Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2019-18

Slachtofferschap van online criminaliteit

Prevalentie, risicofactoren en gevolgen

T. Sipma
E.M.C. van Leijsen

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Inhoud

Samenvatting

Online criminaliteit vormt een belangrijk maatschappelijk probleem dat door de digitalisering van de maatschappij in allerlei verschijningsvormen opduikt, zoals pogingen tot oplichting via verkoopsites en online bedreigingen. De continue aansluiting van mensen op het internet creëert een grootschalige potentiële blootstelling aan online criminaliteit. In het onderhavige onderzoek staat de burgerbevolking als doelwit van diverse vormen van online criminaliteit centraal. Het doel is om beter zicht te krijgen op de omvang, risicofactoren en gevolgen van diverse vormen van online slachtofferschap.

Bij online criminaliteit wordt onderscheid gemaakt tussen cybercriminaliteit en gedigitaliseerde criminaliteit. Cybercriminaliteit betreft misdrijven waarbij zowel het middel als het doel een component van informatie- en communicatietechnologie (ICT) bevat. Computervirussen en hacken, waarbij onrechtmatig toegang tot computers, e-mailaccounts of online bankierplatformen wordt verkregen, zijn voorbeelden van cybercriminaliteit. Bij gedigitaliseerde criminaliteit gaat het om misdrijven waarbij alleen het middel een ICT-component bevat en het misdrijf gericht is op de persoon, zoals online bedreiging (bijvoorbeeld via e-mail of social media) en oplichting (zoals aan- of verkoopfraude). Het huidige onderzoek omvat delicten uit beide typen online criminaliteit.

De meerwaarde van het huidige onderzoek is het gebruik van longitudinale paneldata, verzameld tussen 2008 en 2018. De volgorde waarin verschillende gebeurtenissen, gedragingen en gemoedstoestanden zich bij mensen voordoen, kunnen in deze panelstudie duidelijk in de tijd worden geplaatst. Hierdoor is dit onderzoek beter in staat risicofactoren en gevolgen van online slachtofferschap in kaart te brengen dan eerdere cross-sectionele studies die gebruik hebben gemaakt van data verzameld op één meetmoment.

Er is gekeken naar slachtofferschap van zeven online delicten: creditcard fraude, gehackt worden, online aankoopfraude, online bedreiging, het oplopen van een computervirus, ongeautoriseerde bankafschrijving en identiteitsfraude. Allereerst is onderzocht hoe vaak online slachtofferervaringen de afgelopen jaren voorkomen en hoe ernstig deze zijn. Ten tweede is gekeken naar de risicofactoren van verschillende vormen van online slachtofferschap. Risicofactoren die onder de loep zijn genomen, zijn onder andere leeftijd, geslacht, opleidingsniveau, online gedragingen en verschillende persoonlijkheidskenmerken waaronder impulsiviteit. Tevens is vergeleken in hoeverre de risicofactoren van online slachtofferschap overeenkomen met risicofactoren van offline slachtofferschap. Ten derde is onderzocht in hoeverre online slachtofferervaringen samengaan met veranderingen in online gedragingen en welbevinden van burgers. Tot slot is herhaald slachtofferschap in kaart gebracht en is onderzocht of de eerdergenoemde risicofactoren ook verklaren waarom sommige burgers een grotere kans hebben om opnieuw slachtoffer te worden van online criminaliteit.

Vraagstelling

De centrale vraagstelling van het onderzoek is als volgt: wat zijn patronen van (herhaald) slachtofferschap van online criminaliteit en in hoeverre kunnen die

worden verklaard door persoonskenmerken, online gedragingen en de gevolgen van eerder slachtofferschap?

Op basis van empirisch onderzoek zijn de volgende onderzoeksvragen beantwoord:
1 In welke mate ervaren Nederlandse burgers slachtofferschap van online criminaliteit?
2 In hoeverre hangt online slachtofferschap samen met eerdere slachtoffererva-ringen, internetgebruik, beschermingsmaatregelen en persoonskenmerken?
3 In hoeverre heeft online slachtofferschap gevolgen voor angst voor online criminaliteit, internetgebruik, beschermingsmaatregelen en mentale gezondheids-problemen?
4 In welke mate is er sprake van herhaald slachtofferschap en in welke mate vormen de mogelijke gevolgen van online slachtofferschap een verklaring voor patronen in herhaald slachtofferschap?

Methoden

In dit onderzoek is gebruikgemaakt van het LISS-panel, een online dataverzameling onder een representatieve steekproef van Nederlandse huishoudens, waarin panel-leden sinds 2007 maandelijks online een wisselende vragenlijst invullen over onder andere hun persoonlijkheid, werksituatie en vrijetijdsbesteding. Sinds februari 2008 heeft eens in de twee jaar ook een uitgebreide slachtofferenquête plaatsgevonden, waarin respondenten zijn gevraagd naar slachtoffererervaringen van diverse vormen van offline en online criminaliteit. Inmiddels is er sprake van zes meetmomenten (2008-2018), waarbij iedere keer vijf- à zesduizend respondenten hebben mee-gewerkt. Aan de hand van deze longitudinale panelgegevens zijn de prevalentie, risicofactoren en gevolgen van (herhaald) online slachtofferschap bestudeerd.

Resultaten

Online slachtofferschap gedaald tussen 2010 en 2018

Uit de resultaten blijkt een significante daling in de prevalentie van slachtofferschap van de totaalscore van de zeven typen online delicten, van 15,1% in 2010 naar 9,5% in 2018. Ook het type online delict blijkt veranderd te zijn, in 2010 komen computervirussen het meest voor, in 2018 is dit aankoopfraude. Het aantal perso-nen dat aangeeft slachtoffer te zijn geweest van offline delicten is hoger dan dat van online delicten, al is ook deze prevalentie significant gedaald (van 20,5% in 2010 naar 12,4% in 2018). De daling in online slachtofferschap is vooral te zien in de daling in het aantal slachtoffers van computervirussen (8,9% in 2010 en 1,7% in 2018). In iets mindere mate is tevens een daling in het aantal slachtoffers van hacken (1,4% in 2010 en 0,9% in 2018) en ongeautoriseerde bankafschrijvingen (3,0% in 2010 en 1,2% in 2018) te zien. Daarentegen zijn de prevalenties van online aankoopfraude en identiteitsfraude in diezelfde periode significant gestegen, respectievelijk van 2,4% in 2010 naar 4,4% in 2018 en van 0,1% naar 0,3%. Bij een aantal online delicten is gevraagd of slachtoffers aangifte hebben gedaan, waaruit blijkt dat slechts een minderheid van de slachtoffers naar de politie stapt. 11,6% van de slachtoffers van ongeautoriseerde bankafschrijving heeft aangifte gedaan bij de politie. Bij slachtoffers van online aankoopfraude is dit 12,0%, bij online bedreiging 20,2% en bij identiteitsfraude 46,0%.

Onder andere eerdere slachtoffers, jongeren, mannen en frequente internetgebruikers hebben meer risico op online slachtofferschap

Eerdere slachtofferervaringen hangen samen met de kans op een nieuwe slachtofferervaring: respondenten die tijdens een eerder meetmoment hebben aangegeven slachtoffer te zijn geweest van online criminaliteit, hebben een grotere kans ook op een volgend meetmoment slachtoffer te zijn. Verder hebben respondenten die meer gebruikmaken van internet een grotere kans om slachtoffer van online criminaliteit te worden. De kans op online slachtofferschap is echter niet geassocieerd met het aantal genomen beschermingsmaatregelen tijdens een voorgaand meetmoment. Daarnaast hangen diverse persoonskenmerken samen met de kans op online slachtofferschap. Zowel jongere als mannelijke respondenten hebben een grotere kans om slachtoffer te worden van online criminaliteit. Daarnaast blijken respondenten die impulsief, open of emotioneel instabiel zijn vatbaarder voor online slachtofferschap. Leeftijd, emotionele instabiliteit en openheid vormen ook risicofactoren van offline criminaliteit. Geslacht vormt voor beide vormen van criminaliteit een risicofactor. Waar mannen een grotere kans hebben om slachtoffer te worden van online criminaliteit, hebben vrouwen juist een grotere kans om slachtoffer te worden van offline criminaliteit. Een hogere score op altruïsme en een lagere score op consciëntieusheid hangen samen met offline slachtofferschap, maar niet met online slachtofferschap. Impulsiviteit is de enige risicofactor die enkel is voorbehouden aan online slachtoffers, en kan daardoor worden gezien als een kenmerkende risicofactor van online criminaliteit.

Angst neemt toe, maar mentale gezondheid verslechtert niet na online slachtofferschap

Slachtoffers van online criminaliteit hebben na hun slachtofferervaring meer angst voor online criminaliteit dan voorheen. Deze angst zou er mogelijk voor kunnen zorgen dat slachtoffers wegblijven van het internet. Echter, in het huidige onderzoek hangt slachtofferschap niet significant samen met een daling in internetgebruik. In plaats van weg te blijven van het internet, hebben respondenten nadat zij slachtoffer zijn geworden van online criminaliteit significant meer beschermingsmaatregelen getroffen. Wanneer nader onderscheid is gemaakt op basis van aangiftebereidheid, is zichtbaar dat slachtoffers die geen aangifte hebben gedaan van hun slachtofferervaring meer beschermingsmaatregelen treffen, terwijl dat niet het geval was bij slachtoffers die wel aangifte hadden gedaan. Een mogelijke verklaring is dat voornamelijk slachtoffers van computervirussen meer beschermingsmaatregelen treffen, terwijl deze slachtoffers waarschijnlijk relatief minder vaak aangifte doen bij politie dan slachtoffers van ander type delicten.
Tenslotte neemt de mentale gezondheid niet af onder de totale groep van online slachtoffers. Dat is echter wel het geval als alleen slachtoffers van online bedreiging worden meegenomen: na slachtofferschap van online bedreiging neemt het mentaal welbevinden van slachtoffers af, mogelijk omdat van de onderzochte delicten dit delict de grootste impact op iemands persoonlijke levenssfeer heeft.

Impulsiviteit, emotionele stabiliteit en openheid belangrijke voorspellers van herhaald slachtofferschap

Van de respondenten die tenminste tweemaal hadden deelgenomen aan de slachtofferschap-vragenlijst, gaf 16,6% aan eenmalig slachtoffer en 17,5% herhaald slachtoffer te zijn geweest van online criminaliteit. De resultaten van dit onderzoek laten zien dat mannen, of impulsieve, emotioneel instabiele of meer open respon-

denten een grotere kans hebben om herhaald slachtoffer te worden dan om eenmalig slachtoffer te worden. Impulsiviteit, emotionele instabiliteit en openheid hangen bovendien samen met de frequentie van slachtofferervaringen. De samenhang verloopt gradueel: hoe hoger men scoort op deze persoonlijkheidskenmerken, hoe vaker men kans loopt slachtoffer te worden van online criminaliteit. Deze bevinding wordt bevestigd in verschillende robuustheidsanalyses.

Daarnaast kan eerder online slachtofferschap en de gevolgen daarvan, een risicofactor vormen voor een nieuwe slachtofferervaring. Een daling in internetgebruik en mentale gezondheid zou een gevolg van eerder slachtofferschap kunnen zijn, maar deze kenmerken blijken niet te veranderen na online slachtofferschap. Hoewel internetgebruik wel samenhangt met de kans om (een eerste keer) slachtoffer te worden, vormen internetgebruik en mentale gezondheid geen verklaring waarom sommige slachtoffers *opnieuw* slachtoffer worden. Beschermingsmaatregelen nemen wel toe na een slachtofferervaring, maar het nemen van beschermingsmaatregelen lijkt vervolgens het risico op slachtofferschap niet te verlagen. Deze resultaten over herhaald slachtofferschap suggereren dat het eerder de meer stabiele persoonskenmerken zijn die herhaald slachtofferschap verklaren, dan de hier onderzochte gevolgen van een eerdere slachtofferervaring.

Sterke punten en verbeterpunten

Een belangrijke meerwaarde ten opzichte van eerder onderzoek is het longitudinale en representatieve karakter van het huidige onderzoek. Door mensen over een langere periode te volgen, is het in dit onderzoek mogelijk geweest om verschillende gebeurtenissen, gedragingen en gemoedstoestanden voor en na een slachtofferervaring te meten. Hiermee kunnen deze factoren duidelijker in de tijd worden geplaatst dan mogelijk is met een studie die gebruikmaakt van slechts één meetmoment. Een ander pluspunt is dat er gebruik is gemaakt van zelfrapportage van online slachtofferschap. Omdat slechts een beperkt deel van de cyber- en gedigitaliseerde criminaliteit in beeld is bij politie of justitie – in het huidige onderzoek stapte een minderheid van de online slachtoffers naar de politie – levert het gebruik van zelfrapportage naar verwachting een beter beeld op van de omvang van online slachtofferschap. De zelfrapportage kent echter ook een aantal beperkingen. Vanwege de retrospectieve aard van zelfrapportage, kunnen slachtoffers zich mogelijk gebeurtenissen niet meer (goed) herinneren of plaatsen zij gebeurtenissen eerder of later in de tijd. Naast deze beperkingen van zelfrapportage zijn in dit onderzoek niet alle typen online delicten meegenomen. Op sommige meer recent ontstane delicten, zoals malware en ransomware, is hierdoor geen zicht gekomen.

Conclusie

De eerste conclusie van dit rapport is dat slachtofferschap van zeven typen online delicten tussen 2010 en 2018 is gedaald onder een representatieve steekproef van de Nederlandse bevolking, waarbij het meest voorkomende type online delict is verschoven van computervirussen naar aankoopfraude. Hoewel over het algemeen een dalende trend aanwezig is, laat dit onderzoek onverminderd zien dat een deel van de Nederlandse bevolking ooit slachtoffer is geworden van één van de onderzochte online delicten. Om die reden zijn ook de risicofactoren en gevolgen van deze slachtofferervaringen in kaart gebracht.

Internetgebruik blijkt – niet geheel verassend – één van de risicofactoren voor online slachtofferschap, aangezien de gelegenheid tot online criminaliteit groter is naarmate men zich meer online begeeft. Mensen die eerder online slachtoffer zijn geworden, mannen en jongere mensen, lopen ook een verhoogd risico op online slachtofferschap. Impulsieve mensen, emotioneel instabiele mensen en meer open mensen hebben daarentegen niet alleen meer kans om één keer slachtoffer te worden, maar ook om herhaald slachtoffer te worden van online criminaliteit. Een mogelijke verklaring voor de sterke samenhang tussen deze persoonlijkheidskenmerken en online slachtofferschap, is dat deze kenmerken een indicatie zijn voor online risicogedrag. Zo zullen impulsieve mensen tijdens hun handelen minder nadenken over mogelijke risico's, hebben emotioneel instabiele mensen meer moeite om risico's in te schatten, en hebben open mensen een grotere kans om online gegevens te delen. Niet alleen het internetgebruik zelf, maar ook de manier waarop men zich op het internet gedraagt, lijkt dus een risicofactor voor online slachtofferschap. Beleid dat burgers wil wijzen op online gevaren kan rekening houden met de persoonlijkheidskenmerken van potentiële slachtoffers. Waarschuwingen over online risico's hebben mogelijk een minder goede uitwerking op impulsieve mensen dan op niet-impulsieve mensen, omdat impulsieve mensen eerder geneigd zijn te handelen zonder na te denken over de mogelijke consequenties van hun online gedrag.

Het huidige onderzoek laat zien dat slachtoffers van online criminaliteit niet minder gebruikmaken van het internet na hun slachtofferervaring. Uit de literatuur naar offline slachtofferschap weten we dat die slachtoffers de plek waar het delict heeft plaatsgevonden na hun slachtofferervaring zijn gaan mijden. In deze steeds meer gedigitaliseerde samenleving is het echter voor online slachtoffers haast onmogelijk om zich aan het digitale leven te onttrekken. Slachtoffers van online criminaliteit ervaren over het algemeen geen verslechtering in hun mentale gezondheid. Alleen slachtoffers van online bedreiging laten een daling in hun mentale gezondheid zien. Slachtoffers van online criminaliteit lijken zich desalniettemin bewust van hun eerdere slachtofferervaring, gezien de bevinding dat ze gemiddeld genomen een grotere angst voor online criminaliteit rapporteren en meer beschermingsmaatregelen hebben getroffen dan vóór hun slachtofferervaring. Deze bevinding laat zien dat slachtoffers bereid zijn hun online gedrag aan te passen, en dat het relevant is (potentiële) slachtoffers te wijzen op wat ze kunnen doen om de kans op een (nieuwe) slachtofferervaring te verkleinen.

1 Inleiding

1.1 Achtergrond en aanleiding onderzoek

Online criminaliteit vormt een belangrijk maatschappelijk probleem dat door digitalisering van de maatschappij in allerlei verschijningsvormen opduikt, zoals malware (schadelijke software) in computers, pogingen tot oplichting via verkoopsites en bedreigingen die via social media worden geuit. De continue aansluiting van mensen op het internet creëert een grootschalige potentiële blootstelling aan online criminaliteit. Dat kan via interpersoonlijk digitaal contact, zoals bij online bedreiging en oplichting, maar ook via diefstal van digitale goederen of gegevens, zoals bij identiteitsfraude. Het doel van dit onderzoek is om beter zicht te krijgen op de omvang, ernst, risicofactoren en gevolgen van diverse vormen van online slachtofferschap onder de Nederlandse bevolking.

Er is vanuit de politiek veel aandacht voor het aanpakken, voorkomen en terugdringen van cybercriminaliteit. Mede naar aanleiding van de motie Recourt, waarin opgeroepen wordt tot een integraal plan voor de aanpak van cybercrime (Kamerstukken II, 2016-2017, 34 550 VI, nr. 87), heeft de Minister van Justitie en Veiligheid (JenV) op 20 april 2018 een brief naar de Tweede Kamer gestuurd waarin de integrale aanpak van cybercrime wordt gepresenteerd (Kamerstukken II, 2017-2018, 28684, nr. 522). Onderdeel van deze integrale aanpak is een breed wetenschappelijk onderzoeksprogramma van het WODC voor de versterking van de wetenschappelijke kennis over cybercrime en de beleidsvorming in de toekomst. In dat kader is het huidige onderzoek naar slachtofferschap van cyber- en gedigitaliseerde criminaliteit gestart. Naast onderhavig onderzoek, wordt ook onderzoek uitgevoerd naar de risicoperceptie en het cyberbewustzijn van slachtoffers, de aard en omvang van cyber- en gedigitaliseerde criminaliteit en de opsporing, vervolging en verstoring van cyber- en gedigitaliseerde criminaliteit.

In onderhavig onderzoek staat de burgerbevolking als doelwit van online criminaliteit centraal. Bij online criminaliteit wordt onderscheid gemaakt tussen cybercriminaliteit en gedigitaliseerde criminaliteit (zie bijvoorbeeld Rokven, Weijters & Van der Laan, 2017). Cybercriminaliteit betreft misdrijven waarbij zowel het middel als het doel een component van informatie- en communicatietechnologie (ICT) bevat. Computervirussen en *hacken*, waarbij onrechtmatig toegang tot computers, e-mailaccounts of online bankierplatformen wordt verkregen, zijn voorbeelden van cybercriminaliteit. Bij gedigitaliseerde criminaliteit gaat het om misdrijven waarbij alleen het middel een ICT-component bevat en het misdrijf gericht is op de persoon, zoals online bedreiging (bijvoorbeeld via e-mail of social media) en oplichting (zoals aan- of verkoopfraude). In het huidige onderzoek zijn beide typen delicten onderzocht en is hiervoor de term online criminaliteit gebruikt.

Een belangrijke meerwaarde ten opzichte van eerder onderzoek is het longitudinale karakter van het huidige onderzoek. In dit onderzoek wordt gebruikgemaakt van het *Longitudinal Internet Studies for the Social sciences* (LISS) panel, een online dataverzameling onder een representatieve steekproef van Nederlandse huishoudens, waarin panelleden sinds 2007 maandelijks online een wisselende vragenlijst invullen over onder andere hun persoonlijkheid, werksituatie en vrijetijdsbesteding. Sinds februari 2008 heeft eens in de twee jaar ook een uitgebreide slachtofferenquête plaatsgevonden, waarin respondenten zijn gevraagd naar slachtoffer-

ervaringen van diverse vormen van offline en online criminaliteit. Inmiddels is er sprake van zes meetmomenten (2008-2018), waaraan iedere keer vijf- à zesduizend respondenten hebben meegewerkt. Aan de hand van deze longitudinale data kan het onderscheid in risicofactoren en gevolgen van slachtofferschap beter worden gemaakt dan in het gangbare cross-sectionele slachtofferonderzoek. De volgorde waarin verschillende gebeurtenissen, gedragingen en gemoedstoestanden zich bij mensen voordoen, kunnen in deze panelstudie duidelijker in de tijd worden geplaatst dan in cross-sectioneel onderzoek, waarin deze factoren tegelijkertijd worden bevraagd. Een voorbeeld is de mogelijk wederkerige relatie tussen preventiegedrag en online slachtofferschap. Door beschermingsmaatregelen te treffen (bijvoorbeeld een firewall op de computer installeren), zou de kans op slachtofferschap omlaag gaan, maar andersom kan het ook zijn dat men al slachtoffer is geweest en als gevolg daarvan beschermingsmaatregelen treft. Vanuit het cross-sectionele onderzoek naar preventie en online slachtofferschap is het vooralsnog niet duidelijk wat eerder plaatsvindt: slachtofferschap of preventiegedrag. Door via een longitudinale studie helder te hebben wanneer slachtofferervaringen plaats hebben gevonden en hoe preventiegedrag door de tijd heen verandert, wordt dit wel duidelijk. Als zodanig kunnen de resultaten uit dit onderzoek meer aanknopingspunten bieden voor toekomstig beleid, bijvoorbeeld om te bepalen welke factoren relevant zijn op het gebied van preventie en welke op het gebied van nazorg (bijvoorbeeld slachtofferhulp) en op mogelijke doelgroepen waar deze initiatieven het best op kunnen worden gericht.

Aan de hand van een panelstudie van tien jaar (2008 tot 2018) is allereerst onderzocht hoe vaak online slachtofferervaringen de afgelopen jaren voorkomen en hoe ernstig deze zijn. De in dit onderzoek meegenomen delicten zijn: creditcard fraude, gehackt worden, online aankoopfraude, online bedreiging, het oplopen van een computervirus, ongeautoriseerde bankafschrijving en identiteitsfraude. Ten tweede is gekeken naar de risicofactoren van verschillende vormen van online slachtofferschap. Risicofactoren die onder de loep zijn genomen, zijn onder andere leeftijd, geslacht, opleidingsniveau, online gedragingen en verschillende persoonlijkheidskenmerken waaronder impulsiviteit. Ten derde is onderzocht in hoeverre online slachtofferervaringen samengaan met veranderingen in online gedragingen en mentaal welbevinden van burgers. Tot slot is herhaald slachtofferschap in kaart gebracht en is onderzocht of de eerdergenoemde risicofactoren ook verklaren waarom sommige burgers een grotere kans hebben om opnieuw slachtoffer te worden van online criminaliteit. Deze vier doelen zijn hieronder nader uitgewerkt (paragraaf 1.3 tot en met 1.6).

1.2 Vraagstelling en onderzoeksvragen

De centrale vraagstelling van het onderzoek is als volgt: wat zijn patronen van (herhaald) slachtofferschap van online criminaliteit en in hoeverre kunnen die worden verklaard door persoonskenmerken, online gedrag en de gevolgen van eerder slachtofferschap?

Op basis van empirisch onderzoek zijn de volgende onderzoeksvragen beantwoord:
1 In welke mate ervaren Nederlandse burgers slachtofferschap van online criminaliteit?
2 In hoeverre hangt online slachtofferschap samen met eerdere slachtofferervaringen, internetgebruik, beschermingsmaatregelen en persoonskenmerken?

3 In hoeverre heeft online slachtofferschap gevolgen voor angst voor online criminaliteit, internetgebruik, beschermingsmaatregelen en mentale gezondheidsproblemen?
4 In welke mate is er sprake van herhaald slachtofferschap en in welke mate vormen de mogelijke gevolgen van online slachtofferschap een verklaring voor patronen in herhaald slachtofferschap?

1.3 Trends in slachtofferschap van online criminaliteit

Het eerste doel van dit onderzoek is om de omvang en ernst van online slachtofferschap onder Nederlandse burgers in kaart te brengen. Om dit doel te volbrengen, zal getracht worden onderzoeksvraag 1 te beantwoorden: *in welke mate ervaren Nederlandse burgers slachtofferschap van online criminaliteit?*

Op basis van eerder onderzoek in Nederland kan al een aantal uitspraken worden gedaan over aard en omvang van online slachtofferschap. Zo is uit de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek (CBS) af te leiden hoeveel mensen gedurende het afgelopen jaar in aanraking zijn gekomen met online criminaliteit. In de Veiligheidsmonitor van het CBS wordt de ontwikkeling van sociale (on)veiligheid in Nederland beschreven, op basis van een grootschalige enquête onder de Nederlandse bevolking van 15 jaar en ouder. In een recente editie kwam naar voren dat 11% van de bevolking van 15 jaar en ouder een vorm van online criminaliteit heeft meegemaakt gedurende het afgelopen jaar (CBS, 2017). Specifieke delicten die relatief veel voorkomen zijn online aankoopfraude (3,9%) en gehackt worden (4,9%). Verder wordt uit diezelfde Veiligheidsmonitor duidelijk dat bepaalde groepen in de samenleving een verhoogd risico op online slachtofferschap lopen. Zo ervaren jongeren (15-24) bijna drie keer zo vaak online slachtofferschap als ouderen (65+): 17% tegenover 6%. Uit ander onderzoek op basis van deze gegevensbron blijkt dat er relatief weinig aangifte wordt gedaan van uiteenlopende vormen van online criminaliteit, zoals identiteitsfraude (26% van de slachtoffers), online oplichting (24%) en gehackt worden (7%; Van de Weijer, Leukfeldt & Bernasco, 2018).

Een representatieve survey onder de Nederlandse bevolking uit 2010 van Domenie, Leukfeldt, Van Wilsem, Jansen & Stol (2013) laat zien dat een paar procent van de burgerbevolking het jaar voorafgaand aan de enquête slachtoffer was geworden van uiteenlopende online delicten, zoals gehackt worden (4,3%), online oplichting (2,4%), cyberstalking (1,1%), online bedreiging (0,7%) en identiteitsfraude (0,9%). Anderhalf procent van de bevolking gaf aan meervoudig slachtoffer te zijn, dat wil zeggen meerdere typen online criminaliteit te hebben meegemaakt. Uit dezelfde studie blijkt een geringe bereidheid van slachtoffers om het delict bij de politie te melden: circa 13%.

