

**Hoe ‘Ideaal’ zijn Slachtoffers van Cybercrime? Een Onderzoek naar Secundaire
Victimisatie in de Nederlandse Maatschappij Anno 2022**

Mathilde Maat

Studentnummer: s4010914

Afdeling Psychologie, Rijksuniversiteit Groningen

PSB3A-BT15: Bachelor These

Begeleidster: dr. C. Gerlsma

Tweede beoordelaar: prof. dr. E. Gordijn

In samenwerking met: Vincent Bakkeren, Fleur van Harmelen, Puck Pacilly, en Jonas

Tjallema

21 juni 2022

Een scriptie is een proeve van bekwaamheid voor studenten. De goedkeuring van de scriptie is het bewijs dat de student over voldoende onderzoeks- en rapportagevaardigheden beschikt om af te studeren, maar biedt geen garantie voor de kwaliteit van het onderzoek en de resultaten van het onderzoek als zodanig, en de scriptie is daarom niet per se geschikt als academische bron om naar te verwijzen. Als u meer wilt weten over het in deze scriptie besproken onderzoek en de daarop gebaseerde publicaties waarnaar u zou kunnen verwijzen, neem dan contact op met de genoemde begeleider.

How 'Ideal' Are Victims of Cybercrime? An Investigation of Secondary Victimization in Dutch Society Anno 2022

Abstract

Secondary victimization can occur when there is a denial of victimization. Victims feel like repeated victims because they don't feel heard, are not treated respectfully or are not well informed. In this study 113 participants gave an indication of how much recognition they attribute to victims of similar online and traditional offline crimes (fraud, sexual harassment, home/computer trespass, stalking and bullying). Although the average recognition was lower for victims of the online versions of the crimes, the differences were only statistical significant in the cases of online sexual harassment and cyberstalking. This is a worrying state of affairs, because the denial of victimization can have far-reaching consequences for victims. Awareness is essential to draw more attention to the situation of victims of cybercrime.

Keywords: secondary victimization, victims, recognition, victimization denial, online crime, cybercrime

Samenvatting

Secundaire victimisatie kan optreden wanneer er sprake is van ontkenning van slachtofferschap. Slachtoffers voelen zich herhaald slachtoffer, omdat ze zich niet gehoord, niet respectvol behandeld of niet goed geïnformeerd voelen. In dit onderzoek hebben 113 deelnemers aangegeven hoeveel erkenning zij toeschrijven aan slachtoffers van vergelijkbare online en traditionele offline delicten (oplichting, seksuele intimidatie, huis-/computervredesbreuk, stalking en pesten). Alhoewel de gemiddelde erkenning lager was voor slachtoffers van alle online versies van de delicten, waren de verschillen enkel statistisch significant voor online seksuele intimidatie en cyberstalking. Dit is een zorgwekkende stand van zaken, omdat de ontkenning van slachtofferschap verregaande gevolgen kan hebben voor slachtoffers. Bewustwording is essentieel om meer aandacht te vestigen op de situatie van slachtoffers van cybercrime.

Sleutelwoorden: erkenning, slachtoffers, secundaire victimisatie, ontkenning slachtofferschap, online delicten, cybercrime

Hoe 'Ideaal' zijn Slachtoffers van Cybercrime? Een Onderzoek naar Secundaire Victimisatie in de Nederlandse Maatschappij anno 2022

Cybercrime is momenteel een actueel thema in de Nederlandse maatschappij. Zo is er onlangs een wetsvoorstel ingediend om *doxing*, het verstrekken of verspreiden van persoonlijke gegevens met als doel intimidatie, strafrechtelijk te kunnen bestrijden (Grapperhaus, 2021). In Nederland is er sprake van een afname van traditionele criminaliteit; daar staat tegenover dat het aantal slachtoffers van cybercrime toeneemt (Centraal Bureau voor de Statistiek, 2022). Waar fietsendiefstal traditioneel het meest voorkomende delict in Nederland was, is dit ingehaald door online oplichting en fraude (Centraal Bureau voor de Statistiek, 2022). De meest recente cijfers tonen aan dat 16,9% van de Nederlandse bevolking slachtoffers is geweest van online delicten in 2021, vrijwel hetzelfde percentage, 17,1%, geldt voor traditionele delicten (Centraal Bureau voor de Statistiek, 2022).

Gevolgen van traditionele delicten

Uit onderzoek van Lefebvre et al. (2020) blijkt dat slachtoffers van geweldsmisdrijven het risico lopen om een acute stressstoornis en daaropvolgend een posttraumatische stressstoornis (PTSS) te ontwikkelen, wat vaak samengaat met depressie, angst en een verminderde kwaliteit van leven. Bovendien blijkt uit het onderzoek dat slachtoffers van geweldsmisdrijven vaker een gebrek aan sociale steun ervaren door stigmatisering en *victim blaming*, waarbij de schuld (deels) bij het slachtoffer wordt gelegd.

Wat betreft zedendelicten blijkt dat vrouwen die slachtoffer zijn geweest van seksueel geweld meer angst, depressie en stress ervaren (Brunton & Dryer, 2022). Ook in de context van seksueel geweld komt *victim blaming* voor, waarbij het slachtoffer de schuld krijgt van het seksuele geweld of niet wordt geloofd (Hughes et al., 2020). Naast de financiële verliezen zijn mogelijke gevolgen van vermogensdelicten gevoelens van angst, een verminderde tevredenheid met het leven, slaapproblemen, PTSS, depressie en paniekaanvallen (Gale &

Coupe, 2005; O'Brien & Burrell, 2020; Shapland & Hall, 2007; Tan & Haining, 2016). Het meest voorkomende gevolg van stalking is het gevoel van onveiligheid en de angst dat de stalking nooit ophoudt (Baum et al., 2009). *Victim blaming* en de gevoelens van schuld, schaamte en onveiligheid zijn universele gevolgen voor slachtoffers van verschillende delicten (Elbers & Becx, 2020; Hughes et al., 2020; Lefebvre et al., 2020).

Gevolgen van cybercrime

Slachtoffers van cybercrime worden door het ontbreken van direct fysiek contact met de dader regelmatig minder serieus genomen dan slachtoffers van traditionele delicten (Henson et al., 2016). Desalniettemin kunnen de gevolgen van cybercrime groot zijn. Volgens Notté et al. (2021) komen de meeste gevolgen van cybercrime bij Nederlandse slachtoffers overeen met de gevolgen van traditionele delicten, zoals gevoelens van schuld, schaamte, machteloosheid, verlies van vertrouwen, en een onveilig gevoel. Deze conclusie trekken Button et al. (2021) ook, zij stellen dat de gevolgen voor veel slachtoffers van cybercrime vergelijkbaar, zo niet erger, zijn dan traditionele delicten zoals inbraak.

Volgens Notté et al. (2021) zijn er een aantal gevolgen uniek voor slachtoffers van cybercrime. Ten eerste is dat de schaal en zichtbaarheid van het slachtofferschap. Hiermee wordt niet alleen bedoeld dat een dader via het internet een groot aantal slachtoffers kan maken, maar een dader kan ook een slachtoffer zichtbaar maken voor een grote (mogelijk onbeperkte) groep 'toeschouwers'. Daarnaast kan onophoudelijk slachtofferschap voorkomen, bijvoorbeeld doordat materiaal niet van het internet kan worden verwijderd. Bovendien speelt de verwevenheid van de online en offline wereld een rol, vooral bij stalking en bedreiging, waarbij het slachtoffer online wordt lastiggevallen ondanks maatregelen in de 'offline' wereld. Ten slotte stellen Notté et al. (2021) dat er ook in het geval van cybercrime sprake kan zijn *victim blaming*. Door deze gevolgen worden slachtoffers soms dubbel, driedubbel of viervoudig getroffen; dit komt door de opeenstapeling van verschillende soorten impact van

een delict en dit maakt slachtofferschap van cybercrime zo ingrijpend.

