Slachtofferschap cybercrime onder burgers

Malware, hacken, financiële en persoonlijke delicten in kaart gebracht

Rijksuniversiteit Groningen
Faculteit Gedrags- en Maatschappijwetenschappen
vakgroep Sociologie

Naam student: Miranda Domenie
Studentnummer: s1836811
Begeleider: R. Veenstra
Referent: J.K. Dijkstra

Oktober 2012

Voorwoord

Het Programma Aanpak Cybercrime (PAC) is een versterkingsprogramma van de politie en heeft dit onderzoek gefinancierd. Het Korps Landelijke Politiediensten (KLPD) is de formele opdrachtgever. Hun belangen stonden tijdens de uitvoering van dit onderzoek dan ook voorop. Het combineren van hun belangen met de eisen van de studierichting sociologie was een mooie uitdaging. Ik kreeg van de vertegenwoordigers van beide partijen volop de gelegenheid aan de eisen van de studie te voldoen. Van het PAC wil ik graag Henk Klap en Han Vriend bedanken en van het KLPD Timo Kansil en Rudie Neve.

Een tweede grote uitdaging was het vinden van samenwerking met het Centraal Bureau voor de Statistiek (CBS). Het CBS is de enige instantie in Nederland die beschikt over een bestand met gegevens uit alle Gemeentelijke Basisadministraties van Nederland, die ook nog eens driemaandelijks bijgewerkt wordt. Een steekproef van het CBS is de beste steekproef voor landelijk onderzoek en dus was ik er op gebrand deze te verkrijgen. Het CBS zag na een intensief overleg van bijna een jaar meerwaarde in de samenwerking, aangezien het project onder meer eindigt in een vragenset over cybercrime voor in de Integrale Veiligheidsmonitor (IVM). Zij leverden de steekproef en sloten aan bij de al ingestelde klankbordgroep. Van het CBS wil ik graag Elke Moons, Ger Linden en Jan van Lanen hartelijk bedanken. Ook de andere leden van de klankbordgroep en in het bijzonder de voorzitter, Bert-Jaap Koops, wil ik langs deze weg bedanken voor hun kritische blik en inzet.

De interviews met politiemedewerkers waren informatief. Ik wil alle geïnterviewden hartelijk bedanken voor hun medewerking.

Het veldwerk van een onderzoek van deze omvang vraagt de nodige organisatiecapaciteit en doorzettingsvermogen. Wie had verwacht dat meer dan 1.300 mensen het nummer van de ingestelde helpdesk zouden bellen? Ik wil Marja Blok, Bianca van Brummelen en Anna van der Werff bedanken voor het afhandelen van alle telefoontjes die binnen kwamen terwijl ik zelf in gesprek was.

Het uitvoeren van het onderzoek was niet mogelijk geweest zonder mijn collega's Wouter Stol, Rutger Leukfeldt, Joyce Kerstens, Sander Veenstra en Jurjen Jansen. Zij steunden mij ook als ik niet te genieten was op kantoor, bedankt. En als laatste wil ik mijn co-ouder Jan-Peter Lukkes bedanken die de zorg voor onze dochter, Welmoed, op zich nam als ik extra tijd nodig had. En natuurlijk Welmoed zelf, voor haar liefde, geduld en begrip.

Inhoudsopgave

1 Inleiding

Dit onderzoek gaat over wat er in de samenleving gaande is op het gebied van slachtofferschap van delicten met een digitale component. Hieronder valt een groot aantal verschillende strafbare feiten zoals hacken, verspreiden van malware, maar ook e-fraude en stalking via internet. Bij dergelijke delicten wordt ook wel gesproken over 'cybercrime', maar omdat die term bij politie en justitie niet onomstreden is, gebruiken we die niet zonder eerst op de actuele discussie in te gaan.

1.1 Context: cybercrime als begrip in discussie

Met de komst van internet zijn er nieuwe mogelijkheden gekomen voor het plegen van criminaliteit, en daarvan wordt veelvuldig gebruik gemaakt. Deze nieuw mogelijkheden worden ook wel aangeduid als cybercrime, hoewel termen als internet criminaliteit, e-crime of online criminaliteit eveneens gangbaar zijn. Zowel cyberterrorisme als de productie en verspreiding van kinderpornografie en industriële spionage kunnen vallen onder het koepelbegrip cybercrime. Er bestaat geen internationaal geaccepteerde definitie van cybercrime (Gordon & Ford, 2006; Ngo & Paternoster, 2011; Sommer, 2009). Het definiëren van cybercrime is geen eenvoudig zaak, omdat het bij cybercrime gaat om traditionele of klassieke criminaliteit – met een digitale component – en nieuwe delicten, die een digitale omgeving vereisen (Grabovsky, 2001). Deze zogeheten nieuwe delicten worden ook wel '*third generation crimes*' genoemd (Wall, 2007, p. 10). Computers of computernetwerken kunnen immers middel en doel zijn van cybercrime, maar zij kunnen ook dienen als een omgeving voor criminele activiteiten (Britz, 2008; Parker, 1973; Newman, 2009). Computers kunnen bijvoorbeeld een middel zijn bij fraude, een doelwit zijn van hacken en een virtuele omgeving bieden voor *grooming*[1]. Bij de keuze welke vormen van cybercrime onderzocht worden, wordt – net als bij dit onderzoek – rekening gehouden met de belangen van opdrachtgevers. Onderzoek in het kader van het Europese beleid om de online veiligheid voor kinderen te bevorderen richt zich op *grooming*, cyberpesten en online pornografie. Onderzoek in opdracht van het bankwezen focust op *phishing*[2] en allerlei vormen van online fraude en voor uitgevers van muziek, film en software gaat het om illegaal downloaden en piraterij.

[1] Grooming is het online benaderen van minderjarigen voor seksuele doeleinden. Zie: Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik (CETS No. 201).

[2] De term 'phishing' is een analogie van 'fishing': aas (een email) wordt gebruikt om een vis (internetgebruiker) te vangen. In overeenstemming met de hackerstraditie is de letter 'f' vervangen door de lettercombinatie 'ph' (zie Lynch, 2005, p. 259). '*Phishing is an attempt by an individual or a group to thieve personal confidential information, such as passwords, creditcard information etc*' (James& Philip, 2012, p. 207).De Nederlandse wetgever heeft *phishing* strafbaar gesteld door middel van een aanpassing van de oplichtingsbepaling (art. 326 Sr) (Stb. 2009, 245).

Verkopers van antivirusprogramma's doen onderzoek naar de verspreiding van computervirussen en andere vormen van malware (Koops, 2010). Dit gegeven maakt het definiëren van cybercrime en het bepalen van welke misdrijven precies tot de familie van de cybercrimes behoren niet gemakkelijker (Sommer, Wall). Een factor die het definiëren van cybercrime verder compliceert, is het gegeven dat bepaalde zogeheten cybercrimes die het afgelopen decennium aanleiding waren voor maatschappelijke onrust geen misdrijven zijn in strafrechtelijke zin. Het gaat hierbij bijvoorbeeld om controversiële online gedragingen als *cyber-rape* (McKinnon, 1997) en vandalisme in virtuele werelden (Williams, 2006)[3]. De meeste – algemeen geformuleerde – definities van cybercrime verbinden criminaliteit aan het gebruik van computers of computernetwerken. Een voorbeeld van een dergelijke definitie is: cybercrime is '*any crime that is facilitated or committed using a computer, network or hardware device*' (Gordon & Ford, p. 13). De Europese Commissie (2007) hanteert een inhoudelijk nagenoeg gelijke definitie: '*criminal acts committed using electronic communications networks and information systems or against such networks and systems*.' De hierboven genoemde indeling van computers als middel, doel en omgeving van cybercrime is terug te vinden in de categorisering van cybercrime in het Cybercrime Verdrag van de Raad van Europa. Dit verdrag criminaliseert:

1. *Offences against the confidentiality, integrity and availability of computer data and systems; these include illegal access (hacking), illegal interception, data interference (e.g., viruses), system interference (e.g., denial-of-service attacks), and misuses of devices (e.g., possessing hacker software)*;
2. *Computer-related offences; these include forgery and fraud*;
3. *Content-related offences and copyright offences; the former covers child pornography*.

Wall (2007, pp. 44-48) komt tot een meer chronologische typologie van cybercrime die de zich voortdurend ontwikkelende digitale technologie als uitgangpunt neemt: criminaliteit verandert als gevolg van internetgebruik, neemt nieuwe vormen aan en verandert de verhouding tussen dader en slachtoffer. De eerste generatie cybercrimes gebruikt de (*stand alone*) computer als middel, de tweede generatie cybercrimes maakt gebruik van wereldwijde

[3] In de rechtspraak zijn wel allerlei ontwikkelingen te zien met betrekking tot controversiële online gedragingen en de toepassing van bestaand recht. Zo is in 2008 in Nederland voor het eerst iemand veroordeeld voor virtuele diefstal (Rb. Leeuwarden 21 oktober 2008, LJN BG0939 (RuneScape). Zie: Van Kokswijk & Lodder, 2008. Voor een discussie over de wenselijkheid van de kwalificatie van een virtuele object als een goed in civielrechtelijke zin zie: Hoekman & Dirkzwager, 2009 en Moszkowicz, 2009.

computernetwerken en stelt het strafrecht voor nieuwe uitdagingen en, de derde generatie cybercrimes tenslotte zou zonder internet niet eens bestaan. Het zijn '*true crimes wholly mediated by technology*' (p. 47). Koops (2010, p. 3) stelt de vraag of er ook een vierde generatie cybercrimes zal of is ontstaan en doelt hierbij op misdrijven die zich geheel in de virtuele wereld voordoen: het stelen van virtuele zwaarden, seks hebben met avatars die schijnbaar jonger zijn dan achttien jaar, geweld tegen avatars. Een antwoord op deze misdrijven vraagt om een herziening van begrippen als nadeel of schade en slachtofferschap. Ten aanzien van virtuele diefstal heeft de rechtbank zoals hierboven aangegeven een – in ieder geval voorlopig - antwoord geformuleerd. Slachtoffers van virtuele kinderpornografie - in Nederland in 2002 strafbaar gesteld – zijn feitelijk lastig aan te wijzen; volgens de Nederlandse wetgever moeten kinderen beschermd worden tegen gedragingen en uitingen die bijdragen aan een subcultuur die seksueel misbruik van kinderen bevordert[4]. De typologie van Wall benadrukt in ieder geval de voortdurende ontwikkeling van cybercrime en onderstreept eens te meer de moeilijkheden bij het definiëren en afbakenen van het begrip cybercrime.