Vanuit het voor dit rapport gebruikte (en voor Nederlandse huishoudens representatieve) LISS-panel zijn enkele eerdere studies verschenen die inzicht geven in de omvang en ernst van diverse vormen van online criminaliteit (Paulissen & Van Wilsem, 2015; Van Wilsem, 2011, 2013a, 2013b). Ook hieruit komt naar voren dat op jaarbasis een paar procent van de Nederlandse bevolking met online slachtofferschap te maken heeft, waaronder identiteits- en bankfraude (4,6%), bedreiging (0,9%), oplichting (2,5%) en gehackt worden (2,3%). Daarnaast is er bij bankfraude – waarbij bedragen ongeautoriseerd van de bankrekening worden afgeschreven – relatief veel sprake van herhaald slachtofferschap: één op de drie à vier

slachtoffers maakt het binnen de periode van een jaar vaker dan één keer mee (Paulissen & Van Wilsem, 2015). Circa de helft van de slachtoffers van bankfraude is oorspronkelijk een bedrag van meer dan honderd euro kwijt, maar meestal slaagt men er in de schade vergoed te krijgen. Slechts een paar procent van de slachtoffers houdt na pogingen tot vergoeding een schade van meer dan 100 euro over. Van Wilsem, Van der Meulen & Kunst (2013) vonden dat lager opgeleide slachtoffers van bankfraude minder vaak de schade vergoed krijgen dan hoger opgeleide slachtoffers. Tot slot geldt dat weinig slachtoffers van dit delict aangifte doen bij de politie, circa 10%. Dit betreft met name degenen die in eerste instantie veel geld kwijt zijn geraakt (Paulissen & Van Wilsem, 2015).

Dat ongeveer 11% van de Nederlanders in 2017 slachtoffer is geworden van online criminaliteit (CBS, 2017), laat zien dat slachtofferschap een relevant maatschappelijk probleem is. Om de relevantie van dit probleem nog beter in kaart te brengen, is het interessant om de omvang van online slachtofferschap over de tijd te bestuderen. In dit rapport is onderzocht of slachtofferervaringen in een steeds meer gedigitaliseerde samenleving zijn toe- of afgenomen. Door verschillende typen delicten te belichten, kan tevens een uitspraak worden gedaan over het soort delicten waarbij slachtofferschap is toe- dan wel afgenomen. De relevantie van een slachtofferervaring is ook afhankelijk van de ernst van het delict. Voor sommige delicten is om die reden aan slachtoffers doorgevraagd in hoeverre ze het delict als ernstig hebben ervaren, wat de financiële schade van het delict was en of ze aangifte hebben gedaan bij de politie. Tot slot is een vergelijking gemaakt met offline slachtofferschap. Offline criminaliteit lijkt in de afgelopen jaren te dalen; dat blijkt uit eerdere onderzoeken op basis van zowel zelfrapportage als geregistreerde criminaliteit (CBS, 2017; Kalidien, 2018). Een mogelijke verklaring hiervoor is een verplaatsing van offline naar online criminaliteit. Door de ontwikkeling van online slachtofferschap te vergelijken met de ontwikkeling van offline slachtofferschap kan worden bepaald of er evidentie bestaat voor deze verplaatsing van criminaliteit.

1.4 Risicofactoren voor online slachtofferschap

Nadat de omvang van online slachtofferschap in kaart is gebracht, rijst de vraag welke mensen het grootste risico lopen om slachtoffer te worden. Onderzoeksvraag 2 luidt dan ook: *in hoeverre hangen ervaringen met online slachtofferschap samen met eerdere slachtofferervaringen, internetgebruik, beschermingsmaatregelen en persoonskenmerken?*

1.4.1 Eerdere slachtofferervaringen

Uit eerder onderzoek naar offline criminaliteit is gebleken dat eerdere slachtofferervaringen een risicofactor vormen om (nogmaals) slachtoffer te worden (Ousey, Wilcox & Brummel, 2008; Van Reemst, Fischer & Van Dongen, 2013; Wittebrood, 2006). Zo kan een slachtofferervaring bepaalde gevolgen hebben die vervolgens een risicofactor vormen voor een nieuwe slachtofferervaring. In paragraaf 1.6, waarin herhaald slachtoffer aan bod komt, wordt hier dieper op ingegaan.

1.4.2 Internetgebruik en beschermingsmaatregelen

In het onderzoek naar wie verhoogde risico's lopen om slachtoffer te worden, speelt het begrip 'gelegenheid' een belangrijke rol. Uitgangspunt daarbij is dat mensen door het ondernemen van reguliere (routine) activiteiten – zoals het bezoeken van

een website – onbedoeld gelegenheid creëren om slachtoffer te worden door zich bloot te stellen aan de acties van een (online) dader. Deze gelegenheid kan beperkt worden door het nemen van beschermingsmaatregelen die de toegang tot het doelwit beperken, zoals het installeren van een spamfilter. Dit idee, afkomstig uit de routine activiteitentheorie (Cohen & Felson, 1979), veronderstelt dat de mate waarin een (online) doelwit geschikt is voor een dader bepaald wordt door de zogenoemde VIVA-criteria: *value, inertia, visibility, accessibility* (Felson & Clarke, 1998). Oftewel: een doelwit is geschikter naarmate het meer waarde vertegenwoordigt, makkelijk te vervoeren is (en daarmee gemakkelijk ontvreemd kan worden), zichtbaar is en toegankelijk is. In empirische studies waarin deze aannames worden getoetst, is vooral geconstateerd dat naarmate er meer blootstelling aan online daders is via het ondernemen van online activiteiten, het risico op online slachtofferschap hoger is. Per type delict is de online activiteit, die gepaard gaat met een hoger risico op online slachtofferschap, wel verschillend. Voor bijvoorbeeld malwarebesmetting gaat het bekijken van porno, het bezoeken van datingsites en het veelvuldig downloaden van online content gepaard met een hoger risico (Holt & Bossler, 2013; Holt, Van Wilsem, Van de Weijer & Leukfeldt, 2018), terwijl frequent internetaankopen doen een risicoactiviteit lijkt voor online oplichting (Van Wilsem, 2013a). Het ervaren van identiteitsfraude lijkt een uitzondering te zijn op de regel van verhoogd risico via blootstelling aan online activiteiten: voor dit delict waren nauwelijks activiteiten aanwijsbaar die verschilden tussen slachtoffers en niet-slachtoffers. Een mogelijke verklaring is dat identificerende informatie ook in omgevingen opgeslagen is die buiten het bereik van het doelwit liggen, zoals cliëntbestanden bij bedrijven (Paulissen & Van Wilsem, 2015). Al met al kan verwacht worden dat mensen die vaker het internet gebruiken een grotere kans hebben om slachtoffer te worden. Deze verwachting is in het huidige onderzoek getoetst.

Naast de rol van gelegenheid is in diverse studies ook aandacht geweest voor de rol van beveiliging of beschermingsmaatregelen – het beperken van de toegankelijkheid van het doelwit. Zoals eerder genoemd, stelt het cross-sectionele karakter van studies hierbij beperkingen aan de kwaliteit van het 'bewijs'. Diverse onderzoeken stellen dat beschermingsmaatregelen geen beschermende werking bieden tegen identiteitsfraude (Paulissen & Van Wilsem, 2015), *phishing*[1] (Leukfeldt, 2014, 2015), malware (Leukfeldt, 2015) en gehackt worden (Van Wilsem, 2013b). Sommige cross-sectionele studies suggereren zelfs een hoger risico onder degenen die zich hebben beschermd (Bossler, Holt & May, 2011; Holt & Bossler, 2013) – wat echter ook een indicatie kan zijn voor omgekeerde causaliteit: door slachtofferschap gaat men zich beter beveiligen. In een studie waarin niet naar slachtofferschap werd gevraagd, maar naar problemen op de computer die duiden op malwarebesmetting, leek de beveiliging van het persoonlijke wifinetwerk een consistent (in diverse modellen) beschermende werking te hebben: mensen die zich hadden beveiligd, rapporteerden minder problemen (Holt et al., 2018). De mate waarin beschermingsmaatregelen een rol spelen bij slachtofferschap van online criminaliteit zijn in het huidige onderzoek onderzocht.

1.4.3 Persoonskenmerken

De mate van internetgebruik kan mogelijk ook verklaren waarom bepaalde groepen in de samenleving een groter risico lopen op online slachtofferschap. Zo is uit onderzoek duidelijk geworden dat jongeren vaker het internet gebruiken dan ouderen,

1 *Phishing* is een vorm van internetfraude waarbij middels een link naar een valse website geprobeerd wordt om (inlog)gegevens van slachtoffers te achterhalen.

waarmee zij ook een grotere kans hebben om slachtoffer te worden (Oksanen & Keipi, 2013). Hetzelfde geldt voor mannen, die zich gemiddeld genomen vaker online begeven dan vrouwen (Holt & Bossler, 2008). Ook opleidingsniveau zal worden meegenomen als mogelijke risicofactor voor online slachtofferschap.

Naast de mate van internetgebruik, zou het verschil in slachtofferschap tussen mannen en vrouwen ook verklaard kunnen worden door de mate van impulsiviteit. Mannen gedragen zich over het algemeen impulsiever dan vrouwen (Chapple & Johnson, 2007), wat invloed kan hebben op hun online gedrag en hun kans op online slachtofferschap. Impulsieve mensen nemen over het algemeen sneller beslissingen en hebben een verminderde oriëntatie op de lange-termijn consequenties van het eigen handelen, wat samengaat met (online) gedrag dat vaker resulteert in slachtofferschap. De meta-analyse van Pratt, Turanovic, Fox & Wright (2014) laat zien dat er in de algemene slachtofferliteratuur brede ondersteuning is gevonden voor de relatie tussen impulsiviteit en slachtofferschap. Dit lijkt ook te gelden voor studies naar online slachtofferschap, aangezien impulsiviteit samenhangt met uiteenlopende vormen van online slachtofferschap, zoals bedreiging, oplichting, gehackt worden, *sexting*[2] en malwarebesmetting (Holt et al., 2018; Reyns, Burek, Henson & Fisher, 2013; Van Wilsem, 2011, 2013a, 2013b). Deze relatie lijkt deels indirect te zijn, omdat impulsiviteit ook gepaard gaat met het vaker ondernemen van online activiteiten (zoals aankopen doen) en het minder nemen van beschermingsmaatregelen (Van Wilsem, 2013a).

Naast impulsiviteit bepalen mogelijk ook andere persoonlijkheidskenmerken het risico om slachtoffer te worden van online criminaliteit. Daarvoor is gebruikgemaakt van de bekende Big Five persoonlijkheidskenmerken: extraversie, altruïsme, consciëntieusheid, emotionele stabiliteit en openheid (Goldberg, 1993). Het persoonlijkheidsdomein extraversie beschrijft in hoeverre mensen naar buiten gericht, optimistisch en energiek zijn. Mensen die hoog scoren op altruïsme zijn inschikkelijk en gericht op interpersoonlijke relaties. Consciëntieusheid meet de mate van zorgvuldigheid en bedachtzaamheid. Mensen die hoog scoren op emotionele stabiliteit kunnen goed omgaan met stress en ervaren minder vaak negatieve emoties. Openheid geeft weer in hoeverre mensen flexibel en nieuwsgierig zijn. Deze persoonlijkheidskenmerken hangen dus sterk samen met de manier waarop mensen op bepaalde situaties reageren en hierop handelen, en kunnen daarmee invloed hebben op online risicogedrag dat mogelijk online slachtofferschap tot gevolg heeft (Wijn, Van den Berg, Wetzer & Broekman, 2016). Zo zullen extraverte mensen een grotere kans hebben om online risico's te nemen, altruïstische mensen eerder geneigd zijn mensen te vertrouwen, niet-consciëntieuze mensen minder bedachtzaam en minder risicomijdend zijn, emotioneel instabiele mensen minder goed risico's kunnen inschatten en open mensen eerder online informatie delen, met mogelijk online slachtofferschap tot gevolg (Borwell, Jansen & Stol, 2018). Uit eerder onderzoek is gebleken dat slachtoffers van *phishing* hoger scoren op openheid en lager op emotionele stabiliteit (Halevi, Lewis & Memon, 2013). Slachtoffers van online fraude scoren hoger op extraversie en altruïsme, en – tegen de verwachting in – scoren zij ook hoger op consciëntieusheid en emotionele stabiliteit (Borwell et al., 2018). In dit rapport zal worden gekeken of deze persoonlijkheidskenmerken ook samenhangen met een meer algemene maat van online slachtofferschap.

2 Het verzenden of ontvangen van seksueel getinte beelden of tekstberichten door middel van een mobiele telefoon of internetapplicaties.

1.4.4 Vergelijking met offline slachtofferschap

Tot slot zal in deze studie de vergelijking worden gemaakt tussen de risicofactoren van online en offline slachtofferschap om verschillen en overeenkomsten in beide typen slachtofferschap vast te stellen. Door de link met 'oude' criminaliteit te leggen, kan worden nagegaan in hoeverre er sprake is van een nieuwe groep slachtoffers, met mogelijk andere kenmerken en andere reacties op slachtofferschap. Het kan ook zo zijn dat online criminaliteit zich voordoet bij hen die ook al offline slachtofferschap hebben ervaren.

1.5 Gevolgen van online slachtofferschap

Vanuit de victimologie zijn er veel aanknopingspunten dat offline slachtofferschap negatieve repercussies kan hebben op diverse leefgebieden, zoals mentale gezondheid en angst voor criminaliteit (Lamet & Wittebrood, 2009; Turanovic & Pratt, 2012). In dit rapport is gekeken in hoeverre dit ook van toepassing is op online slachtofferschap. Aan de hand van de panelgegevens kan worden onderzocht of het hebben van een slachtofferervaring samenhangt met een verandering in de mentale gezondheid. Daarnaast wordt ingegaan op een mogelijke verandering in internetgebruik en beveiligingsgedrag. De onderzoeksvraag met betrekking tot gevolgen van online slachtofferschap luidt: *in hoeverre heeft online slachtofferschap gevolgen voor angst voor online criminaliteit, internetgebruik, beschermingsmaatregelen en mentale gezondheidsproblemen?*

1.5.1 Angst voor online criminaliteit, internetgebruik en beschermingsmaatregelen

Een van de mogelijke gevolgen van online slachtofferschap is toegenomen angst voor online criminaliteit. Het bestuderen van angst voor online criminaliteit kan beter zicht geven in de gemoedstoestand van slachtoffers. Daarnaast kan een toename in deze angst gepaard gaan met het mijden van het internet. In een steeds meer gedigitaliseerde samenleving is het van belang om hier inzicht in te hebben. Uit een aantal longitudinale studies blijkt dat reacties van offline slachtoffers soms gericht zijn op gelegenheidsbeperking, zoals minder uitgaan of 's avonds de straat op gaan (Averdijk, 2010; Skogan, 1987), het nemen van beschermingsmaatregelen (Skogan, 1987) of zelfs verhuizen naar een andere buurt (Dugan, 1999; Xie & McDowall, 2008). Het is mogelijk dat slachtoffers van online criminaliteit zichzelf ook gelegenheidsbeperking opleggen door minder internet te gaan gebruiken, en zich beter wapenen tegen een mogelijke slachtofferervaring door het nemen van beschermingsmaatregelen. Een longitudinaal onderzoek naar financiële online delicten laat echter zien dat slachtoffers van identiteitsfraude hun online gedrag (online bankieren en winkelen) na het delict niet of nauwelijks bijstellen, ook de slachtoffers die de schade niet vergoed kregen doen dit niet (Van Wilsem, 2017). Zoals eerder vermeld, worden internetgebruik en beschermingsmaatregelen onderzocht als zogenoemde risicofactoren voor online criminaliteit. Aan de hand van de panelgegevens is het interessant om deze factoren ook te beschouwen als mogelijke gevolgen. Sommige studies suggereren dat degenen die zich beter hebben beschermd juist een hoger risico lopen op slachtofferschap (Bossler et al., 2011; Holt & Bossler, 2013) – wat een indicatie kan zijn voor omgekeerde causaliteit: door slachtofferschap gaat men zich beter beveiligen. Door de veranderingen binnen personen chronologisch te onderzoeken, waarbij wordt gekeken of en wanneer slachtoffers hun beschermingsmaatregelen aanpassen, kan een stap worden gezet om deze puzzel omtrent de causaliteit te ontrafelen.

1.5.2 Mentale gezondheid

Er is een beperkte hoeveelheid studies die ingaat op de gevolgen van online slachtofferschap voor de mentale gezondheid. Verschillende onderzoeken gaan in op de gevolgen van cyberpesten (pesten op internet of via een mobiele telefoon) onder scholieren. Hieruit blijkt dat het ondergaan van online pestervaringen gepaard gaat met gevoelens van depressie, zelfmoordintenties, meer middelengebruik en riskant internetgedrag (Gamez-Guadix, Orue, Smith & Calvete, 2013; Sampasa-Kanyinga, Roumeliotis & Xu, 2014). Daarnaast vonden Wright en Li (2013) in een longitudinale studie dat online belediging en bedreiging door *peers* samengaat met het zelf meer uiten van agressieve online berichten. In de studie van Worsley, Wheatcroft, Short & Corcoran (2017) wordt uit interviews met slachtoffers van online stalking afgeleid dat de gebeurtenissen vaak samengaan met angst, depressie, het reduceren van het aantal werkuren en zelfs stoppen met werk en het aanpassen van de dagelijkse routines. De Amerikaanse studie van Golladay en Holtfreter (2016) onder slachtoffers van identiteitsfraude wijst uit dat emotionele en fysieke problemen meer voorkomen naarmate men vaker met identiteitsfraude te maken heeft gehad. Binnen deze groep zijn emotionele problemen ook groter naarmate het schadebedrag van de geleden fraude(s) hoger is.

Ook kwalitatieve studies over online oplichting en fraude wijzen uit dat er, naast de geleden financiële schade, sprake is van (soms aanzienlijke) emotionele schade, die in bepaalde gevallen ook langdurig aan kan houden (Cross, Richards & Smith, 2016; Jansen & Leukfeldt, 2018). In de studie van Jansen en Leukfeldt (2018) naar online fraude wordt de mate waarin het delict een emotionele impact heeft deels afhankelijk geacht van negatieve gebeurtenissen voorafgaand aan slachtofferschap (zoals een scheiding of het overlijden van de partner). Een deel van de slachtoffers probeerde het voorval te rationaliseren (i.e. waarom het plaats had gevonden) of cognitief te neutraliseren door aan te geven dat het ook erger had kunnen uitpakken. In onderzoek naar zogenaamde *romance scams*[3] rapporteren Whitty en Buchanan (2015) dat hierbij vaak sprake is van een *double hit*: naast geleden financieel verlies blijkt de oplichter niet de gehoopte (online) geliefde.

Leukfeldt, Notté & Malsch (2018) onderzochten de ondersteuningsbehoeften van slachtoffers die zich bij instanties melden, zoals bij de politie, de Fraudehelpdesk of Slachtofferhulp Nederland, op basis van interviews met 19 slachtoffers van verschillende typen online criminaliteit. Naast een aantal behoeften die overeen lijken te komen met die van slachtoffers van offline criminaliteit – zoals behoefte aan informatie, emotionele ondersteuning en vergelding – geven Leukfeldt et al. (2018) aan dat de impact bij online delicten in sommige gevallen extra vergroot wordt door aspecten die inherent zijn aan het cyberdomein, zoals de schaal waarop belastende informatie kan worden gedeeld (bij bijvoorbeeld sexting), de moeilijkheid van het verwijderen van online materiaal (waardoor het slachtofferschap kan blijven voortduren), de onbekendheid van de dader en de daarmee ervaren willekeur in het slachtoffer-zijn (bijvoorbeeld bij gehackt worden of *ransomware*[4]) en het niet kunnen opzoeken van een veilige plek (omdat ook thuis de online bedreiging door

3 Een *romance scam* is het oplichten van een slachtoffer door hem of haar verliefd te laten worden op de oplichter of door het slachtoffer (valse) hoop te geven op een liefdesrelatie; ook wel bekend als datingfraude.

4 *Ransomware* is software die een computer en/of bestanden op de computer blokkeert en van de gebruiker losgeld vraagt om weer toegang te krijgen tot de bestanden.

blijft gaan). In het huidige onderzoek wordt bekeken of de bevindingen uit het kwalitatieve onderzoek van Leukfeldt et al. (2018) ook gelden voor een representatieve steekproef van de Nederlandse bevolking.
In dit rapport zal tevens worden onderzocht of slachtoffers van online criminaliteit die hiervan aangifte hebben gedaan andere gevolgen ervaren dan slachtoffers die geen aangifte hebben gedaan. Zo kan de politie wijzen op het belang van beschermingsmaatregelen. Daarnaast kan het doen van aangifte en bijbehorende vervolging en vergelding van de dader een positieve uitwerking hebben op de mentale gezondheid van het slachtoffer. In het onderzoek van Leukfeldt et al. (2018) voldeed de politie echter niet in alle gevallen aan de informatie- en vergeldingsbehoeften van slachtoffers, wat juist negatieve gevolgen kan hebben voor de mentale gezondheid.

1.6 Herhaald online slachtofferschap

Nadat mogelijke risicofactoren en gevolgen van online slachtofferschap in kaart zijn gebracht, zal tot slot worden onderzocht in hoeverre slachtoffers na hun slachtoffer-ervaring opnieuw slachtoffer zijn geworden. Vanuit het oogpunt van slachtofferbeleid is het relevant om te weten of er een bepaalde groep is die steeds opnieuw in aanraking komt met online criminaliteit. De laatste onderzoeksvraag is dan ook: *in welke mate is er sprake van herhaald slachtofferschap, en in welke mate vormen de mogelijke gevolgen van online slachtofferschap een risicofactor voor herhaald slachtofferschap?*

1.6.1 Prevalentie van herhaald online slachtofferschap

Door gebruik te maken van longitudinale gegevens uit een grootschalige slachtofferenquête onder de algemene bevolking -het LISS-panel- en daarmee respondenten over een langere tijd te volgen, is het beter mogelijk om meer zicht te krijgen op cumulatie van slachtofferervaringen. Daarmee wordt ook duidelijker op welke manier online slachtofferschap een maatschappelijk en beleidsmatig probleem vormt: is het bijvoorbeeld een verschijnsel dat een bepaalde groep mensen eenmalig treft of is er sprake van concentratie van slachtofferschap, waarbij er naast eenmalige slachtoffers ook groepen mensen zijn die herhaald en wellicht meervoudig slachtofferschap ervaren? In het gangbare cross-sectionele slachtofferonderzoek wordt onderzoek naar herhaald slachtofferschap uitgevoerd binnen een beperkte tijdsspanne, vaak van een jaar. Omdat slachtofferschap een relatief zeldzame gebeurtenis is (en herhaald slachtofferschap des te meer), is de gevonden mate van herhaald slachtofferschap in korte-termijn-studies dan ook vaak beperkt. Door mensen over een langere periode te volgen – in dit geval over een periode van tien jaar – is het mogelijk beter zicht te krijgen op een eventuele stapeling van slachtofferervaringen. In het huidige onderzoek wordt iemand beschouwd als herhaald slachtoffer van online criminaliteit als hij of zij: meer dan één keer van hetzelfde online delict slachtoffer is geworden (1) of één (of meer) keer slachtoffer is geworden van meer dan één delict (2). De eerste groep wordt in de literatuur doorgaans aangeduid als herhaald slachtoffer, terwijl de tweede groep wordt aangeduid als meervoudig slachtoffer. Voor beide groepen geldt dat ze meer dan één keer slachtoffer zijn geworden van online criminaliteit.

1.6.2 Risicofactoren voor herhaald online slachtofferschap

In de literatuur naar de risicofactoren van herhaald slachtofferschap worden twee stromingen onderscheiden (Van Reemst et al., 2013). Volgens de eerste stroming kunnen risicofactoren voor slachtofferschap in algemene zin ook de kans op herhaald slachtofferschap verklaren. Als mannen en jongeren een grotere kans hebben om een eerste keer slachtoffer te worden van een online delict, bijvoorbeeld omdat ze meer internet gebruiken, zullen ze om dezelfde reden ook een grotere kans hebben om een tweede keer slachtoffer te worden. Daarnaast kunnen risicofactoren van slachtofferschap samenhangen met de manier hoe mensen reageren op een slachtofferervaring (Schreck, Stewart & Fisher, 2006). De slachtoffers die opnieuw slachtoffer zijn geworden, hebben hun gedrag mogelijk in mindere mate aangepast naar aanleiding van hun eerdere slachtofferervaring dan slachtoffers die niet opnieuw slachtoffer zijn geworden. In dat licht is impulsiviteit wederom een relevant aspect. Impulsieve mensen handelen eerder zonder na te denken over de mogelijke gevolgen van hun handelen, waardoor de kans op herhaald slachtofferschap wordt vergroot. Als iemand slachtoffer is geweest van een bepaald online delict, is men zeer waarschijnlijk meer bewust van de mogelijke gevolgen. Verwacht kan worden dat minder impulsieve mensen in hun handelen meer rekening houden met deze gevolgen dan impulsieve mensen. Dit zal worden onderzocht door de te kijken of bepaalde sociaal-demografische en persoonlijkheidskenmerken invloed hebben op de kans om herhaald slachtoffer te worden.

Volgens een tweede stroming in de literatuur kan de slachtofferervaring *zelf* leiden tot een vergrote kans om nog een keer slachtoffer te worden (Wittebrood, 2006). Uit eerder onderzoek is gebleken dat het gevolg van een offline slachtofferervaring, zoals een afname in mentaal welbevinden, vervolgens weer invloed kan hebben op de kans om opnieuw slachtoffer te worden (Ousey et al., 2008; Schreck et al., 2006; Turanovic & Pratt, 2012; Wittebrood & Nieuwbeerta, 2000). De vraag is of de gevolgen van online slachtofferschap ook een risicofactor voor herhaald online slachtofferschap vormen. In dit onderzoek is meer inzicht in deze dynamische factoren voor herhaald online slachtofferschap gegeven door de bevindingen met betrekking tot de eerder besproken risicofactoren en gevolgen te combineren.