Ook Cross (2015) spreekt in de context van cybercrime over *victim blaming*. Slachtoffers van online fraude worden eerder gezien als hebzuchtig en goedgelovig, bovendien ervaren slachtoffers een groot gevoel van schuld en verantwoordelijkheid voor hun daden die hebben geleid tot de online fraude. Volgens Leukfeldt et al. (2018) worden slachtoffers van cybercrime vaker slachtoffer van *victim blaming*, omdat politiemedewerkers onvoldoende kennis hebben van online delicten en deze delicten vaker inschatten als complex, waardoor er niet wordt overgegaan tot opsporingsonderzoek.

Kowalski en Giumetti (2017) beargumenteren dat de cyberversies van traditionele delicten niet simpelweg een uitbreiding zijn. In het geval van cyberpesten is ten eerste de waargenomen anonimiteit een belangrijk onderdeel; dit kan leiden tot een gevoel van macht bij de dader. Zo blijkt dat mensen anoniem meer dingen durven te zeggen en doen dan in persoonlijke interacties (Suler, 2004). Ten tweede vindt traditioneel pesten met name plaats op school tijdens schooldagen; bij cyberpesten is de toegankelijkheid tot het slachtoffer onbeperkt. Ten derde hebben veel jonge slachtoffers van cyberpesten het gevoel dat hun ouders het niet zullen begrijpen als ze over hun slachtofferervaringen vertellen. Wanneer slachtoffers van cyberpesten zich niet uitspreken, zullen ze waarschijnlijk geen of onvoldoende erkenning en steun ontvangen voor hun slachtofferschap.

Het 'ideale slachtoffer'

De Noorse criminoloog Nils Christie (1986) heeft het 'ideale slachtoffer' beschreven aan de hand van vijf kenmerken. Wanneer slachtoffers voldoen aan het in de samenleving heersende beeld van het 'ideale slachtoffer', zullen zij eerder een slachtofferstatus toegekend krijgen en erkenning ontvangen. Het eerste kenmerk van het 'ideale slachtoffer' volgens Christie (1986) is dat het slachtoffer zwak is, in het bijzonder ziek, oud of zeer jong. Daarnaast was het slachtoffer bezig met een respectabel project, het slachtoffers was iets

goeds aan het doen. Bovendien was het slachtoffer waar hij of zij onmogelijk de schuld kon krijgen; het slachtoffer bevond zich op een veilige plek en moet energie hebben gestoken in het zichzelf beschermen. Tevens is de dader groot en kwaadaardig en heeft de dader geen persoonlijke relatie met het slachtoffer. Uit de literatuur blijken nog meer factoren die meespelen in de beoordeling van anderen of een slachtoffer gezien wordt als ‘ideaal slachtoffer’. Het slachtoffer dient geen gevoelens van woede of wraak te tonen (Van Dijk, 2009) en het slachtoffer moet zelf niets te verwijten vallen aan het delict (Bosma et al., 2018).

Cross (2018) heeft de kenmerken van het ‘ideale slachtoffer’ uit het werk van Christie (1986) toegepast op slachtoffers van cybercrime. Volgens Cross worden slachtoffers van cybercrime over het algemeen gezien als ‘niet-ideale slachtoffers’, met als gevolg een verminderde mate van erkenning voor wat het slachtoffer is overkomen en de impact hiervan. Dit geldt zowel in de privésfeer, zoals door familieleden en vrienden, als in de publieke sfeer, zoals door justitie en overheid.

Wat betreft het eerste kenmerk, het zwakke slachtoffer, is er volgens Cross (2018) tegenstrijdig bewijs. Ouderen zijn aan de ene kant een aantrekkelijk doelwit, vanwege hun hoge mate van financiële aantrekkelijkheid. Aan de andere kant beargumenteert Cross (2016) dat 45- tot 54-jarigen de meest voorkomende slachtoffers zijn, omdat in deze levensfase veel langdurige relaties worden beëindigd, waardoor de vatbaarheid voor online fraude wordt vergroot. Uit cijfers van het CBS blijkt dat in Nederland jongeren vaker slachtoffer zijn van cybercrime dan ouderen. In 2020 was dit bij jongeren van vijftien tot 25 jaar 17,6 procent, bij mensen van 65 jaar of ouder was dit 7,2 procent. Wat betreft specifiek koop- en verkoopfraude zijn mensen van 25 tot 45 jaar het meest voorkomende slachtoffer (6,5%) (Centraal Bureau voor de Statistiek, 2020). Het eerste kenmerk van het ‘ideale slachtoffer’ lijkt niet volledig van toepassing te zijn op cybercrime in Nederland. Dit is in overeenstemming met het idee van Van 't Hoff et al. (2021) dat cybercriminelen niet al te

kieskeurig zijn: iedereen is een potentieel slachtoffer van cybercriminaliteit.

Cross (2018) beschrijft dat slachtoffers van cybercrime in het bijzonder niet voldoen aan het tweede kenmerk van Christie (1986) dat het slachtoffer iets goeds aan het doen was. Er heerst een sterk negatief stereotype dat stelt dat slachtoffers van cybercrime hebzuchtig en goedgelovig zijn en daarnaast het slachtofferschap enigszins verdienen (Cross, 2013, 2015). Volgens Cross (2013) krijgt het slachtoffer hierdoor de schuld van en verantwoordelijkheid voor het slachtofferschap; wanneer een slachtoffer in eerste instantie niet hebzuchtig zou zijn geweest, zou de persoon geen slachtoffer zijn geworden. Men is van mening dat slachtoffers hebben bijgedragen aan hun slachtofferschap, een reden hiervoor is dat in het bijzonder voor fraude een actieve bijdrage van het slachtoffer vereist is. In de context van online fraude heeft een slachtoffer op een bepaald moment geld naar een dader overgemaakt. Cross benadrukt dat slachtoffers dit onder valse voorwendselen hebben gedaan en dat de rol van de dader in dit geval volledig wordt ontkend (Cross, 2018).

Ook lijkt het derde kenmerk dat het slachtoffer zich op een veilige plek bevond niet van toepassing te zijn op slachtoffers van cybercrime. Volgens Cross (2018) geldt in het geval van cybercrime dat elk potentieel van sympathie of overtuiging dat het slachtoffer onrecht is aangedaan teniet wordt gedaan door het feit dat het slachtoffer het delict zelf heeft gefaciliteerd. Zo worden slachtoffers van online fraude verantwoordelijk gehouden voor hun acties op het internet en de communicatie met de dader, waardoor hen in de context van online fraude gemakkelijker geld afhandig gemaakt kan worden.

Het vierde kenmerk van het 'ideale slachtoffer' wordt beschreven door Christie (1986) als het slachtoffer van een grote en kwaadaardige dader. Cross (2018) beargumenteert dat er regelmatig sprake is van een kwaadaardige dader in de context van online fraude. Daders worden gekenmerkt door leugens en bedrog, mede doordat ze het vertrouwen en de volgzzaamheid van slachtoffers proberen te winnen (Cross, 2013). Bovendien maken daders

opzettelijk gebruik van zwaktes of kwetsbaarheden van slachtoffers (Cross, 2018). Dit suggereert dat ook in de context van cybercrime er sprake is van een *'big and bad'* dader. In vergelijking met traditionele delicten is er bij cybercrime sprake van een grotere mate van anonimiteit van de dader (Jewkes, 2010). Volgens Cross (2018) wordt de meeste fraude uitgevoerd door *unknown identities*, ondanks dat het slachtoffer denkt de dader te kennen. In de context van het 'ideale slachtoffer' van cybercrime kan beargumenteerd worden dat er zowel niet als wel wordt voldaan aan het kenmerk van de onbekende dader.

Cross (2018) heeft in haar analyse getracht de vijf kenmerken van Christie's (1986) 'ideale slachtoffer' toe te passen op cybercrime. Ondanks dat slachtoffers van cybercrime kunnen voldoen aan een aantal van de 'ideale' slachtofferkenmerken, lijkt de discutabele aard van de overige kenmerken de mogelijkheid voor slachtoffers van cybercrime om de status te krijgen van 'ideaal slachtoffer' teniet te doen. Dit heeft mogelijk als gevolg dat het slachtofferschap wordt ontkend, wat kan leiden tot een verminderde mate van erkenning.