Ook in Nederland is in politie- en justitiekringen de discussie gevoerd over het onderscheid tussen traditionele of klassieke criminaliteit en cybercrime. Tot voor kort was de leidende opvatting dat de 'oude criminaliteit in een nieuw jasje' weliswaar onderscheiden moest worden van hardcore cybercrime zoals hacken en het verspreiden van virussen, maar dat deze toch wel behoorde tot de familie der cybercrimes. Die 'oude criminaliteit in een nieuw jasje' heet dan doorgaans 'cybercrime in brede zin' (Leukfeldt, Domenie, & Stol, 2010). De 'hardcore cybercrime' heet dan 'cybercrime in enge zin' – met als belangrijkste - kenmerk dat het niet gepleegd kan worden buiten de digitale wereld omdat deze criminaliteit niet alleen wordt gepleegd *met* ICT maar tegelijk ook *tegen* ICT (dus ICT als doelwit heeft).

Het is beter om 'cybercrime in brede zin' niet te rekenen tot de cybercrimefamilie. Wanneer criminaliteit gekarakteriseerd wordt aan de hand van het middel waarmee een delict wordt gepleegd, zou immers bij elke nieuwe technologie het strafrechtelijk en strafvorderlijk begrippenkader moeten worden geherdefinieerd. Als politie en justitie (menen dat zij) met een nieuwe klasse van delicten worden geconfronteerd, dan ontstaat al snel de discussie of daarvoor niet ook nieuwe organisatieonderdelen en nieuwe procedures moeten worden ontworpen, en of daarvoor nieuwe specialisten moeten worden opgeleid. Die discussie kan worden voorkomen als 'cybercrime in brede zin' niet gezien wordt als een nieuwe

[4] Zie *Kamerstukken I* 2001/02, 27 745, nr. 299b.

criminaliteitsklasse maar als criminaliteit die er altijd al was maar dan op een nieuwe wijze gepleegd. Er is dan immers geen noodzaak om in de strafrechtketen veel te veranderen.

Als politie en justitie 'cybercrime in brede zin' opvatten als een nieuwe vorm van criminaliteit en daarvoor vervolgens nieuwe afdelingen en specialisten en procedures gaan inrichten, dan ontstaat een tweedeling in de strafrechtketen: een zuil die zich bezig houdt met criminaliteit waarin ICT geen wezenlijke rol speelt en een zuil die zich bezig houdt met criminaliteit waarin dat wel het geval is. Het is niet moeilijk om allerlei (afstemmings)problemen te zien ontstaan. Bovendien kan de eerste zuil toch niet om ICT heen, want ook bij klassieke analoge delicten, zoals moord en mishandeling, zullen politie en justitie zich meteen moeten verdiepen in wat het slachtoffer en de verdachte zoal ondernamen in de digitale wereld[5].

Er is binnen politie- en justitie geen discussie over de vraag of cybercrime in enge zin (criminaliteit gepleegd met en gericht op ICT) een nieuwe vorm van criminaliteit is. Denk aan hacken, het vernielen van computergegevens en het verspreiden van virussen. Voor deze delicten zijn aparte wetsartikelen gekomen (voor de drie genoemde delicten respectievelijk art. 138ab Sr, 350a/350b Sr en 350a/139d Sr). Een deel van 'cybercrime in enge zin' is het werk van high-tech criminelen en vraagt een reactie van high-tech politiefunctionarissen en officieren van justitie; een aanzienlijk deel van de cybercrime is echter het werk van burgers (Leukfeldt e.a., 2010) en naar het zich laat aanzien ook van jongeren die elkaar dwars zitten (Kerstens & Stol, te verwachten).

Leggen we de verbinding tussen ontwikkeling in criminaliteit en organisatie van de strafrechtketen, dan zien we dat politie en justitie voor 'cybercrime in enge zin' speciale maatregelen hebben genomen. Bij de politie is er bijvoorbeeld het Team High Tech Crime (THTC) voor geavanceerde cybercrime in enge zin met een internationaal en innovatief karakter. Het THTC behandelde tot nu toe enkele zaken per jaar. Alle andere cybercrime in enge zin dient te worden behandeld door de reguliere rechercheteams (er zijn in de politiekorpsen geen speciale cybercrime-rechercheurs) en die teams kunnen daarbij worden ondersteund door digitaal specialisten (Stol, Leukfeldt, & Klap, 2012). Het Openbaar Ministerie (OM) heeft voor cybercrime in enge zin specifieke Officieren van Justitie (OvJ's) ingesteld.

Bij cybercrime in brede zin ligt het anders. Bij het OM geldt alle cybercrime in brede zin als oude criminaliteit met een moderne *modus operandi* (MO) en die wordt dus behandeld

[5] Zie hiervoor onder meer de discussie over de betekenis van 'cyberlaw' met behulp van de analogie ' horse law' die in de jaren '90 van de vorige eeuw gevoerd is tussen Easterbrook (1996) en Lessig (1999).

door de OvJ die de oude criminaliteit in portefeuille heeft. Bijvoorbeeld: internetfraude hoort thuis bij de fraude-officier; die moet zich dus een nieuwe MO eigen maken. Ook bij de politie wordt cybercrime in brede zin behandeld door de reguliere teams.

1.2 Context: cybercrime als relatief onbekend fenomeen

De Nederlandse overheid geeft aan de opsporing en bestrijding van cybercrime prioriteit en neemt verschillende juridische en organisatorische maatregelen. Volgens het regeerakkoord 'Vrijheid en Verantwoordelijkheid' van het kabinet Rutte moet worden gewerkt aan een '*integrale aanpak van cybercrime'* (Regeerakkoord, 2010, p. 42). Het doel is om de strafrechtketen in staat te stellen effectief uitvoering te geven aan de bestrijding van cybercrime. Ook binnen de Nederlandse politie kent cybercrime een hoge prioriteit. In navolging van het regeerakkoord van 2007 waarin cybercrime als ernstige vorm van criminaliteit werd bestempeld, stelde de Raad van Hoofdcommissarissen (RvHC) het Programma Aanpak Cybercrime (PAC) in en binnen het Korps Landelijke Politiediensten (KLPD) is het Team High Tech Crime (THTC) opgericht. Ook werd binnen het Openbaar Ministerie (OM) het Intensiveringsprogramma Cybercrime gestart (OM, 2008/2009) en is het Kenniscentrum Cybercrime voor de rechtspraak ingesteld (www.rechtspraak.nl[6]).

Opsporingsbeleid vergt dat politie en justitie prioriteiten stellen. De ernstigste problemen verdienen als eerste aandacht. De ernst van een probleem wordt bepaald door zowel de aard als de omvang ervan. Voor opsporingsbeleid moeten politie en justitie dus beschikken over kennis over aard en omvang van cybercrime. Dat impliceert dat ze moeten beschikken over een methode om die kennis te verwerven. Over de omvang van cybercrime is minder bekend dan over de aard ervan (o.a. Van der Hulst & Neve, 2008; Leukfeldt e.a., 2010). Experts en direct betrokkenen laten bij tijd en wijlen horen dat een bepaalde criminaliteitsvorm verontrustend toeneemt, maar systematisch en deugdelijk onderzoek naar de omvang van cybercrime is opvallend afwezig. In de Integrale Veiligheidsmonitor (IVM) was tot 2009 zelfs helemaal geen aandacht voor slachtofferschap van cybercrime. Sindsdien zijn in enkele regio's al wel vragen over cybercrime opgenomen in de IVM en is er door het Centraal Bureau voor de Statistiek (CBS) ook op landelijk niveau geëxperimenteerd met vragen over slachtofferschap van cybercrime. Op dit moment is in Nederland echter nog geen landelijk instrument om de omvang van cybercrime te monitoren.

[6]http://www.rechtspraak.nl/Organisatie/Gerechtshoven/DenHaag/OverHetGerechtshof/Organisatie/Pages/Kenniscentrum-Cybercrime.aspx, laatst geraadpleegd op: 2012-02-23.

Over de aard van cybercrime – modus operandi, typering en classificering - is meer bekend dan over de omvang. Uit het literatuuronderzoek naar de omvang van cybercrime komt naar voren dat de kennis over de omvang van cybercrime fragmentarisch is en dat slachtofferschap van delicten met een digitale component aanzienlijk te noemen is (zie hoofdstuk 2).

1.3 Onderwerp van onderzoek

Dit onderzoek gaat over slachtofferschap van delicten met een digitale component, onder burgers in Nederland. Criminaliteit wordt op uiteenlopende manieren gedefinieerd. Bonger (1932, aangehaald in Lissenberg, 2001) definieert criminaliteit als ernstige antisociale handelingen, waarop de Staat door toevoeging van leed (straf of maatregel) reageert. Ofwel, zoals beschreven door Ferwerda (2008): criminaliteit is het plegen van delicten. Dit onderzoek definieert criminaliteit conform de benadering van Ferwerda als gedrag dat strafbaar is gesteld door de strafwetgever.

In dit onderzoek is niet gestart vanuit een theoretische definitie van het begrip cybercrime die vervolgens geoperationaliseerd is. Het vertrekpunt zijn delicten waarvan burgers slachtoffer worden en waarbij ICT op dit moment van wezenlijke belang is, en waarover politie en justitie een kennistekort ervaren voor wat betreft slachtofferschap. Het gaat om:

- cybercrime in enge zin:
  - malware en hacken;
- cybercrime in brede zin:
  - in de financiële sfeer: fraude via veiling- of verkoopsites, identiteitsfraude, voorschotfraude;
  - in de persoonlijke sfeer: stalking, bedreiging, smaad/laster/belediging.

Daarmee is aangegeven om welke concrete delicten dit onderzoek gaat. De termen cybercrime in brede of enge zin worden hierna niet meer gebruikt. Gemakshalve wordt soms nog wel de term cybercrime gebruikt wanneer het over de onderzochte delicten in het algemeen gaat.

In dit onderzoek wordt slachtofferschap van cybercrime in eerste instantie gemeten door af te gaan op wat de ondervraagde zelf daarover aangeeft. Daarbij is wel een aantal controlevragen gesteld om een indicatie te krijgen van hoe zeker het is, dat de persoon slachtoffer was.

Verborgen slachtofferschap valt buiten het bereik van dit onderzoek. Het is bijvoorbeeld niet te achterhalen hoe vaak een computer is opgenomen in een botnet terwijl de gebruiker daarvan geen notie heeft. Dat probleem doet zich ook voor bij offline criminaliteit, bijvoorbeeld bij zakkenrollerij en insluiping, maar bij cybercrime is het probleem groter omdat gebruikers niet altijd weten wat er zich op hun computer afspeelt. Ook slachtofferloze cybercriminaliteit wordt met dit onderzoek niet gemeten. Daarvoor zijn slachtofferenquêtes niet geschikt. Als twee mensen een illegale deal sluiten in cyberspace, is sprake van cybercrime, maar zullen de betrokkenen niet aangeven dat zij slachtoffer waren.