1.7 Leeswijzer

In hoofdstuk 2 beschrijven we de onderzoeksmethoden van het onderzoek. Hierin wordt dieper ingegaan op de databron, de gebruikte operationalisaties en de gehanteerde methoden en analyses. In hoofdstuk 3 worden de resultaten van het empirisch onderzoek beschreven. In hoofdstuk 4 wordt op basis van de resultaten een antwoord geformuleerd op elke deelvraag en een algehele conclusie gegeven. Tevens worden de sterke punten en beperkingen van deze studie besproken, en wordt vooruitgeblikt op mogelijk relevante onderzoeksvragen voor vervolgonderzoek.

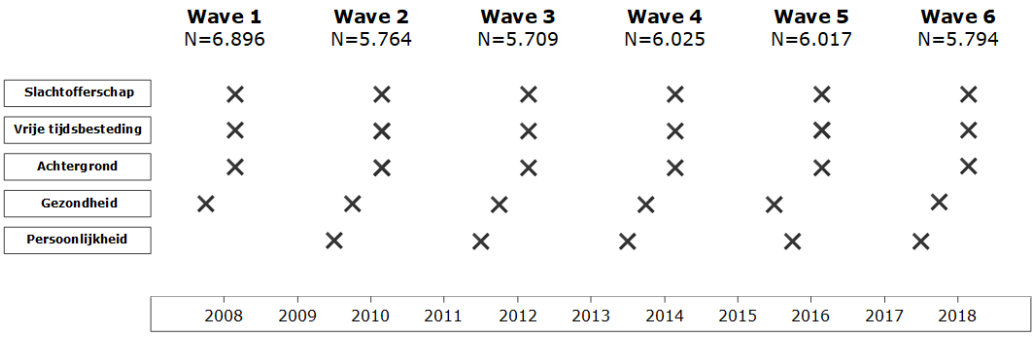
2 Onderzoeksmethoden

In dit hoofdstuk beschrijven we de methoden van het onderzoek. De studie omvat een empirisch onderzoek met een longitudinaal design.

2.1 LISS-panel

In deze studie zijn gegevens gebruikt uit zes metingen van het LISS-panel die tussen 2008 en 2018 zijn verricht.[5] Het LISS-panel is een door het Tilburgse onderzoeksbureau CentERdata opgezette online dataverzameling onder Nederlandse huishoudens, dat in 2007 van start ging en tot op heden doorloopt. Het panel is gebaseerd op een gerandomiseerde steekproef uit de Basisregistratie Personen (BRP). Huishoudens zonder computer krijgen voor de duur van het onderzoek een eenvoudige pc toegewezen voor hun medewerking aan het panel. Er wordt gebruikgemaakt van zelfrapportage, waarbij panelleden per maand een wisselende vragenlijst invullen, over onder andere hun vrijetijdsbesteding, achtergrondkenmerken, gezondheid en persoonlijkheid.[6] Sinds februari 2008 heeft eens in de twee jaar ook een uitgebreide slachtofferenquête plaatsgevonden, waarin respondenten zijn gevraagd naar slachtofferervaringen van diverse vormen van offline en online criminaliteit. Inmiddels is er sprake van zes *waves* (meetmomenten) tussen 2008 en 2018, waarbij iedere keer vijf- à zesduizend respondenten hebben meegewerkt. Figuur 1 geeft een overzicht van de waves en de vragenlijsten die zijn meegenomen in het huidige onderzoek.

Figuur 1 Overzicht van waves binnen het LISS-panel



2.1.1 Respons en non-respons

De respons van de slachtofferenquête is over de zes waves gemiddeld genomen 84,5%. Er zijn 13.430 unieke respondenten die sinds 2008 ten minste eenmaal hebben deelgenomen aan de slachtofferenquête. Van deze groep respondenten nam per meetmoment gemiddeld 48,9% deel. In figuur 1 is het aantal respondenten per

5 Meer informatie over het LISS-panel is te vinden op www.lissdata.nl.

6 In wave 5 is de vragenlijst over gezondheid eerder afgenomen dan gebruikelijk (juli-augustus in plaats van november-december), en de vragenlijst over persoonlijkheid later afgenomen dan gebruikelijk (november-december in plaats van mei-juni). Het verschil in timing leverde geen andere uitkomsten op voor de analyses waar deze vragenlijsten voor zijn gebruikt.

wave weergegeven. Van alle panelleden hebben 1.807 respondenten (13,5%) aan alle zes waves deelgenomen. De non-respons in het LISS-panel is tweedelig: naast de gebruikelijke non-respons per wave, is er ook sprake van uitval van panelleden (dat wil zeggen respondenten die niet aan volgende waves deelnemen). Om deze structurele uitval op te vangen, is het LISS-panel meermalig aangevuld met nieuwe panelleden (Lugtig, Das & Scherpenzeel, 2014). Om ook in de latere waves zorg te dragen voor een representatieve steekproef, is het panel onder andere aangevuld met jonge respondenten. De respondenten die deelnamen waren ouder en vaker man dan degenen die niet (meer) deelnamen. Daarnaast waren uitvallers impulsiever dan deelnemers en namen slachtoffers van online criminaliteit minder vaak deel aan volgende waves dan degenen die geen slachtoffer waren (bijlage 2, tabel b1 t/m b4). In het LISS-panel is dus sprake van selectieve non-respons, waarbij met name het lagere responspercentage van online slachtoffers suggereert dat – als er al een effect van deze non-respons is – er waarschijnlijk sprake is van een onderschatting van (herhaald) online slachtofferschap. Om in dit onderzoek rekening te houden met de non-respons, is de data op basis van leeftijd, geslacht en opleidingsniveau gewogen naar de Nederlandse populatie van 16 jaar en ouder (zie paragraaf 2.3.1). Vanwege de aanwas van nieuwe panelleden is voor elke wave een afzonderlijk weegmodel toegepast.

2.2 Operationalisatie

2.2.1 Slachtofferschap van online criminaliteit

In dit rapport staat slachtofferschap van online criminaliteit centraal. Om de frequentie van slachtofferschap te meten, kregen respondenten van het LISS-panel een serie uiteenlopende online delicten voorgelegd. Vervolgens werd gevraagd of de respondenten voor die delicten konden aangeven of ze er de afgelopen twee jaar slachtoffer van waren geweest. De typen delicten zijn weergegeven in tabel 1. Aan respondenten die aangaven in de afgelopen twee jaar slachtoffer te zijn geweest van een van deze online delicten, werd gevraagd hoe vaak dit in het afgelopen jaar gebeurde. De prevalentie van slachtofferschap is gebaseerd op dezelfde vragen. Als respondenten op tenminste één van deze delicten één of meerdere keren aangeven in het afgelopen jaar slachtoffer te zijn geworden, zijn ze beschouwd als slachtoffer

Tabel 1 Vraagstelling online slachtofferschap LISS-panel

Delict	Vraagstelling
Creditcard fraude	Uw creditcardnummer werd achterhaald en, buiten uw medeweten, gebruikt voor een aankoop
Hacken	Anderen verschaften zich zonder toestemming toegang tot uw computer ('hacken')
Online aankoopfraude	U deed een aankoop via internet, en ontving geen product
Online bedreiging	Bedreiging via social media (bijv. Facebook, Twitter, Instagram), e-mail, WhatsApp of een ander digitaal kanaal
Virus	Uw computer werd getroffen door een virus dat schade veroorzaakte, bijvoorbeeld doordat bestanden op de harde schijf werden gewist of versleuteld
Afschrijving bankrekening	Er is geld van de bankrekening afgeschreven zonder dat u daar toestemming voor had gegeven
Identiteitsfraude	Iemand heeft uw persoonlijke gegevens gebruikt voor identiteitsfraude (bv. doordat iemand zich voor u uitgaf na het begaan van een overtreding, bij het gebruikmaken van medische zorg, of de aanvraag van een hypotheek)

van online criminaliteit. Als respondenten van geen enkel delict aangeven slachtoffer te zijn geweest, zijn ze beschouwd als niet-slachtoffer.[7] Daarnaast is in sommige analyses ook slachtofferschap voor de verschillende typen delicten afzonderlijk meegenomen (zie paragraaf 2.3).

Om de variabele voor herhaald online slachtofferschap te construeren, is de dataset anders vormgegeven dan voor de meting van online slachtofferschap. Voor de algemene meting van online slachtofferschap is de dataset per meetmoment vormgegeven, wat betekent dat één respondent meerdere keren in de dataset te vinden is (*long file*). In de dataset om herhaald slachtofferschap in kaart te brengen is de dataset per respondent vormgegeven (*wide file*). Vervolgens zijn per respondent het totale aantal online slachtofferervaringen van alle meetmomenten tezamen bij elkaar opgeteld. Als iemand meer dan één keer slachtoffer is geworden, wordt die beschouwd als herhaald slachtoffer. Dit betekent dat iemand als herhaald slachtoffer wordt gezien als hij of zij: meer dan één keer van hetzelfde online delict slachtoffer is geworden of één (of meer) keer slachtoffer is geworden van meer dan één delict. Deze herhaalde slachtofferervaringen kunnen zowel binnen één meetmoment als op meerdere meetmomenten hebben plaatsgevonden. De variabele voor herhaald slachtofferschap bestaat uit de volgende subgroepen: geen slachtoffer (1), eenmalig slachtoffer (2), en herhaald slachtoffer (3). Vervolgens is gekeken of er zogenoemde *supertargets* bestaan door binnen de groep van herhaald slachtoffers de frequentie van herhaald slachtofferschap te meten aan de hand van het totale aantal online slachtofferervaringen.

In dit rapport is ook de vergelijking met slachtoffers van offline criminaliteit gemaakt. Slachtofferschap van offline criminaliteit is op dezelfde manier bevraagd als slachtofferschap van online criminaliteit, maar dan op basis van de volgende offline delicten: inbraak of poging tot inbraak, diefstal uit auto, diefstal van portemonnee, tas of ander privébezit, vernieling van auto of ander privébezit, bedreiging, mishandeling waarna doktersbezoek noodzakelijk was, mishandeling zonder doktersbezoek.

Bij slachtoffers van online bedreiging, online aankoopfraude en ongeautoriseerde bankafschrijving is doorgevraagd naar de ernst van het delict. Om de ernst van online bedreiging te meten, is gevraagd hoe ernstig ze de bedreiging hebben ervaren, met als mogelijke antwoordcategorieën niet zo ernstig (1), redelijk ernstig (2) en bijzonder ernstig (3). De ernst van online aankoopfraude en de ernst van ongeautoriseerde bankafschrijving is gemeten aan de hand van de financiële schade in euro's. Aan slachtoffers van online bedreiging, online aankoopfraude, ongeautoriseerde bankafschrijvingen en identiteitsfraude is tevens doorgevraagd naar de genomen vervolgstappen, zoals het doen van aangifte bij de politie. Aan de hand van deze vraag is de variabele aangifte door online slachtoffers geconstrueerd, bestaande uit de volgende categorieën geen slachtoffer (1), slachtoffer, geen aangifte gedaan (2) en slachtoffer, wel aangifte gedaan (3).

2.2.2 Internetgebruik, beschermingsmaatregelen en angst voor criminaliteit

Het internetgebruik van respondenten is in kaart gebracht door te vragen naar het aantal uren dat respondenten per week thuis op het internet doorbrengen. Vanaf

7 Door eerst te vragen naar slachtofferschap over een ruimere referentieperiode (de afgelopen twee jaar) en pas daarna over de eigenlijke referentieperiode (de afgelopen twaalf maanden), kon de kwaliteit van de retrospectieve gegevens positief worden beïnvloed. Tevens is een extra controle ingevoerd door eerst naar de prevalentie en daarna naar de incidentie van slachtofferervaringen te vragen.

2012 is deze vraag opgesplitst naar internetgebruik op computer of laptop, smartphone en tablet. We meten daarom het internetgebruik in 2008 en 2010 op basis van de algemene vraag hoeveel uur respondenten thuis internet gebruiken, en vanaf 2012 op basis van een somscore op de drie vragen over hoeveel uur respondenten thuis internet gebruiken op hun computer of laptop, smartphone en tablet. Somscores hoger dan 168 uur per week zijn afgekapt op 168 uur, omdat een week uit 168 uur bestaat. De range van het aantal uur loopt daarmee van nul uur (bijvoorbeeld respondenten die geen toegang hebben tot internet) tot 168 uur.

Naast het aantal uren dat respondenten zich op internet begeven, bestuderen we ook de mate van getroffen beschermingsmaartregelen om hun privé-computer te beschermen.[8] Er is aan respondenten gevraagd of ze de volgende zes maatregelen hebben getroffen: firewall, virus-scanner, anti-spyware, trojan-scanner, spam-filter en beveiliging draadloos netwerk. Deze maatregelen zijn voornamelijk relevant om te beschermen tegen slachtofferschap van een computervirus en minder relevant voor bijvoorbeeld online bedreiging en online aankoopfraude. Bij elk type beschermingsmaatregel is uitleg gegeven over wat het precies inhoudt. Vervolgens zijn al deze maatregelen bij elkaar opgeteld. De range loopt van 0 beschermingsmaatregelen tot maximaal 6 beschermingsmaatregelen. Hoe hoger de score, des te meer beschermingsmaatregelen de respondent heeft getroffen.

Op basis van zeven items zijn respondenten bevraagd over hun angst voor online criminaliteit. Deze items hebben betrekking op angst voor creditcardfraude, online aankoopfraude, hacken en computervirussen. Uit een factoranalyse is gebleken dat zes van de zeven items hetzelfde onderliggende construct meten (bijlage 2, tabel b5). Alleen het item 'ik controleer de computer vaak op de aanwezigheid van virussen' laadt laag op de eerste factor (factorlading < 0,3). Om die reden is dit item niet in de uiteindelijke schaal meegenomen. Het item 'ik ben bang dat er een keer wordt ingebroken op mijn computer' heeft een hoge factorlading op beide factoren. Aangezien we slechts één schaal construeerden, is dit item wel meegenomen. Van de zes items is een schaal geconstrueerd op basis van het gemiddelde die loopt van weinig angst (1) tot veel angst (5). Respondenten moesten op tenminste vier van de zes items een geldige score hebben, anders werd hun score niet meegenomen. De Cronbach's alpha per wave ligt tussen de 0,83 en 0,85, waarbij een $\alpha \geq 0{,}70$ aangeeft dat de constructen op betrouwbare wijze zijn gemeten.

2.2.3 Persoonskenmerken

De sociaal-demografische variabelen die zijn meegenomen als mogelijke risicofactor zijn leeftijd, geslacht en opleidingsniveau. Deze kenmerken zijn bevraagd in een doorlopende vragenlijst naar achtergrondkenmerken en zijn gemeten op hetzelfde moment als de rest van de vragen. Leeftijd van respondenten is gemeten in jaren. De jongste persoon die heeft deelgenomen is 16 jaar en de oudste persoon is 100 jaar oud. Geslacht bestaat uit de categorieën man (1) en vrouw (2). Opleidingsniveau is gebaseerd op het hoogst genoten opleidingsniveau dat is afgesloten met een diploma en bestaat uit de volgende categorieën: basisonderwijs (1), mavo/vmbo (2), havo/vwo (3), mbo (4), hbo (5) en wo (6).

Impulsiviteit van respondenten is gemeten aan de hand van dysfunctionele impulsiviteit van de Dickman Impulsivity Inventory (Dickman, 1990). Aan respondenten zijn 12 stellingen voorgelegd, waarmee zij het ofwel oneens (0), ofwel eens (1)

8 Er is niet gevraagd of respondenten maatregelen hebben genomen om hun tablet en smartphone te beschermen.

konden zijn. Deze items zijn zo gecodeerd dat een hogere score, een hogere mate van impulsiviteit weergeeft. Voor respondenten die op tenminste zeven items een geldige score hebben gerapporteerd, is een schaal geconstrueerd op basis van het gemiddelde (Cronbach's alpha = 0,74).

De Big Five persoonlijkheidskenmerken zijn gemeten met behulp van 60 stellingen uit de gevalideerde NEO-FFI-3 vragenlijst (Hoekstra & De Fruyt, 2014). In tegenstelling tot de items over impulsiviteit – die wel in de slachtofferenquête zijn opgenomen – komen deze stellingen uit een aparte vragenlijst. Deze vragenlijst is negen maanden voor de slachtofferenquête afgenomen. De vijf persoonlijkheidsdomeinen zijn: extraversie, altruïsme, consciëntieusheid, emotionele stabiliteit en openheid (Goldberg, 1993).

Per persoonlijkheidsdomein zijn de gebruikte stellingen weergegeven in bijlage 2, tabel b6. Respondenten konden op een vijfpuntsschaal van helemaal mee oneens (1) tot helemaal mee eens (5) aangeven in hoeverre de stelling op hen van toepassing was. De items zijn zo gecodeerd dat een hogere itemscore staat voor een hogere score op het betreffende domein. Respondenten moesten op tenminste acht van de tien items een geldige score hebben. Per domein zijn de items opgeteld tot domeinscores. De Cronbach's alpha per wave van de persoonlijkheidsdomeinen varieert tussen de 0,86 en 0,87 voor extraversie, 0,81 en 0,82 voor altruïsme, 0,77 en 0,81 voor consciëntieusheid, 0,88 en 0,90 voor emotionele stabiliteit en 0,76 en 0,79 voor openheid, wat aangeeft dat de interne consistentie van deze schalen goed is.

2.2.4 Gezondheid

Aan de hand van de jaarlijkse vragenlijsten over gezondheid is de mentale gezondheid van respondenten in kaart gebracht. Aan respondenten zijn vijf vragen voorgelegd die samen de *Mental Health Index* vormen (MHI-5, Berwick et al., 1991). Er is aan respondenten gevraagd of ze in de afgelopen maand het volgende hebben ervaren: 'was ik erg zenuwachtig', 'zat ik zo erg in de put dat niets mij kon opvrolijken', 'voelde ik me kalm en rustig', 'voelde ik me neerslachtig en somber' en 'voelde ik me gelukkig'. De antwoordmogelijkheden zijn: nooit (1), zelden (2), soms (3), vaak (4), meestal (5) en altijd (6). De items zijn zo gecodeerd dat een hogere score een betere mentale gezondheid aangeeft. Vervolgens is een schaal berekend op basis van het gemiddelde op alle vijf de items. De Cronbach's alpha van deze schaal varieert per wave tussen de 0,83 en 0,86.

Deze items zijn afkomstig van een aparte vragenlijst waaraan niet alle respondenten hebben meegedaan. Ongeveer 13% van de respondenten die wel aan de slachtofferenquête hebben meegedaan, hebben niet aan de gezondheidsenquête meegedaan. De analyses waarin mentale gezondheid wordt meegenomen, bestaan daarom uit een lager aantal respondenten. Bovendien zijn deze items drie maanden voor de slachtofferenquête gemeten. Om te controleren of dit de resultaten beïnvloedt, is gekeken of de bevindingen veranderen als de gezondheidsenquêtes die negen maanden na de slachtofferenquêtes zijn afgenomen worden gebruikt.

2.2.5 Controlevariabelen

In de analyses zijn leeftijd, geslacht en opleidingsniveau ook meegenomen als controlevariabelen die mogelijk invloed hebben op slachtofferschap of samenhangen met de andere variabelen in het analytische model. Daarnaast zijn twee variabelen

die de huishoudsamenstelling representeren meegenomen als controlevariabelen. Het aantal kinderen is gebaseerd op het aantal thuiswonende kinderen, en loopt van nul tot acht kinderen. Kinderen zijn mogelijk onzorgvuldiger op internet en de aanwezigheid van kinderen in het huishouden kan de kans op slachtofferschap van bijvoorbeeld een computervirus vergroten. Daarnaast kan het krijgen of verliezen van een kind een impact hebben op de mentale gezondheid. Het is relevant om hiervoor te controleren als we de mogelijke impact van slachtofferschap op mentale gezondheid onderzoeken. Hetzelfde geldt voor het al dan niet hebben van een partner. Daarnaast wordt ook stedelijkheid van de woonplaats meegenomen, omdat dit een belangrijke voorspeller is van slachtofferschap van offline criminaliteit (Kalidien, 2018). Het is interessant om te zien in hoeverre stedelijkheid samenhangt met slachtofferschap van online criminaliteit. Stedelijkheid is gebaseerd op de dichtheid van de adressen per km^2 (de omgevingsadressendichtheid) van iemands leefomgeving, zoals vastgesteld door het CBS, en kent de volgende categorieën: niet stedelijk: minder dan 500 adressen per km^2 (1), weinig stedelijk: 500 tot 1.000 adressen per km^2 (2), matig stedelijk: 1.000 tot 1.500 adressen per km^2 (3), sterk stedelijk: 1.500 tot 2.500 adressen per km^2 (4) en zeer sterk stedelijk: 2.500 of meer adressen per km^2 (5).

2.3 Analyses

Ter beantwoording van de onderzoeksvragen zijn verschillende statistische analyses toegepast. In deze paragraaf worden de analyses per onderzoeksvraag toegelicht.

2.3.1 Trends in slachtofferschap van online criminaliteit

Om in kaart te brengen in welke mate Nederlandse burgers slachtofferschap van online criminaliteit ervaren, is de prevalentie van online slachtofferschap vastgesteld in de periode van 2010 tot 2018.[9] De prevalentie van online slachtofferschap is zowel voor alle typen delicten gezamenlijk als per delict afzonderlijk weergegeven. Om te toetsen of de prevalentie van slachtofferschap na verloop van tijd significant is toegenomen of afgenomen, zijn logistische regressieanalyses gebruikt. Vervolgens zijn per delict, voor zover bekend, de ervaren ernst, geleden financiële schade en de genomen vervolgstappen, zoals de aangiftebereidheid, bepaald. Daarnaast is de prevalentie van online slachtofferschap vergeleken met de prevalentie van offline slachtofferschap om de resultaten in perspectief te kunnen plaatsen.

Bij het beantwoorden van deze eerste onderzoeksvraag is rekening gehouden met de non-respons, om de uitkomsten zo representatief mogelijk te houden voor de Nederlandse populatie, door alle gegevens op basis van leeftijd, geslacht en opleidingsniveau te wegen naar de Nederlandse populatie van 16 jaar en ouder. Hiervoor is de leeftijd van de respondenten opgesplitst in categorieën van vijf jaar, met uitzondering van de eerste categorie (16 tot 20 jaar) en de laatste categorie (75 jaar en ouder). Om de weegfactor te bepalen is opleidingsniveau in plaats van de eerdergenoemde zes categorieën verdeeld in vijf categorieën, overeenkomstig

9 In 2008 was de vraagstelling verschillend ten opzichte van de latere waves; i.e. in 2008 is ter referentie als startvraag gevraagd of de respondent *ooit* slachtoffer is geweest en in de waves daarna of de respondent *in de afgelopen twee jaar* slachtoffer is geweest. Hoewel in alle waves uiteindelijk is gevraagd naar slachtofferschap in de afgelopen twaalf maanden, kunnen de antwoorden mogelijk beïnvloed zijn door de vraagstelling en referentieperiode van de startvraag (Lamet & Wittebrood, 2009).Om die reden worden de trends van slachtofferschap over tijd weergegeven van 2010 tot 2018, waarin de vraagstelling gelijk was.

met de CBS categorieën (basisonderwijs, vmbo, havo/vwo, mbo en hbo/wo). Vanwege de aanwas van nieuwe panelleden is voor elke wave een afzonderlijk weegmodel toegepast. Dat wil zeggen dat voor elke wave afzonderlijk een ratio is bepaald van het aantal respondenten in de genoemde categorieën van leeftijd, geslacht en opleidingsniveau in het LISS-panel ten opzichte van het aantal personen in diezelfde categorieën in de Nederlandse populatie van 16 jaar en ouder in datzelfde jaar. Hierdoor zijn de gepresenteerde trends in cyber- en gedigitaliseerde criminaliteit representatief voor de gehele Nederlandse populatie van 16 jaar en ouder.

2.3.2 Risicofactoren voor online slachtofferschap

Om risicofactoren voor online slachtofferschap vast te stellen in een groep respondenten die meerdere malen zijn bevraagd naar hun slachtofferervaringen, zijn zogenoemde multilevel analyses gebruikt, waarbij tijdsmomenten zijn genest in respondenten. Deze methode is geschikt voor het analyseren van longitudinale cohorten, omdat ook de respondenten die niet in alle waves hebben deelgenomen, kunnen worden meegenomen in de analyses. Specifiek zijn zogenoemde mixed effect modellen gebruikt, waarmee het effect van de risicofactoren op de prevalentie van slachtofferschap kan worden bepaald, terwijl rekening wordt gehouden met individuele verschillen.

Als afhankelijke variabele is hierin de prevalentie van online slachtofferschap meegenomen. Daarnaast zijn de volgende onafhankelijke variabelen meegenomen: eerder online slachtofferschap (zoals aangegeven in de voorgaande wave), internetgebruik, beschermingsmaatregelen, leeftijd, geslacht, opleiding, impulsiviteit, extraversie, altruïsme, consciëntieusheid, emotionele stabiliteit en openheid. Aanvullend zijn de achtergrondkenmerken leeftijd, geslacht, opleiding en aantal kinderen in alle modellen als controlevariabelen toegevoegd. Tot slot zijn de risicofactoren voor online slachtofferschap vergeleken met de risicofactoren voor offline slachtofferschap. Daarbij is ook stedelijkheid als controlevariabele toegevoegd. Buitenom geslacht, leeftijd, opleidingsniveau en aantal kinderen, die over het algemeen minder over de tijd fluctueren, zijn risicofactoren gemeten voorafgaand aan de slachtofferervaring. Dit betekent dat respondenten aan tenminste twee opeenvolgende waves moeten hebben deelgenomen. Respondenten zijn niet meegenomen in de analyses als ze een missende waarde hebben op tenminste één van de in het model opgenomen variabelen.[10]

2.3.3 Gevolgen van online slachtofferschap

Om de gevolgen van slachtofferschap in kaart te brengen, zijn *fixed effects panel analyses* in Stata gebruikt. Hiermee wordt rekening gehouden met het dynamische perspectief van het LISS-panel, en kan worden geschat in hoeverre de prevalentie van slachtofferschap samengaat met een verandering in één van de volgende gevolgen: angst voor online criminaliteit, internetgebruik in uren per week, getroffen beschermingsmaatregelen en mentale gezondheid. Vervolgens is nagegaan of de

10 Voor de analyses zijn telkens zo veel mogelijk respondenten meegenomen: eerder slachtofferschap Nresp=6.623, Nobs=16.742; internetgebruik Nresp=12.322, Nobs=30.976; beschermingsmaatregelen Nresp=6.769, Nobs=16.949; persoonskenmerken & online slachtofferschap Nresp=6.336, Nobs=13.331; persoonskenmerken & offline slachtofferschap Nresp=6.392, Nobs=13.516; persoonskenmerken & online versus offline slachtofferschap Nresp=1.968, Nobs=2.394.

gevolgen sterker of zwakker waren voor slachtoffers die geen aangifte bij de politie hebben gedaan dan voor slachtoffers die wel aangifte hebben gedaan.