Ontkenning van Slachtofferschap

Het gevolg van ontkenning van slachtofferschap is dat tevens wordt ontkend dat slachtoffers onrecht is aangedaan (Cross et al., 2016). Slachtofferschap kan voordelen met zich meebrengen, zoals sympathie, aandacht voor *victim blaming*, de mogelijkheid om betekenis te geven aan een negatieve ervaring, het ontvangen van validatie, vrijstelling van vervolging, strafvermindering en financiële en emotionele compensatie (Cross, 2018; Jägervi, 2014). Wanneer slachtoffers van cybercrime niet erkend worden als 'echte' slachtoffers, worden ze vervolgens niet gezien als een groep waardige slachtoffers die ondersteuning en hulp verdienen (Cross, 2018). Ten slotte is secundaire victimisatie een mogelijk direct gevolg van de ontkenning van slachtofferschap voor slachtoffers van zowel traditionele delicten als cybercrime (Cross, 2018; Cross et al., 2016).

Secundaire Victimisatie

Vaak wordt de impact van cybercrime verergerd door een gebrek aan begrip voor de ervaringen van de slachtoffers in hun sociale omgeving, problemen met opsporing en vervolging en een gebrek aan steun van politie en andere organisaties (Cross et al., 2016; Worsley et al., 2017). In de literatuur wordt er gesproken van secundaire victimisatie wanneer een slachtoffer zich na een misdrijf voor een tweede keer slachtoffer voelt, bijvoorbeeld doordat ze zich niet gehoord, niet respectvol behandeld of niet goed geïnformeerd voelen; er wordt ook wel gesproken van ‘hernieuwd slachtofferschap’ (Elbers & Becx, 2020; Van Dijk et al., 2007). Door secundaire victimisatie kunnen slachtoffers bang zijn om niet geloofd te worden of om zelf beschuldigd te worden. Hierbij speelt schaamte een grote rol (Akkermans & Van Wees, 2007). Ook kan het idee bij slachtoffers ontstaan dat het doen van aangifte zinloos is, waardoor het *dark number* van delicten stijgt en daders niet vervolgd worden en daardoor onbestraft blijven (Instituut voor de Gelijkheid van Vrouwen en Mannen, 2019). Daarnaast kan secundaire victimisatie bijdragen aan een grotere kans op discriminatie van kwetsbare groepen door strafrechtelijke instanties of hulpverleningsinstanties (Crenshaw, 1991).

Wanneer slachtoffers geen aangifte doen, kan er geen compensatie worden ontvangen. Hierdoor ontstaat er een discrepantie tussen de impact van het delict en de geringe aanpak vanuit politie en justitie, dit kan bij slachtoffers leiden tot frustratie en een gevoel van oneerlijkheid (Leukfeldt et al., 2018). Groenhuijsen en Penders (1989) beargumenteren dat een schadevergoeding belangrijk is voor slachtoffers, maar dat dit niet de meest wezenlijke factor is waardoor secundaire victimisatie kan worden voorkomen. Het is vooral van belang dat een slachtoffer in het strafrechtelijke systeem kan rekenen op respect en begrip voor zijn of haar situatie. Het ontvangen en ervaren van erkenning kan ervoor zorgen dat slachtoffers de nodige ondersteuning krijgen om vooruitgang te boeken in hun herstel (Cross, 2018). Er wordt niet altijd in de behoefte van slachtoffers voorzien, slachtoffers van zowel online als

offline delicten voelen zich niet altijd erkend als slachtoffer, waardoor zij zich niet serieus genomen en geholpen voelen (Leukfeldt et al., 2018).

Relevantie

De impact van victimisatie door cybercrime is ondanks de toenemende prevalentie een relatief onderbelicht onderwerp op het gebied van slachtofferschap (Notté et al., 2021). Daarbij is het huidige slachtoffer(hulp)beleid gebaseerd op slachtoffers van traditionele delicten, waarbij er weinig aandacht is voor de ervaringen van slachtoffers van cybercrime (Leukfeldt et al., 2018). Vincent en Jane (2017) stellen dat slachtoffers van cybercrime momenteel worden verwaarloosd, omdat er onvoldoende aandacht wordt besteed aan hun benarde situatie. Het is daarom van belang om de overeenkomsten en verschillen in de mate van erkenning voor slachtoffers van cybercrime en traditionele delicten beter te begrijpen.

De aanbeveling uit het onderzoek van Button et al. (2021) is dat beleidsmakers en uitvoerders in de praktijk in het Verenigd Koninkrijk slachtoffers van online delicten serieuzer moeten nemen, er meer middelen besteed moeten worden aan het voorkomen en onderzoeken van cybercrime en dat slachtoffers van cybercrime de ondersteuning moeten krijgen die ze nodig hebben. In Nederland lijkt er weinig onderzoek voorhanden dat specifiek gericht is op de erkenning van slachtoffers van cybercrime.

De relevantie van dit onderzoek ligt met name in de bewustwording over de mate van erkenning die de Nederlandse bevolking toeschrijft aan slachtoffers van zowel traditionele delicten als cybercrime. In lijn met de literatuur is de verwachting dat slachtoffers van cybercrime in mindere mate worden gezien als 'ideaal slachtoffer' en hierdoor minder erkenning krijgen van de huidige Nederlandse samenleving dan slachtoffers van traditionele delicten. Wanneer dit het geval is, kunnen mensen bewust (gemaakt) worden van de stereotype wijze waarop er naar slachtoffers gekeken wordt. Er zijn in de afgelopen periode stappen gezet in de bewustwording omtrent slachtofferschap, onder andere door slachtoffers

van seksueel grensoverschrijdend gedrag die zich hebben uitgesproken in de media. Mogelijk is een dergelijke taboesignalering en -doorbreking ook noodzakelijk voor slachtoffers van cybercrime. Dit is van cruciaal belang, omdat slachtoffers door secundaire victimisatie niet of weinig als slachtoffer herkend en erkend worden, wat er vervolgens toe kan leiden dat ze er van worden weerhouden om hun recht te halen.

De onderzoeksvraag van dit onderzoek luidt als volgt: ontvangen slachtoffers van cybercrime in de Nederlandse samenleving anno 2022 minder erkenning dan slachtoffers van vergelijkbare traditionele delicten?

Methode

Onderzoeksdeelnemers

In totaal zijn 177 deelnemers gestart met het invullen van de vragenlijst. Achttien deelnemers hebben geen toestemming gegeven voor de verwerking van hun gegevens, van deze personen is geen data verzameld. Negentien deelnemers hebben hun leeftijd niet ingevuld, waardoor er niet gecontroleerd kon worden of zij ouder waren dan achttien jaar. In het rapport dat opgesteld is voor de Ethische Commissie is vastgelegd dat er enkel data verzameld werd van deelnemers van achttien jaar of ouder. De deelnemers waarvan onduidelijk is wat hun leeftijd was, zijn derhalve verwijderd uit de database. Er zijn 27 mensen gestopt met het invullen van de vragenlijst na de introductie, ook de data van deze personen is uit de database verwijderd.

Honderddertien deelnemers hebben de *Victim Concern Scale* (VCS; Clements et al., 2006) volledig ingevuld; hierbij hebben ze aangegeven hoeveel schadevergoeding ze verschillende slachtoffers zouden toekennen. Van deze deelnemers zijn zeven mensen tijdens of na het invullen van de vragen met betrekking tot de vignetten gestopt, waardoor ze niet zijn toegekomen aan de sociale wenselijkheidsvragenlijst, de *Marlowe-Crowne Social Desirability Scale* (MC-SDS; Crowne & Marlowe, 1960). Dit brengt het totaal aantal deelnemers dat de

MC-SDS heeft ingevuld op 106.