1.4 Onderzoeksvragen

In dit onderzoek staan twee thema's centraal. Ten eerste willen we weten wat de omvang van slachtofferschap cybercrime is. De centrale onderzoeksvraag is:

Wat is de omvang van slachtofferschap van cybercrime onder internetters?

Verder is onderzocht wat volgens internetters de rol is van de politie als het gaat om veiligheid op internet, of slachtoffers aangifte doen bij de politie en of ze tevreden zijn over de reactie van de politie op de aangifte. De onderzoeksvragen die hierbij horen zijn:

1. Wat is volgens internetters de rol van de politie in het waarborgen van de veiligheid op internet?
2. Welk deel van de slachtoffers van cybercrime neemt contact op met de politie wanneer zij slachtoffer zijn geworden van cybercrime?
3. In hoeverre zijn slachtoffers tevreden over de reactie van de politie op de aangifte?

1.5 Bruikbaarheid voor de praktijk

De uitkomsten van dit onderzoek kunnen door politie en bestuur gebruikt worden bij het bepalen van (nieuw) beleid. De uitkomsten van het onderzoek kunnen ondersteuning bieden bij het aanbrengen van prioriteiten in preventie en opsporing, het maken van criminaliteitsbeeldanalyses, het ontwikkelen van een Nationaal Dreigingsbeeld, het beantwoorden van kamervragen over de aard, omvang en aanpak van cybercrime en het evalueren van beleidsmaatregelen. Ook kunnen de uitkomsten bruikbaar zijn voor het ontwerpen van verdergaand, met name verdiepend onderzoek op het gebied van cybercrime. Verder beoogt het onderzoek bij te dragen tot een gevalideerde vragenlijst die geschikt is voor

herhaalmetingen. Een deel van de vragenlijst zal door het CBS gebruikt worden in de Integrale Veiligheidsmonitor (IVM). Hierdoor kan op lange termijn inzicht verkregen worden in de ontwikkelingen in aard en omvang van het slachtofferschap.

1.6 Leeswijzer

In hoofdstuk 2 staan de bevindingen uit het literatuuronderzoek waarbij de focus ligt op de bevindingen uit onderzoek met betrekking tot de omvang van de voor het onderzoek relevante vormen van cybercrime. Hoofdstuk 3 beschrijft de gehanteerde onderzoeksmethode. Hoofdstuk 4 is een overzicht van de respons en representativiteit van het onderzoek. In de hoofdstukken 5 tot en met 7 komt aan bod wat de prevalentie is per delict, wat de modus operandi is geweest van de dader, wat de relatie is tussen dader en slachtoffer, wat de materiële schade is voor het slachtoffer, de aangiftebereidheid en de reactie van de politie. Hoofdstuk 5 gaat over het verspreiden van malware en hacken, in hoofdstuk 6 worden financiële delicten besproken (fraude via veiling- of verkoopsites, voorschotfraude en identiteitsmisbruik) en in hoofdstuk 7 staan delicten in de persoonlijke sfeer centraal (stalking, smaad/laster en bedreiging). In hoofdstuk 8 wordt meervoudig slachtofferschap besproken. Hierin wordt duidelijk gemaakt wie slachtoffer zijn van meerdere delicten. Hoofdstuk 9 is een overkoepelend hoofdstuk waarin twee onderwerpen centraal staan: wat zou volgens burgers de rol van de politie zou moeten zijn en wat is het effect van het al dan niet opnemen van een aangifte op de tevredenheid van burgers over de politie. In hoofdstuk 10 staan de conclusies en aanbevelingen. In hoofdstuk 11 staat discussie centraal: wat is de betekenis van de resultaten uit het onderzoek voor toekomstig onderzoek.

2 Onderzoek naar en theorie over slachtofferschap van cybercrime

In dit hoofdstuk wordt eerst de ontwikkeling van de victimologie als subdiscipline van de criminologie beschreven (§ 2.1) waarna kort de theorieën van belang voor de verklaring van slachtofferschap worden beschreven (§ 2.2). Vervolgens wordt een overzicht gegeven van voor dit onderzoek relevante gegevens uit bestaand onderzoek naar cybercrime (§2.3).

2.1 De victimologie als subdiscipline van de criminologie

De achttiende eeuw wordt algemeen beschouwd als de ontstaansperiode van de criminologie, waarvan de historie zich volgens Garland (2002, p. 4) laat lezen als een verhaal van elkaar opvolgende 'iconen en demonen', zoals Beccaria en Lombroso. Begin twintigste eeuw ontwikkelde de criminologie zich tot een empirische wetenschap (McLennan, Pawson, & Fitzgerald, 1980). Een veelvuldig geciteerde definitie van criminologie is afkomstig van de Amerikaanse criminologen Sutherland en Cressey: criminologie is '*the body of knowledge regarding delinquency and crime as a social phenomenon*' (1960, p. 3). Sutherland en Cressy geven vervolgens aan dat de criminologie zich bezighoudt met '*the process of making laws, of breaking laws, and of reacting toward the breaking of laws*' (p.3). In de criminologie staat onderzoek naar verklaringen voor daderschap centraal en in deze verklaringen speelde het slachtoffer van als crimineel bestempelde gedragingen lang geen rol (Wittebrood, 2006). In de jaren veertig van de twintigste eeuw werd het slachtoffer van misdaden 'herontdekt' en in 1947 werd de term 'victimologie' gemunt door de jurist Benjamin Mendelsohn (Boutellier, 2008; Wilson, 2009). De eerste studies naar slachtofferschap waren speculatief, maar vanaf de jaren zeventig van de vorige eeuw heeft de victimologie als wetenschappelijke discipline een grote ontwikkeling doorgemaakt en kreeg empirisch onderzoek naar slachtofferschap internationaal aandacht (Drapkin & Viano, 1974; Joutsen, 1998; Schneider, 2001; Van Dijk, 1997).

Er zijn drie redenen aan te wijzen voor het gegeven dat slachtofferschap pas laat in de twintigste eeuw in de belangstelling kwam te staan en er een begin werd gemaakt met de emancipatie van het slachtoffer: het rechtssysteem diende primair als reden tot de vereffening van schuld door de dader aan de gemeenschap; er bestond weinig aandacht voor en kennis over de gevolgen van slachtofferschap en; juristen waren lang huiverig voor de vergeldingsbehoefte van slachtoffers tijdens het strafproces (Lissenberg, 1997). Schneider verbindt de toenemende aandacht van wetenschappers en de bevolking in het algemeen voor slachtoffers en slachtofferschap aan het civilisatieproces zoals beschreven door Norbert Elias.

Mensen zijn zich in toenemende mate bewust van de problematiek rond geweld binnen hun eigen sociale omgeving en tegelijkertijd worden geweld en inbreuken op sociale normen steeds meer afgewezen (p. 450). Dignan (2005, pp. 14-15) noemt drie concrete factoren die eind vorige eeuw een rol zijn gaan spelen: strafrechthervormers die compensatie voor slachtoffers promoten; de toegenomen zichtbaarheid van slachtoffers in de media en; de erkenning van het bestaan van kwetsbare groepen: kinderen die slachtoffer worden van seksueel misbruik, geweld of verwaarlozing en vrouwen die slachtoffer worden van huiselijk en seksueel geweld. De feministische beweging heeft er met name toe bijgedragen dat slachtofferschap onder deze groepen hoog op de politieke en sociale agenda is geplaatst (Dignan, 2005; Groenhuijsen, 2008b). Inmiddels zijn de zogeheten basisrechten voor slachtoffers algemeen erkend, wat onder meer blijkt uit de politieke vertaling hiervan in de *Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power* van de Verenigde Naties en de *Recommendation on the Position of Victims in the Framework of Criminal Law and Procedure* van de Raad van Europa. Criminaliteit wordt niet meer opgevat als (alleen) een aantasting van de rechtsorde, maar als een aantasting van de rechten van het individuele slachtoffer.

Er bestaat vooralsnog geen sluitende definitie van victimologie en Rock (1994, p. XI) omschreef victimologie zelfs als een '*relatively amorpheus discipline*'. In de discussie rond de definiëring en afbakening van deze wetenschappelijke discipline kunnen wel twee richtingen worden onderscheiden. Aan de ene kant staan de pleitbezorgers van een brede definitie, waarbij het uitgangspunt is dat mensen slachtoffer kunnen worden van een veelheid aan fenomenen, zoals ziekte en ongelukken, armoede en rampen. Aan de andere kant staan de voorstanders van een smalle definitie, waarbij slachtofferschap alleen verbonden wordt aan als crimineel bestempelde gedragingen (Van Dijk, 1997, p. 296; Zijderveld, Cleiren, & Du Perron, 2005, p. 7). Een voorbeeld van een smalle definitie van victimologie is: '[*t*]*he scientific study of victimization, including the relationship between victims and offenders, the interactions between victims and the criminal justice system – that is, the police and courts, and corrections officials – and the connections between victims and others societal groups, such as the media, businesses, and social movements*' (Karmen, 1990, p. 18). De victimologie wordt gezien als een subdiscipline van de criminologie (Fatah, 2000) en zij heeft een multidisciplinair karakter (Groenhuijsen, 2008a). De victimologie – theorievorming en onderzoek – houdt zich hoofdzakelijk bezig met de prevalentie van slachtofferschap, de kenmerken van slachtoffers, de relatie van slachtoffers met daders en de wisselwerking tussen dader- en slachtofferschap en, de analyse van het gedrag van slachtoffers als situationele

variabele. Ook vanuit de criminologie is er aandacht voor slachtofferschap; niet alleen wordt er gekeken naar een mogelijke wisselwerking tussen dader- en slachtofferschap, maar ook naar de mogelijke invloed van (gedragingen van) slachtoffers op crimineel gedrag.

Informatie over criminaliteit en slachtofferschap is meestal gebaseerd op officiële registraties, slachtofferenquêtes en *self-report*-onderzoek. Er zijn verschillende internationale statistieken over criminaliteit en slachtofferschap. Zo publiceren de Verenigde Naties onder andere het *World Drug Report* en de *United Nations Surveys on Crime Trends and the Operations of the Criminal Justice Systems*. Het *European Sourcebook of Crime and Criminal Justice Statistics* verbonden aan de Raad van Europa verschijnt sinds 1999 en omvat criminaliteits- en rechtshandhavingsstatistieken van 40 Europese landen met onder meer slachtoffergegevens, politionele registraties en berechtingen. In Nederland maakt het Centraal Bureau voor de Statistiek (CBS) sinds 1948 criminaliteitsstatistieken op basis van politiegegevens, via Statline[7] maakt het gegevens openbaar over de rechtspraak en publiceert het over ontwikkelingen op het gebied van criminaliteit (Bijleveld, 2005). Officiële registraties geven geen volledig beeld van criminaliteit en slachtofferschap. Dit heeft te maken met de *dark number*-problematiek, dat wil zeggen, de geregistreerde criminaliteit is slechts een deel van de totale criminaliteit. De volgende factoren zijn van invloed op deze problematiek: de aangiftebereidheid van slachtoffers, prioriteitenstelling en capaciteit van politie en justitie en de onzichtbaarheid van bepaalde misdrijven, zoals fraude (Wittebrood & Nieuwbeerta, 2006). Slachtofferenquêtes en *self-report*-onderzoek geven een aanvulling op het onvolledige beeld van criminaliteit en slachtofferschap uit de officiële registraties (Pauwels & Pleysier, 2008).