In *fixed effect panel analyses* wordt gekeken naar verandering *binnen* personen. Ter illustratie: voor respondenten die in 2012 aangaven in de afgelopen 12 maanden slachtoffer te zijn geweest van een online delict, is bestudeerd of ze in 2012 een slechtere mentale gezondheid rapporteerden dan in 2010. Door te kijken naar verschillen *binnen* personen, wordt rekening gehouden met alle tijds-constante variabelen, zoals geslacht. Verder is gecontroleerd voor periode, aantal kinderen en het al dan niet hebben van een partner. Alle respondenten die tenminste aan twee waves hebben meegedaan, zijn meegenomen in de analyses. Daarnaast dienen respondenten een geldige score te hebben op alle meegenomen variabelen, zodat elk model op dezelfde steekproef wordt berekend. In totaal zijn de gevolgen van slachtofferschap geanalyseerd voor 5.776 respondenten, met in totaal 20.222 observaties over alle waves.

2.3.4 Herhaald online slachtofferschap

Om de prevalentieschattingen van herhaald online slachtofferschap weer te geven, zijn de volgende categorieën onderscheiden: niet slachtoffers (1), eenmalig slachtoffers (2) en herhaald slachtoffers (3). Binnen de groep van herhaald slachtoffers is vervolgens nog een onderscheid gemaakt in herhaald slachtoffers van hetzelfde delict, herhaald slachtoffers van meerdere delicten (meervoudig slachtoffer) en zowel herhaald slachtoffer als meervoudig slachtoffers. Aangezien de kans op herhaald slachtofferschap groeit naarmate men vaker deelneemt aan de vragenlijst, zijn de prevalentieschattingen ook opgesplitst naar het aantal deelnames. De prevalenties zijn geschat op basis van 7.071 respondenten die tenminste twee keer hebben meegedaan.

Door middel van multinomiale logistische regressieanalyses is bestudeerd of achtergrondkenmerken (als leeftijd, geslacht en opleiding) en persoonlijkheidskenmerken (impulsiviteit, extraversie, altruïsme, consciëntieusheid, emotionele stabiliteit en openheid) invloed hebben op de kans om geen slachtoffer, eenmalig of herhaald slachtoffer te worden. Geslacht en opleiding zijn gemeten op het moment van de laatste deelname, terwijl leeftijd en de persoonlijkheidskenmerken zijn berekend op basis van het gemiddelde over verschillende deelnames. Of de risicofactoren verschillen voor herhaald en meervoudig slachtoffers, is in een robuustheidsanalyse met multinomiale logistische regressie getest. Ook is in deze robuustheidsanalyses onderzocht of er een verschil bestaat tussen de respondenten die op meerdere meetmomenten slachtoffer zijn geworden en respondenten die op slechts één meetmoment meerdere keren slachtoffer zijn geworden. Respondenten met een missende waarde op één van de in de analyses meegenomen variabelen zijn verwijderd uit de regressieanalyses. In totaal zijn de risicofactoren voor herhaald slachtofferschap voor 6.332 respondenten geanalyseerd.

Aanvullend is binnen de groep herhaald slachtoffers, bestaande uit 1.123 respondenten, gekeken of de persoons- en achtergrondkenmerken invloed hebben op het aantal slachtofferervaringen, om zogenoemde supertargets in kaart te brengen (Farrell, Clark, Ellingworth & Pease, 2005). Hierbij is gebruikgemaakt van een negatieve binomiale regressieanalyse waarmee rekening wordt gehouden met de scheve verdeling van het aantal slachtofferervaringen. In deze analyses wordt tevens gecontroleerd voor het aantal deelnames van de respondenten.

3 Resultaten

In dit hoofdstuk zijn de resultaten van het empirisch onderzoek weergegeven, waarmee de centrale vraagstelling wordt beantwoord: wat zijn patronen van (herhaald) slachtofferschap van online criminaliteit en in hoeverre kunnen die worden verklaard door persoonskenmerken, online gedrag en de gevolgen van eerder slachtofferschap? Daartoe wordt in paragraaf 3.1 eerst de prevalentie van online slachtofferschap besproken. Vervolgens wordt in paragraaf 3.2 ingegaan op risicofactoren voor online slachtofferschap en in paragraaf 3.3 op de gevolgen daarvan. Tenslotte komt in paragraaf 3.4 herhaald slachtofferschap aan de orde.

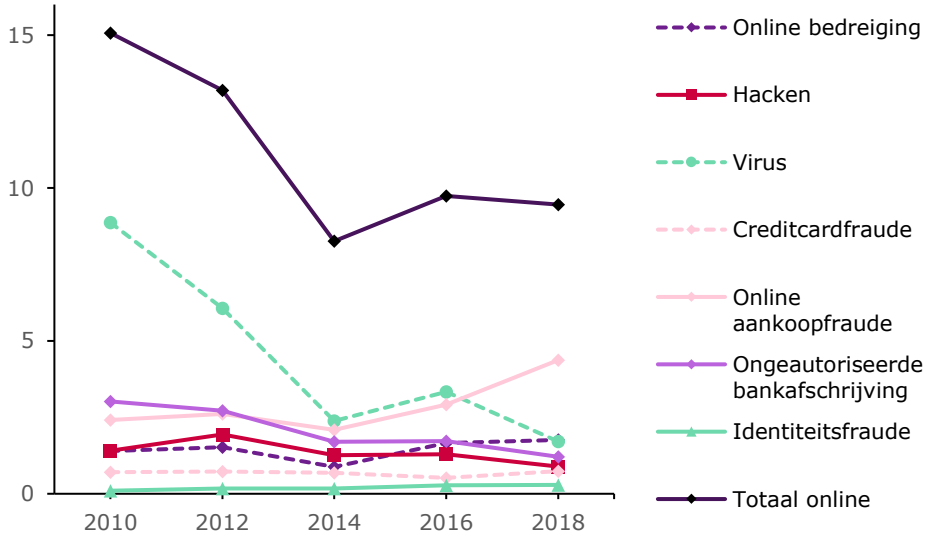
3.1 Trends in slachtofferschap van online criminaliteit

Om inzicht te bieden in de mate waarin slachtofferschap van online criminaliteit zich voordoet, zijn in dit gedeelte de trends van de prevalentie van slachtofferschap van online criminaliteit over tijd beschreven op basis van zelfrapportage in de periode van 2010 tot 2018. Daarbij is ook onderscheid gemaakt tussen verschillende typen online criminaliteit, waaronder diverse cyber- en gedigitaliseerde delicten vallen. Vervolgens wordt ingegaan op de ernst van online criminaliteit en aangiftebereidheid onder slachtoffers. Daarnaast worden de trends van offline criminaliteit weergegeven, om de resultaten in perspectief te kunnen plaatsen.

3.1.1 Online criminaliteit over tijd

De prevalentie van slachtofferschap van de zeven onderzochte online delicten samen is in de periode van 2010 tot 2018 significant gedaald van 15,1% in 2010 naar 9,5% in 2018 (p<0,001). De prevalenties van de verschillende typen online criminaliteit zijn weergegeven in figuur 2. Daarin is zichtbaar dat computervirussen tot en met 2016 (8,9% in 2010 en 3,3% in 2016) het grootste aandeel van online

Figuur 2 Prevalentie slachtofferschap van verschillende typen online criminaliteit



slachtofferschap vormden. In 2018 kwam online aankoopfraude (4,4%) het meest voor. Daarnaast is zichtbaar dat in de periode van 2010 tot 2018 significant minder personen slachtoffer zijn geworden van een computervirus, van hacken en van ongeautoriseerde bankafschrijvingen. Waar in 2010 nog 8,9% aangaf een computervirus te hebben gehad, is dat gedaald tot 1,7% in 2018. De prevalentie van slachtofferschap van hacken is gedaald van 1,4% in 2010 naar 0,9% in 2018 en voor ongeautoriseerde bankafschrijvingen van 3,0% naar 1,2%. Deze dalingen in prevalentie zijn statistisch significant (allen $p<0,001$). Daarentegen zijn de prevalenties van online aankoopfraude en identiteitsfraude in diezelfde periode significant gestegen, respectievelijk van 2,4% in 2010 naar 4,4% in 2018 ($p<0,001$) en van 0,1% naar 0,3% ($p=0,012$). Het aantal personen dat aangaf slachtoffer te zijn geweest van online bedreiging is ook gestegen: van 1,4% naar 1,8%, maar deze ontwikkeling was niet statistisch significant ($p=0,080$). De prevalentie van creditcard fraude is met 0,7% constant gebleven tussen 2010 en 2018.

3.1.2 Ernst van online criminaliteit

Voor online bedreiging, online aankoopfraude en ongeautoriseerde bankafschrijving is doorgevraagd naar de ervaren ernst en geleden financiële schade bij slachtofferschap. Ongeveer de helft van de slachtoffers van online bedreiging (52,5%) heeft aangegeven het voorval niet als ernstig te hebben ervaren, terwijl een derde (32,5%) het als redelijk ernstig en 15,0% het zelfs als bijzonder ernstig heeft ervaren. De impact van slachtofferschap van online aankoopfraude en ongeautoriseerde bankafschrijving is gemeten aan de hand van de geleden financiële schade in euro's. In 30,2% van de gevallen hebben slachtoffers van online aankoopfraude hun geld terug kunnen krijgen. Slachtoffers van een ongeautoriseerde bankafschrijving zijn in aanzienlijk meer gevallen gecompenseerd voor de geleden schade (81,6%). Voor de respondenten die hun geld niet of slechts deels hebben teruggekregen, is de impact vergeleken over de tijd. Aangezien de geleden financiële schade met enkele hoge uitschieters scheef verdeeld is, is de mediaan de meest relevante maat om de schade over de jaren te vergelijken. Bij online aankoopfraude lag een bedrag van 30 euro in het midden van de genoemde schade, met een maximum van €6.000. De mediaan voor ongeautoriseerde bankafschrijving is 60 euro, en dit is over de jaren hoger geworden: in 2010 was de mediaan 33,50 euro (range: €1 tot €1.250) en in 2018 was dat 99 euro (range: €1 tot €1.500). In 2012 heeft één respondent aangegeven meer dan €10.000 schade te hebben opgelopen.

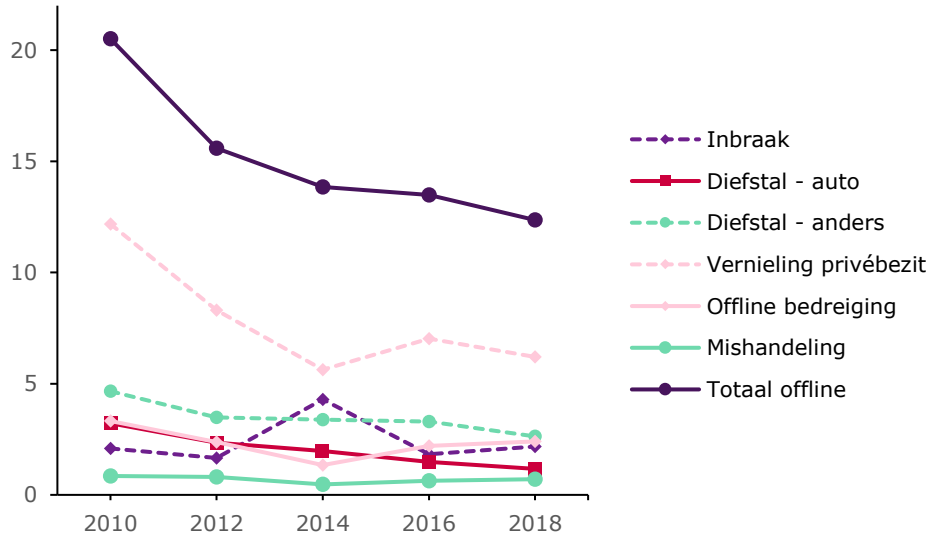
3.1.3 Aangiftebereidheid onder slachtoffers van online criminaliteit

Aan slachtoffers van online bedreiging, online aankoopfraude, ongeautoriseerde bankafschrijvingen en identiteitsfraude is vervolgens gevraagd of slachtoffers aangifte hebben gedaan bij de politie. Na slachtofferschap van online bedreiging heeft 20,2% van de slachtoffers aangifte gedaan bij de politie. Dit percentage is licht gedaald over de tijd (van 23,9% in 2010 naar 18,9% in 2018). De aangiftebereidheid van ongeautoriseerde bankafschrijvingen is 11,6% en tevens lichtelijk gedaald (12,1% in 2010 en 9,8% in 2018). Van de slachtoffers van online aankoopfraude heeft 12% aangifte gedaan, zowel in 2010 als in 2018 (met een uitschieter in 2014; in dat jaar deed 26,4% van de slachtoffers aangifte bij de politie). Na slachtofferschap van identiteitsfraude was de aangiftebereidheid hoger: in totaal heeft 46,0% van deze slachtoffers aangifte gedaan bij de politie. Dit fluctueerde sterk over de tijd. Dit is voornamelijk te verklaren door het relatief lage aantal respondenten dat überhaupt slachtoffer is geworden van identiteitsfraude (6 respondenten (0,1%) in 2010 en 17 (0,3%) in 2018).

3.1.4 Offline criminaliteit over tijd

De prevalentie van slachtofferschap van diverse vormen van offline criminaliteit is gedaald in de periode van 2010 tot 2018. Dit geldt met name voor vernieling van privébezit en diefstal (figuur 3). Dit zijn, statistisch gezien, significante ontwikkelingen (p<0,001). Ook de prevalentie van offline bedreiging is significant gedaald, van 3,3% in 2010 naar 2,4% in 2018 (p=0,002). Het aantal personen dat aangeeft slachtoffer te zijn geweest van mishandeling en inbraak is in diezelfde periode niet significant veranderd.

Figuur 3 Prevalentie slachtofferschap van verschillende typen offline criminaliteit

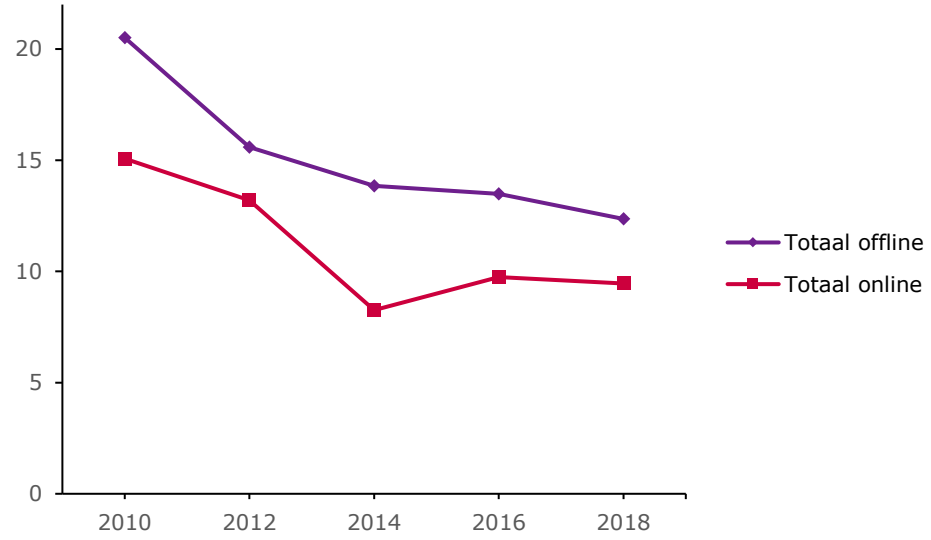


3.1.5 Online versus offline criminaliteit

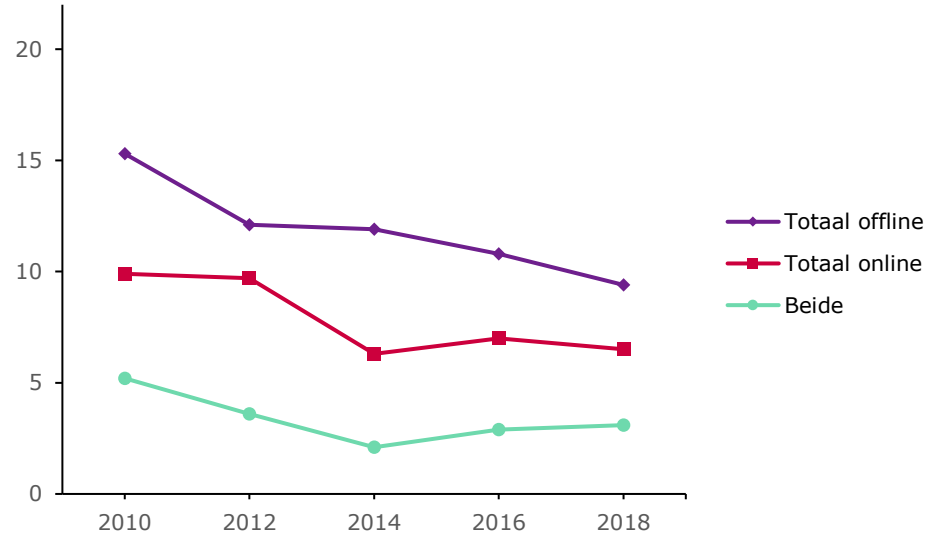
Wanneer de verschillende typen online en offline criminaliteit samen worden bestudeerd, is een daling zichtbaar in de prevalenties van slachtofferschap van zowel online als offline criminaliteit na verloop van tijd (figuur 4). De prevalentie van slachtofferschap van online delicten is in acht jaar tijd gedaald van 15,1% in 2010 naar 9,5% in 2018 (p<0,001). Het aantal personen dat heeft aangegeven slachtoffer te zijn geweest van offline delicten is hoger dan van online delicten, al is ook deze prevalentie significant gedaald: van 20,5% in 2010 naar 12,4% in 2018 (p<0,001).

Wanneer deze resultaten verder worden opgesplitst, is zichtbaar dat de groep respondenten die zowel slachtoffer van online als offline delicten was, nagenoeg gelijk is gebleven (figuur 5).

Figuur 4 Prevalentie online versus offline criminaliteit



Figuur 5 Prevalentie online versus offline criminaliteit



3.2 Risicofactoren voor online slachtofferschap

In deze paragraaf wordt ingegaan op een aantal risicofactoren voor slachtofferschap van online criminaliteit. Daartoe wordt bestudeerd in hoeverre eerder online slachtofferschap (paragraaf 3.2.1), internetgebruik en beschermingsmaatregelen (paragraaf 3.2.2) en persoonskenmerken (paragraaf 3.2.3) samenhangen met online slachtofferschap. Tot slot zal in paragraaf 3.2.4 worden beschreven of deze factoren verschillen tussen slachtoffers van online en offline criminaliteit.

3.2.1 Eerder slachtofferschap

Eerdere slachtofferervaringen hangen samen met de kans op een nieuwe slachtofferervaring (tabel 2). De respondenten die in een vorige wave hebben aangegeven slachtoffer te zijn geweest van online criminaliteit, hebben een grotere kans ook in de volgende wave slachtoffer te worden (e^b=3,43, p<0,001)[11], ook na correctie voor leeftijd, geslacht, opleidingsniveau en het aantal kinderen in het huishouden. In paragraaf 3.4 zal verder worden ingegaan op herhaalde slachtofferervaringen.

Tabel 2 Eerder slachtofferschap en slachtofferschap van online criminaliteit

	Online slachtofferschap		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	0,99	***	0,99 – 1,00
Geslacht			
Vrouw	Ref.		
Man	1,13	*	1,02 – 1,25
Opleiding			
Basisonderwijs	Ref.		
Vmbo	0,97		0,77 – 1,24
Havo/vwo	1,15		0,89 – 1,48
Mbo	1,16		0,91 – 1,46
Hbo	1,19		0,94 – 1,50
Wo	1,30	*	1,00 – 1,68
Aantal kinderen	1,06		0,95 – 1,19
Wave			
2010	Ref.		
2012	0,99		0,96 – 1,14
2014	0,62	***	0,53 – 0,73
2016	0,66	***	0,57 – 0,77
2018	0,62	***	0,53 – 0,72
Eerder slachtofferschap			
Slachtofferschap op *t-1*	3,43	***	3,07 – 3,84

Noot: Omdat het verband tussen eerder slachtofferschap en de kans op een nieuwe slachtofferervaring wordt geschat, is slachtofferschap in de eerste wave (2008) wel als onafhankelijke maar niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

Logistische multilevel regressie analyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; Nresp=6.623, Nobs=16.742

11 De verbanden tussen kenmerken en de kans op online slachtofferschap worden weergegeven met de e^b. Een e^b groter dan 1 betekent bij categorische variabelen (zoals geslacht) een hogere kans op online slachtofferschap ten opzichte van de referentiecategorie en bij continue variabelen (zoals leeftijd) een positief verband tussen het kenmerk en de kans op slachtofferschap. Een e^b kleiner dan 1 betekent het tegenovergestelde: een lagere kans op online slachtofferschap ten opzichte van de referentiecategorie en een negatief verband tussen het kenmerk en de kans op slachtofferschap (e.g. e^b kleiner dan 1 voor leeftijd betekent dat *jongere* mensen (d.w.z. met een *lagere* leeftijd) een *grotere* kans hebben op online slachtofferschap).

3.2.2 Internetgebruik en beschermingsmaatregelen

Om inzicht te krijgen in hoeverre de kans op slachtofferschap samenhangt met online gedragingen, zijn respondenten gevraagd naar hun internetgebruik (tabel 3) en getroffen beschermingsmaatregelen (tabel 4). Daarbij is zichtbaar dat respondenten die meer gebruikmaken van internet meer kans hebben om slachtoffer van online criminaliteit te worden (e^b=1,01, p<0,001). Deze samenhang is gecontroleerd voor de leeftijd, het geslacht, het opleidingsniveau en het aantal kinderen van respondenten. Daarnaast is de kans op online slachtofferschap houdt geen verband met het aantal getroffen beschermingsmaatregelen (zoals een virusscanner) in de vorige wave (e^b=1,01, p=0,617).[12]

Tabel 3 Online gedragingen en slachtofferschap van online criminaliteit: internetgebruik in uren per week

	Online slachtofferschap		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	0,99	***	0,98 - 0,99
Geslacht			
Vrouw	Ref.		
Man	1,16	**	1,04 - 1,29
Opleiding			
Basisonderwijs	Ref.		
Vmbo	1,05		0,81 - 1,36
Havo/vwo	1,27		0,96 - 1,67
Mbo	1,29		1,00 - 1,66
Hbo	1,28		0,99 - 1,65
Wo	1,42	*	1,07 - 1,88
Aantal kinderen	1,15	*	1,02 - 1,29
Wave			
2010	Ref.		
2012	0,94		0,81 - 1,07
2014	0,53	***	0,44 - 0,61
2016	0,57	***	0,49 - 0,66
2018	0,48	***	0,41 - 0,56
Online gedragingen			
Internetgebruik op *t-1*	1,01	***	1,01 - 1,01

Noot: Omdat het verband tussen internetgebruik in de voorafgaande wave en de kans op slachtofferschap wordt geschat, is slachtofferschap in de eerste wave (2008) niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

*p<0,05, **p<0,01, ***p<0,001; Nresp=6.936, Nobs=17.880

12 Uit analyses met de zeven online delicten afzonderlijk bleek dat beschermingsmaatregelen met geen van de zeven onderzochte online delicten een significant samenhangt.

Tabel 4 Online gedragingen en slachtofferschap van online criminaliteit: beschermingsmaatregelen

	Online slachtofferschap		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	0,99	***	0,98 - 0,99
Geslacht			
Vrouw	Ref.		
Man	1,19	**	1,06 - 1,32
Opleiding			
Basisonderwijs	Ref.		
Vmbo	1,01		0,77 - 1,32
Havo/vwo	1,21		0,91 - 1,61
Mbo	1,25		0,95 - 1,62
Hbo	1,22		0,94 - 1,58
Wo	1,36	*	1,02 - 1,82
Aantal kinderen	1,12		0,99 - 1,26
Wave			
2010	Ref.		
2012	0,94		0,81 - 1,07
2014	0,53	***	0,44 - 0,62
2016	0,58	***	0,49 - 0,67
2018	0,50	***	0,42 - 0,57
Online gedragingen			
Beschermingsmaatregelen op *t-1*	1,01		0,97 - 1,03

Noot: Omdat het verband tussen beschermingsmaatregelen in de voorafgaande wave en de kans op slachtofferschap wordt geschat, is slachtofferschap in de eerste wave (2008) niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

Logistische multilevel regressie analyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; Nresp=6.769, Nobs=16.949

3.2.3 Persoonskenmerken

Vervolgens is bestudeerd in hoeverre persoonskenmerken samenhangen met online slachtofferschap (tabel 5). Daaruit blijkt dat slachtoffers van online criminaliteit jonger zijn (e^b=0,99, p<0,01) en dat mannen (e^b=1,27, p<0,001) en respondenten met kinderen (e^b=1,18, p<0,05) meer kans hebben om slachtoffer te worden. Verder scoren slachtoffers van online criminaliteit hoger op impulsiviteit (e^b=2,20, p<0,001) en openheid (e^b=1,37, p<0,001), maar lager op emotionele stabiliteit (e^b=0,78, p<0,001).[13]

13 Aanvullend is bestudeerd of er sprake was van interactie tussen de verschillende persoonlijkheidskenmerken en of juist deze interactie de verhoogde kans op online slachtofferschap bepaalde (bijvoorbeeld of de kans op online slachtofferschap van online criminaliteit alleen verhoogd was in impulsieve respondenten die emotioneel instabiel waren). Dat bleek niet het geval: geen enkele van de interacties tussen de persoonlijkheidskenmerken was statistisch significant.