Van de 113 deelnemers (74 vrouwen (65,5%); 39 mannen (34,5%)) was de gemiddelde leeftijd 33,19 jaar ($SD = 16,10$). Op één Indonesische deelnemer na hebben alle deelnemers de Nederlandse nationaliteit. Het opleidingsniveau werd in dit onderzoek opgedeeld in ‘lager onderwijs’ (lagere school, middelbare school en beroepsonderwijs) en ‘hoger onderwijs’ (hogeschool en universiteit). Negenennegentig (87.6%) deelnemers waren volgens deze criteria ‘hoger opgeleid’ en veertien (12.4%) deelnemers ‘lager opgeleid’. De onderzoeksopzet en de vragenlijst die de deelnemers hebben ingevuld zijn goedgekeurd door de ethische commissie van de Rijksuniversiteit Groningen.

Design

Het onderzoek had een cross-sectioneel en within-subjects onderzoeksdesign, waarbij het verband tussen de online, dan wel offline, aard van het delict en de erkenning die aan slachtoffers werd gegeven is onderzocht. De afhankelijke variabele in dit onderzoek was de hoogte van de tegemoetkoming die de deelnemers toekennen aan slachtoffers van verschillende offline en online delicten. Dit is in het onderzoek de operationalisatie van de mate van erkenning die de Nederlandse maatschappij anno 2022 toekent aan slachtoffers van verschillende online en offline delicten.

Procedure

Deelnemers zijn geworven via het sociale netwerk van de onderzoekers door middel van de sneeuwbal methode (*convenience sampling*), allen uit de Nederlandse volwassen populatie. De werving vond online plaats, door middel van een wervingsbrief met een hyperlink die is gedeeld via online platformen zoals e-mail en WhatsApp. De vragenlijst is geprogrammeerd in het softwareprogramma Qualtrics. Allereerst werden de deelnemers geïnformeerd over het onderzoeksdoel en de procedure. Om het onderzoek te kunnen starten, moesten de deelnemers geïnformeerde toestemming geven. Ook was toestemming nodig voor

de verwerking van de demografische gegevens. De vragen waren in de Nederlandse taal en het invullen van de vragenlijst duurde ongeveer vijftien minuten.

Ten eerste werden de demografische gegevens verkregen, de deelnemers hebben vragen over hun leeftijd, geslacht, hoogst behaalde opleiding en nationaliteit beantwoord. Daarna werden de deelnemers gevraagd de VCS in te vullen. De deelnemers werden vervolgens willekeurig toegewezen aan een vignet waarin een verslag van een rechtszaak werd beschreven. Voor het meten van ‘erkenning voor het slachtoffer’ moesten de deelnemers hierbij zeven stellingen beoordelen door middel van een 5-punts Likertschaal (1 = helemaal niet mee eens; 5 = helemaal mee eens). Voorbeelden van items zijn: “Ik kan me goed identificeren met het slachtoffer” en “Ik vind dat dit slachtoffer serieus genomen moet worden”. Hierbij is vervolgens gevraagd om met de getoonde schuifbalk, lopende van €1000,- tot €35000,-, aan te geven hoe hoog de schadevergoeding voor het slachtoffer zou moeten zijn volgens de deelnemer. De soorten delicten en slachtoffers die centraal stonden in de vignetten waren niet relevant voor de onderzoeksvraag van dit onderzoek. Derhalve zijn de resultaten van de vignetten buiten beschouwing gelaten in dit onderzoek. Na het vignet vulden de deelnemers de MC-SDS in. Tot slot werden de deelnemers bedankt voor hun deelname, werden de contactgegevens van de onderzoekers getoond voor verdere vragen en konden de deelnemers hun interesse aangeven in het ontvangen van de resultaten van het onderzoek.

Materiaal

Victim Concern Scale (VCS)

De VCS (Clements et al., 2006) is een gevalideerde zelfrapportage vragenlijst bestaande uit 22 items die beoogt de mate van bezorgdheid voor verschillende slachtoffers van verschillende misdrijven te beoordelen. Om de onderzoeksvraag te kunnen beantwoorden, is de originele VCS (Cronbach's $\alpha = .96$ in dit onderzoek) aangevuld met tien zelf geconstrueerde items (Cronbach's $\alpha = .98$ in dit onderzoek). De items van de VCS werden op

de gestandaardiseerde volgorde aan de deelnemers getoond; de tien items ter aanvulling op de VCS werden vervolgens op een gerandomiseerde volgorde aan de deelnemers getoond. Voorbeelden van items van de originele VCS zijn: “Slachtoffers van huiselijk geweld” en “Slachtoffers die grootouders zijn”. De tien zelf geconstrueerde items die zijn toegevoegd aan de originele VCS zijn slachtoffers van de volgende delicten: oplichting, online oplichting, seksuele intimidatie, online seksuele intimidatie, huisvredebreuk, computervredebreuk, stalking, cyberstalking, pesten en cyberpesten. Hierbij is aan de deelnemers gevraagd om met de getoonde schaal aan te geven hoe hoog de financiële tegemoetkoming voor slachtoffers van de verschillende delicten naar hun mening zou moeten zijn, waarbij nul punten stond voor geen tegemoetkoming en honderd punten voor de hoogst mogelijke tegemoetkoming.

Door middel van Cronbach’s alfa is de mate van samenhang tussen de vijf offline delicten (vijf items; $\alpha = .94$) en de vijf online delicten (vijf items; $\alpha = .94$) geanalyseerd. Dit suggereert dat de schaal voor de mate van erkenning, geoperationaliseerd als de hoogte van de tegemoetkoming voor de delicten van de VCS, de vijf online en de vijf offline delicten betrouwbaar is (Nunnally, 1978).

Marlowe-Crowne Social Desirability Scale (MC-SDS)

Na de vragen met betrekking tot het vignet vulden de deelnemers de gevalideerde korte variant van de MC-SDS (Crowne & Marlowe, 1960) in. De MC-SDS is een gevalideerde zelfrapportagevragenlijst bestaande uit 33 items die beoogt de mate van sociaalwenselijke antwoorden van de deelnemers te beoordelen. In dit onderzoek is gekozen voor de korte versie van de MC-SDS (Cronbach’s $\alpha = .50$ in dit onderzoek) met tien items, zodat de duur van de participatie aan het onderzoek beperkt zou blijven en de deelnemers hun concentratie en motivatie voor het geven van weloverwogen antwoorden zouden behouden. Voorbeelden van items van de MC-SDS zijn: “Ik heb nog nooit een ontzettende hekel aan iemand gehad” en “Ik ben altijd beleefd, zelfs tegen mensen die onvriendelijk zijn”. De

deelnemers konden de vragen beantwoorden met ‘waar of ‘niet waar’. Als maat voor de ‘mate van sociaalwenselijke antwoorden’ is een somscore berekend van de gegeven antwoorden op de MC-SDS. De betrouwbaarheid van de schaal voor de MC-SDS is onvoldoende (Nunnally, 1978), waardoor bij de interpretatie van de resultaten enige behoedzaamheid is geboden.

Data-Analyse

De data is geanalyseerd middels beschrijvende statistieken, hierbij zijn de assumpties voor de statistische methode geverifieerd. Voor de toetsing van de hypothese dat de Nederlandse maatschappij slachtoffers van online delicten minder erkenning geeft dan slachtoffers van offline delicten zijn gepaarde t-toetsen uitgevoerd. Als maat voor ‘erkenning van het slachtoffer’ zijn de somscores berekend van de gegeven tegemoetkoming op de verschillende variabelen. Bij de statistische toetsen zijn de somscores van de gemiddelde scores van de gegeven antwoorden op de VCS in paren vergeleken. De somscores van de vijf online delicten zijn apart van elkaar vergeleken met de gemiddelde scores van de vijf offline delicten apart van elkaar. Daarnaast zijn voor de vijf online en de vijf offline delicten tezamen gemiddelde somscores (‘online delicten’ en ‘offline delicten’) berekend en zijn deze met elkaar vergeleken. Ten slotte zijn de somscores van de offline en online delicten vergeleken met de somscore van de VCS vragenlijst, om vergelijking mogelijk te kunnen maken met gestandaardiseerde items.

Door middel van Cronbach’s alfa is de mate van samenhang tussen de verschillende online en offline delicten geanalyseerd om de betrouwbaarheid van de schaal voor de mate van erkenning voor de verschillende soorten slachtoffers van verschillende delicten vast te stellen.