De eerste slachtofferenquêtes werden uitgevoerd in de Verenigde Staten in de jaren zestig van de vorige eeuw. Na een evaluatie van de gegevens uit deze enquêtes, is in 1972 het *National Crime Victimization Survey* (NCVS)[8] ingesteld. Dit is een periodieke, nationale slachtofferenquête met als doel de prevalentie van veelkomende criminaliteit in kaart te brengen (Wittebrood, 2006). Naar Amerikaans voorbeeld worden nu in de meeste westerse landen nationale slachtofferenquêtes gehouden (Van Kerckvoorde, 1995) en in Nederland is deze ontwikkeling ingezet met de enquête van Fiselier in 1973. Slachtofferenquêtes zijn sindsdien uitgevoerd onder verschillenden benamingen – bijvoorbeeld Enquête Slachtoffers Misdrijven – en sinds 1 januari 2006 kent Nederland de Veiligheidsmonitor (VM) (Wittebrood, 2006). De VM maakt gebruik van verschillende dataverzamelingsmethoden:

[7] Zie http://statline.cbs.nl/statweb.
[8] Tot 1991 heette het NCVS National Crime Survey (NCS).

respondenten kunnen via internet, schriftelijk, telefonisch of *face to face* worden bevraagd. De vragenlijst bestaat uit vaste en facultatieve modules (Versteegh & Van den Heuvel, 2007). Daarnaast is er de *International Crime Victims Survey* (ICVS), een enquête die wordt afgenomen in meer dan 60 landen en die gebruik maakt van een gestandaardiseerde vragenlijst. De ICVS uit 2004/2005 voor 15 EU-landen wordt aangeduid als de *European Crime Survey* (Wittebrood). Een ander voorbeeld is de Eurobarometer *Public Safety* van de Europese Unie.

Ook via (potentiële) daders kan inzicht worden verkregen in criminaliteit en slachtofferschap en met dit doel is het *self-report*-onderzoek ontwikkeld (Pauwels & Pleysier, 2009). In 1990 is de International *Self-reported Delinquency Study* opgezet (ISRD). De ISRD brengt crimineel en afwijkend gedrag van jongeren in de leeftijd tussen 14 en 21 jaar in kaart. In Nederland wordt sinds 1986 door het Wetenschappelijk Onderzoek en Documentatie Centrum (WODC) iedere twee jaar de Monitor Zelfgerapporteerde Jeugdcriminaliteit uitgevoerd. Een voorbeeld van onderzoek dat inmiddels niet meer wordt uitgevoerd is een module van het Permanent Onderzoek Leefsituatie van het CBS, waarin jongeren in de leeftijd van 12 tot en met 29 jaar een vragenlijst invulden over onder meer daderschap van (kleine) criminaliteit (Bijleveld, 2005; Vanderveen, 2004).

Er zijn nog nauwelijks nationale slachtofferenquêtes die cybercrime of bepaalde vormen van cybercrime hebben opgenomen in hun vragenlijsten. In het eerder genoemde NCVS uit de Verenigde Staten worden aan ongeveer 100.000 personen van 12 jaar en ouder afkomstig uit 50.000 huishoudens twee keer per jaar vragen gesteld over slachtofferschap van criminaliteit. In de tweede helft van 2001 zijn in NCVS ook vragen opgenomen over cybercrime; in de tweede helft van het jaar 2004 zijn deze vragen over cybercrime weer verwijderd[9] (Lauritsen, 2005; Kowalsi, 2002). De NCVS uit deze periode verschaft als enige gegevens over cybercrime op nationaal niveau (Yucedal, 2010). In de Verenigde Staten wordt cybercrime gericht tegen bedrijven periodiek onderzocht door middel van het *National Computer Security Survey* (NCSS). In Nederland zijn in 2010 voor het eerst vragen over cybercrime opgenomen in de Veiligheidsmonitor. Het gaat om pilotvragen die alleen zijn voorgelegd aan respondenten die door het CBS voor de landelijke waarneming zijn benaderd. De onderzoeksresultaten worden (nog) niet opgenomen in de landelijke rapportage.

[9] Voor de vragenlijsten, methodologie en publicaties zie http://bjs.ojp.usdoj.gov/index.cfm?ty=dcdetail&iid=245#Documentation.

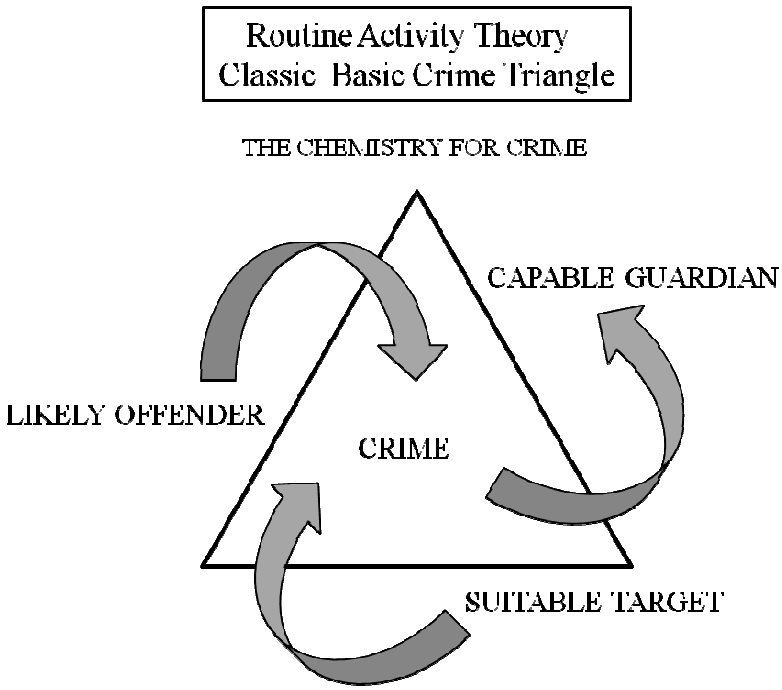
2.2 Theorieën slachtofferschap

Theoretische concepten om oorzaken van of correlaties met slachtofferschap van criminaliteit te identificeren en te verklaren zijn overwegend gebaseerd op twee theorieën: de leefstijltheorie en de routineactiviteitentheorie (Wittebrood, 2006). Deze theorieën zijn ontwikkeld op basis van empirisch onderzoeksmateriaal dat verzameld werd in de jaren zeventig van de vorige eeuw en beide theorieën zijn onderdeel van het theoretische raamwerk aangeduid als rationele keuzebenadering (Williams & McShane, 1999, pp. 233-235). De leefstijltheorie is door Hindelang, Gottfredson en Gaffolo (1978) voor het eerst uiteengezet in *Victims of Personal Crime: an Empirical Foundation for a Theory of Personal Vicitimization*. Hindelang e.a. gaan ervan uit dat de sociale rol en sociale positie van een individu van invloed is op de persoonlijke levensstijl en op de keuze van een individu om deel te nemen aan bepaalde (risicovolle) activiteiten of zich te begeven in bepaalde (risicovolle) situaties. Jonge mannen en oudere vrouwen lopen bijvoorbeeld uiteen qua leefstijlactiviteiten – regelmatig terugkerende activiteiten rondom werk, school en vrije tijd. Omdat de leefstijlen van jonge mannen en oudere vrouwen verschillen, loopt ook de kans op slachtofferschap van criminaliteit tussen deze twee groepen uiteen. HOE DAN

In tegenstelling tot de leefstijltheorie die vooral individuele verschillen in de kans op slachtofferschap beoogd te duiden, is de routineactiviteitentheorie, oftewel de theorie van de alledaagse bezigheden, eerder een typische macro-theorie: de theorie richt zich op het verklaren van patronen, zoals de spreiding van delicten en de toename of afname van een bepaald delict in de tijd. Cohen en Felson, de bedenkers van de routineactiviteitentheorie, stellen in hun artikel *Social Change and Crime Rate Trends: a Routine Activity Approach* uit 1979 dat de focus bij het verklaren van trends in criminaliteit meer gelegd moet worden bij omstandigheden om criminaliteit te plegen en minder bij kenmerken van daders. De aanleiding voor het schrijven van het artikel was het gegeven dat in de jaren zestig van de vorige eeuw de criminaliteit in de Verenigde Staten sterk toenam, terwijl de sociale problemen juist minder werden. Cohen en Felson verklaren de toename van criminaliteit door te wijzen op sociale veranderingen binnen gezinnen – bijvoorbeeld de participatie van vrouwen op de arbeidsmarkt en het toenemend aantal echtscheidingen - waardoor de leden van huishoudens vaker thuis afwezig zijn en de toename van waardevolle, transporteerbare goederen in huishoudens, zoals televisies en videoapparatuur. Daders kregen meer mogelijkheden om lege huizen binnen te gaan waar zij onbewaakte goederen aantroffen. Volgens de routineactiviteitentheorie vindt criminaliteit plaats wanneer drie essentiële elementen samenkomen in tijd en ruimte : (1) een gemotiveerde dader (*a likely offender*); (2)

een geschikt doelwit (*a suitable target*), en (3) de afwezigheid van goede bescherming (*the absence of a capable guardian*). Wanneer een van deze elementen ontbreekt, zal dit crimineel of deviant gedrag voorkomen (Miethe & Meier, 1994). Zo zal gemotiveerde dader geen misdrijf kunnen plegen wanneer een geschikt doelwit ontbreekt of wanneer het doelwit afdoende beschermd wordt (Mustaine & Tewksbury, 1998).