Tabel 5 Persoonskenmerken en slachtofferschap van online criminaliteit

	Online slachtofferschap		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	0,99	**	0,99 – 1,00
Geslacht			
Vrouw	Ref.		
Man	1,27	***	1,11 – 1,45
Opleiding			
Basisonderwijs	Ref.		
Vmbo	1,12		0,84 – 1,49
Havo/vwo	1,24		0,90 – 1,69
Mbo	1,32		1,00 – 1,76
Hbo	1,33	*	1,00 – 1,77
Wo	1,32		0,96 – 1,83
Aantal kinderen	1,18	*	1,03 – 1,35
Wave			
2010	Ref.		
2012	0,98		0,85 – 1,13
2014	0,56	***	0,47 – 0,66
2016	0,58	*	0,34 – 0,99
2018	0,53	***	0,45 – 0,62
Persoonlijkheidskenmerken			
Impulsiviteit	2,20	***	1,51 – 3,21
Extraversie	1,02		0,92 – 1,13
Altruïsme	1,08		0,94 – 1,24
Consciëntieusheid	0,91		0,81 – 1,03
Emotionele stabiliteit	0,78	***	0,71 – 0,85
Openheid	1,37	***	1,19 – 1,57

Noot: Omdat het verband tussen impulsiviteit in de voorafgaande wave en de kans op slachtofferschap wordt weergegeven, is slachtofferschap in de eerste wave (2008) niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

Logistische multilevel regressie analyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; Nresp=6.336, Nobs=13.331

3.2.4 Vergelijking met offline slachtofferschap

Vervolgens is de samenhang bestudeerd tussen persoonskenmerken en slachtofferschap van offline criminaliteit (tabel 6). Daaruit blijkt dat jongeren (e^b=0,99, p<0,001) en vrouwen (e^b=0,80, p<0,001) meer kans hebben om slachtoffer te worden van offline criminaliteit. Daarnaast hangt de stedelijkheid van de woonplaats van respondenten sterk samen met de kans op offline slachtofferschap (e^b=1,14, p<0,001). In tegenstelling tot slachtoffers van online criminaliteit is er, na controle voor achtergrondkenmerken, bij offline criminaliteit geen associatie zichtbaar tussen impulsiviteit en de kans op slachtofferschap (e^b=1,36, p=0,090). Slachtoffers van offline criminaliteit scoren wel hoger op altruïsme (e^b=1,17, p<0,05) en openheid (e^b=1,23, p<0,01), en lager op consciëntieusheid (e^b=0,81, p<0,001) en emotionele stabiliteit (e^b=0,82, p<0,001).

Tabel 6 Persoonskenmerken en slachtofferschap van offline criminaliteit

	Offline slachtofferschap		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	0,99	***	0,98 – 0,99
Geslacht			
Vrouw	Ref.		
Man	0,80	***	0,71 – 0,90
Opleiding			
Basisonderwijs	Ref.		
Vmbo	1,06		0,81 – 1,34
Havo/vwo	1,15		0,88 – 1,49
Mbo	1,01		0,79 – 1,28
Hbo	1,28	*	1,01 – 1,62
Wo	1,34	*	1,02 – 1,76
Stedelijkheid	1,14	***	1,10 – 1,19
Wave			
2010	Ref.		
2012	0,36	***	0,32 – 0,42
2014	0,28	***	0,24 – 0,33
2016	0 58	*	0,35 – 0,95
2018	0,26	***	0,22 – 0,29
Persoonlijkheidskenmerken			
Impulsiviteit	1,36		0,95 – 1,93
Extraversie	1,04		0,95 – 1,14
Altruïsme	1,17	*	1,03 – 1,33
Consciëntieusheid	0,81	***	0,73 – 0,91
Emotionele stabiliteit	0,82	***	0,75 – 0,89
Openheid	1,23	**	1,08 – 1,39

Noot: Omdat het verband tussen impulsiviteit in de voorafgaande wave en de kans op slachtofferschap wordt weergegeven, is slachtofferschap in de eerste wave (2008) niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

Logistische multilevel regressie analyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; Nresp=6.392, Nobs=13.516

Wanneer online en offline slachtofferschap rechtstreeks worden vergeleken (tabel 7), blijkt dat mannen een grotere kans hebben om slachtoffer te worden van online dan van offline criminaliteit (e^b=1,48, p<0,001). Verder is ook zichtbaar dat respondenten met een hogere score op impulsiviteit een hogere kans hebben op slachtofferschap van online dan van offline criminaliteit (e^b=1,94, p<0,05).

3.3 Gevolgen van online slachtofferschap

Nadat de invloed van mogelijke risicofactoren op online slachtofferschap in kaart is gebracht, zijn in deze paragraaf mogelijke gevolgen van online slachtofferschap onderzocht. Allereerst is bestudeerd in hoeverre een online slachtofferervaring samengaat met een verandering in angst voor online criminaliteit, internetgebruik en preventiegedrag (paragraaf 3.3.1). Vervolgens toetsen we in hoeverre een online slachtofferervaring invloed heeft op de mentale gezondheid van respondenten

Tabel 7 Persoonskenmerken en slachtofferschap van online versus offline criminaliteit

	Online versus offline slachtofferschap (ref.)		
	e^b		95%BI
Achtergrondkenmerken			
Leeftijd	1,00		1,00 – 1,01
Geslacht			
Vrouw	Ref.		
Man	1,48	***	1,21 – 1,81
Opleiding			
Basisonderwijs	Ref.		
Vmbo	1,22		0,77 – 1,94
Havo/vwo	1,18		0,72 – 1,94
Mbo	1,65	*	1,05 – 2,60
Hbo	1,21		0,77 – 1,91
Wo	1,24		0,75 – 2,04
Aantal kinderen	1,16		0,94 – 1,42
Stedelijkheid	0,95		0,88 – 1,03
Wave			
2010	Ref.		
2012	2,59	***	2,05 – 3,27
2014	1,78	***	1,37 – 2,33
2016	0,80		0,29 – 2,15
2018	1,90	***	1,47 – 2,45
Persoonlijkheidskenmerken			
Impulsiviteit	1,94	*	1,03 – 3,65
Extraversie	0,92		0,79 – 1,08
Altruïsme	0,90		0,73 – 1,11
Consciëntieusheid	1,15		0,95 – 1,39
Emotionele stabiliteit	0,96		0,83 – 1,10
Openheid	1,09		0,88 – 1,35

Noot: Omdat het verband tussen impulsiviteit in de voorafgaande wave en de kans op slachtofferschap wordt weergegeven, is slachtofferschap in de eerste wave (2008) niet als afhankelijke variabele meegenomen. Derhalve is de tweede wave (2010) hier de referentiecategorie.

Logistische multilevel regressie analyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; Nresp=1.968, Nobs=2.394

(paragraaf 3.3.2). In een verdiepende analyse wordt nagegaan of de gevolgen verschillen tussen slachtoffers die geen aangifte hebben gedaan en slachtoffers die dat wel hebben gedaan.[14]

3.3.1 Angst voor online criminaliteit, internetgebruik en beschermingsmaatregelen

Uit model 8.1 in tabel 8 blijkt dat het hebben van een online slachtofferervaring significant samenhangt met een toename in angst voor online criminaliteit. De b-coëfficiënt van 0,10 geeft aan dat gemiddeld genomen de angst voor online criminaliteit op een schaal van 1 tot 5 met 0,10 stijgt na het hebben van een

14 In dit hoofdstuk zijn de gevolgen weergegeven van totaal online slachtofferschap. De gevolgen zijn aanvullend ook per type delict bestudeerd; deze resultaten zijn weergegeven in Bijlage 3 en zijn indien relevant in de lopende tekst besproken.

slachtofferervaring. Mensen die slachtoffer zijn geworden van online criminaliteit rapporteren in een daaropvolgend jaar een hogere mate van angst voor online criminaliteit, terwijl de angst voor online criminaliteit over het algemeen juist af lijkt te nemen over tijd. Dit geldt zowel voor slachtoffers die geen aangifte hebben gedaan (b=0,12, p<0,001) als voor slachtoffers die wel aangifte hebben gedaan (b=0,13, p<0,01). De toename in angst voor criminaliteit is het grootst onder slachtoffers van creditcardfraude, online aankoopfraude, een computervirus of ongeautoriseerde bankafschrijvingen (bijlage 3, tabel b7).

Tabel 8 Online slachtofferschap en angst voor online criminaliteit

	Angst voor online criminaliteit Model 8.1			Angst voor online criminaliteit Model 8.2		
	b		95%BI	b		95%BI
Online slachtofferschap	0,10	***	0,07 - 0,12			
Aangifte†						
Geen slachtoffer				Ref.		
Slachtoffer, geen aangifte				0,12	***	0,08 - 0,16
Slachtoffer, wel aangifte				0,13	**	0,04 - 0,22
Wave						
2008	Ref.			Ref.		
2010	-0,09	***	-0,11 - -0,06	-0,10	***	-0,12 - -0,07
2012	-0,13	***	-0,15 - -0,10	-0,14	***	-0,16 - -0,10
2014	-0,10	***	-0,13 - -0,07	-0,12	***	-0,14 - -0,08
2016	-0,17	***	-0,20 - -0,14	-0,19	***	-0,21 - -0,15
2018	-0,16	***	-0,18 - -0,13	-0,18	***	-0,20 - -0,14
Aantal kinderen	0,01		-0,01 - 0,03	0,01		-0,01 - 0,03
Partner	0,05	*	0,01 - 0,09	0,06	*	0,01 - 0,09

*p<0,05, **p<0,01, ***p<0,001; Nresp=5.776, Nobs=20.222

Fixed effect panel analyses in Stata

† Aangifte is alleen bevraagd voor de volgende type delicten: online aankoopfraude, online bedreiging, ongeautoriseerde bankafschrijving en identiteitsfraude.

Waar we in de vorige paragraaf hebben gezien dat online slachtofferschap samengaat met een toename in angst voor deze vorm van criminaliteit, bestuderen we in deze paragraaf of slachtofferschap gevolgen heeft voor het daadwerkelijk online gedrag van respondenten. Tabel 9 laat zien dat het aantal uren per week dat men internet gebruikt niet verandert nadat men slachtoffer is geworden (b=0,01, p=0,97). Een slachtofferervaring weerhoudt respondenten er dus niet van om zich op internet te begeven.[15] Dit geldt voor elk delict (bijlage 3, tabel b8). Gemiddeld is het internetgebruik sterk gestegen in de periode van 2008 tot 2018: in 2018 besteed men gemiddeld ruim 7 uur per week meer aan internet dan in 2008 (b=7,37, p<0,001).

15 Vanaf 2012 is internetgebruik gemeten met aparte vragen over internetgebruik op computer of laptop, smartphone en tablet (zie ook paragraaf 2.2.2). Als alleen de waves vanaf 2012 worden meegenomen, zijn de verbanden hetzelfde.

Tabel 9 Online slachtofferschap en internetgebruik in uren per week

	Internetgebruik in uren Model 9.1			Internetgebruik in uren Model 9.2		
	b		95%BI	b		95%BI
Online slachtofferschap	0,01		-0,51 - 0,53			
Aangifte†						
Geen slachtoffer				Ref.		
Slachtoffer, geen aangifte				0,28		-0,49 - 1,06
Slachtoffer, wel aangifte				-1,14		-2,90 - 0,63
Wave						
2008	Ref.			Ref.		
2010	0,31		-0,980	0,31		-0,18 - 0,80
2012	2,67	***	2,14 - 3,19	2,68	***	2,15 - 3,20
2014	5,13	***	4,58 - 5,67	5,15	***	4,60 - 5,69
2016	6,31	***	5,78 - 6,84	6,32	***	5,79 - 6,84
2018	7,37	***	6,81 - 7,93	7,38	***	6,82 - 7,94
Aantal kinderen	0,20		-0,16 - 0,57	0,20		-0,16 - 0,57
Partner	-0,27		-1,16 - 0,62	-0,26		-1,15 - 0,63

*p<0,05, **p<0,01, ***p<0,001; Nresp=5.776, Nobs=20.222

Fixed effect panel analyses in Stata

† Aangifte is alleen bevraagd voor de volgende type delicten: online aankoopfraude, online bedreiging, ongeautoriseerde bankafschrijving en identiteitsfraude.

Tabel 10 Online slachtofferschap en beschermingsmaatregelen

	Beschermingsmaatregelen Model 10.1			Beschermingsmaatregelen Model 10.2		
	b		95%BI	b		95%BI
Online slachtofferschap	0,12	***	0,05 - 0,19			
Aangifte†						
Geen slachtoffer				Ref.		
Slachtoffer, geen aangifte				0,14	**	0,03 - 0,23
Slachtoffer, wel aangifte				-0,04		-0,27 - 0,18
Wave						
2008	Ref.			Ref.		
2010	0,12	***	0,05 - 0,18	0,11	**	0,04 - 0,17
2012	0,21	***	0,13 - 0,27	0,20	***	0,13 - 0,26
2014	0,32	***	0,24 - 0,38	0,31	***	0,23 - 0,37
2016	0,13	***	0,05 - 0,19	0,12	**	0,04 - 0,18
2018	-0,02		-0,09 - 0,04	-0,03		-0,10 - 0,03
Aantal kinderen	0,02		-0,02 - 0,07	0,03		-0,02 - 0,07
Partner	0,06		-0,05 - 0,17	0,06		-0,05 - 0,17

*p<0,05, **p<0,01, ***p<0,001; Nresp=5.776, Nobs=20.222

Fixed effect panel analyses in Stata

† Aangifte is alleen bevraagd voor de volgende type delicten: online aankoopfraude, online bedreiging, ongeautoriseerde bankafschrijving en identiteitsfraude.

In tegenstelling tot het internetgebruik zien we wel een verandering in de getroffen beschermingsmaatregelen (tabel 10). Slachtoffers van online criminaliteit zijn meer beschermingsmaatregelen gaan treffen om zichzelf te beschermen tegen een mogelijke nieuwe slachtofferervaring (b=0,12, p<0,001). Wat opvalt is dat voornamelijk de slachtoffers die geen aangifte hebben gedaan meer beschermingsmaatregelen zijn gaan treffen (b=0,14, p<0,001). Respondenten die wel aangifte hebben gedaan, nemen niet meer beschermingsmaatregelen dan toen ze geen slachtoffer waren (b=-0,04, p=0,72). De type delicten die slachtoffers ertoe zetten meer maatregelen te treffen, zijn de delicten die direct betrekking hebben op de computer, namelijk computervirussen en ongeautoriseerde bankafschrijvingen (bijlage 3, tabel b9).

3.3.2 Mentale gezondheid

In tabel 11 is de samenhang tussen online slachtofferschap en zelfgerapporteerde mentale gezondheid weergegeven.[16] Er is geen verandering in zelfgerapporteerde

Tabel 11 Online slachtofferschap en mentale gezondheid

	Mentale gezondheid Model 11.1			Mentale gezondheid Model 11.2		
	b		95%BI	b		95%BI
Online slachtofferschap	-0,02		-0,05 - 0,01			
Aangifte†						
Geen slachtoffer				Ref.		
Slachtoffer, geen aangifte				-0,02		-0,06 - 0,01
Slachtoffer, wel aangifte				-0,03		-0,12 - 0,06
Wave						
2008	Ref.			Ref.		
2010	0,05	***	0,02 - 0,08	0,06	***	0,02 - 0,08
2012	0,10	***	0,07 - 0,12	0,10	***	0,07 - 0,12
2014	0,12	***	0,09 - 0,14	0,12	***	0,09 - 0,15
2016	0,16	***	0,12 - 0,18	0,16	***	0,13 - 0,18
2018	0,16	***	0,13 - 0,19	0,16	***	0,13 - 0,19
Aantal kinderen	-0,04	***	-0,05 - -0,01	-0,04	***	-0,05 - -0,01
Partner	0,15	***	0,09 - 0,19	0,15	***	0,09 - 0,19

*p<0,05, **p<0,01, ***p<0,001; Nresp=5.776, Nobs=20.222

Fixed effect panel analyses in Stata

† Aangifte is alleen bevraagd voor de volgende type delicten: online aankoopfraude, online bedreiging, ongeautoriseerde bankafschrijving en identiteitsfraude.

16 Zelfgerapporteerde mentale gezondheid is drie maanden voor slachtofferschap gemeten. Gezien slachtofferschap is gebaseerd op slachtofferervaringen in de afgelopen 12 maanden, is het mogelijk dat slachtofferervaringen in werkelijkheid na de meting van mentale gezondheid hebben plaatsgevonden. Als controle zijn de analyses ook toegepast op basis van de mentale gezondheid negen maanden ná de slachtofferervaring. Uit deze analyses blijkt ook geen significante samenhang tussen slachtofferschap en mentale gezondheid te bestaan. Voor slachtoffers van online bedreiging was in de originele analyses wel een significante afname in mentale gezondheid gevonden, maar dit verband is niet aanwezig wanneer we de mentale gezondheid 9 maanden na het meten van slachtofferschap gebruiken. Een mogelijke verklaring hiervoor is dat de invloed van een slachtofferervaring op de mentale gezondheid in de maanden na de ervaring wegebt. We kiezen er daarom voor om de meting van drie maanden voor de meting van slachtofferschap te rapporteren.

mentale gezondheid zichtbaar na een online slachtofferervaring (b=-0,02, *p*=0,12), ook niet wanneer slachtoffers zijn opgesplitst op basis van aangiftebereidheid. Als we echter kijken naar specifieke delicten (bijlage 3, tabel b10), blijkt dat slachtoffers van online bedreiging wel een lagere mentale gezondheid rapporteren (b=-0,15, *p*<0,01). Slachtoffers van identiteitsfraude rapporteren ook een minder goede mentale gezondheid, maar dit is niet significant (b=-0,06, *p*=0,70). Mogelijk komt dit door een relatief laag aantal slachtoffers van dit type delict (N=28).[17]

3.4 Herhaald online slachtofferschap

In deze paragraaf zal verder worden ingegaan op herhaald slachtofferschap (zie ook paragraaf 3.2.1). Eerst is de prevalentie van herhaald slachtofferschap weergegeven (paragraaf 3.4.1), waarna verder wordt ingegaan op de kenmerken van deze groep herhaald slachtoffers (paragraaf 3.4.2).

3.4.1 Prevalentie van herhaald online slachtofferschap

In tabel 12 is de verdeling van herhaald slachtofferschap weergegeven. In totaal heeft 17,5% van de respondenten die aan ten minste twee waves hebben deelgenomen, aangegeven meer dan één keer slachtoffer te zijn geworden van een online delict. Deze groep is daarmee iets groter dan de groep die slechts eenmalig slachtoffer is geworden (16,6%). Dit is afhankelijk van het aantal deelnames, aangezien het percentage respondenten dat aangeeft meerdere keren slachtoffer te zijn geworden toeneemt naarmate men vaker deelneemt aan de dataverzameling (bij 2 deelnames is 12,9% herhaald slachtoffer, bij 5 deelnames is 23,4% herhaald slachtoffer).

Binnen de groep van herhaald slachtoffers is 45,3% meerdere malen slachtoffer geworden van hetzelfde delict en 20,7% eenmalig slachtoffer geworden van meerdere delicten (meervoudig slachtoffers). De overige 34% is zowel meerdere malen slachtoffer geworden van hetzelfde delict als meervoudig slachtoffer (bijlage 4, tabel b11).

Tabel 12 Prevalentie herhaald slachtofferschap (naar aantal deelnames)

	Nooit slachtoffer		Eenmalig slachtoffer		Herhaald slachtoffer		Totaal	
	N	%	N	%	N	%	N	%
Totaal	4.666	66,0	1.171	16,6	1.234	17,5	7.071	100
Aantal deelnames								
2	1.488	71,9	314	15,2	267	12,9	2.069	100
3	1.065	69,3	238	15,5	234	15,2	1.537	100
4	760	62,8	217	17,9	233	19,3	1.210	100
5	686	59,6	196	17,0	269	23,4	1.151	100
6	667	60,4	206	18,7	231	20,9	1.104	100

17 Gezien het relatief lage aantal slachtoffers en mensen die een psycholoog bezoeken, was het niet mogelijk om de samenhang in een fixed-effect model te schatten.

3.4.2 Risicofactoren voor herhaald online slachtofferschap

In tabel 13 is weergegeven in hoeverre eenmalig en herhaald slachtoffers qua risicofactoren met elkaar verschillen. Daarvoor vergeleken we (1) eenmalige slachtoffers met niet-slachtoffers, (2) herhaald slachtoffers met niet-slachtoffers en (3) herhaald slachtoffers met eenmalige slachtoffers. Respondenten zonder geldige score op één van de meegenomen variabelen zijn uit deze analyses verwijderd. De modellen zijn gecontroleerd voor het aantal keer dat respondenten hebben geparticipeerd, aangezien respondenten die vaker hebben meegedaan meer mogelijkheden hebben gehad om slachtofferschap te rapporteren.

Mannen hebben, in vergelijking met vrouwen, een grotere kans om herhaaldelijk online slachtoffer te worden dan om eenmalig (e^b=1,34, p<0,01; model 13.2) of nooit slachtoffer te worden (e^b=1,50, p<0,001; model 13.2). Mannen hebben daarentegen geen grotere kans om eenmalig slachtoffer te worden dan om nooit slachtoffer te worden (e^b=1,12, p=0,15; model 13.1). Geslacht is dus een risicofactor van herhaald online slachtofferschap en niet van eenmalig online slachtofferschap. Jongeren en hoger opgeleiden hebben een grotere kans op zowel eenmalig als herhaald slachtofferschap ten opzichte van niet-slachtofferschap dan ouderen en lager opgeleiden, maar leeftijd en opleidingsniveau hangen niet samen met het verschil tussen eenmalig en herhaald slachtofferschap. Leeftijd en opleidingsniveau zijn dus risicofactoren van zowel herhaald als eenmalig online slachtofferschap, maar verklaren niet het verschil tussen herhaald en eenmalig online slachtofferschap.

Uit paragraaf 3.2 van dit rapport bleek dat naarmate men impulsiever is, men een grotere kans heeft om slachtoffer van online criminaliteit te worden. Tabel 13 laat zien dat impulsiviteit zowel een risicofactor is voor eenmalig slachtofferschap (e^b=1,91, p<0,05; model 13.1) als voor herhaald slachtofferschap e^b=4,52, p<0,001; model 13.2). Uit model 13.3 blijkt tevens dat impulsievere mensen een significant grotere kans hebben op herhaald slachtofferschap dan op eenmalig slachtofferschap (e^b=2,36, p<0,01). Deze bevindingen impliceren dat hoe impulsiever iemand is, hoe vaker iemand online slachtoffer wordt. Hoewel emotionele stabiliteit en openheid met zowel eenmalig als herhaald slachtofferschap samenhangen, zien we dat emotioneel instabiele respondenten (e^b=0,75, p<0,001) en meer open respondenten (e^b=1,38, p<0,01) een grotere kans hebben op herhaald slachtofferschap dan op eenmalig online slachtofferschap.

Aangezien herhaald slachtofferschap op meerdere manieren tot stand kan komen, hebben we in robuustheidsanalyses de groep herhaald slachtoffers opgesplitst (bijlage 4). Hierin zijn herhaald slachtoffers vergeleken met eenmalige slachtoffers. Ten eerste is onderscheid gemaakt tussen respondenten die herhaald slachtoffer zijn geworden van (1) meerdere delicten, (2) hetzelfde delict of (3) van zowel meerdere als hetzelfde delict (tabel b12). De significante verbanden gevonden in model 13.3 uit tabel 13 zien we allemaal terug in de derde categorie (model b12.3, tabel b12), oftewel de respondenten die van meerdere delicten én van hetzelfde delict meerdere keren slachtoffer zijn geworden verschillen met eenmalig slachtoffers op geslacht, impulsiviteit, emotionele stabiliteit en openheid. Ten tweede is onderscheid gemaakt tussen respondenten die herhaald slachtoffer zijn geworden (1) binnen één meetmoment, (2) op meerdere meetmomenten en (3) op zowel één als meerdere meetmomenten (tabel b13). Deze categorieën zijn vervolgens vergeleken met de eenmalig slachtoffers. Ook hier vinden we de eerder gevonden significante verbanden terug bij de derde categorie; zij die zowel op één moment als op

Tabel 13 Risicofactoren voor herhaald slachtofferschap van online criminaliteit

	Eenmalig vs. nooit (ref.) Model 13.1			Herhaald vs. nooit (ref.) Model 13.2			Herhaald vs. eenmalig (ref.) Model 13.3		
	e^b		95%BI	e^b		95%BI	e^b		95%BI
Achtergrondkenmerken									
Leeftijd	0,99	***	0,98 - 0,99	0,98	***	0,97 - 0,98	1,00		0,99 - 1,00
Geslacht									
Vrouw	Ref.			Ref.			Ref.		
Man	1,12		0,96 - 1,30	1,50	***	1,29 - 1,74	1,34	**	1,11 - 1,62
Opleidingsniveau									
Basisonderwijs	Ref.			Ref.			Ref.		
Vmbo	1,34		0,95 - 1,89	1,19		1,06 - 2,08	0,88		0,56 - 1,37
Havo/vwo	1,26		0,86 - 1,84	1,37		0,94 - 1,97	1,08		0,67 - 1,73
Mbo	1,36	*	0,96 - 1,91	1,49	*	1,06 - 2,08	1,09		0,70 - 1,68
Hbo	1,53	*	1,08 - 2,15	1,50	*	1,07 - 2,10	0,98		0,63 - 1,51
Wo	1,75	**	1,20 - 2,53	1,19		0,81 - 1,73	0,68		0,42 - 1,09
Persoonlijkheidskenmerken									
Impulsiviteit	1,91	*	1,10 - 3,32	4,52	***	2,72 - 7,49	2,36	**	1,25 - 4,44
Extraversie	1,12		0,98 - 1,27	1,10		0,96 - 1,24	0,98		0,83 - 1,14
Altruïsme	0,96		0,80 - 1,13	1,02		0,86 - 1,21	1,07		0,86 - 1,32
Consciëntieusheid	0,99		0,84 - 1,15	0,89		0,76 - 1,03	0,90		0,74 - 1,08
Emotionele stabiliteit	0,87	*	0,77 - 0,98	0,65	***	0,58 - 0,73	0,75	***	0,64 - 0,86
Openheid	1,25	*	1,04 - 1,49	1,73	***	1,45 - 2,05	1,38	**	1,11 - 1,71
Aantal deelnames	1,16	***	1,09 - 1,21	1,31	***	1,24 - 1,38	1,14	***	1,06 - 1,20

Multinomiale regressieanalyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; N=6.332

meerdere momenten herhaald slachtoffer zijn geworden (model b13.3, tabel b13). Opvallend is dat in zowel tabel b11 als tabel b12 de effecten van geslacht, impulsiviteit, emotionele stabiliteit en openheid aanwezig zijn bij de groepen die de meeste slachtofferervaringen hebben meegemaakt (model b12.3, tabel b12; model b13.3, tabel 13). Deze kenmerken hangen dus samen met alle vormen van herhaald slachtofferschap, en lijken daarmee robuuste indicatoren van herhaald slachtofferschap.