Resultaten

Beschrijvende statistieken

De VCS is ingevuld door 113 deelnemers, waarvan 74 vrouwen (65,5%) en 39

mannen (34,5%). De gemiddelde leeftijd was 33.19 jaar ($SD = 16.10$). De gemiddelde leeftijd van de vrouwen was 33.00 jaar ($SD = 16.96$) en de gemiddelde leeftijd van de mannen was 33.56 jaar ($SD = 16.57$). De afhankelijke variabele was de mate van erkenning, geoperationaliseerd als de toegekende tegemoetkoming voor de verschillende soorten slachtoffers. Binnen een range van nul tot en met honderd was de gemiddeld toegekende tegemoetkoming voor traditionele delicten 52.23 ($SD = 26.27$) en voor online delicten 48.77 ($SD = 25.39$). In Tabel 1 zijn de gemiddelden en standaarddeviaties voor de gegeven tegemoetkoming voor de vijf online en offline delicten weergegeven; waarbij de gemiddelde mate van erkenning, geoperationaliseerd als hoogte van de tegemoetkoming, voor alle vijf de delicten hoger is voor de traditionele offline delicten.

Tabel 1

Gemiddelden en Standaarddeviaties van de Gegeven Mate van Erkenning voor Slachtoffers van de Verschillende Online en Offline Delicten

	Traditioneel delict ($N = 113$)		Online delict ($N = 113$)	
	Gemiddelde	SD	Gemiddelde	SD
1. Oplichting	48.65	28.07	48.31	28.80
2. Seksuele Intimidatie	57.97	29.40	50.82	29.22
3. Huisvredebreuk (Computervredebreuk)	49.60	29.15	48.02	28.99
4. Stalking	53.98	28.95	47.86	27.63
5. Pesten	50.92	30.39	48.83	27.12
Somscore van de Vijf Delicten	52.22	26.27	48.77	25.39
Somscore van de 22 Delicten van de Originele VCS	54.00	20.30		

Noot. Alle beoordelingen waren op een continue schaal variërend van 0 = *geen*

tegemoetkoming (erkenning) tot 100 = *de hoogst mogelijke tegemoetkoming (erkenning)*.

Er was sprake van een significante, sterke correlatie tussen de hoogte van de tegemoetkoming van de offline en online delicten, de offline delicten en de VCS, en de online delicten en de VCS. Tussen de offline delicten en de MC-SDS was er sprake van een significante, zwakke correlatie. Hetzelfde geldt voor de online delicten en de MC-SDS en de VCS en de MC-SDS. In Tabel 2 zijn deze correlaties en Cronbach's alfa tussen de relevante variabelen in het onderzoek weergegeven.

Tabel 2

Correlaties en (Cronbach's Alfa) tussen de Variabelen in het Onderzoek.

	1	2	3	4
1. Tegemoetkoming Offline Delicten	(.94)			
2. Tegemoetkoming Online Delicten	.96**	(.94)		
3. Tegemoetkoming Originele VCS	.81**	.81**	(.96)	
4. Marlowe-Crowne Social Desirability Scale	-.23*	-.25*	-.32**	(.50)

Noot. * $p < .05$, ** $p < .01$, tweezijdig. De Cronbach's Alfa coëfficiënten zijn weergegeven in de correlatiematrixdiagonaal.

Toets van de onderzoeksvraag

Assumptiecontrole

Uit inspectie van de frequenties, histogrammen, boxplots en QQ-plots bleek dat een aantal afhankelijke variabelen niet normaal verdeeld waren. Door middel van de Kolmogorov-Smirnov toets is de normaliteitsassumptie gecontroleerd, er was bewijs voor non-normaliteit voor de volgende variabelen: slachtoffers van stalking, cyberstalking, huisvredebreuk, computervredebreuk, online oplichting en pesten. De onderzoeksgroep bevatte 113 deelnemers, waardoor er volgens de centrale limietstelling aangenomen kan worden dat er aan de aanname van normaliteit is voldaan. Bovendien is vanwege het aantal

deelnemers de gepaarde t-toets voldoende robuust om uit te voeren zonder dat er voldaan is aan de assumptie van normaliteit.

Acht deelnemers hebben bij (vrijwel) iedere slachtoffercategorie van de VCS hetzelfde antwoord gegeven, veelal de minimale of maximale tegemoetkoming die te vergeven was. Er is voor gekozen om deze data niet te verwijderen, omdat er bij deze deelnemers een (kleine) afwijking in hun antwoordpatroon zat; er waren uitzonderingen waarbij niet de minimale of maximale tegemoetkoming is gegeven. De verwachting is dat de deelnemers weloverwogen herhaaldelijk hetzelfde antwoord hebben gegeven. Bovendien hadden deze antwoorden een relatief kleine invloed op de resultaten vanwege de robuustheid van de data wegens het aantal deelnemers.

Toetsbevindingen

De gemiddelde toegekende erkenning voor de vijf delicten met een online en offline tegenhanger zijn middels een gepaarde t-toets vergeleken. De hypothese was dat deelnemers meer erkenning zouden toeschrijven aan slachtoffers van offline delicten dan slachtoffers van online delicten bij een vergelijkbaar delict. Er is eenzijdig getoetst ($\alpha < .05$).

De gemiddelde toegekende erkenning was in het geval van alle delictparen hoger voor slachtoffers van de traditionele offline versies dan voor slachtoffers van de online versies van de delicten. Het verschil in de hoogte van de toegekende erkenning tussen slachtoffers van seksuele intimidatie en online seksuele intimidatie was significant ($t(112) = 4.15; p < .05$). Ook het verschil tussen slachtoffers van stalking en cyberstalking was significant ($t(112) = 0.20; p < .05$). Het verschil in de hoogte van de toegekende erkenning was niet significant voor slachtoffers van oplichting en online oplichting (phishing) ($t(112) = 0.20; p = .42$), slachtoffers van huisvredebreuk en computervredebreuk ($t(112) = 0.83; p = .20$) en slachtoffers van pesten en cyberpesten ($t(112) = 1.44; p = .08$).

Het verschil in de hoogte van de somscore van de toegekende erkenning voor

slachtoffers van de vijf offline delicten en de somscore van de slachtoffers van de vijf online delicten was significant ($t(112) = 4.84; p < .05$); dit geeft aan dat de deelnemers slachtoffers van offline delicten significant meer erkenning gaven dan slachtoffers van online delicten.

Daarnaast zijn de somscores van de toegekende erkenning van de vijf online en offline delicten vergeleken met de somscore van de toegekende erkenning van de 22 delicten van de VCS. In de VCS werd niet gevraagd naar online delicten. Het verschil in de hoogte van de somscore van de toegekende erkenning voor slachtoffers van de vijf offline delicten en de somscore van de slachtoffers van de VCS was niet significant ($t(112) = -1.23; p = 0.22$). Het verschil in de hoogte van de somscore van de toegekende erkenning voor slachtoffers van de vijf online delicten en de somscore van de slachtoffers van de VCS was wel statistisch significant ($t(112) = -3.70; p < .05$).

De invloed van de Social Desirability Response Bias op de Resultaten

Er is sprake van een significante, zwakke, negatieve correlatie tussen de MC-SDS en de mate van erkenning voor slachtoffers van de vijf offline delicten ($r = -.25; p < .05$), de vijf online delicten ($r = -.23; p < .05$), en de VCS delicten ($r = -.32; p < .05$). Dit impliceert dat het sociaal onwenselijk is wanneer deelnemers slachtoffers een hogere mate van erkenning geven. Deze relatief kleine effectgrootte van de samenhang tussen de mate van erkenning en de sociale wenselijkheid impliceert dat de kans klein is dat de antwoorden op de vragenlijsten in belangrijke mate zijn gegeven door sociale wenselijkheid.