Figuur 1: Routine activiteiten driehoek



(Bron: Felson, 1998)

Het risico van slachtofferschap van criminele activiteiten wordt bepaald door de dagelijkse routineactiviteiten van individuen waardoor zij in contact komen met potentiële daders. Mustain en Tewksbury (1998) stellen dat '*the routines of activities influence the degree of exposure one has to potential offenders, how valuable or vulnerable individuals or their property are as targets, and whether/or how well guarded they or their property is*' (p. 830). Volgens Miethe en Meier (1994, p. 30) is er een oorzakelijk verband tussen gelegenheid gecreëerd door dagelijkse routineactiviteiten en crimineel gedrag. De routineactiviteitentheorie richt zich met name op het doelwit of het slachtoffer van criminaliteit en de bescherming van het doelwit of slachtoffer. Volgens Felson en Clarke (1998) is een doelwit kwetsbaar op het moment dat het voldoet aan het acroniem VIVA: *value* (waarde), *inertia* (gewicht), *visibility* (zichtbaarheid) en *access* (toegang). Later zijn daar nog

de kenmerken meeneembaar, verbergbaar en verhandelbaar aan toegevoegd (Clarke, 1999). Met bescherming bedoelen Felson en Clarke niet alleen politieagenten of beveiligers, maar iedere aanwezige die een dader kan ontmoedigen criminaliteit te plegen. Wanneer het gaat om preventie van criminaliteit wijzen Felson en Clarke nadrukkelijk op de rol die de inrichting van de omgeving hierbij kan spelen: '*crime pattern theorists and other environmental criminologists have shown that the design and management of town, city, and business areas can produce major shifts in crime rates*' (p. 6). Felson (2002) wijst op de mogelijkheden die de architectuur heeft om het aantal mogelijke slachtoffers op een bepaalde tijd en plaats te beïnvloeden en op de rol die het inrichten van een omgeving kan spelen bij de bescherming van burgers. Hierbij kan gedacht worden aan het ontwerp en de inrichting van metrostations, parkeergarages en winkelcentra. De architect Newman (1972) duidt dit aan met de benaming '*defensible space architecture*'.

In empirisch onderzoek wordt nog nauwelijks een verschil gemaakt tussen de leefstijltheorie en de routineactiviteitentheorie (Choi, 2008); de twee theorieën worden samen ook wel de leefstijl/routineactiviteiten theorie genoemd (Ngo & Paternoster, 2011; Schneider, 2001) of gezien als een onderdeel van de '*general opportunity theory*' of algemene gelegenheidstheorie zoals beschreven door Cohen, Kluegel en Land (1981). Sampson and Wooldredge (1987) stellen dat '*the more general opportunity model* […], *which incorporates lifestyles and routine activities with a more explicit focus on ecological proximity and macro sociological processes … provides the most promising path for future multilevel victimization research*' (p. 391). Het belang van de leefstijltheorie en routineactiviteitentheorie voor de verklaring van slachtofferschap van criminaliteit is aangetoond door empirisch onderzoek (Cohen & Felson, 1979; Coupe & Blake, 2006; Holtfreter, Reisig, & Pratt, 2008; Messner, & Blau, 1987; Messner, Zhou, Lening, & Jianhong, 2007; Spano & Nagy, 2005; Stewart, Elifson, & Sterk, 2004; Tewksbury & Mustaine, 2000), hoewel de theorieën meer geschikt lijken voor het verklaren van slachtofferschap van vermogensdelicten dan van geweldsmisdrijven (Miethe, e.a.; Miethe & Meier, 1994).

Naast de hierboven theorieën wordt ook steeds vaker de zelfcontroletheorie, een theorie oorspronkelijk ontwikkeld om daderschap te verklaren, gebruikt om slachtofferschap van criminaliteit te duiden. Gottfredson en Hirschi (1990) ontwikkelden samen de zelfcontroletheorie waarin één mechanisme, te weten (onvoldoende) zelfcontrole, wordt aangewezen als de oorzaak van crimineel en afwijkend gedrag en waarin de vroege kindertijd – meer specifiek het opvoedingspatroon van opvoeders – bepalend wordt geacht voor de ontwikkeling van zelfcontrole. Sociale factoren spelen tijdens de volwassenheid geen causale

rol voor de verklaring en duiding van crimineel of afwijkend gedrag. Personen met een hoge zelfcontrole kunnen weerstand bieden aan de verleiding toe te geven aan behoeftebevrediging op de korte termijn en personen met een lage zelfcontrole zijn hiertoe niet of minder in staat. Crimineel gedrag levert op korte termijn allerlei beloningen op, zoals geld, spanning, ontsnapping aan sociale verplichtingen. Uit de kenmerken van criminele handelingen leiden Gottfredson en Hirschi de eigenschappen af van mensen met een lage zelfcontrole – *the elements of self-control*. Criminaliteit biedt ogenblikkelijke en gemakkelijke behoeftebevrediging (*easy or simple gratification of desires*), is opwindend (*exiting*), is niet of nauwelijks gericht op de lange termijn (*few or meager long-term benefits*), vereist geen speciale vaardigheden (*little skill or planning*) en brengt slachtoffers schade of leed toe (*pain or discomfort for the victim*). Mensen met een lage zelfcontrole die de wet overtreden zullen dus gekenmerkt worden door een grotere gerichtheid op het hier en nu (*have a concrete 'here and now' orientation*), een gering doorzettingsvermogen (*lack diligence, tenacity, or persistence*) en een voorkeur voor avontuurlijke, fysieke activiteiten (*tend to be adventuresome, active, and physical*). Ook neigen zij ertoe ongevoelig te zijn voor het leed en de behoeftes van anderen (*insensitive to the needs and sufferings of others*) (pp. 85-102). Het gevaar van een cirkelredenering – een geringe zelfcontrole moet een verklaring bieden voor crimineel gedrag, terwijl een geringe zelfcontrole juist vastgesteld zou moeten worden aan de hand van crimineel gedrag – inherent aan de theorie van Gottfredson en Hirschi is opgelost met behulp van de zelfcontrole-schaal van Grasmick, waarmee niveaus van zelfcontrole kunnen worden vastgesteld (Grasmick, Tittle, Bursik, & Arneklev, 1993). Uit empirisch onderzoek komt een duidelijk verband naar voren tussen een geringe zelfcontrole en crimineel of afwijkend gedrag van jongeren en volwassenen (zie Arneklev, Grasmick, Tittle, & Bursik, 1993; Burton, Cullen, Evans, Fiftal Alarid, & Dunaway, 1998; Evans, Cullen, Burton, Dunaway, & Benson, 1998; Grasmick, e.a; Polakowski, 1994; Gibbs, Giever, & Martin, 1998; Piquero & Tibbets, 1996). Volgens Pratt en Cullen (2000) vormt zelfcontrole zelfs een van de sterkste bekende correlaties met crimineel gedrag.

Hoewel de zelfcontroletheorie is ontwikkeld om crimineel gedrag te verklaren en dus geen victimologische theorie is, stellen Gottfredson en Hirschi dat de sterke correlatie tussen dader- en slachtofferschap het gevolg is van onvoldoende zelfcontrole (pp. 92-94). De hierboven beschreven kenmerken van mensen met een lage zelfcontrole resulteren niet alleen in een grotere kans op crimineel gedrag, maar dragen ook bij tot een grotere kans op slachtofferschap (Forde & Kennedy, 1997). Personen met een geringe zelfcontrole kunnen eerder verzeild raken in risicovolle situaties waarin zij te maken kunnen krijgen met

criminaliteit – bijvoorbeeld het bezoeken van een discotheek waar drugs worden verkocht – en, daarnaast kan hun gedrag binnen risicovolle situaties – bijvoorbeeld impulsief reageren in een discotheek – de kans om slachtoffer te worden van criminaliteit vergroten. De gerichtheid op de korte termijn zou ook preventief gedrag minder waarschijnlijk maken (Schreck, Stewart, & Fisher, 2006). Aanwijzingen uit onderzoek ondersteunen de opvatting dat de zelfcontrole theorie van Gottfredson en Hirschi ook van toepassing is op slachtofferschap van criminaliteit (Holtfreter, Reisig, & Pratt, 2008; Piquero, MacDonald, Dobrin, Daigle, & Cullen, 2005; Schreck, 1999; Schreck, e.a.; Schreck, Wright, & Miller, 2002; Stewart, Elifson, & Sterk, 2004).

2.3 Onderzoek naar slachtofferschap cybercrime

De prevalentie van slachtofferschap van cybercrime is grotendeels onbekend. Dit geldt voor Nederland, maar ook voor andere delen van de wereld waar het gebruik van computers en internet onderdeel is van het dagelijks leven, zoals de Verenigde Staten en Australië. Jacques Bus, Hoofd van de *ICT-Security Unit* van de Europese Commissie stelt dat …'*there is a clear lack of adequate statistics measuring the state of trust and security in the Information Society. Current data available is insufficient, fragmented, and often incomparable. There exists no coherent set of reliable data based on… threats, incidents or perceptions of trust and security*' (Galetsas, 2007, p. 2). Moitra (2005) geeft aan dat de studie naar (slachtofferschap van) cybercrime bemoeilijkt wordt door het ontbreken van relevante data en de moeilijkheid van het verzamelen van dergelijke data. Veel wetenschappers zijn het er over eens dat officiële cijfers verstrekt door overheden geen volledig beeld geven van de prevalentie van cybercrime, omdat burgers niet elke cybercrime melden bij de instanties. Sommigen denken dat het melden bij de politie geen zin heeft, anderen vinden de schade veroorzaakt door cybercrime te gering om te moeite te nemen het misdrijf te melden en sommigen zijn zich er niet van bewust dat zij een slachtoffer zijn van cybercrime (Goodman & Brenner, 2002; Moitra; Wall, 2007). Voor overheden is het vervolgen van cybercriminelen bovendien een lastige zaak, omdat deze criminelen in toenemende mate gebruik maken van anonieme remailers, encryptie software en zogeheten '*third-party-systems*' (Furnell, 2002; Grabovsky & Smith, 2001; Yar, 2005). In onderstaande tekst wordt een overzicht gegeven van wat momenteel bekend is over de omvang van cybercrime. Het overzicht betreft alleen vormen van cybercrime die relevant zijn voor dit onderzoek (zie ook §1.3).

2.3.1 Malware en hacken

Het verspreiden van malware en hacken houdt verband met elkaar. Zo kan een hacker gebruik maken van malware om zonder toestemming een computer of computernetwerk binnen te dringen (Leukfeldt, e.a., 2010). Degene die op internet malware ter beschikking stelt, hoeft echter niet per se een hacker te zijn en daarnaast kan een hacker ook zonder gebruik te maken van malware een computer binnendringen (Chu, Holt, & Joon Ahn, 2010).