Nadat het onderscheid is gemaakt tussen de groep van eenmalig en herhaald slachtoffers van online criminaliteit, is gekeken of binnen de groep van herhaald slachtofferschap de frequentie van herhaald slachtofferschap ook begrepen kan worden aan de hand van achtergrond- en persoonlijkheidskenmerken. Hierbij zijn alleen de respondenten geselecteerd die twee keer of vaker slachtoffer zijn geworden van online criminaliteit. Binnen deze groep is men gemiddeld genomen 3,9 keer slachtoffer geworden, en is de persoon met de meeste slachtofferervaringen 36 keer slachtoffer geworden van online criminaliteit. De resultaten zijn weergegeven in tabel 14. Net als de eerdere analyses over herhaald slachtofferschap in tabel 13 zien we geen significante samenhang van leeftijd en opleidingsniveau met de frequentie van herhaald online slachtofferschap. Hieruit blijkt dat leeftijd, geslacht en opleiding niet samenhangen met het aantal keren dat men slachtoffer wordt van online criminaliteit. Waar model 13.3 uit tabel 13 nog liet zien

Tabel 14 Risicofactoren voor frequentie slachtofferschap van online criminaliteit

	Frequentie herhaald slachtofferschap†		
	e[b]		95%BI
Achtergrondkenmerken			
Leeftijd	1,00		0,99 - 1,00
Geslacht			
Vrouw	Ref.		
Man	1,08		0,91 - 1,28
Opleidingsniveau			
Basisonderwijs	Ref.		
Vmbo	1,13		0,77 - 1,64
Havo/vwo	0,78		0,52 - 1,16
Mbo	0,90		0,62 - 1,30
Hbo	0,97		0,66 - 1,40
Wo	1,00		0,66 - 1,50
Persoonlijkheidskenmerken			
Impulsiviteit	3,72	***	2,25 - 6,13
Extraversie	1,01		0,86 - 1,16
Altruïsme	0,86		0,71 - 1,03
Consciëntieusheid	1,11		0,93 - 1,30
Emotionele stabiliteit	0,80	**	0,70 - 0,91
Openheid	1,22	*	1,02 - 1,45
Aantal deelnames	1,07	*	1,00 - 1,12

† min=2, max=36, gem=3,90

Negatieve binomiale regressieanalyse in SPSS

*p<0,05, **p<0,01, ***p<0,001; N=1.123

dat geslacht wel samenhangt met de kans op herhaald slachtofferschap ten opzichte van eenmalig slachtofferschap, laat tabel 14 zien dat het niet samenhangt met het aantal slachtofferervaringen. Drie persoonlijkheidskenmerken lijken daarentegen wel te correleren met de frequentie van herhaald slachtofferschap: hoe impulsiever (e^b=3,72, p<0,001), emotioneel instabieler (e^b=0,80, p<0,01) en opener (e^b=1,22, p<0,05) iemand is, des te vaker iemand slachtoffer wordt van online criminaliteit.

4 Discussie en conclusie

De centrale vraagstelling van dit onderzoek luidt: *wat zijn patronen van (herhaald) slachtofferschap van online criminaliteit en in hoeverre kunnen die worden verklaard door persoonskenmerken, online gedrag en de gevolgen van eerder slachtofferschap?* Om deze vraag te beantwoorden is een empirisch onderzoek met een longitudinaal design uitgevoerd. In dit hoofdstuk zijn de onderzoeksvragen beantwoord. Paragraaf 4.1 bevat een overzicht van de onderzoeksvragen en een beknopte weergave van de belangrijkste bevindingen. In paragraaf 4.2 worden sterke punten en beperkingen van het onderzoek besproken en in paragraaf 4.3 worden aanbevelingen voor vervolgonderzoek gedaan. Tot slot volgt in paragraaf 4.4 de conclusie van het onderzoek.

4.1 Belangrijkste bevindingen

Hieronder worden de belangrijkste bevindingen van het onderzoek beschreven en bediscussieerd.

4.1.1 Trends in slachtofferschap van online criminaliteit

Het eerste doel van het huidige onderzoek was om zicht te krijgen op de prevalentie van ervaren cyber- en gedigitaliseerde criminaliteit: *in welke mate ervaren Nederlandse burgers slachtofferschap van online criminaliteit?* Daarvoor zijn de trends in de prevalentie van online slachtofferschap over de tijd beschreven, op basis van zelfrapportage in de periode van 2010 tot 2018.

In dit onderzoek is gekeken naar slachtofferschap van de volgende online delicten: creditcard fraude, gehackt worden, online aankoopfraude, online bedreiging, het oplopen van een computervirus, ongeautoriseerde bankafschrijving en identiteitsfraude. Uit de resultaten blijkt een significante daling in de prevalentie van slachtofferschap van de totaalscore van deze zeven typen online delicten. In 2010 was ongeveer 1 op de 7 respondenten (15,1%) slachtoffer van tenminste één van deze online delicten. In 2018 was dat ongeveer 1 op de 10 (9,5%). Ter vergelijking: het aantal personen dat heeft aangegeven slachtoffer te zijn geweest van offline delicten is hoger dan dat van online delicten, al is ook deze prevalentie significant gedaald. Waar in 2010 1 op de 5 respondenten (20,5%) slachtoffer was van één of meerdere van de onderzochte offline delicten, was dat in 2018 ongeveer 1 op 8 (12,4%). De daling in online slachtofferschap is vooral te zien in de daling in het aantal slachtoffers van computervirussen (8,9% in 2010 en 1,7% in 2018). In iets mindere mate is tevens een daling in het aantal slachtoffers van hacken (1,4% in 2010 en 0,9% in 2018) en ongeautoriseerde bankafschrijvingen (3,0% in 2010 en 1,2% in 2018) te zien. Daarentegen zijn de prevalenties van online aankoopfraude en identiteitsfraude in diezelfde periode significant gestegen, respectievelijk van 2,4% in 2010 naar 4,4% in 2018 en van 0,1% naar 0,3%.

De daling in online criminaliteit sluit aan bij bevindingen over offline criminaliteit, die reeds jaren een daling in delicten laat zien. De geregistreerde criminaliteit in Nederland is met ruim een derde is afgenomen over de periode 2007-2017. In 2017 registreerde de politie 830.000 misdrijven, terwijl er in 2007 nog 1.300.000 werden geregistreerd (Kalidien, 2018). Ook de Veiligheidsmonitor rapporteerde een duidelijk

dalende trend in slachtofferschap van traditionele criminaliteit, op basis van zelfgerapporteerde slachtofferervaringen over de periode 2005-2017 (CBS, 2017). Als mogelijke verklaring voor de daling in offline criminaliteit werd eerder genoemd dat er, in plaats van een daling in criminaliteit, door de digitalisering van de samenleving mogelijk sprake was van een verschuiving van offline naar online criminaliteit (Rokven et al., 2017). Op basis van het huidige onderzoek wordt deze veronderstelling echter niet bevestigd, aangezien onze resultaten ook een daling in online slachtofferschap laten zien. Ook in eerder onderzoek is een lichte daling in zelfgerapporteerd online slachtofferschap beschreven: van 12% in 2012 tot 11% in 2017 (CBS, 2017). De daling is opvallend gezien de toename van het gebruik van internet, gemiddeld ruim 7 uur per week meer in 2018 dan in 2008, en de samenhang tussen internetgebruik online slachtofferschap die in het huidige onderzoek is gevonden. In dit onderzoek is niet specifiek gekeken naar mogelijke oorzaken voor de dalende trend van online slachtofferschap. Daarvoor zou aanvullend onderzoek nodig zijn. Veranderingen in macrofactoren, zoals toegenomen welvaart of meer gerichte inzet van de politie, kunnen bijvoorbeeld een rol spelen in de dalende (online) criminaliteit (Van der Laan, Rokven, Weijters & Beerthuizen, 2018).

Een opvallende bevinding is de sterke daling in online slachtofferschap tot 2014 (zie paragraaf 3.1, figuur 2 en figuur 4). Deze daling in online slachtofferschap lijkt met name veroorzaakt door een sterke daling in slachtofferschap van computervirussen van 2010 tot 2014. Ook in eerder onderzoek was in 2014 een sterke daling in online criminaliteit zichtbaar (Kalidien, 2018), waardoor methodologische verklaringen voor deze daling minder waarschijnlijk zijn. Ook een verschuiving van criminaliteit van computervirussen naar bijvoorbeeld fraude lijkt de sterke daling in slachtofferschap in 2014 niet te verklaren: de prevalenties van online aankoopfraude en identiteitsfraude zijn weliswaar gestegen, maar de grootste stijging heeft pas na 2014 plaatsgevonden (figuur 2, paragraaf 3.1).

De in dit onderzoek gepresenteerde daling in slachtofferschap van online criminaliteit is gebaseerd op zelfrapportage onder een representatieve steekproef van 13.430 respondenten. Een groot deel hiervan heeft echter niet aan alle meetmomenten deelgenomen. De vraag is of, en in hoeverre, deze uitval invloed heeft op de in dit onderzoek gepresenteerde prevalenties. Doordat het LISS-panel meermalig is aangevuld met – veelal jonge – nieuwe panelleden, is de uitval zo goed mogelijk opgevangen en dit heeft ook op de latere meetmomenten gezorgd voor een representatieve steekproef. Daarnaast zijn de gegevens op basis van leeftijd, geslacht en opleidingsniveau voor elk meetmoment afzonderlijk gewogen naar de populatie, waardoor de weergegeven trends in slachtofferschap een zo goed mogelijk beeld geven van de mate van online slachtofferschap onder de Nederlandse bevolking. Aanvullende analyses lieten zien dat uitvallers op een aantal vlakken verschilden van de deelnemers: uitvallers bleken impulsiever dan deelnemers en slachtoffers van online delicten namen minder vaak deel aan een volgend meetmoment dan degenen die geen slachtoffer waren. In het LISS-panel is dus sprake van selectieve non-respons, waarbij met name het lagere responspercentage van online slachtoffers suggereert dat – als er al een effect van deze non-respons is – er waarschijnlijk sprake is van een onderschatting van de prevalentie van (herhaald) slachtofferschap. Aangezien ongeveer 1 op de 4 respondenten aangifte heeft gedaan van zijn/haar slachtofferervaring (paragraaf 3.1.3), geeft de huidige studie waarschijnlijk alsnog een completer beeld van de prevalentie van online slachtofferschap dan studies op basis van politieregistraties.

4.1.2 Risicofactoren voor online slachtofferschap

Het tweede deel van dit onderzoek richtte zich op mogelijke risicofactoren voor online slachtofferschap: *in hoeverre hangt online slachtofferschap samen met eerder slachtofferschap, internetgebruik, beschermingsmaatregelen en persoonskenmerken?* Doordat respondenten in het LISS-panel in zes meetmomenten over tien jaar zijn bevraagd naar hun slachtofferervaringen, online gedragingen en persoonlijkheidskenmerken, was het mogelijk de samenhang van de risicofactoren op de kans op online slachtofferschap vast te stellen.

Eerder slachtofferschap
Eerdere slachtofferervaringen hangen samen met de kans op een nieuwe slachtofferervaring: respondenten die tijdens een vorig meetmoment aangaven slachtoffer te zijn geweest van online criminaliteit, hebben een grotere kans ook in het jaar voorafgaand de volgende meting slachtoffer te worden. In paragraaf 4.1.4 wordt uitgebreid ingegaan op de groep herhaald slachtoffers.

Internetgebruik en beschermingsmaatregelen
Om inzicht te krijgen in de mate waarin de kans op slachtofferschap samenhangt met online gedragingen, zijn respondenten gevraagd naar hun internetgebruik en getroffen beschermingsmaatregelen. Respondenten die meer gebruikmaken van internet hebben meer kans om slachtoffer van online criminaliteit te worden. Hoewel de *overall* prevalentie van online slachtofferschap is gedaald, toont deze bevinding dat er op individueel niveau wel een samenhang is tussen internetgebruik en slachtofferschap van online criminaliteit. Deze bevinding kan worden verklaard vanuit de routine activiteiten theorie (Cohen & Felson, 1979), waarin het uitgangspunt is dat slachtofferschap van een online delict waarschijnlijker wordt naarmate internetgebruikers door middel van online activiteiten meer blootgesteld worden aan daders.

Daarnaast was, in tegenstelling tot wat we zouden verwachten, de kans op online slachtofferschap niet geassocieerd met het aantal getroffen beschermingsmaatregelen tijdens een voorgaand meetmoment. Een mogelijke verklaring hiervoor is dat de in dit onderzoek meegenomen beschermingsmaatregelen (o.a. het hebben van een virusscanner of een beveiligd draadloos netwerk) met name beschermen tegen computervirussen en in mindere mate tegen online bedreiging. Dit is getest in aanvullende analyses, maar ook in de analyses opgesplitst naar delict is er geen samenhang tussen beschermingsmaatregelen en online slachtofferschap gevonden. Dit in tegenstelling tot de studie van Wijn et al. (2016) die laat zien dat beschermende maatregelen zoals virusscanners een risicoverlagende werking hebben op hacken.

Persoonskenmerken
Vervolgens is bestudeerd in hoeverre persoonskenmerken samenhangen met online slachtofferschap. Daaruit blijkt dat jongere respondenten meer kans hadden om online slachtoffer te worden. Ook mannen en respondenten met kinderen hebben een grotere kans om slachtoffer van online criminaliteit te worden. Verder hebben respondenten met een hogere score op impulsiviteit of openheid, of een lagere score op emotionele stabiliteit een grotere kans om online slachtoffer te worden. In tegenstelling tot slachtofferschap van online criminaliteit is er bij offline criminaliteit geen samenhang zichtbaar tussen impulsiviteit en de kans op slachtofferschap. De kans op offline slachtofferschap is wel geassocieerd met een hogere score op altruïsme en openheid en een lagere score op consciëntieusheid en emotionele stabiliteit.

De bevindingen komen overeen met een aantal eerdere studies naar de relatie tussen persoonskenmerken en online slachtofferschap. Zo worden impulsieve mensen beduidend vaker gehackt (Van Wilsem, 2013b), beantwoorden emotioneel instabiele mensen vaker *phishing* e-mails (Halevi et al., 2013), en zijn open mensen meer geneigd online informatie te delen en schermen zij deze informatie minder goed af (Halevi et al., 2013). In een eerder onderzoek onder e-fraudeslachtoffers waren echter andere verbanden zichtbaar: slachtoffers van *phishing* en online aankoopfraude scoorden hoger op extraversie, altruïsme en consciëntieusheid en emotionele stabiliteit (Borwell et al., 2018). Dit verschil komt mogelijk doordat het een apart type slachtoffers betreft en het aandeel fraudeslachtoffers in onze studie relatief klein was.

De samenhang tussen bovenstaande persoonlijkheidskenmerken en online criminaliteit kunnen worden bezien in het licht van de *zelfcontroletheorie* (Gottfredson & Hirschi, 1990; Pratt et al., 2014), die stelt dat impulsief handelen, een focus op korte-termijndoelen en het negeren van lange-termijndoelen ertoe kunnen leiden dat men sneller betrokken raakt in diverse probleemsituaties. Deze theorie is in cross-sectioneel onderzoek al eerder bevestigd: impulsieve mensen hebben een grotere kans om te worden gehackt (Van Wilsem, 2013b). Door de bevindingen in het huidige onderzoek kan deze zelfcontroletheorie ook voor andere online delicten worden bevestigd: respondenten met een hogere impulsiviteitsscore hebben een grotere kans om slachtoffer te worden van online criminaliteit.

4.1.3 Gevolgen van online slachtofferschap

Door te kijken naar de verandering in angst voor criminaliteit, internetgebruik en mentaal welbevinden na een slachtofferervaring, zijn mogelijke gevolgen van online slachtofferschap onderzocht. De onderzoeksvraag '*in hoeverre heeft online slachtofferschap gevolgen voor angst voor criminaliteit, internetgebruik, beschermingsmaatregelen en mentale gezondheidsproblemen?*' kon hiermee worden beantwoord.

Angst voor online criminaliteit, internetgebruik en beschermingsmaatregelen

De eerste bevinding is dat slachtoffers van online criminaliteit een grotere angst voor online criminaliteit laten zien. Deze angst is met name relevant omdat het mogelijk weerslag heeft op de online participatie van slachtoffers. Van slachtoffers van offline criminaliteit is bekend dat ze bepaalde gelegenheden mijden om de kans om opnieuw slachtoffer te worden te verkleinen, zoals 's avonds de straat op gaan (Averdijk, 2010; Skogan, 1987). Mensen die de gevaren van online criminaliteit zien, zullen mogelijk wegblijven van het internet (Brands & Van Wilsem, 2019). Echter, in het huidige onderzoek hangt slachtofferschap niet significant samen met een verandering in internetgebruik. In deze steeds meer gedigitaliseerde samenleving is het haast onmogelijk om je aan het digitale leven te onttrekken, en dit geldt ook voor slachtoffers van online criminaliteit. De angst voor criminaliteit neemt vooral toe onder slachtoffers van fraude gerelateerde delicten, zoals creditcardfraude, ongeautoriseerde bankafschrijvingen en online aankoopfraude. Het is daarom interessant om te onderzoeken of online gedragingen die meer direct gerelateerd zijn aan dit type criminaliteit wel gemeden worden, zoals online bankieren of online shoppen.

Beschermingsmaatregelen nemen toe na een slachtofferervaring. Dit is in lijn met de eerdere bevinding van Holt en Bossler (2013). Hun cross-sectionele studie laat zien dat mensen die meer beschermingsmaatregelen treffen een grotere kans

hebben om slachtoffer te worden, terwijl je zou verwachten dat deze mensen juist een kleinere kans hebben om slachtoffer te worden. Een logische verklaring is dat genomen beschermingsmaatregelen een gevolg in plaats van een oorzaak zijn van een slachtofferervaring. Onze longitudinale studie laat zien dat beschermingsmaatregelen voorafgaand aan de meting van slachtofferschap geen invloed hebben op de kans op online slachtofferschap, terwijl online slachtoffers wel meer beschermingsmaatregelen gaan treffen. Interessant is dat het treffen van beschermingsmaatregelen het risico op slachtofferschap dus niet zozeer lijkt te verkleinen, maar wel een gevolg van online slachtofferschap lijkt te zijn.

Verder is gekeken naar verschillen in beschermingsmaatregelen tussen slachtoffers die aangifte hebben gedaan versus degenen die dat niet hebben gedaan. Opvallend is dat slachtoffers die geen aangifte hebben gedaan meer beschermingsmaatregelen treffen, terwijl er geen verandering in beschermingsmaatregelen is onder de slachtoffers die wel aangifte hebben gedaan. Verwacht werd dat juist degenen die aangifte doen door de politie worden gewezen op het belang van beschermingsmaatregelen en daardoor bij deze groep een stijging in het aantal beschermingsmaatregelen te zien zou zijn. Een mogelijke verklaring voor deze tegenstrijdige bevinding is dat de beschermingsmaatregelen die in dit onderzoek zijn gemeten, betrekking hebben op het beschermen van de pc, zoals het installeren van een virusscanner of het beveiligen van het online netwerk, terwijl juist de delicten die ernstiger van aard zijn en waar slachtoffers eerder aangifte van zullen doen, zoals online bedreiging of online aankoopfraude waar een hoog bedraag mee gemoeid is, niet opgelost kunnen worden met deze beschermingsmaatregelen. De typen delicten die slachtoffers ertoe zetten meer maatregelen te treffen, zijn vooral de delicten die direct betrekking hebben op de computer, namelijk computervirussen of ongeautoriseerde bankafschrijvingen. Een mogelijke andere verklaring is dat slachtoffers op het moment dat ze aangifte doen de verantwoordelijkheid voor de oplossing van het probleem bij de politie neerleggen. Daardoor zijn ze mogelijk minder geneigd om zelf handelingen te verrichten die een kans op een nieuwe slachtofferervaring verkleinen, zoals het nemen van beschermingsmaatregelen.

Mentale gezondheid

Hoewel de angst voor online criminaliteit is toegenomen, neemt het mentaal welbevinden niet af na een online slachtofferervaring. In tegenstelling tot de kwalitatieve studie van Leukfeldt et al. (2018) liet zien dat online slachtofferschap grote impact kan hebben op het mentaal welbevinden, blijkt dit niet te gelden als we een representatieve steekproef van slachtoffers onderzoeken. Waar relatief veel mensen een slachtofferervaring hebben (van 15,1% in 2010 tot 9,5% in 2018), heeft dit *overall* geen grote invloed op hun mentaal welbevinden. Een mogelijke verklaring waarom voor algemeen online slachtofferschap geen effect is gevonden, is de ernst van de onderzochte delicten, die – als alle type delicten samen worden onderzocht – relatief laag is. Een andere mogelijke verklaring waarom uit ons onderzoek geen negatieve invloed van online slachtofferschap op de mentale gezondheid naar voren komt, is dat de invloed slechts van korte duur is en daarna weer wegebt. In het huidige onderzoek is gewerkt met afnamen die twee jaar uit elkaar liggen. Als de metingen van slachtofferschap en mentale gezondheid korter na elkaar zouden zijn, zouden we mogelijk wel een daling in de mentale gezondheid ontdekken.

De relatie tussen mentale gezondheid en de zeven typen delicten apart, is ook onderzocht. Hieruit blijkt een significante relatie tussen negatieve gevolgen op de mentale gezondheid na online bedreiging. Van alle delicten die we onderzoeken, valt te verwachten dat online bedreiging, naast identiteitsfraude, de grootste inbreuk

heeft op de persoonlijke levenssfeer en daarmee de sterkste invloed op de mentale gezondheid. Voor identiteitsfraude vinden we geen significante samenhang met mentaal welbevinden. Een mogelijke verklaring hiervoor is het relatief lage aantal slachtoffers van dit type delict in onze data (n=28). Online bedreiging kan bijvoorbeeld als ernstiger worden ervaren dan het oplopen van een computervirus. Ook de onderzochte delicten in Leukfeldt et al. (2018) zijn ernstiger van aard (bijvoorbeeld *sexting*) dan sommige van de in dit onderzoek meegenomen delicten. Een interessante vervolgvraag is om dieper in te gaan in de (ervaren) ernst van een slachtofferervaring om beter onderscheid te maken welke slachtoffers wel en welke slachtoffers geen negatieve gevolgen ervaren. Daarnaast zou het ook kunnen komen doordat zelfgerapporteerde mentale gezondheid een vrij algemene maat is, die sterk beïnvloed wordt door andere aspecten in iemands leven. Mogelijk zouden we wel een effect vinden als we meer specifieke problemen zouden bevragen, zoals 'Houdt die gebeurtenis u nog bezig?' met mogelijk antwoordcategorieën van 'in het geheel niet' tot 'het beheerst mijn hele doen en laten' (zie ook Lamet & Wittebrood, 2009).

4.1.4 Herhaald online slachtofferschap

De laatste onderzoeksvraag had betrekking op herhaald slachtofferschap en luidde: *in welke mate is er sprake van herhaald slachtofferschap en in welke mate vormen de mogelijke gevolgen van online slachtofferschap een verklaring voor herhaald slachtofferschap?*

Mate van herhaald slachtofferschap
Om de mate van herhaald online slachtofferschap te meten, zijn alle online slachtofferervaringen per respondent bij elkaar opgeteld. De groep respondenten die herhaald slachtoffer was geworden, was met 17,5% iets groter dan de groep eenmalig slachtoffers (16,6%). Als we alleen respondenten meenemen die op alle zes de meetmomenten hebben deelgenomen, en daarmee een grotere kans hebben gehad om online slachtofferschap te rapporteren, ligt het percentage van herhaald en eenmalig slachtoffers iets hoger (respectievelijk 20,9% en 18,7%). Deze percentages zijn afhankelijk van het aantal deelnames, en gezien de eerder benoemde selectieve paneluitval is er hier mogelijk in mindere mate sprake is van een representatieve steekproef dan bij de onder paragraaf 4.1.1 besproken prevalenties.

Verklaringen herhaald online slachtofferschap
In dit rapport is onderzocht of achtergrond- en persoonlijkheidskenmerken invloed hebben op de cumulatie van slachtofferervaringen. Hieruit blijkt dat impulsieve, emotioneel instabiele en meer open respondenten een grotere kans hebben om herhaald slachtoffer te worden, maar ook een grotere kans hebben om eenmalig dan nooit slachtoffer te worden. Tevens blijken deze persoonlijkheidskenmerken binnen de groep van herhaald slachtoffers samen te hangen met het aantal slachtofferervaringen. Uit de robuustheidsanalyses waar een nog specifieker onderscheid in de groep herhaald slachtoffers is gemaakt komt ook weer naar voren dat de verbanden het sterkst zijn voor de groep die het vaakst slachtoffer is geworden, namelijk de slachtoffers die zowel meerdere delicten als hetzelfde delict herhaaldelijk hebben meegemaakt. De invloed van impulsiviteit, emotionele instabiliteit en openheid is robuust en verloopt dus gradueel: hoe hoger men scoort op deze persoonlijkheidskenmerken, hoe vaker men kans loopt slachtoffer te worden van online criminaliteit. De overige bevindingen laten zien dat mannen in vergelijking met vrouwen een grotere kans hebben om herhaald slachtoffer te worden. Mannen hebben echter geen grotere kans om eenmalig slachtoffer te worden dan nooit

slachtoffer, wat betekent dat geslacht wel een risicofactor is voor herhaaldelijk slachtofferschap en niet voor eenmalig slachtofferschap. Leeftijd, daarentegen, is een risicofactor voor zowel eenmalig als herhaald slachtofferschap, maar lijkt vervolgens geen invloed te hebben op het verschil tussen herhaald en eenmalig slachtoffers.