Discussie

De onderzoeksvraag van dit onderzoek luidde als volgt: ontvangen slachtoffers van cybercrime in de Nederlandse samenleving anno 2022 minder erkenning dan slachtoffers van vergelijkbare traditionele delicten? Hierbij was de hypothese, gebaseerd op de literatuur, dat slachtoffers van cybercrime minder erkenning ontvangen dan slachtoffers van traditionele offline delicten. In lijn met de literatuur en hypothese waren de bevindingen dat de

deelnemers meer erkenning gaven aan slachtoffers van offline traditionele delicten dan aan de online versie van het delict. Dit verschil was significant voor slachtoffers van de online versie van seksuele intimidatie en stalking. Het verschil was niet groot genoeg en hierdoor niet significant voor de delicten oplichting, huisvredebreuk/computervredebreuk en pesten. Uit de literatuur blijken verschillende geluiden dat slachtoffers van cybercrime niet altijd worden erkend als slachtoffers, waardoor zij onder andere minder sympathie, validatie, aandacht voor *victim blaming* en financiële en/of emotionele compensatie ontvangen (Cross, 2018; Jägervi, 2014). Dit is in overeenstemming met de resultaten van dit onderzoek.

Een mogelijke verklaring is dat slachtoffers van cybercrime in mindere mate voldoen aan de slachtofferkenmerken van het 'ideale slachtoffer' (Christie, 1986) en hierdoor minder snel de status van slachtoffer krijgen, met als gevolg een mindere mate van erkenning van de maatschappij. Daarnaast is *victim blaming* een mogelijke oorzaak voor de mindere mate van erkenning voor slachtoffers van online delicten. Mogelijk zijn de deelnemers van het huidige onderzoek van mening dat de slachtoffers van cybercrime in grotere mate zelf iets te verwijten valt door de eigen acties op het internet en de online communicatie met de dader (Cross, 2018). Daarnaast worden slachtoffers van cybercrime regelmatig beschuldigd van het overdrijven of verzinnen van hun ervaringen en de gevolgen hiervan en het gebrek aan besef dat wat er online gebeurt niet 'echt' is (O'Neill, 2011). Ook is het mogelijk dat de deelnemers de overtuiging hebben dat de slachtoffers van cybercrime hebzuchtig en goedgelovig zijn, waardoor zij een gemakkelijk doelwit zijn voor daders (Cross, 2015).

Methodologische kenmerken en Toekomstig Onderzoek

In dit onderzoek is de mate van erkenning geoperationaliseerd als de hoogte van de toegekende tegemoetkoming voor slachtoffers van verschillende delicten. De VCS is een gevalideerd meetinstrument voor de mate van bezorgdheid over slachtoffers. Zowel de mate van bezorgdheid als de hoogte van de toegekende tegemoetkoming zijn indicaties van het

concept ‘erkenning’, maar geen van beiden is een volledig dekkende operationalisatie van dit brede concept. De validiteit van het onderzoek is mogelijk ten koste gegaan van de operationalisatie.

Het onderzoek is uitgevoerd middels een online vragenlijst, waardoor er niet gegarandeerd kan worden dat de deelnemers de vragenlijst onder dezelfde condities hebben ingevuld. Mogelijk hebben ongemotiveerde deelnemers de vragenlijst onzorgvuldig ingevuld. Bovendien hadden deelnemers niet de mogelijkheid om de onderzoekers terstond vragen te stellen bij onduidelijkheden. Dit kan als gevolg hebben gehad dat deelnemers de vragen verkeerd geïnterpreteerd hebben. Daarentegen is een meerwaarde van de online afname van de vragenlijsten dat deelnemers waarschijnlijk minder sociale druk hebben ervaren om sociaal wenselijk te antwoorden wegens de afwezigheid van de onderzoekers.

In dit onderzoek is de mate van sociaal wenselijkheid opgenomen middels het gevalideerde meetinstrument de MC-SDS. Vanwege de onvoldoende interne consistentie en zwakke psychometrische eigenschappen van de MC-SDS dient de zwakke samenhang tussen de MC-SDS en de VCS met voorzichtigheid te worden geïnterpreteerd. Er kan op grond van dit onderzoek niet met zekerheid gesteld worden dat de ‘erkenning’ die de deelnemers aan slachtoffers zeggen te geven niet samenhangt met sociale wenselijkheidstendensen.

Er is een toets uitgevoerd om te onderzoeken of de interne consistentie van de constructen die zouden moeten samenhangen daadwerkelijk samenhangen. De aanvulling van de originele VCS (Cronbach’s $\alpha = .96$) met vijf additionele offline delicten is betrouwbaar (Cronbach’s $\alpha = .97$). Hetzelfde geldt voor de aanvulling met vijf online delicten (Cronbach’s $\alpha = .97$). Volgens de vuistregel (Nunnally, 1978) is de Cronbach’s alfa uitstekend voor het gebruik van deze vragenlijst. Dit heeft de betrouwbaarheid van het onderzoek vergroot.

Er is gepoogd om een aselechte en representatieve onderzoeksgroep te representeren uit de Nederlandse samenleving. Het onderzoek had betrekking op alle leeftijdscategorieën vanaf

achttien jaar; echter in de samenstelling van de onderzoeksgroep werden niet alle leeftijdscategorieën in even grote mate gerepresenteerd. Vermoedelijk is de oorzaak hiervan de manier van werving, met name het sociale netwerk van de onderzoekers heeft geparticipeerd in het onderzoek. Van de deelnemers was 60,2 procent 26 jaar of jonger. Bovendien waren er aanzienlijk meer vrouwelijke dan mannelijke deelnemers. Daarnaast hadden vrijwel alle deelnemers de Nederlandse nationaliteit en was het aantal ‘hoger opgeleide’ deelnemers sterk overgerepresenteerd in vergelijking met ‘lager opgeleide’ deelnemers. Dit heeft de externe validiteit van het onderzoek mogelijk beïnvloed, waardoor de conclusies uit het onderzoek niet generaliseerbaar zijn naar de gehele Nederlandse populatie.

Het huidige onderzoek is een aanvulling op de bestaande literatuur over slachtoffers van cybercrime, omdat er in een gering aantal eerdere studies onderzoek is gedaan naar het verschil in de mate van erkenning tussen slachtoffers van online en traditionele offline delicten in Nederland. De resultaten van dit onderzoek zijn zorgelijk; er is echter verder onderzoek nodig om de resultaten te bevestigen en te generaliseren naar een grotere populatie. Hierbij dient rekening te worden gehouden met het feit dat dit onderzoek zich uitsluitend heeft gefocust op vijf specifieke delicten. Toekomstig onderzoek zou gericht kunnen zijn op andersoortige delicten, zoals *phishing*, *malware* of idenditeitsfraude, zodat vastgesteld kan worden of slachtoffers van meer varianten van cybercrime minder erkenning ontvangen. Wanneer helder is bij welke delicten de discrepantie tussen de mate van erkenning het grootst is en welke doelgroep het hardnekkigst het slachtofferschap van slachtoffers van cybercrime ontkent, kunnen pogingen om attitudeveranderingen in gang te zetten gericht worden op deze specifieke doelgroepen.

Tevens is voor de generaliseerbaarheid naar de volledige Nederlandse bevolking onderzoek nodig met een groter aantal deelnemers, waarbij de maatschappij representatiever

vertegenwoordigd wordt. Daarnaast is de aanbeveling om in vervolgonderzoek ‘erkenning’ op verschillende manieren in kaart te brengen met degelijke en gevalideerde meetinstrumenten om een volledig beeld van dit concept te krijgen. Ten slotte wordt aanbevolen om in vervolgonderzoek covariaten op te nemen die mogelijk invloed hebben op de gegeven mate van erkenning. Een voorbeeld hiervan is de *just-world* theorie, waarbij mensen de opvatting hebben dat ‘mensen krijgen wat ze verdienen’ (Lerner, 1980).

Theoretische en Praktische Implicaties

De resultaten uit dit onderzoek leveren aanwijzingen dat er in de Nederlandse samenleving anno 2022 het beeld heerst dat slachtoffers van cybercrime minder erkenning zouden moeten krijgen voor hun slachtofferschap. Uit de literatuur blijkt dat de gevolgen van cybercrime net zo ernstig, dan wel ernstiger, kunnen zijn dan de gevolgen van traditionele criminaliteit (Notté et al., 2021). Door het heersende beeld in de samenleving krijgen slachtoffers van cybercrime mogelijk onvoldoende erkenning, wat secundaire victimisatie als gevolg kan hebben.