Malware

Malware is kwaadaardige software die ongevraagd en meestal ongemerkt wordt geïnstalleerd op de computer (Furnell, 2002) en het creëren en distribueren van malware is een winstgevende onderneming (Schiller, Binkley, Harley, Evron, Bradley, Williams, & Cross, 2007). Voorbeelden van malware zijn virussen[10], *trojan horses*[11], wormen[12] en *spyware*[13] die in staat zijn de functies binnen computerprogramma's en databestanden te veranderen of te vernietigen of hele computernetwerken lam te leggen. Malware kan onder meer worden verspreid via bijlagen in e-mails, het downloaden van bestanden, en *instant messaging* (Kaperski, 2003; Szor, 2005). Malware kan worden geactiveerd door het openen van bestanden, maar sommige malware wordt geactiveerd door alleen al het bezoeken van – meestal pornografische – websites, waarvan de web browser onvoldoende beschermd is of gebreken vertoond (Taylor, Caeti, Loper, Fritsch, & Liederbach, 2006). De verspreiding van malware leidt tot schade vanwege de kosten van identiteitsdiefstal, verlies van (beschermde) data, inkomstenderving als gevolg van verlies consumentenvertrouwen in e-commerce en verlies van productiviteit en functionaliteit van computersystemen (Symantec, 2012; Taylor, e.a.).

In Nederland is het verspreiden of ter beschikking stellen van programma's die bestemd zijn om schade aan te richten in een geautomatiseerd werk strafbaar gesteld in art. 350a lid 3 Sr. Het maken en verspreiden van schadelijke wormen en virussen is daarmee strafbaar onder voornoemd artikel. Wanneer er geen schade aangericht wordt, kan het

[10] Cohen definieert een computer virus als '*a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself*' (1987, p. 23).

[11] Een *trojan horse* is '*a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality*' (Skoudis & Zeltzer, 2004, p. 251).

[12] Internet wormen zijn schadelijke programma's die in staat zijn zichzelf te kopiëren en zich verder te verspreiden (Nazario, 2003).

[13] *Spyware* is software die zonder dat de gebruiker er weet van heeft en zonder diens toestemming op de computer wordt geïnstalleerd en dat informatie over de gebruiker verzamelt en verstuurt naar de cybercrimineel. Het kan onder andere gaan om toetsaanslagen (*keyloggers*), surfgedrag, creditcardnummers (Bocij, 2006; Hackworth, 2005).

verspreiden van malware worden gezien als een hulpmiddel voor computervredebreuk, strafbaar gesteld in art. 139d lid 2 onder a Sr. Dit geldt ook voor *trojan horse* software die meestal indirect schade aanricht. Het verspreiden van *spyware* valt niet onder art. 350a lid 3 Sr: het heimelijk doorgeven van privégegevens valt niet onder schade in de zin van het strafrecht. Mogelijk is het installeren van *spyware* op een computer strafbaar wegens computervredebreuk (art. 138ab Sr).

Symantec, een bedrijf dat zich wereldwijd bezig houdt met bescherming, opslag en beheer van online data en systemen, publiceert jaarlijks het *Internet security threat report*, gebaseerd op gegevens afkomstig van cliënten afkomstig uit tweehonderd landen, het zogeheten *Global Intelligence Network* . Uit het rapport gepubliceerd in mei 2012 komt naar voren dat Symantec in 2011 meer dan 5,5 miljard kwaadaardige aanvallen blokkeerde – een stijging van 81 procent ten opzicht van 2010 – en dat 38 procent van de cliënten van Symantec malware heeft aangetroffen op computers en databestanden. Daarnaast steeg het aantal unieke malware-varianten naar 403 miljoen (een stijging van 41 % ten opzicht van 2010) (Symanctec Coorporation, 2012). McAfee ontdekte in 2011 eveneens een groot aantal nieuwe malware-varianten (McAfee Labs, 2011). De toename van malware-varianten wordt verklaard door het toegenomen gebruik van zogeheten '*polymorphic malware variants*': '*this technique enables attackers to generate an almost unique version of their malware for each potential victim*' (Symantec Coorporation, p. 35). De British Computer Society geeft aan dat er geen officiële statistieken bestaan aangaande de verspreiding van malware in Groot-Brittannië; zij geven aan dat het percentage geïnfecteerde computers tussen de vijf en vijftien procent zal liggen (House of Commons Science and Technology Comittee, 2012). Uit een Australisch onderzoek onder duizend volwassenen internetgebruikers kwam naar voren dat 23 procent van de ondervraagden malware op hun computer heeft aangetroffen (AusCERT, 2008). In het *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010* wordt gemeld dat naar schatting 0,5 tot 5 procent van alle aan het internet verbonden computers is geïnfecteerd met malware die het mogelijk koppelt aan een botnet (Govcert.nl, 2010).

Er zijn echter aanwijzingen dat er sprake is van een overrapportage van de omvang van verspreide malware (Anderson, Barton, Böhme, Clayton, Van Eeten, Levi, Moore, e.a., 2012; Fafinski, 2010). De data over de verspreiding van malware zijn immers vaak afkomstig van bedrijven die een belang hebben bij de verkoop van beveiligingssoftware (Newman & Clarke, 2003; Wall, 2007). Daarnaast zijn de data van deze onderzoeken verkregen uit niet-representatieve steekproeven (Ryan & Jefferson, 2003). De onderzoeken van of in opdracht van deze bedrijven zijn echter wel van belang voor het verkrijgen van inzicht in

veranderingen in de *modus operandi* van cybercriminelen en eindgebruikers (Newman & Clarke, 2003;Wall, 2008).

Hacken

In de beginjaren van het internet had het begrip 'hacking' nog een positieve lading. Zo beweert Sterling (1992) dat '*hacking can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems. Hacking can describe the determination to make access to computers and information as free and open as possible*' (p. 53). Het zijn de hackers die internet en de personal computers hebben ontwikkeld en Chandler (1996) suggereert zelfs dat '*the personal computer would never have existed without the computer hacker*' (p. 229). Het begrip 'hacker' heeft tegenwoordig een negatieve connotatie: computercrimineel and elektronische vandaal (Chandler, 1996), een bedreiging voor de nationale veiligheid en een dief van intellectueel eigendom (Halbert, 1997). Hacken wordt nu algemeen beschouwd als het zich zonder toestemming toegang verschaffen tot computers en computernetwerken. Hieronder valt ook '*guessing, randomly generating or stealing a password*' (Jordan & Taylor, 1998, p. 759). Hacken wordt gezien als een bedreiging voor de veiligheid op internet, maar Skibell (2002) stelt dat slechts weinig hackers over voldoende vaardigheden beschikken om daadwerkelijk gevaarlijk te zijn. Aan de andere kant is het relatief eenvoudig om informatie te verwerven over de praktijk van hacken door deel te nemen aan internetfora. Uit een kwalitatief onderzoek naar internetfora en de draden[14] (*threads)* op deze fora kwam naar vormen dat op deze fora hacking software wordt aangeboden en verkocht, informatie wordt gedeeld en hulp wordt geboden bij het hacken (Chu, e.a., 2010).

In 1993 is computervredebreuk, oftewel hacken, in Nederland strafbaar gesteld, mits daarbij de beveiliging van de computer is doorbroken of toegang is verschaft door slinkse of technische ingrepen. In 2006 heeft de wetgever de beveiligingseis in art. 138a Sr laten vallen (Koops, 2012). Wanneer een hacker opzettelijk of door schuld een geautomatiseerd werk vernielt, kan er sprake zijn van het in gevaar brengen van de algemene veiligheid strafbaar gesteld in de artikelen 161sexties en 161septies Sr. In de artikelen 139d en 139e Sr zijn de voorbereidingshandelingen voor hacken strafbaar gesteld (Leukfeldt, e.a., 2010). Hacken is in veel gevallen geen op zichzelf staand misdrijf, maar houdt onder andere verband met internetfraude en bedreiging. Technieken die worden gebruikt voor hacken zijn onder meer:

[14] Een draad is een verzameling van reacties op een bepaald onderwerp binnen een internetforum meestal in chronologische volgorde en vaak voorzien van een titel.

defacing[15] en *phishing*[16]. Er zijn algemene *phishing*aanvallen gericht op duizenden potentiële slachtoffers en er zijn doelgerichte campagnes gericht op specifieke slachtoffers. Tot de laatste groep behoort het zogeheten *spear phishing* (EECFT, 2011).

In de literatuur is weinig bekend over de omvang van hacken en ook cijfers over de technieken die hackers gebruiken zijn schaars. Een van de redenen hiervoor is dat softwarefabrikanten die weliswaar onderzoek doen naar cybercrime en de effectiviteit van hun producten juist geen anti-*phishing* software voorhanden hebben. *Phishing* is namelijk een techniek die misbruik maakt van het vertrouwen van gebruikers (Bradley, 2010). Daarnaast is hacken vaak geen doel op zich, maar een middel om andere vormen van cybercrime te plegen (Leukfeldt, e.a., 2010). Het softwarebedrijf Symantec meldt dat in 2011 de persoonlijke gegevens van meer dan 187,2 miljoen personen als gevolg van hacken op straat kwamen te liggen. De hoofdoorzaak van verlies van persoonlijke data was in 2011 echter nog steeds diefstal of verlies van een computer of een andere gegevensdrager. In 2011 zijn de *phishing* activiteiten wereldwijd toegenomen: 0,33 procent of 1 op de 298 e-mails in 2011 ten opzichte van 0,23 procent of 1 op de 442 e-mails in 2010 (Symantec Coorporation, 2012). Sinds begin 2010 neemt – na een eerdere daling – het aantal waargenomen *phishing*aanvallen in Nederland weer toe: GOVCERT.NL heeft in het tweede kwartaal een grote stijging in het aantal *Notice and Takedown* verzoeken[17] gehad (Govcert.nl, 2010). De meeste *phishing*sites worden gehost in de Verenigde Staten (48,5 %) (Symantec, 2012). Nederland staat regelmatig in de top 10 van landen die deze sites hosten: tussen de een en vijf procent van de *phishing*sites (AWPG, 2009). Uit statistieken blijkt dat financiële instituten, social media sites en gaming sites het meest te maken hebben met *phishing*. Uit het *Global Phishing Survey* komt naar voren dat in 2011 vooral in China het aantal *phishing*aanvallen fors is toegenomen (AWPG, 2012).

2.3.2 Financiële delicten

Volgens Leukfeldt e.a. (2010) is de essentie van fraude: 'mensen eigenen zich door middel van bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan'(p 73). Voor fraude op internet zijn diverse benamingen in omloop, zoals internetfraude (Van der Hulst & Neve, 2008), fraude in e-commerce (Stol & Van Treeck, 2001) en e-fraude (Leukfeldt, e.a., 2010). Voor fraude op internet geldt dat ICT

[15] *Defacing* is '[h]et zonder toestemming veranderen, vervangen of vernielen van een website' (Van Geest, 2006, p. 35).
[16] Supra 5, noot 2.
[17] *Notice and Takedown* verzoeken zijn verzoeken om websites die worden gebruikt voor bijvoorbeeld *phishing* uit de lucht te halen.

van wezenlijk belang is bij de uitvoering de definitie van fraude (Leukfeldt & Stol, 2011). Fraude op internet kent verschillende verschijningsvormen. Voor dit onderzoek zijn fraude via veiling- en verkoopsites, identiteitsfraude en voorschotfraude relevant.