In de literatuur bestaan twee theoretische stromingen die de kans op herhaald slachtofferschap kunnen verklaren (Van Reemst et al., 2013). Ten eerste kunnen de factoren die een risico vormen voor een eerste slachtofferervaring ook verklaren waarom iemand nogmaals slachtoffer wordt. Aangezien de besproken risicofactoren van herhaald slachtofferschap ook invloed hebben op online slachtofferschap in algemene (paragraaf 4.2), betekent dit dat risicofactoren voor herhaald slachtofferschap overeenkomen met de risicofactoren voor een *eerste* slachtofferervaring. Volgens een tweede theoretische stroming kan eerder slachtofferschap zelf, en de gevolgen daarvan, een risicofactor vormen voor een nieuwe slachtofferervaring (Wittebrood, 2006). Door de eerder besproken resultaten met betrekking tot de risicofactoren en gevolgen van online slachtofferschap te combineren, kan worden nagegaan in hoeverre evidentie bestaat voor deze theoretische stroming. De mate van internetgebruik en de mentale gezondheid veranderen niet na online slachtofferschap en bieden daarmee geen verklaring waarom slachtoffers *opnieuw* slachtoffer worden. Wel vinden we dat beschermingsmaatregelen toenemen na een slachtofferervaring, maar het nemen van beschermingsmaatregelen lijkt vervolgens het risico op slachtofferschap niet te verlagen. Deze resultaten impliceren dat de hier onderzochte dynamische kenmerken niet bijdragen aan een beter begrip van herhaald slachtofferschap.[18]

Herhaald versus meervoudig slachtofferschap
De door ons gehanteerde operationalisatie van herhaald slachtofferschap was vrij breed. Zowel degenen die meerdere keren slachtoffer waren van hetzelfde delict als degenen die slachtoffer waren van verschillende delicten werden meegenomen als herhaald slachtoffer. Uit robuustheidsanalyses bleek dat dit onderscheid tussen deze twee vormen van herhaald slachtofferschap niet uitmaakte. De risicofactoren geslacht, impulsiviteit, emotionele stabiliteit en openheid hingen juist samen met de groep die van zowel hetzelfde delict als meerdere delicten herhaald slachtoffer was geworden. Ook kon herhaald slachtofferschap zowel op één meetmoment als verspreid over meerdere meetmomenten hebben plaatsgevonden. Uit de robuustheidsanalyses is ook gebleken dat de gevonden effecten het sterkst zijn voor de groep die zowel op één meetmoment als op meerdere meetmomenten herhaald slachtoffer is. Ook als we kijken naar de frequentie van herhaald slachtofferschap, om de risicofactoren van zogenoemde *supertargets* in kaart te brengen (Farrell et al., 2005), zien we een effect van impulsiviteit, emotionele stabiliteit en openheid. De invloed van deze risicofactoren op de kans om vaak slachtoffer te worden, lijkt dus vrij robuust te zijn.

Al met al kan dus worden geconcludeerd dat het met name de meer statische persoonskenmerken zijn die herhaald slachtofferschap verklaren, en in mindere mate de dynamische factoren. Interessant is dat uit paragraaf 3.2 bleek dat deze kenmerken ook de risicofactoren zijn waardoor respondenten überhaupt slachtoffer werden. De verklaringen voor de prevalentie van eenmalig online slachtofferschap

18 Angst voor criminaliteit lijkt ook toe te nemen na een slachtofferervaring, maar is in dit rapport niet meegenomen als risicofactor.

lijken dus overeen te komen met de verklaringen voor de frequentie van herhaald slachtofferschap.

4.2 Sterke punten en beperkingen van het onderzoek

4.2.1 Sterke punten van het onderzoek

Een belangrijke meerwaarde ten opzichte van eerder onderzoek is het longitudinale en representatieve karakter van het huidige onderzoek. In Nederland zijn nog relatief weinig studies uitgevoerd naar online slachtofferschap op basis van een steekproef die representatief is voor de Nederlandse bevolking. Bovendien zijn in dit onderzoek dezelfde groep respondenten op meerdere momenten bevraagd. Doordat respondenten zesmaal over een periode van tien jaar (2008-2018) zijn bevraagd naar hun slachtofferervaringen, gedragingen en gemoedstoestanden, kunnen oorzaak-gevolgrelaties beter worden vastgesteld dan in het reguliere cross-sectionele slachtofferonderzoek waarin deze factoren tegelijkertijd worden bevraagd. Dergelijk longitudinaal slachtofferonderzoek is dun gezaaid – en dat geldt des te meer voor onderzoek naar online slachtofferschap. Een voorbeeld van een oorzaak-gevolgrelatie waar meer zicht op is gekomen, is de wederkerige relatie tussen preventiegedrag en slachtofferschap: het treffen van beschermingsmaatregelen (zoals een virusscanner) kan de kans op slachtofferschap verlagen, maar andersom kan het ook zijn dat men als gevolg van slachtofferschap juist meer beschermingsmaatregelen zal treffen. Op basis van cross-sectioneel onderzoek kan dit onderscheid niet gemaakt worden, immers beide factoren zijn in dergelijk onderzoek niet in de tijd te onderscheiden. Een groot voordeel aan het huidige onderzoek is dat dit onderscheid hier wel gemaakt kan worden en eerdere cross-sectionele bevindingen beter kunnen worden geduid. Met betrekking tot beschermingsmaatregelen vonden we bijvoorbeeld dat het treffen van beschermingsmaatregelen geen effect had op de kans op online slachtofferschap, maar dat slachtoffers van online criminaliteit na hun slachtofferervaring wel meer beschermingsmaatregelen troffen.

Het gebruik van zelfrapportage is, ondanks dat het ook zijn beperkingen kent (zoals wordt besproken in de volgende paragraaf), ook een belangrijk pluspunt van de huidige studie. Omdat slechts een beperkt deel van de cyber- en gedigitaliseerde criminaliteit in beeld is bij politie of justitie, levert het gebruik van zelfrapportage naar verwachting een beter beeld op van de omvang van online slachtofferschap. Dit wordt in de vraag naar de aangiftebereidheid in het huidige onderzoek ook bevestigd, waarin gemiddeld één op de vier respondenten heeft aangegeven bij de politie aangifte te hebben gedaan van de slachtofferervaring. De huidige studie geeft dus zeer waarschijnlijk een completer beeld van de prevalentie van online slachtofferschap dan studies op basis van politieregistraties.

4.2.2 Beperkingen van het onderzoek

De huidige studie kent een aantal beperkingen. Een eerste beperking is dat het aantal delicten met betrekking tot online criminaliteit in het huidige onderzoek beperkt is gebleven tot zeven delicten: gehackt worden, computervirussen, ongeautoriseerde bankafschrijvingen, creditcard fraude, online aankoopfraude, identiteitsfraude en online bedreiging. Dat betekent dat verschillende typen van cyber- en gedigitaliseerde criminaliteit weliswaar onderzocht zijn, maar dat er alsnog relevante delicten ontbreken, zoals de verspreiding van seksueel beeldmateriaal. Mogelijk heeft er in de loop van de tijd een verschuiving plaatsgevonden

in de aard van online delicten, waardoor een aantal 'nieuwe' delicten (malware, ransomware, etc.) onderbelicht zijn gebleven. Dit betekent dat er met het huidige onderzoek geen zicht is gekomen op *alle* vormen van online criminaliteit – maar dat is in de context van een langlopend longitudinaal onderzoek ook nauwelijks mogelijk. Ook de ernst van de delicten is in deze studie onderbelicht gebleven. Weliswaar is voor sommige delicten verder gevraagd naar de ervaren ernst of geleden (financiële) schade, maar omdat die bevraging beperkt bleef tot drie delicten is dit niet uitgebreid onderzocht. Extra vragen over alle typen delicten zouden een waardevolle toevoeging zijn geweest om meer inzicht te bieden in de onderliggende ernst van de delicten – ook om na te gaan of deze ernst gerelateerd is aan de gevolgen voor het slachtoffer op het gebied van mentaal welzijn, internetgebruik en preventiegedrag. Zo kan gehackt worden inhouden dat een ander eenmalig op een Facebook account is ingelogd, maar ook dat de gehele computer is overgenomen.

Een tweede beperking van dit onderzoek is dat, ondanks de grote steekproef van 13.430 respondenten, het aantal slachtoffers van bepaalde delicten toch beperkt was. Dat is niet direct zorgwekkend, aangezien bepaalde delicten gewoonweg weinig voorkomen in de populatie. Dat houdt echter wel in dat het lastig was om de gevolgen van de betreffende delicten te bestuderen. Identiteitsfraude kwam bijvoorbeeld relatief weinig voor in de steekproef en bleek geen significante gevolgen te hebben voor de mentale gezondheid van slachtoffers. Het is echter lastig vast te stellen of identiteitsfraude daadwerkelijk geen effect had op de mentale gezondheid, of dat dat door het beperkte aantal respondenten en het gebrek aan zogenoemde power in de statistische modellen niet naar voren is gekomen in de analyses.

Hoewel slachtofferenquêtes een krachtig instrument zijn om slachtofferervaringen onder een representatief deel van de Nederlandse bevolking te achterhalen, is ook dit instrument niet perfect. Slachtofferenquêtes zijn namelijk retrospectief van aard en uit eerdere studies is gebleken dat dergelijke gegevens niet altijd even nauwkeurig of betrouwbaar zijn, doordat respondenten gebeurtenissen niet meer konden herinneren of doordat zij gebeurtenissen eerder of later in de tijd plaatsten (Lamet & Wittebrood, 2009). De kwaliteit van de retrospectieve gegevens kan echter positief worden beïnvloed door de vraagstelling en de gebruikte referentieperiode. In het huidige onderzoek is bijvoorbeeld eerst gevraagd naar slachtofferschap over een ruimere referentieperiode (de afgelopen twee jaar) en pas daarna over de eigenlijke referentieperiode (de afgelopen twaalf maanden) (Lamet & Wittebrood, 2009). Tevens is een extra controle ingevoerd door eerst naar de prevalentie en daarna naar de incidentie van slachtofferervaringen te vragen.

Ten slotte kent de huidige studie, ondanks het longitudinale panel-design, ook een beperking in het vaststellen van oorzaak-gevolgrelaties. Hierbij is het belangrijk ons te realiseren dat het gros van de gegevens retrospectief over de afgelopen twaalf maanden is bevraagd, waardoor de exacte timing van verschillende gebeurtenissen lastig vast te stellen is. We hebben geprobeerd dit te verhelpen door voor de risicofactoren te kijken naar de samenhang tussen factoren op het voorgaande meetmoment (bijvoorbeeld 2010) en slachtofferschap op het daaropvolgende meetmoment (bijvoorbeeld 2012; waarbij slachtofferschap retrospectief over de twaalf maanden voorafgaand – en dus over de periode 2011-2012 – is gevraagd), waardoor de mogelijke risicofactoren in ieder geval zijn gemeten vóórdat het slachtofferschap heeft plaatsgevonden. Voor de gevolgen hebben we om diezelfde reden bestudeerd of slachtofferschap in de twaalf maanden voorafgaand aan het

moment dat het mogelijke gevolgen zijn gemeten. Hierdoor is zo goed mogelijk rekening gehouden met de timing van de gebeurtenissen, maar is het niet zeker dat deze gebeurtenissen daadwerkelijk strikt gescheiden zijn. Specifiek voor mentale gezondheid geldt dat dit drie maanden vóór slachtofferschap is gemeten, waardoor het mogelijk is dat slachtofferervaringen niet in de negen maanden voor de meting van mentale gezondheid, maar in werkelijkheid in de drie maanden ná de meting van mentale gezondheid hebben plaatsgevonden. Als controle hebben we de analyses ook uitgevoerd op basis van de mentale gezondheid negen maanden ná de slachtofferervaring. Voor totaal online slachtofferschap was er – in beide analyses – geen significant effect op mentale gezondheid zichtbaar. Voor slachtoffers van online bedreiging was in de originele analyses (i.e. waarin mentale gezondheid drie maanden vóór slachtofferschap is gemeten) wel een significante afname in mentale gezondheid gevonden, maar wanneer de mentale gezondheid negen maanden na slachtofferschap was gemeten, was dit effect niet meer aanwezig. Een mogelijke verklaring hiervoor is dat de invloed van een slachtofferervaring op de mentale gezondheid in de maanden na de ervaring wegebt. We hebben daarom de meting van drie maanden voor slachtofferschap gebruikt in dit onderzoek.

4.3 Aanbevelingen voor vervolgonderzoek

Op basis van de huidige studie kunnen enkele suggesties gedaan worden voor toekomstig onderzoek. Allereerst verdient het de aanbeveling om de afname van de vragenlijst onder het LISS-panel te continueren. De huidige dataverzameling is uniek in zijn soort, en een nieuwe meting zou meer inzicht bieden in het verloop van de trend. Gezien de verschillende vragenlijsten die bij het LISS-panel worden afgenomen, biedt het panel mogelijkheden om de slachtofferenquêtes te verrijken met andere data. Bij een nieuwe afname van het LISS-panel kan tevens slachtofferschap over meer – met name nieuwe – vormen van online criminaliteit worden meegenomen. De vraag over computervirussen zou bijvoorbeeld vervangen kunnen worden met een vraag over *ransomware*, en vragen over *phishing, sexting* of diefstal van digitale goederen zouden kunnen worden toegevoegd. Bovendien kunnen vragen worden opgenomen over de overlap tussen offline en online slachtofferervaringen. Bijvoorbeeld of er opnames zijn gemaakt van een offline slachtofferervaring, zoals mishandeling, die vervolgens online verschijnt, wat de negatieve impact op het slachtoffer kan vergroten. In een toekomstige afname onder het LISS-panel zou het waardevol zijn om de vragenlijst uit te breiden met nieuwere delicten en daarbij de vergelijkingsmogelijkheden met eerdere meetmomenten te behouden.

In dit onderzoek hebben we verschillende risicofactoren voor online slachtofferschap naast elkaar gezet. Hieruit blijkt echter geen slachtofferprofiel, de risicofactoren zijn niet bij elkaar ‘op te tellen’. Een interessante vervolgstap is om slachtofferprofielen in kaart te brengen, bijvoorbeeld aan de hand van clusteranalyse. Zijn bepaalde risicofactoren geconcentreerd in een bepaalde groep die mogelijk de grootste kans heeft om slachtoffer te worden? Deze vraag kan nog beter inzicht bieden op wie beleidsinterventies zich dienen te richten om online slachtofferschap te voorkomen.

Een tweede suggestie voor vervolgonderzoek is om de invloed van beleid in Nederland op online slachtofferschap te bestuderen. In het huidige onderzoek hebben we ons met name gericht op factoren op persoonlijk niveau die van invloed zijn op de kans op online slachtofferschap. Ook veranderingen in macrofactoren, zoals meer

gerichte inzet van de politie of effectieve (preventie)campagnes, kunnen een rol spelen in de dalende online criminaliteit. Het huidige onderzoek kan echter geen inzicht bieden in de invloed van dergelijke macrofactoren. Daarvoor zou aanvullend (internationaal) onderzoek een waardevolle toevoeging zijn.

4.4 Conclusie

De eerste conclusie van dit rapport is dat slachtofferschap van zeven typen online delicten tussen 2010 en 2018 is gedaald onder een representatieve steekproef van de Nederlandse bevolking, waarbij het type online delict dat het meeste voorkomt is verschoven van computervirussen naar aankoopfraude. Hoewel over het algemeen een dalende trend aanwezig is, laat dit onderzoek onverminderd zien dat een deel van de Nederlandse bevolking ooit slachtoffer is geworden van één van de onderzochte online delicten. Om die reden zijn ook de risicofactoren en gevolgen van deze slachtofferervaringen in kaart gebracht.

Internetgebruik blijkt – niet geheel verassend – één van de risicofactoren voor online slachtofferschap, aangezien de gelegenheid tot online criminaliteit groter is naarmate men zich meer online begeeft. Mensen die eerder online slachtoffer zijn geworden, mannen en jongere mensen, lopen ook een verhoogd risico op online slachtofferschap. Impulsieve mensen, emotioneel instabiele mensen en meer open mensen hebben daarentegen niet alleen meer kans om één keer slachtoffer te worden, maar ook om herhaald slachtoffer te worden van online criminaliteit. Een mogelijke verklaring voor de sterke samenhang tussen deze persoonlijkheidskenmerken en online slachtofferschap, is dat deze kenmerken een indicatie zijn voor online risicogedrag. Zo zullen impulsieve mensen tijdens hun handelen minder nadenken over mogelijke risico's, hebben emotioneel instabiele mensen meer moeite om risico's in te schatten, en hebben open mensen een grotere kans om online gegevens te delen. Niet alleen het internetgebruik zelf, maar ook de manier waarop men zich op het internet gedraagt, lijkt dus een risicofactor voor online slachtofferschap. Beleid dat burgers wil wijzen op online gevaren kan rekening houden met de persoonlijkheidskenmerken van potentiële slachtoffers. Waarschuwingen over online risico's hebben mogelijk een minder goede uitwerking op impulsieve mensen dan op niet-impulsieve mensen, omdat impulsieve mensen eerder geneigd zijn te handelen zonder na te denken over de mogelijke consequenties van hun online gedrag.

Het huidige onderzoek laat zien dat slachtoffers van online criminaliteit niet minder gebruikmaken van het internet. Uit de literatuur naar offline slachtofferschap weten we dat slachtoffers de plek waar het delict heeft plaatsgevonden na hun slachtofferervaring zijn gaan mijden. In deze steeds meer gedigitaliseerde samenleving is het echter voor online slachtoffers haast onmogelijk om zich aan het digitale leven te onttrekken. Slachtoffers van online criminaliteit ervaren over het algemeen geen verslechtering in hun mentale gezondheid. Alleen slachtoffers van online bedreiging laten een daling in hun mentale gezondheid zien. Slachtoffers van online criminaliteit lijken zich desalniettemin bewust van hun eerdere slachtofferervaring, gezien ze gemiddeld genomen een grotere angst voor online criminaliteit rapporteren en meer beschermingsmaatregelen hebben getroffen dan vóór hun slachtofferervaring. Deze bevinding laat zien dat slachtoffers bereid zijn hun online gedrag aan te passen, en dat het relevant is (potentiële) slachtoffers te wijzen op wat ze kunnen doen om de kans op een nieuwe slachtofferervaring te verkleinen.

Summary

Online victimization
Prevalence, risk factors and consequences

Online crime victimization has become one of the major challenges in our digitalized society. Almost everybody is connected to the internet and exposed to potential online offenders. The goal of this study is to gain more insight in the prevalence, risk factors and consequences of online victimization among Dutch people aged 16 years and older. Online crime can be divided into cybercrime and digitalized crime. Cybercrimes can only be committed using information communications technology (ICT), like computer viruses and hacking. Digitalized crimes are traditional offline crimes that are enabled by an ICT-component, such as online fraud and online harassment.

This study includes seven types of online crime: credit card fraud, hacking, online consumer fraud, online harassment, computer viruses, unauthorized bank withdrawal and identity fraud. First, the prevalence of these types of crime is estimated. Second, the question to what extent age, gender, education, internet use, online protection measures and personality traits affect the chance to become victim of online crime is answered. We also investigate to what extent these risk factors for online crime are risk factors for offline crime. Third, we study to what extent online victimization correlates with changes in fear of online crime, internet use, online protection measures and mental health of victims. Fourth, we study to what extent risk factors for a first online victimization are also risk factors for repeated online victimization.

Research questions

The central research question of this study is: what are the trends, risk factors and consequences of (repeated) online victimization?

In order to answer this research question, we answered the following sub-questions:
1 To what extent have Dutch citizens become victim of online crime?
2 To what extent does online victimization correlate with previous online victimization, internet use, online protection measures, socio-demographic characteristics and personality traits?
3 To what extent are fear of online crime, internet use, online protection measures and mental health consequences of online victimization?
4 To what extent have Dutch citizens become repeated victims of online crime, and to what extent do potential consequences of previous online victimization affect the chance on repeated online victimization?

Methods

In order to answer the research questions, we use data from the LISS-panel, an online survey among a representative sample of Dutch households. Participants of the LISS-panel have been questioned monthly on various themes, such as their personality, health and leisure activities. Since February 2008, respondents have

participated in a biennial survey on victimization that includes question about victimization of several types of online and offline crimes. We used six waves of this survey with around 5,000 to 6,000 respondents each.

Results

Online victimization decreased between 2010 and 2018

Results show a significant decrease in the number of victims of the seven types of online crimes combined, from 15.1% in 2010 to 9.5% in 2018. The most prevalent type of online crime has also changed, from computer viruses in 2010 to online consumer fraud in 2018. The number victims of offline crime was slightly higher, but also significantly decreased in the past decade (from 20.5% in 2010 to 12.4% in 2018). The decline in prevalence of online victimization is mainly attributed to the decrease in victims of computer viruses (8.9% in 2010 and 1.7% in 2018). The prevalence of hacking (1.4% in 2010 and 0.9% in 2018) and unauthorized bank withdrawal (3.0% in 2010 and 1.2% in 2018) has also decreased. The prevalence of online consumer fraud and identity fraud has significantly increased. Only a minority of victims have filed a police report: 11.6% of unauthorized bank withdrawal victims, 12.0% of online consumer fraud victims, 20.2% of online harassment victims and 46.0% of identity fraud victims.

Higher risks among men, young people and frequent internet users

Victims of online crime in a previous wave are at higher risk of becoming victim in a subsequent wave. The more hours one spends online, the more likely one is to become victim of online crime. One would expect that using more online protection measures would protect internet users against online victimization, but, surprisingly, having taken more protection measures does not lower the risk of online victimization. Other people who are at higher risk of online victimization are men, young people, impulsive people, emotionally instable and more open people. We also tested whether these risk factors for online victimization are risk factors for offline victimization. Age, emotional instability and openness appeared to be risk factors for both types of crime. Gender is also a risk factor for offline victimization, but in an opposite direction. Men are more likely to become online victim than women, whereas women are more likely to become offline victim than men. Offline victimization is also more prevalent among more altruistic and less conscientiousness people. Impulsivity is correlated with online victimization, but not with offline victimization, and can therefore be regarded as a distinctive risk factor for online victimization.

Fear of online crimes increases, but mental well-being does not change after online victimization

Victims of online crime report an increased fear for online crime. Even though this fear may withhold victims to use the internet, this study does not show a change in internet use among online victims. They do, however, take more protection measures than before, especially those who did not report the crime to the police. A possible explanation is that protection measures are taken by victims of computer viruses, whereas these victims may be less likely to report to the police compared to victims of more serious crimes. The mental well-being of victims does not change among online victims in general, but it decreases among victims of online harass-

ment, possibly because online harassment has a more serious impact on a victim's personal life than other types of online crime.

Repeat victimization correlates with impulsivity, emotional instability and openness

16.6% of the respondents who participated at least two times reported that they fell victim to online crime just once, whereas 17.5% reported to have fallen victim repeatedly. The more impulsive, emotionally instable or open, the higher the chance to become a repeat victim of online crime. Possible consequences of previous online victimization do not seem to explain why people fall victim again. Internet use and mental well-being do not change after previous online victimization, and can therefore not explain why these people would be more likely to be victimized again. The number of protection measures do increase after online victimization, but do not affect the chance to become victim again.

Strengths and weaknesses

The main contribution to the existing literature on online victimization is the use of longitudinal panel data, gathered between 2008 and 2018. The temporal order of events and behaviour is clearer using panel data and therewith more suited in estimating risk factors and consequences of online victimization than studies that use cross-sectional data. Another strength of this study is the use of self-reported online victimization. Because not all crimes are reported to the police, these data have a larger scope than police records. The weakness of self-reported online victimization is that it depends on the interpretation and memory of victims themselves who, for instance, may forget when the crime has actually taken place. Besides, not every type of crime was included in the survey. More recent types of online crime, such as malware and ransomware, were therefore not taken into account in estimating the number of online victims.

Conclusion

The number of victims of seven types of online crimes has decreased among a representative sample of Dutch citizens. One of the risk factors is internet use, as people are more likely to be exposed to potential cyber offences when they spend more hours online. People who fell victim to an online crime before, men and young people have a higher risk to become victim. People who are impulsive, emotionally instable or more open are even more likely to be victimized repeatedly than people who are respectively less impulsive, less emotionally instable or less open. These personality traits are possible proxies of online behaviour. Impulsive people may think less about possible consequences of their online behaviour, emotionally instable people may have more difficulties in assessing online risks, and more open people are more likely to share personal information online.

Victims of online crime do not report a change in hours spend online, nor do they report a change in mental well-being. Victims of online harassment, however, report a slight decrease in their mental well-being, possibly because this type of crime has a more serious impact in a victim's personal life. Online crime victims show an increase in fear of online crime and take more protection measures than before. This implies that victims tend to adjust their behaviour after a crime experience, and it is therefore relevant to inform (potential) victims about the actions they can take to prevent (repeat) online victimization.

Literatuur

Averdijk, M. (2010). Reciprocal effects of victimization and routine activities. *Journal of Quantitative Criminology, 27*(2), 125-149. doi:10.1007/s10940-010-9106-6

Berwick, B.M., Murphy, J.M., Goldman, P.A., Ware, J.E., Jr., Barsky, A.J., & Weinstein, M.C. (1991). Performance of a five-item mental health screening test. *Medical Care, 29*(2), 169-176. doi:10.1097/00005650-199102000-00008

Borwell, J., Jansen, J., & Stol, W. (2018). Persoonlijkheidskenmerken van e-fraudeslachtoffers. *Tijdschrift voor Veiligheid, 17*(1-2), 54-65. doi:10.5553/TvV/187279482018017102005

Bossler, A.M., Holt, T.J., & May, D.C. (2011). Predicting online harassment victimization among a juvenile population. *Youth & Society, 44*(4), 500-523. doi:10.1177/0044118x11407525

Brands, J., & Wilsem, J. van (2019). Connected and fearful? Exploring fear of online financial crime, internet behaviour and their relationship. *European Journal of Criminology*, 1-22. doi:10.1177/1477370819839619

CBS (2017). *Veiligheidsmonitor 2017*. Den Haag: CBS.

Chapple, C.L., & Johnson, K.A. (2007). Gender differences in impulsivity. *Youth Violence and Juvenile Justice, 5*(3), 221-234. doi:10.1177/1541204007301286

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44*, 588-608. doi:10.2307/2094589

Cross, C., Richards, K., & Smith, R.G. (2016). *The reporting experiences and support needs of victims of online fraud*. Canberra: Australian Institute of Criminology.