Deze resultaten en mogelijke verklaringen zijn onder andere relevant voor professionals, zoals politie, justitie en andere beroepsgroepen die diensten en/of hulp verlenen aan slachtoffers van cybercrime. Het is van groot belang dat professionals slachtoffers van cybercrime tegemoetkomen in hun behoeften en hen de benodigde erkenning geven, zodat slachtoffers de nodige ondersteuning kunnen krijgen om vooruitgang te boeken in hun herstel (Cross, 2018) en zich serieus genomen en geholpen voelen (Leukfeldt et al., 2018). Bovendien zijn de resultaten en mogelijke verklaringen relevant voor de gehele Nederlandse maatschappij. Mogelijk kunnen mensen bewust (gemaakt) worden van de heersende stigma’s in de samenleving wanneer zij geïnformeerd worden over dit thema.

Conclusie

Het lijkt zo te zijn dat er in de Nederlandse samenleving anno 2022 stigma’s heersen

omtrent slachtoffers van online delicten, waardoor zij minder erkenning ontvangen dan slachtoffers van traditionele offline delicten. Dit is een zorgwekkende stand van zaken, omdat de ontkenning van slachtofferschap verregaande gevolgen kan hebben voor slachtoffers. Het is van groot belang dat ook slachtoffers van cybercrime herkend en erkend worden als slachtoffer, zij geen slachtoffer worden van secundaire victimisatie en er niet van worden weerhouden om hun recht te halen.

Referenties

- Akkermans, A., & Van Wees, K. (2007). Het letselschadeproces in therapeutisch perspectief. *Tijdschrift voor Vergoeding Personenschade*, 4, 103-118.
- Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). Stalking victimization in the United States. *Bureau of Justice Statistics*. <https://doi.org/10.1177/0886260515573577>
- Bosma, A., Mulder, M., & Pemberton, A. (2018). The ideal victim through other(s') eyes. In M. Duggan (Ed.), *Revisiting the 'ideal victim': Developments in critical victimology* (pp. 27-41). Bristol: Policy Press. <https://doi.org/10.2307/j.ctv301ds5.10>
- Brunton, R., & Dryer, R. (2022). Sexual violence and Australian women: A longitudinal analysis of psychosocial and behavioral outcomes. *Social Science & Medicine*, 292. <https://doi.org/10.1016/j.socscimed.2021.114334>
- Button, M., Blackburn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). Victims of Cybercrime: Understanding the Impact Through Accounts. In M. Weulen-Kranenberg, & R. Leukfeldt, *Crime and Justice in Digital Society* (pp. 137-156). Cham: Springer. <https://doi.org/10.1007/978-3-030-60527-8>
- Centraal Bureau voor de Statistiek. (2020, December). *Nederland in Cijfers*. <https://longreads.cbs.nl/nederland-in-cijfers-2020/hoe-zit-het-met-cybercrime/>
- Centraal Bureau voor de Statistiek. (2022). *Veiligheidsmonitor 2021*. <https://www.cbs.nl/nl-nl/publicatie/2022/09/veiligheidsmonitor-2021>
- Christie, N. (1986). The Ideal Victim. *From crime policy to victim policy*, 17-30. https://doi.org/10.1007/978-1-349-08305-3_2
- Clements, C., Brannen, D., Kirkley, S., Gordon, T., & Church, W. (2006). The measurement of concern about victims: Empathy, victim advocacy and the Victim Concern Scale (VCS). *Legal and Criminological Psychology*, 11(2), 283-295. <https://doi.org/10.1348/135532505X79573>

- Crenshaw, K. (1991). Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, 43(6), 1241-1299.
<https://doi.org/10.2307/1229039>
- Cross, C. (2013). “Nobody’s holding a gun to your head...”: examining current discourses surrounding victims of online fraud. *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference*, 1, 25-32.
<https://doi.org/10.1177/0269758015571471>
- Cross, C. (2015). No laughing matter: blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187-204. <https://doi.org/10.1177/0269758015571471>
- Cross, C. (2016). “They’re very lonely”: understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy*, 5(4), 60-75.
<https://doi.org/10.5204/ijcjsd.v5i4.268>
- Cross, C. (2018). Denying victim status to online fraud victims: the challenges of being a ‘non-ideal victim’. In M. Duggan, *Revisiting the 'ideal victim': Developments in critical victimology* (pp. 243-259). Bristol: Policy Press.
<https://doi.org/10.1332/policypress/9781447338765.003.0015>
- Cross, C., Richards, K., & Smith, R. (2016). *Improving the Response to Online Fraud Victims: An Examination of Reporting and Support: Final Report*. Canberra: Criminology Research Grant Scheme, Australian Institute of Criminology.
<http://crg.aic.gov.au/reports/1617/29-1314-FinalReport.pdf>
- Crowne, D., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology*, 24(4), 349-354.
<https://doi.org/10.1037/h0047358>
- Elbers, N., & Becx, I. (2020). *Secundaire victimisatie als probleem. Herstelrecht als oplossing? Een onderzoek naar de reikwijdte van secundaire victimisatie en*

- herstelrecht in het straf-, civiel- en bestuursrecht in Nederland*. Amsterdam: Boom Juridisch.
- Gale, J., & Coupe, T. (2005). The behavioural, emotional and psychological effects of street robbery on victims. *International Review of Victimology*, *12*, pp. 1-22. <https://doi.org/10.1177/026975800501200101>
- Grapperhaus, F. (2021, November 3). *Conceptwetsvoorstel doxing [Kamerbrief]*. <https://www.rijksoverheid.nl/documenten/kamerstukken/2021/11/03/tk-conceptwetsvoorstel-doxing>
- Groenhuijsen, M., & Penders, A. (1989). De positie van slachtoffers van delicten in het burgerlijke en het strafrecht. *Slachtoffers van misdrijven*, 25-50.
- Henson, B., Reyns, B., & Fisher, B. (2016). Cybercrime victimization. In C. Cuevas, & C. Rennison, *The Wiley handbook on the psychology of violence* (pp. 555–570). Wiley Blackwell. <https://doi.org/10.1002/9781118303092.ch28>
- Hughes, S., Skoda, K., Parsons, A., Brown, K., & Pedersen, C. (2020). (Dis)abling Blame: the Influence of Disability Status on Attributions of Blame Toward Victims of Sexual Assault. *Sexuality Research and Social Policy*, *17*(2), pp. 219-228. <https://doi.org/10.1007/s13178-019-00384-2>
- Instituut voor de Gelijkheid van Vrouwen en Mannen. (2019). *Nationaal actieplan ter bestrijding van alle vormen van gendergerelateerd geweld 2015-2019*. https://igvm-iefh.belgium.be/sites/default/files/nap_2015-2019_lange_versie_0.%20pdf
- Jägervi, L. (2014). Who wants to be an ideal victim? A narrative analysis of crime victims' self-presentation. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *15*(1), 73-88. <https://doi.org/10.1080/14043858.2014.893479>
- Jane, E. (2018). Gendered cyberhate, victim-blaming, and why the internet is more like driving a car on a road than being naked in the snow. In E. Martellozzo, & E. Jane,

- Cybercrime and its Victims* (pp. 61-78). Londen: Routledge.
<https://doi.org/10.4324/9781315637198-4>
- Jewkes, Y. (2010). *Handbook of Internet crime*. Devon, United Kingdom: Willan Publishing.
- Kowalski, R., & Giumetti, G. (2017). Bullying in the digital age. In E. Martellozzo, & E. Jane, *Cybercrime and its Victims* (pp. 167-186). Londen: Routledge.
- Lefebvre, C., Fortin, C., & Guay, S. (2020). Quality of life after violent crime: The impact of acute stress disorder, posttraumatic stress disorder, and other consequences. *Journal of Traumatic Stress*. <https://doi.org/10.1002/jts.22623>
- Lerner, M. J. (1980). *The belief in a just world: A fundamental delusion*. New York: Plenum Press. https://doi.org/10.1007/978-1-4899-0448-5_2
- Leukfeldt, E., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. Amsterdam: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.
- Notté, R., Leukfeldt, E., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, 27(3), 272–294. <https://doi.org/10.1177/02697580211010692>
- Nunnally, J. (1978). An Overview of Psychological Measurement. In B. Wolman, *Clinical Diagnosis of Mental Disorders* (pp. 97-146). Boston: Springer.
- O'Brien, F., & Burrell, A. (2020). The impact of property crime on victims. In A. Burrell, & M. Tonkin, *Property crime : criminological and psychological perspectives* (pp. 59-70). Routledge. <https://doi.org/10.4324/9781315208237>
- O'Neill, B. (2011, November 7). 'The campaign to "Stamp Out Misogyny Online" echoes Victorian efforts to protect women from coarse language. *The Telegraph*.
<http://blogs.telegraph.co.uk/news/brendanoneill2/100115868/the-campaign-to-stamp->

out-misogyny-online-echoes-victorian-efforts-to-protect-women-from-coarse-
%20language/

Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims?