Fraude via veiling- en verkoopsites

Online veilingsites behoren tot de meest succesvolle nieuwe ondernemersformules van de huidige kenniseconomie (Kambil & Heck, 2002). Het aantal klanten van eBay, een van de grootste veilinghuizen te wereld, is de afgelopen jaren exponentieel toegenomen, evenals het aantal verkochte producten (eBay Inc, 2010). De grootste veilingsite in Nederland is Marktplaats.nl. Ter illustratie, op de website van Marktplaats stonden in juni 2011 6,5 miljoen advertenties online en werden dagelijks 268.000 nieuwe advertenties geplaatst. Deze advertenties werden dagelijks door meer dan 1,8 miljoen mensen bekeken.[18] In Nederland is het aantal e-shoppers[19] in 2009 sterk gegroeid tot 8,8 miljoen personen. In de Europese Unie is online winkelen het meest ingeburgerd in Nederland, Denemarken en het Verenigd Koninkrijk (CBS, 2009). Van fraude via veiling- en verkoopsites (*online auction fraud*) is sprake wanneer een koper (een deel van) de afgesproken prijs betaalt en de verkoper de dienst of het goed niet levert of wanneer de verkoper de dienst of het goed levert en de koper (een deel van) de afgesproken prijs niet betaalt (Leukfeldt & Stol, 2011; Taylor, e.a., 2006; Van der Hulst & Neve, 2008).

In het Nederlandse Wetboek van Strafrecht komt de term 'fraude' niet voor. Wanneer op slinkse wijze producten of geld afhandig worden gemaakt, is er sprake van oplichting en dit is strafbaar volgens artikel 326 Sr. Wanneer iemand er een gewoonte van maakt goederen te kopen en vervolgens niet te betalen heet dit flessentrekkerij (artikel 326a Sr). Wanneer zonder opzet goederen niet betaald of geleverd worden is er sprake van wanprestatie, een tekortkoming in de nakoming van een overeenkomst (art. 6:74 BW). Wanprestatie is geen delict.

Het *Internet Crime Report 2008* van het *Internet Crime Complaint Center*[20] wijst uit dat er in 2008 in de Verenigde Staten ruim 275.000 klachten zijn ingediend waarvan bijna 26 procent betrekking had op fraude via veiling- of verkoopsites. Deze vorm van fraude stond daarmee op de tweede plaats in de klachten top-10 van cybercrimes (Internet Crime Complaint Center, 2009). In het rapport uit 2010 wordt geconstateerd dat het aantal klachten

[18] Zie: http://statisch.marktplaats.nl/html/about_us.html. Laatst geraadpleegd op 29 augustus 2012.
[19] E-shoppers zijn personen die online goederen of diensten kopen, bestellen of boeken (CBS, 2009, p. 150).
[20] Het *Internet Crime Complaint Center* is een samenwerkingsverband tussen het *Federal Bureau of Investigation* (FBI) en het *National White Collar Crime Center* (NW3C).

over fraude via veiling- of verkoopsites sinds 2004 dalende is: in 2004 ging het nog om 71,2 procent en in 2010 was dit nog maar iets meer dan tien procent. In de klachten top-10 van cybercrimes daalde fraude via veiling- of verloopsites naar de derde plaats. In het rapport wordt geen verklaring gegevens voor deze daling (Internet Crime Complaint Center, 2011). De officieel geregistreerde klachten waarop de rapporten van het *Internet Complaint Center* zijn gebaseerd dekken niet de totale hoeveelheid incidenten van fraude via veiling- of verkoopsites en daarnaast is niet beoordeeld of de klachten terecht waren. Uit een onderzoek onder Nederlandse jongeren in de leeftijd tien tot achttien jaar kwam naar voren dat 3,9 procent wel eens voor een product heeft betaald, maar dit product nooit heeft ontvangen. De top-drie van productgroepen is: spelcomputers (41,3%), kleding/schoenen/sieraden (32,4%) en games/spelletjes (29,6%). Van de jongeren die wel eens een product aan een koper heeft opgestuurd, heeft 2 procent het geld vervolgens niet gekregen. De top-drie van productgroepen is nu: kleding/schoenen/sieraden (39,2%), games/spelletjes (28,4%) en cd's/dvd's/boeken (19,6%) (Jansen, 2012).

Identiteitsfraude

Identiteitsfraude kan worden gedefinieerd als 'het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan' (De Vries, Tigchelaar, Van der Linden, & Hol, 2007, p. 228). Identiteitsfraude kent twee stappen. De eerste stap bestaat uit het in handen krijgen van persoonsinformatie, oftewel identiteitsdiefstal. Het is echter ook mogelijk om een fictieve identiteit te creëren of om met toestemming van een persoon diens identiteit overnemen. De tweede stap is het gebruiken van de gestolen persoonsinformatie voor financieel gewin (Van Wilsem, 2012). Technieken om persoonsinformatie in handen te krijgen zijn onder meer *skimmen*[21] en het gebruik van *spyware*[22].

Identiteitsdiefstal is in Nederland niet strafbaar. Dit komt omdat een identiteit juridisch gezien niet kwalificeerbaar is als een goed in de zin van art. 310 Sr (diefstal), art. 321 Sr (verduistering) of art. 416 Sr (heling). Daarnaast is in Nederland het gebruik (misbruik) van de identiteit(sgegevens) van een andere persoon geen zelfstandig strafbaar feit. De feiten kunnen wel vallen onder de delicten valsheid in geschrift (art. 225 Sr) en oplichting (326 Sr).

[21] Skimmen kan worden omschreven als '*an organized activity where data is surreptitiously read from credit cards and used to make counterfeit cards*'(Sproule & Archer, 2006, p. 20).
[22] Supra 22, noot 13.

Er zijn twee bronnen beschikbaar over identiteitsfraude: registraties van officiële klachten en gegevens uit slachtofferenquêtes. Uit gegevens van de *Federal Trade Commission* blijkt dat in 2010 de meest klachten van Amerikaanse consumenten over fraude gaan over identiteitsfraude (19 %) (Federal Trade Commission, 2011). Gegevens van het *Internet Crime Complaint Center* geven aan dat er in 2010 300.000 klachten binnengekomen zijn waarbij het in tien procent van de gevallen om identiteitsfraude ging (Internet Crime Complaint Center, 2011). In Nederland zijn in 2009 241 fraudemeldingen binnengekomen bij het Centraal Meldpunt Identiteitsfraude (CMI, 2010). Volgens een survey van *Javelin Strategy & Research* is identiteitsfraude in 2011 toegenomen met 13 procent en in totaal werden 11,6 miljoen volwassen Amerikanen slachtoffer van deze vorm van fraude. Slachtofferschap van identiteitsfraude wordt in verband gebracht met het gedrag van consumenten op sociale media en het gebruik van de mobiele telefoon (Javelin Strategy & Research, 2012). Uit een onderzoek gehouden in opdracht *Federal Office of the Privacy Commissioner* in Australië komt naar voren dat negen procent van de respondenten zegt slachtoffer te zijn geworden van identiteitsdiefstal, 17 procent van hen geeft aan iemand te kennen die slachtoffer is geworden van identiteitsdiefstal en 60 procent geeft aan bezorgd te zijn slachtoffer te worden van deze vorm van cybercrime (Wallis Consulting, 2007). Het Amerikaanse *National Crime Victimization Survey* (N=56.840) geeft aan dat naar schatting vijf procent van de burgers van 16 jaar en ouder in een periode van twee jaar slachtoffer is geweest van identiteitsfraude (Langton & Planty, 2010). Op basis van gegevens van het LISS-panel[23] uit 2010 wordt geschat dat in Nederland 3,7 procent van de bevolking de afgelopen twee jaar heeft meegemaakt dat er ten onrechte geld is afgeschreven van een bankrekening (Van Wilsem, 2011).

Voorschotfraude

Bij voorschotfraude (*advance fee fraud*[24]) wordt het internet gebruikt om op oneigenlijke wijze geld, goederen en diensten te verwerven zonder hiervoor te betalen of een tegenprestaties te leveren (Morris, 2004). De essentie van voorschotfraude is '*to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return form providing some modest payment in advance*' (Smith,

[23] LISS staat voor Langlopende Internet Studies voor de Sociale wetenschappen. Dit is een grootschalige, longitudinale online survey, opgezet door het Tilburgse bureau CentERdata.

[24] Er wordt ook wel gesproken over 419-oplichting (naar het betreffende artikel in het Nigeriaanse wetboek van strafrecht) of Nigeriaanse oplichting: '*the e-mails often come from individuals who claim to reside in a foreign country such as Nigeria or other African nations*' (Holt & Graves, 2007, p. 137).

Holmes, Kaufmann, 1999, p. 1). Dion (2010) onderscheidt zes categorieën van voorschotfraude: *lottery scams, humanitarian gifts, abandoned money, business opportunities, deceased estate/last will, gold bars and diamonds* (p. 633). Criminelen die zich bezighouden met voorschotfraude zijn goed georganiseerd en hebben een uitgebreid crimineel netwerk (Tanfa, 2006). Voorschotfraude is daarnaast steeds meer een transnationaal verschijnsel. De leden van de groep criminelen die zich hiermee bezig houdt leven en opereren in verschillende landen. De afzender van de e-mails kan bijvoorbeeld woonachtig zijn in Italië, terwijl de intermediair in Hong Kong woont en degene die uiteindelijk het geld binnenhaalt een Nederlander is met een huis in België (Dion). Uit een onderzoek naar spam mail kwam naar voren dat het vaak onmogelijk is om te achterhalen uit welk land een spam mail – en dus ook een e-mail om personen te verleiden om een voorschot te verstrekken – oorspronkelijk is verstuurd (Ahmed & Oppenheim, 2006). In Nederland is voorschotfraude strafbaar op grond van artikel 326 Sr.