Dickman, S.J. (1990). Functional and dysfunctional impulsivity: Personality and cognitive correlates. *Journal of Personality and Social Psychology, 58*(1), 95-102. doi:10.1037/0022-3514.58.1.95

Domenie, M.M.L., Leukfeldt, E.R., Wilsem, J.A. van, Jansen, J., & Stol, W.P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma uitgevers.

Dugan, L. (1999). The effect of criminal victimization on a household's moving decision. *Criminology, 37*(4), 903-930.

Farrell, G., Clark, K., Ellingworth, D., & Pease, K. (2005). Of targets and super-targets: A routine activity theory of high crime rates. *Internet Journal of Criminology*.

Felson, M., & Clarke, R.V. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Londen: Policing and Reducing Crime Unit, Home Office Research, Development and Statistics Directorate.

Gamez-Guadix, M., Orue, I., Smith, P.K., & Calvete, E. (2013). Longitudinal and reciprocal relations of cyberbullying with depression, substance use, and problematic internet use among adolescents. *Journal of Adolescent Health, 53*(4), 446-452. doi:10.1016/j.jadohealth.2013.03.030

Goldberg, L.R. (1993). The structure of phenotypic personality traits. *The American Psychologist, 48*(1), 26-34.

Golladay, K., & Holtfreter, K. (2016). The consequences of identity theft victim-ization: An examination of emotional and physical health outcomes. *Victims & Offenders, 12*(5), 741-760. doi:10.1080/15564886.2016.1177766

Gottfredson, M., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737-744.
Hoekstra, H., & Fruyt, F. de (2014). *NEO-PI-3 en NEO-FFI-3 persoonlijkheidsvragenlijsten: Handleiding.* Amsterdam: Hogrefe.
Holt, T.J., & Bossler, A.M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. doi:10.1080/01639620701876577
Holt, T.J., & Bossler, A.M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436. doi:10.1177/1043986213507401
Holt, T.J., Wilsem, J. van, Weijer, S. van de, & Leukfeldt, R. (2018). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*. doi:10.1177/0894439318805067
Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into the impact and change. *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 205-228.
Jones, C.S., & Hartley, N.T. (2013). Comparing correlations between four-quadrant and five-factor personality assessments. *American Journal Of Business Education, 6*(4), 459-470.
Kalidien, S.N. (2018). *Criminaliteit en rechtshandhaving 2017*. Den Haag: WODC/CBS. Cahier 2018-19.
Laan, A.M. van der, Rokven, J.J., Weijters, G., & Beerthuizen, M. (2018). De daling in jeugddelinquentie: Minder risico, meer bescherming? *Tijdschrift voor Criminologie, 60*(1), 35-58. doi:10.5553/TvC/0165182X2018060001002
Lamet, W., & Wittebrood, K. (2009). *Nooit meer dezelfde. Gevolgen van misdrijven voor slachtoffers*. Den Haag: Sociaal en Cultureel Planbureau/WODC.
Leukfeldt, E.R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555. doi:10.1089/cyber.2014.0008
Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of advanced studies in Computer Science and Engineering, 4*(5), 26-32.
Leukfeldt, E.R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Amsterdam: NSCR/WODC.
Lugtig, P., Das, M., & Scherpenzeel, A. (2014). Nonresponse and attrition in a probability-based online panel for the general population. In M. Callegaro, R.P. Baker, J. Bethlehem, A.S. Göritz, J. Krosnick & P.J. Lavrakas (red.), *Online panel research: A data quality perspective* (pp. 135-153). Chichester: John Wiley & Sons.
Macmillan, R. (2001). Violence and the life course: The consequences of victimization for personal and social development. *Annual Review of Sociology, 27*, 1-22. doi:10.1146/annurev.soc.27.1.1
Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies, 8*(4), 298-309. doi:10.1080/17450128.2012.752119
Ousey, G.C., Wilcox, P., & Brummel, S. (2008). Déjà vu all over again: Investigating temporal continuity of adolescent victimization. *Journal of Quantitative Criminology, 24*(3), 307-335. doi:10.1007/s10940-008-9046-6

Paulissen, L., & Wilsem, J. van (2015). *Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*. Apeldoorn: Politie & Wetenschap/Universiteit Leiden.
Pratt, T.C., Turanovic, J.J., Fox, K.A., & Wright, K.A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*(1), 87-116. doi:10.1111/1745-9125.12030
Reemst, L. van, Fischer, T., & Dongen, S. van (2013). *Risicofactoren voor herhaald slachtofferschap: Een literatuurscan*. Rotterdam: Erasmus Universiteit Rotterdam.
Reyns, B.W., Burek, M.W., Henson, B., & Fisher, B.S. (2013). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice, 36*(1), 1-17. doi:10.1080/0735648x.2011.641816
Rokven, J.J., Weijters, G., & Laan, A.M. van der (2017). *Jeugddelinquentie in de virtuele wereld: Een nieuw type daders of nieuwe mogelijkheden voor traditionele daders?* Den Haag: WODC. Cahier 2017-2.
Sampasa-Kanyinga, H., Roumeliotis, P., & Xu, H. (2014). Associations between cyberbullying and school bullying victimization and suicidal ideation, plans and attempts among Canadian schoolchildren. *Plos One, 9*(7), e102145. doi:10.1371/journal.pone.0102145
Schreck, C.J., Stewart, E.A., & Fisher, B.S. (2006). Self-control, victimization, and their influence on risky lifestyles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology, 22*(4), 319-340. doi:10.1007/s10940-006-9014-y
Skogan, W.G. (1987). The impact of victimization on fear. *Crime & Delinquency, 33*(1), 135-154. doi:10.1177/0011128787033001008
Turanovic, J.J., & Pratt, T.C. (2012). "Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology, 30*(1), 29-56. doi:10.1007/s10940-012-9188-4
Weijer, S.G.A. van de, Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486-508. doi:10.1177/1477370818773610
Wilsem, J. van (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127. doi:10.1177/1477370810393156
Wilsem, J. van (2013a). 'Bought it, but never got it': Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178. doi:10.1093/esr/jcr053
Wilsem, J. van (2013b). Hacking and harassment – do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453. doi:10.1177/1043986213507402
Wilsem, J. van (2017). Exploring the possibility of 'moral hazard' among victims of identity fraud: The relation between reimbursement for unauthorized cash withdrawals and risky online behavior. In T.J. Holt (red.), *Cybercrime through an interdisciplinary lens*. Londen, New York: Routledge.
Wilsem, J. van, Meulen, N. van der, & Kunst, M. (2013). Je geld kwijt, en dan? Financiële schade bij slachtoffers van onterechte bankafschrijvingen. *Tijdschrift voor Criminologie, 55*(4), 360-374.
Whitty, M.T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice, 16*(2), 176-194. doi:10.1177/1748895815603773
Wijn, R., Berg, H. van den, Wetzer, I.M., & Broekman, C.C.M.T. (2016). *Supertargets: Verkenning naar voorspellende en verklarende factoren voor slachtofferschap van cybercriminaliteit*. Soesterberg: TNO.

Wittebrood, K. (2006). *Slachtoffers van criminaliteit*. Den Haag: SCP.
Wittebrood, K., & Nieuwbeerta, P. (2000). Criminal victimization during one's life-course: The effects of previous victimization and patterns of routine activities. *Journal of Research in Crime and Delinquency, 37*(1), 91-122. doi:10.1177/0022427800037001004
Worsley, J.D., Wheatcroft, J.M., Short, E., & Corcoran, R. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *SAGE Open, 7*(2). doi:10.1177/2158244017710292
Wright, M.F., & Li, Y. (2013). Normative beliefs about aggression and cyber aggression among young adults: A longitudinal investigation. *Aggressive Behavior, 39*(3), 161-170. doi:10.1002/ab.21470
Xie, M., & McDowall, D. (2008). The effects of residential turnover on household victimization. *Criminology, 46*(3), 539-575. doi:10.1111/j.1745-9125.2008.00123.x

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter

Prof. dr. M. Kunst	Universiteit Leiden

Leden

S. Dickie (per 5-4-2019)	Slachtofferhulp NL
Dr. J. Jansen	NHL Stenden Hogeschool
Dr. S. Leferink (tot 5-4-2019)	Slachtofferhulp NL
M. de Vries	Ministerie van Justitie en Veiligheid, Slachtofferbeleid
Dr. J. van Wilsem	Algemene Rekenkamer

Bijlage 2 LISS-panel

Tabel b1 Non-respons in het LISS-panel: leeftijd

	Respondenten		Niet-deelnemers		Verschil
	Aantal	Leeftijd	Aantal	Leeftijd	p-waarde
2008	6.896	45,5	6.534	37,6	<0,001
2010	5.764	48,6	7.666	40,0	<0,001
2012	5.709	50,1	7.721	42,4	<0,001
2014	6.025	50,1	7.405	45,8	<0,001
2016	7.413	50,5	6.017	49,0	<0,001
2018	7.636	51,7	5.794	51,7	0,923
Alle waves	1.807	49,8	11.623	40,4	<0,001

Noot: De respons is berekend over de groep respondenten die aan tenminste één wave hebben deelgenomen, waaronder nieuwe panelleden die pas tijdens een later meetmoment voor het eerst zijn benaderd.
Verschillen tussen respondenten en niet-deelnemers zijn bepaald middels eenwegvariantie-analyses.

Tabel b2 Non-respons in het LISS-panel: geslacht

	Respondenten		Niet-deelnemers		Verschil
	Aantal	Geslacht (%man)	Aantal	Geslacht (%man)	p-waarde
2008	6.896	45,9%	6.534	45,2%	0,208
2010	5.764	46,2%	7.666	45,1%	0,100
2012	5.709	46,6%	7.721	44,9%	0,024
2014	6.025	46,3%	7.405	45,0%	0,074
2016	7.413	46,2%	6.017	45,1%	0,110
2018	7.636	45,7%	5.794	45,5%	0,460
Alle waves	1.807	49,0%	11.623	45,1%	0,001

Noot: De respons is berekend over de groep respondenten die aan tenminste één wave hebben deelgenomen, waaronder nieuwe panelleden die pas tijdens een later meetmoment voor het eerst zijn benaderd.
Verschillen tussen respondenten en niet-deelnemers zijn bepaald middels chi-kwadraat-analyses.

Tabel b3 Non-respons in het LISS-panel: impulsiviteit

	Respondenten		Niet-deelnemers		Verschil
	Aantal	Impulsiviteits-score	Aantal	Impulsiviteits-score	p-waarde
2008	6.896	1,115	6.534	1,130	<0,001
2010	5.764	1,115	7.666	1,128	<0,001
2012	5.709	1,114	7.721	1,128	<0,001
2014	6.025	1,114	7.405	1,129	<0,001
2016	7.413	1,114	6.017	1,129	<0,001
2018	7.636	1,109	5.794	1,132	<0,001
Alle waves	1.807	1,093	11.623	1,127	<0,001

Noot: De respons is berekend over de groep respondenten die aan tenminste één wave hebben deelgenomen, waaronder nieuwe panelleden die pas tijdens een later meetmoment voor het eerst zijn benaderd.
Verschillen tussen respondenten en niet-deelnemers zijn bepaald middels eenwegvariantie-analyses.

Tabel b4 Non-respons in het LISS-panel: slachtofferschap

	Slachtoffers		Niet-slachtoffers		Verschil
	Aantal	% deelname aan volgende wave	Aantal	% deelname aan volgende wave	p-waarde
2008	705	56,0%	2.883	60,3%	1
2010	564	67,9%	2.964	71,3%	0,050
2012	541	72,6%	3.103	74,8%	0,218
2014	386	78,8%	3.489	80,4%	0,402
2016	404	69,9%	3.523	74,6%	0,018

Verschillen tussen percentages slachtoffers en niet-slachtoffers die aan de volgende wave hebben deelgenomen zijn bepaald middels chi-kwadraat-analyses.

Tabel b5 Factoranalyse angst voor online criminaliteit

	Factor		Factor
	1	2	1
Ik maak me zorgen dat mijn credit card nummer via het internet wordt achterhaald	0,72	0,33	0,74
Ik vind het een probleem om mijn credit card nummer via internet prijs te geven	0,75	0,20	0,75
Ik ben bang dat de dingen die ik via het internet koop niet geleverd worden	0,80	-0,07	0,75
Ik wantrouw verkoopsites op het internet	0,76	-0,08	0,71
Ik ben bang dat er een keer wordt ingebroken op mijn computer	0,64	0,61	0,70
Ik maak me zorgen dat door internetbankieren mijn bankgegevens worden achterhaald	0,75	0,40	0,79
Ik controleer de computer vaak op de aanwezigheid van virussen.	0,11	0,85	-

Principal component analysis met een oblique rotatie; resultaten patroonmatrix worden getoond. De factoranalyses per wave hebben dezelfde uitkomst.

Tabel b6 Overzicht stellingen Big-V persoonlijkheidskenmerken

Persoonlijkheidskenmerken
Extraversie
Breng leven in de brouwerij
Praat niet veel
Voel me goed in het gezelschap van mensen
Blijf op de achtergrond
Begin gesprekken
Heb weinig te zeggen
Praat met veel verschillende mensen op feestjes
Houd er niet van de aandacht op mijzelf te vestigen
Vind het niet erg om in het middelpunt van de belangstelling te staan
Ben stil in het gezelschap van vreemden
Altruïsme
Voel me weinig begaan met anderen
Ben geïnteresseerd in mensen
Beledig mensen
Voel mee met de gevoelens van anderen
Ben niet geïnteresseerd in de problemen van andere mensen
Ben sentimenteel
Ben niet echt geïnteresseerd in anderen
Neem de tijd voor anderen
Voel de emoties van anderen
Zorg dat mensen zich op hun gemak voelen.
Consciëntieusheid
Ben altijd voorbereid
Laat mijn persoonlijke bezittingen rondslingeren
Besteed aandacht aan details
Maak een puinhoop van dingen
Doe karweitjes meteen
Vergeet vaak om dingen op de juiste plaats terug te zetten
Houd van orde
Onttrek me aan mijn verplichtingen
Volg een planning
Ben veeleisend in mijn werk
Emotionele stabiliteit
Raak makkelijk gestresst
Ben meestal ontspannen
Maak me zorgen over dingen
Voel me zelden neerslachtig
Ben snel verontrust
Raak makkelijk van streek
Verander vaak van stemming
Heb regelmatig stemmingswisselingen
Raak snel geërgerd
Voel me vaak neerslachtig.
Openheid
Heb een uitgebreide woordenschat
Heb moeite om abstracte ideeën te begrijpen
Heb een levendige fantasie
Ben niet geïnteresseerd in abstracte ideeën
Heb uitstekende ideeën
Heb geen goede verbeelding
Begrijp dingen snel
Gebruik moeilijke woorden
Besteed tijd om over dingen na te denken
Zit vol met ideeën.

Bijlage 3 Gevolgen van slachtofferschap per delict

Tabel b7 Fixed effect panel analyses op angst voor online criminaliteit

	Model b7.1			Model b7.2		
	b		95%BI	b		95%BI
Creditcard fraude	0,16	**	0,06 - 0,25	0,14	**	0,04 - 0,24
Hacken	0,05		-0,02 - 0,12	0,03		-0,05 - 0,12
Online aankoopfraude	0,11	***	0,05 - 0,16	0,12	***	0,06 - 0,18
Online bedreiging	0,04		-0,05 - 0,12	-0,02		-0,11 - 0,08
Virus	0,06	**	0,02 - 0,09	0,07	**	0,01 - 0,11
Afschrijving bankrekening†				0,10	**	0,03 - 0,16
Identiteitsfraude†				-0,03		-0,3 - 0,23
Wave						
2008	Ref.					
2010	-0,09	***	-0,11 - -0,06	Ref.		
2012	-0,13	***	-0,15 - -0,09	-0,04	*	-0,06 - 0,01
2014	-0,11	***	-0,13 - -0,07	-0,01		-0,03 - 0,01
2016	-0,18	***	-0,2 - -0,15	-0,09	***	-0,11 - -0,06
2018	-0,17	***	-0,19 - -0,13	-0,08	***	-0,10 - -0,04
Aantal kinderen	0,01		-0.01 - 0,03	0,01		-0.01 - 0,03
Partner	0,05	*	0.01 - 0,09	0,06	*	0.01 - 0,09

Fixed effect panel analyses in Stata

*p<0,5, **p<0,01, ***p<0,001

†Afschrijving bankrekening en identiteitsfraude bevraagd vanaf 2010

Tabel b8 Fixed effect panel analyses op internetgebruik in uren

	Model b8.1			Model b8.2		
	b		95%BI	b		95%BI
Creditcard fraude	1,86	*	0,04 - 3,67	2,55	*	0,38 - 4,71
Hacken	-0,16		-1,57 - 1,25	-0,50		-2,38 - 1,38
Online aankoopfraude	-0,59		-1,64 - 0,47	-0,81		-2,07 - 0,44
Online bedreiging	1,43		-0,23 - 3,09	1,60		-0,54 - 3,73
Virus	-0,37		-1,12 - 0,38	-0,42		-1,47 - 0,63
Afschrijving bankrekening†				0,54		-0,81 - 1,88
Identiteitsfraude†				0,59		-5,14 - 6,32
Wave						
2008	Ref.					
2010	0,29		-0,20 - 0,79	Ref.		
2012	2,64	***	2,10 - 3,16	2,34	***	1,79 - 2,89
2014	5,09	***	4,53 - 5,64	4,81	***	4,22 - 5,38
2016	6,25	***	5,71 - 6,79	6,04	***	5,47 - 6,59
2018	7,35	***	6,77 - 7,91	7,14	***	6,55 - 7,73
Aantal kinderen	0,21		-0,16 - 0,57	0,51	*	0,04 - 0,98
Partner	-0,30		-1,20 - 0,59	-0,05		-1,14 - 1,04

Fixed effect panel analyses in Stata

*p<0,5, **p<0,01, ***p<0,001

†Afschrijving bankrekening en identiteitsfraude bevraagd vanaf 2010

Tabel b9 Fixed effect panel analyses op beschermingsmaatregelen

	Model b9.1			Model b9.1		
	b		95%BI	b		95%BI
Creditcard fraude	0,16		-0,06 - 0,39	0,19		-0,06 - 0,45
Hacken	-0,01		-0,19 - 0,17	-0,04		-0,26 - 0,18
Online aankoopfraude	0,05		-0,08 - 0,18	0,05		-0,09 - 0,20
Online bedreiging	0,08		-0,13 - 0,29	-0,14		-0,39 - 0,12
Virus	0,12	*	0,02 - 0,21	0,06		-0,06 - 0,18
Afschrijving bankrekening†				0,19	*	0,02 - 0,35
Identiteitsfraude†				-0,16		-0,83 - 0,52
Wave						
2008	Ref.					
2010	0,13	***	0,06 - 0,19	Ref.		
2012	0,22	***	0,15 - 0,28	0,08	*	0,01 - 0,15
2014	0,33	***	0,25 - 0,40	0,19	***	0,12 - 0,26
2016	0,15	***	0,07 - 0,21	0,02		-0,04 - 0,08
2018	-0,01		-0,08 - 0,06	-0,14	***	-0,21 - -0,07
Aantal kinderen	0,03		-0,02 - 0,07	0,02		-0,03 - 0,07
Partner	0,07		-0,04 - 0,18	0,06		-0,06 - 0,19

Fixed effect panel analyses in Stata

*p<0,5, **p<0,01, ***p<0,001

†Afschrijving bankrekening en identiteitsfraude bevraagd vanaf 2010

Tabel b10 Fixed effect panel analyses op mentale gezondheid

	Model b10.1			Model b10.1		
	b		95%BI	b		95%BI
Creditcard fraude	0,05		-0,05 - 0,14	0,00		-0,10 - 0,10
Hacken	0,00		-0,07 - 0,07	-0,03		-0,12 - 0,06
Online aankoopfraude	-0,01		-0,06 - 0,05	0,02		-0,04 - 0,08
Online bedreiging	-0,15	**	-0,23 - -0,05	-0,09		-0,19 - 0,01
Virus	-0,01		-0,05 - 0,02	0,03		-0,02 - 0,07
Afschrijving bankrekening†				0,00		-0,06 - 0,06
Identiteitsfraude†				-0,06		-0,33 - 0,22
Wave						
2008	Ref.					
2010	0,05	***	0,02 - 0,07	Ref.		
2012	0,10	***	0,06 - 0,12	0,05	***	0,01 - 0,07
2014	0,12	***	0,08 - 0,14	0,07	***	0,03 - 0,09
2016	0,16	***	0,12 - 0,18	0,11	***	0,07 - 0,13
2018	0,16	***	0,13 - 0,19	0,11	***	0,08 - 0,14
Aantal kinderen	-0,04	***	-0,05 - -0,01	-0,02	***	-0,04 - -0,00
Partner	0,16	***	0,10 - 0,20	0,16	***	0,1 - 0,21

Fixed effect panel analyses in Stata

*p<0,5, **p<0,01, ***p<0,001

†Afschrijving bankrekening en identiteitsfraude bevraagd vanaf 2010

Bijlage 4 Herhaald online slachtofferschap

Tabel b11 Frequentieverdeling subcategorieën herhaald slachtofferschap

	N	%
Meervoudig slachtoffer	255	20,7
Herhaaldelijk slachtoffer van hetzelfde delict	559	45,3
Meervoudig slachtoffer én herhaaldelijk slachtoffer van hetzelfde delict	420	34,0
Totaal	**1.234**	**100**

Tabel b12 Risicofactoren voor herhaald slachtofferschap van online criminaliteit

	Herhaald van meerdere delicten (N=236) vs. eenmalig (ref.) Model b12.1		Herhaald van hetzelfde delict (N=505) vs. eenmalig (ref.) Model b12.2		Herhaald van zowel hetzelfde als meerdere delicten (N=397) vs. eenmalig (ref.) Model b12.3	
	e^b	95%BI	e^b	95%BI	e^b	95%BI
Achtergrondkenmerken						
Leeftijd	0,99 *	0,97 - 0,99	1,00	0,99 - 1,00	1,00	0,99 - 1,00
Geslacht						
Vrouw	Ref.		Ref.		Ref.	
Man	1,06	0,76 - 1,45	1,52 ***	1,19 - 1,92	1,33 *	1,02 - 1,73
Opleidingsniveau						
Basisonderwijs	Ref.		Ref.		Ref.	
Vmbo	0,43	0,20 - 0,90	1,19	0,67 - 2,10	0,85	0,46 - 1,58
Havo/vwo	0,97	0,46 - 2,03	1,13	0,60 - 2,08	1,09	0,56 - 2,10
Mbo	0,91	0,46 - 1,78	1,23	0,70 - 2,15	1,07	0,58 - 1,94
Hbo	0,69	0,34 - 1,37	1,12	0,63 - 1,95	1,03	0,56 - 1,87
Wo	0,77	0,36 - 1,61	0,61	0,32 - 1,14	0,68	0,34 - 1,31
Persoonlijkheidskenmerken						
Impulsiviteit	1,15	0,39 - 3,32	1,75	0,79 - 3,88	4,84 ***	2,15 - 10,83
Extraversie	1,17	0,89 - 1,51	0,91	0,74 - 1,10	0,97	0,78 - 1,19
Altruïsme	0,81	0,57 - 1,14	1,28	0,97 - 1,67	1,01	0,75 - 1,35
Consciëntieusheid	0,94	0,68 - 1,28	0,87	0,68 - 1,09	0,92	0,71 - 1,19
Emotionele stabiliteit	0,84	0,66 - 1,07	0,78 **	0,65 - 0,93	0,66 ***	0,54 - 0,79
Openheid	1,13	0,78 - 1,61	1,37 *	1,04 - 1,79	1,59 **	1,17 - 2,13
Aantal deelnames	1,10	0,99 - 1,22	1,07	0,98 - 1,15	1,27 ***	1,15 - 1,38

Multinomiale regressieanalyse in SPSS

*p<0,5, **p<0,01, ***p<0,001; N=6.332

Tabel b13 Risicofactoren voor herhaald slachtofferschap van online criminaliteit

	Herhaald in één wave (N=222) vs. eenmalig (ref.) Model b13.1		Herhaald in meerdere waves (N=292) vs. eenmalig (ref.) Model b13.2		Herhaald in zowel één wave als in meerdere waves (N=624) vs. eenmalig (ref.) Model b13.3	
	e^b	95%BI	e^b	95%BI	e^b	95%BI
Achtergrondkenmerken						
Leeftijd	1,01	0,99 - 1,01	1,00	0,98 - 1,00	1,00	0,99 - 1,00
Geslacht						
Vrouw	Ref.		Ref.		Ref.	
Man	1,69 **	1,21 - 2,33	1,08	0,80 - 1,44	1,37 **	1,09 - 1,71
Opleidingsniveau						
Basisonderwijs	Ref.		Ref.		Ref.	
Vmbo	1,39	0,65 - 2,92	1,09	0,47 - 2,47	0,70	0,42 - 1,15
Havo/vwo	0,95	0,41 - 2,19	1,60	0,68 - 3,76	0,99	0,58 - 1,69
Mbo	1,32	0,62 - 2,77	1,87	0,84 - 4,13	0,84	0,51 - 1,38
Hbo	1,08	0,50 - 2,28	1,50	0,67 - 3,33	0,82	0,50 - 1,34
Wo	0,40	0,16 - 0,99	1,18	0,50 - 2,78	0,63	0,36 - 1,08
Persoonlijkheidskenmerken						
Impulsiviteit	1,44	0,50 - 4,16	1,32	0,47 - 3,67	3,43 ***	1,68 - 6,98
Extraversie	0,97	0,74 - 1,27	0,94	0,74 - 1,19	1,00	0,83 - 1,20
Altruïsme	1,20	0,83 - 1,73	1,15	0,82 - 1,60	0,99	0,77 - 1,27
Consciëntieusheid	0,98	0,70 - 1,36	0,77	0,57 - 1,03	0,93	0,74 - 1,16
Emotionele stabiliteit	0,78 *	0,60 - 0,98	0,85	0,68 - 1,06	0,69 ***	0,58 - 0,81
Openheid	1,26	0,87 - 1,82	1,44 *	1,02 - 2,00	1,40 **	1,08 - 1,80
Aantal deelnames	0,87 *	0,78 - 0,97	1,30 ***	1,17 - 1,43	1,18 ***	1,09 - 1,26

Multinomiale regressieanalyse in SPSS

*p<0,5, **p<0,01, ***p<0,001; N=6.332