International Review of Victimology, 14, pp. 175-217.

<https://doi.org/10.1177/026975800701400202>

Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior*, 321-326.

<https://doi.org/10.1089/1094931041291295>

Tan, S., & Haining, R. (2016). Crime victimisation and the implications for individual health and well-being: A Sheffield case study. *Social Science & Medicine*, 167, pp. 128-139.

<https://doi.org/10.1016/j.socscimed.2016.08.018>

Van Dijk, J. (2009). Free the Victim: A Critique of the Western Conception of Victimhood.

International Review of Victimology, 16(1), 1-33.

<https://doi.org/10.1177/026975800901600101>

Van Dijk, J., Groenhuisen, M., & Winkel, F. (2007). Victimologie: Voorgeschiedenis en stand van zaken. *Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie*, 9-29.

van 't Hoff-de Goede, M., Leukfeldt, E., van der Kleij, R., & van de Weijer, S. (2021). The Online Behaviour and Victimization Study: The Development of an Experimental Research Instrument for Measuring and Explaining Online Behaviour and Cybercrime Victimization. In M. Weulen-Kranenbarg, & R. Leukfeldt, *Crime and Justice in Digital Society* (pp. 21-157). Cham: Springer. <https://doi.org/10.1007/978-3-030-60527-8>

Vincent, N., & Jane, E. (2017). Beyond law: protecting victims through engineering and design. In E. Martellozzo, & E. Jane, *Cybercrime and its Victims* (pp. 209-223).

Londen: Routledge. <https://doi.org/10.4324/9781315637198-12>

Worsley, D., Wheatcroft, J., Short, E., & Corcoran, R. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *SAGE Open*, 7(2), 1-13. <https://doi.org/10.1177/2158244017710292>

Bijlage A

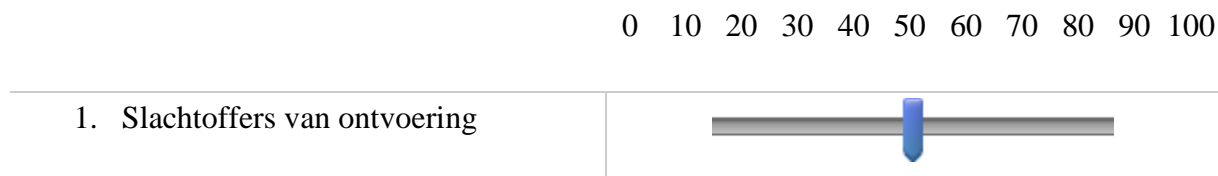
Victim Concern Scale (VCS)

Aandacht voor slachtoffers

In 2021 waren 754.460 Nederlanders (Centraal Bureau voor de Statistiek, 2022) het slachtoffer van een misdrijf. Zij hebben recht op erkenning, genoegdoening en steun, en in bepaalde situaties hebben zij ook recht op een financiële tegemoetkoming. Het vaststellen van de hoogte van de financiële tegemoetkoming is een kwestie van wikken en wegen, waarbij kenmerken van de situatie een rol kunnen spelen. Hoe beoordeelt u de volgende situaties?

Gebruik de onderstaande schaal om aan te geven hoe hoog de financiële tegemoetkoming voor slachtoffers naar uw mening zou moeten zijn. In elke situatie kunt u 0 tot en met 100 punten verdelen, waarbij geldt ‘hoe meer punten, hoe hoger de financiële tegemoetkoming’. Hierbij staat 0 punten voor geen tegemoetkoming en 100 punten voor de hoogst mogelijke tegemoetkoming.

In de vragenlijst was bij alle 32 vragen de onderstaande schuifbalk weergegeven:



2. Slachtoffers van een gewelddadige overval
3. Slachtoffers met een Westerse achtergrond
4. Drugsdealers die het slachtoffer van een misdrijf zijn
5. Slachtoffers van inbraak en diefstal
6. Drugsgebruikers en verslaafden die slachtoffer van een misdrijf zijn
7. Slachtoffers van huiselijk geweld
8. Vrouwelijke slachtoffers
9. Slachtoffers die grootouders zijn
10. Heteroseksuele slachtoffers
11. Slachtoffers van een auto-inbraak
12. Bendeleden die slachtoffer van een misdrijf zijn
13. Slachtoffers van kindermisbruik

14. Slachtoffers van autodiefstal
15. Mannelijke slachtoffers
16. Slachtoffers met een strafblad
17. Slachtoffers met een migratieachtergrond
18. Slachtoffers van verkrachting
19. Slachtoffers met een lichamelijke beperking
20. Lesbische slachtoffers
21. Slachtoffers van zakkenrollerij
22. Slachtoffers van 'hate crime' (delicten gepleegd met discriminerend oogmerk op bijvoorbeeld afkomst, geloof of seksuele oriëntatie)
23. Slachtoffers van cyberpesten
24. Slachtoffers van stalking
25. Slachtoffers van huisvredebreuk (het binnentreden van een woning zonder toestemming)
26. Slachtoffers van oplichting
27. Slachtoffers van cyberstalking
28. Slachtoffers van online seksuele intimidatie
29. Slachtoffers van online oplichting (phishing)
30. Slachtoffers van seksuele intimidatie
31. Slachtoffers van computervredebreuk (hacking)
32. Slachtoffers van pesten

Bijlage B**Marlowe-Crowne Social Desirability Scale (MC-SDS)**

Hierna volgen een aantal uitspraken over persoonlijke attitudes en eigenschappen. Lees elk item en beslis of de uitspraak waar of niet waar is voor u persoonlijk.

Ik doe altijd mijn uiterste best om iemand met problemen te helpen.

- Waar
 Niet waar

Ik heb nog nooit een ontzettende hekel aan iemand gehad.

- Waar
 Niet waar

Er zijn momenten geweest dat ik behoorlijk jaloers was op het geluk van anderen.

- Waar
 Niet waar

Het zou niet in me opkomen om iemand anders voor mijn fouten te laten opdraaien.

- Waar
 Niet waar

Ik voel me soms verontwaardigd wanneer ik mijn zin niet krijg.

- Waar
 Niet waar

Er zijn momenten geweest waarop ik zin had om in opstand te komen tegen mensen met een hogere status, ook al wist ik dat ze gelijk hadden.

- Waar
 Niet waar

Ik ben altijd beleefd zelfs tegen mensen die onvriendelijk zijn.

- Waar
 Niet waar

Wanneer ik iets niet weet vind ik het niet erg dit toe te geven.

- Waar
- Niet waar

Ik heb wel eens gedaan alsof ik ziek was om ergens onder uit te komen.

- Waar
- Niet waar

Ik raak soms geïrriteerd door mensen die gunsten van me vragen.

- Waar
- Niet waar

Ik geloof in een rechtvaardige wereld.

- Waar
- Niet waar

Geluk dwing je af.

- Waar
- Niet waar

Met hard werken kom je verder dan met talent.

- Waar
- Niet waar

Status is belangrijk voor mij.

- Waar
- Niet waar