewijsmateriaal verzamelen* | 1 | 1 |
| *Nummer rapporteren* | 2 | 3 |
| *Aangifte politie* | 4 | 5 |
| *Aangifte fraudehelpdesk* | 2 | 2 |
| *Geen informatie geven** | 1 | 1 |
| *Controleren taalgebruik (spelling/grammatica, maar ook past deze manier van communiceren)** | 9 | 13 |
| *Negeren** | 9 | 19 |
| *Advies naasten vragen** | 6 | 11 |
| *Advies instantie vragen** | 4 | 6 |
| *Nummer blokkeren** | 4 | 8 |
| *Gesprek verwijderen** | 5 | 8 |
| Niet risicobewust handelen | 10 | 17 |
| *Ziet 'red flags' niet* | 3 | 5 |
| *Ziet 'red flags' handelt niet naar* | 6 | 7 |
| **Risicoperceptie** | 15 | 16 |
| Optimistic bias | 9 | 11 |
| **PMT-factoren** | 15 | 101 |
| PMT DE Gepercipieerde impact | 15 | 25 |
| PMT DE Gepercipieerde kwetsbaarheid | 15 | 42 |
| PMT ME Response effectiviteit | 15 | 40 |
| PMT ME Zelfeffectiviteit | 15 | 22 |

| | | |
|---|---|---|
| PMT ME Response kosten | 14 | 17 |
| **Ondersteuning** | 15 | 27 |
| Invalshoeken interventies | 12 | 13 |

*Noot.* De kolom interviews omschrijft het aantal personen dat een code genoemd heeft. Aantal referenties beschrijft hoe vaak een fragment is geplaatst onder deze code.
**Niet vooropgestelde code, opgesteld aan de hand van fragment in de interviews*

Bijlage VI: Stappenplan IT4Senioren


Bron: IT4Senioren, 2021, geraadpleegd via https://www.linkedin.com/posts/it4senioren-nl_it4s-phishing-via-whatsapp-activity-6790923596991643648-E8jp