Over de omvang van voorschotfraude is nog nauwelijks iets bekend. Het Canadese *Anti-Fraud Centre* meldt dat het 167 klachten heeft ontvangen over voorschotfraude in de periode januari tot en met september 2004 (Chawki, 2009). In 2010 had 4,1 procent van de klachten ingediend bij het *Internet Crime Complaint Center* in de Verenigde Staten betrekking op voorschotfraude (Internet Crime Complaint Center, 2011). Uit het Nationaal Dreigingbeeld 2008 komt naar voren dat er in de periode tussen 1 oktober en 1 november in totaal 175 meldingen over voorschotfraude zijn binnengekomen. Naar aanleiding van deze meldingen is nader onderzoek verricht: 2.536 personen, voornamelijk afkomstig uit de Verenigde Staten, Italië, Groot-Brittannië en Duitsland, konden als slachtoffer van voorschotfraude worden aangemerkt. Oplichterbendes in Nederland blijken meestal slachtoffers te maken in het buitenland, terwijl Nederlandse burgers eerder slachtoffer worden van bendes uit het buitenland. Het aantal Nederlandse slachtoffers van voorschotfraude is niet bekend (Boerman, Grapendaal, & Mooij, 2008). De slachtoffers van voorschotfraude doen niet snel aangifte van dit delict. Hiervoor is een aantal redenen te noemen. Ten eerste weet een buitenlands slachtoffer vaak niet waar hij of zij aangifte moet doen en andersom weet een Nederlands slachtoffer niet waar hij of zij in het buitenland aangifte moet. Daar komt bij dat de kennis om een dergelijke aangifte goed af te handelen bij de plaatselijke politie vaak niet aanwezig is. Ook voelen slachtoffers zich vaak schuldig en schamen zij zich. Er is dus sprake van een *dark number*: de totale omvang van slachtofferschap en de geleden schade kan onvoldoende inzichtelijk worden gemaakt (Schoenmakers, De Vries Robbé, & Van Wijk, 2009). De hoeveelheid e-mails en de diversiteit van de e-mails bedoeld om de lezer geld

afhandig te maken suggereert dat criminelen voorschotfraude als een lucratieve bezigheid beschouwen (Anderson, e.a., 2012).

2.3.3 Delicten in de persoonlijke sfeer

De delicten in de persoonlijke sfeer – stalking, bedreiging, smaad, laster en belediging – kunnen zowel op conventionele als op digitale wijze worden gepleegd. Er kan ook sprake zijn van een mix: de dader belaagt het slachtoffer zowel op internet als in de echte wereld of de dader gebruikt online gevonden informatie om het slachtoffer offline te kunnen traceren (zie Jaishankar, Shariff, & Ramdoss, 2008). Het is de vraag in hoeverre de komst van internet heeft geleid tot een nieuwe groep slachtoffers van deze delicten of dat uiteindelijk nog steeds dezelfde groep mensen getroffen wordt (Grabovsky, 2001).

Stalking

Bocij(2004) definieert cyberstalking als '[*a*] *group of behaviors in which an individual, group of individuals, or organization uses information and communications technology to harass another individual, group of individuals, or organization. Such behaviors may include, but are not limited to, the transmission of threats and false accusations, identity theft, data theft, damage to data or equipment, computer monitoring, solicitation of minors for sexual purposes, and any form of aggression*' (p. 14). In de literatuur over cyberstalking worden de begrippen *harassment* (intimidatie) en stalking door elkaar gebruikt. Harvey (2003) stelt echter dat het bij stalken gaat om het (achter)volgen van het slachtoffer en het opzettelijk angst aanjagen door een vaak anonieme dader, terwijl *harassment* minder ernstig is en door het slachtoffer eerder wordt beschouwd als hinderlijk. *Harassment* kan echter ontaarden in stalking en stalking kan uitmonden in gewelddadig gedrag (Ashcroft, 2001). Daarnaast is er een duidelijk verband gevonden tussen (cyber)stalking, seksuele uitbuiting en seksuele intimidatie (Duntley & Buss, 2012). Philips en Morrissey (2004) hebben het seksuele aspect van cyberstalking onderzocht en zij stellen dat '*sex can be a very efficient weapon to make victems feel distressed, vulnerable and threatened*' (p.67). Bij slachtofferschap van stalking en strategieën om stalking tegen te gaan zijn genderverschillen relevant (Duntley & Buss).
De cyberstalker maakt onder andere gebruik van e-mail, instant messager en chat rooms (Baum, Catalano, Rand, & Rose, 2009).

In de Verenigde Staten is stalking begin jaren negentig van de vorige eeuw strafbaar gesteld na de moord op de actrice Rebecca Schaeffer. Cyberstalking wordt vaak subsidiair opgenomen in de aanklacht (Bocij, 2004). In Australië en Nieuw-Zeeland is (cyber)stalking

eveneens strafbaar gesteld in de jaren negentig en daarnaast zijn sommige vormen van (cyber)stalking in Nieuw-Zeeland mogelijk strafbaar op grond van de *Domestic Violence Act* uit 1995 (Philips & Morrissey, 2004). Nederland is stalking – ook wel belaging genoemd – sinds juni 2000 strafbaar op grond van art. 285b Sr. Afhankelijk van de situatie kan stalking ook worden gezien als een vorm van bedreiging (art. 285 Sr).

Hoewel cyberstalking in de belangstelling staat bij onderzoekers (zie Parsons-Pollard, & Moriarty, 2008; Reyns, 2010) en bij de overheid (zie Ashcroft, 2001; Reno, 1999), is er tot nu toe weinig empirisch onderzoek verricht naar deze vorm van cybercrime. Daarnaast wordt er in onderzoek vaak geen onderscheid gemaakt tussen conventioneel stalken en cyberstalken (Parsons-Pollard & Moriarty). Op basis van het aanwezige onderzoek wordt verondersteld dat een aanzienlijk aantal personen op enig moment in zijn of haar leven slachtoffer wordt van een of meer vormen van cyberstalking (Alexy, Burgess, Baker, & Smoyak, 2005; Baum, e.a., 2009; D'Ovidio & Doyle, 2003; Sheridan & Grant, 2007; Spitzberg & Hoobler, 2002a). Uit stalking supplement van de *National Crime Victimization Study* uit 2008 in de Verenigde Staten komt bijvoorbeeld naar voren dat 26 procent van de respondenten zegt een bepaalde vorm van cyberstalking te hebben meegemaakt (Baum, e.a.). In Nederland is het aantal vervolgingen voor stalking toegenomen: in 2001 zijn 389 verdachten vervolgd en in 2003 waren dit 882 verdachten.[25] In 2004 had 3,3 procent van de geregistreerde incidenten over huiselijk geweld betrekking op stalking (Ferwerda, 2004). Uit een onderzoek gebaseerd op vragenlijsten verspreid in juli 2007 aan bezoekers van de Tilburgse kermis kwam naar voren dat van de 1027 respondenten 16,5 procent ooit te maken heeft gehad met stalking. Vrouwen waren significant vaker slachtoffer (20,7 % ten opzichte van 13,4 %) (Van der Aa & Kunst, 2009). Er zijn geen gegevens over de omvang van *cyber*stalking in Nederland.

Bedreiging

Bedreiging kent vele vormen en er bestaat geen internationaal geaccepteerde definitie van bedreiging. Bedreiging via internet wordt in internationale strafrechtelijke bepalingen vaak opgevat het een vorm van misbruik van telecommunicatiediensten. Een voorbeeld is art. 474.17 van de *Criminal Code Act* in Australië. Daarnaast houdt bedreiging vaak verband met de delicten stalking en (seksuele) intimidatie en is het onderscheid tussen deze delicten in de praktijk vaak lastig (Butler, Kift, & Campbell, 2010). Bij bedreiging gaat het om het intentioneel en doelbewust angst veroorzaken bij een persoon. Deze angst moet dan wel verband houden met fysiek geweld of vernieling van eigendom. Angst voor bijvoorbeeld

[25] Zie Openbaar Ministerie: www. om.nl.

reputatieschade valt niet onder bedreiging. Bedreiging wordt meestal onderzocht als onderdeel van ander deviant gedrag, bijvoorbeeld cyberpesten (zie Hinduja & Patchin, 2008), huiselijke geweld (zie Ferwerda, 2004) en cyberstalking (zie Spitzberg, 2002b). Buiten Nederland is er geen onderzoek gedaan naar bedreiging als een zelfstandig delict.

In Nederland is bedreiging strafbaar op grond van artikel 285 Sr. De bedreiging moet dan te maken hebben onder meer verkrachting, moord of mishandeling. Uit een Nederlands onderzoek gebaseerd op data van het LISS-panel[26] uit 2008 komt naar voren dat circa vijf procent van de respondenten te maken heeft gehad met conventionele bedreiging, 0,8 procent met digitale bedreiging en 1,2 procent met zowel conventionele als digitale bedreiging (Van Wilsem, 2010).

Smaad, laster en belediging

Wanneer de eer of goede naam van een persoon wordt aangetast, kan sprake zijn van de strafbare uitingen smaad, laster of belediging. Op internet gaat het om schriftelijke uitingen op sociale netwerk sites, mailinglijsten, blogs, of websites. Smaad (art. 261 Sr) is een specifieke uiting met als doel iemands goede naam aan te tasten. Smaadschrift is smaad door het publiceren van tekst en/of (bewerkte) afbeeldingen. De straf voor smaadschrift is hoger (art. 261 lid 2 Sr). Een verdediging tegen smaad is dat het verweten feit waar is èn dat het in het algemeen belang is om dit feit via internet te verspreiden (art. 261 lid 3 Sr). Wanneer een via internet verspreide uiting niet waar is, wordt dit laster (art. 162 Sr) genoemd. Een belediging (266 Sr) is een algemene negatieve uitspraak over een persoon. Iemand belachelijk maken in een satire of een parodie mag vaak wel. In de praktijk is de grens tussen smaad, laster en belediging lastig aan te geven. Op internet zijn uitingen van smaad of laster en beledigingen eindeloos reproduceerbaar en in de praktijk is het onmogelijk om deze definitief te laten verwijderen. Smaad, laster en belediging worden gerelateerd aan cyberstalking, intimidatie en cyberbullying (zie Butler, Kift, & Campbell, 2009). Er zijn geen gegevens bekend over de prevalentie van slachtofferschap van smaadschrift, laster en belediging op internet.

2.4 Conclusies literatuur

Er is nog nauwelijks onderzoek verricht naar slachtofferschap van cybercrime. Uit het literatuuronderzoek komt naar voren dat bestaand onderzoek overwegend tot doel heeft de prevalentie van slachtofferschap van cybercrime in kaart te brengen. Bestaand onderzoek richt

[26] Supra 28 noot 23.

zich òf op cybercrimes gericht tegen computers en computernetwerken, òf op cybercrimes in de financiële sfeer òf op cybercrimes in de persoonlijke sfeer. Er is geen representatief longitudinaal onderzoek dat een overall beeld geeft van de omvang van slachtofferschap van cybercrime. Bestaand onderzoek verschilt onderling sterk qua omvang en samenstelling van steekproeven, de gehanteerde onderzoekmethoden en de wijze waarop cybercrime en de onderscheiden vormen van cybercrime zijn gedefinieerd en geoperationaliseerd. Gezien de genoemde verschillen in onderzoek kunnen de resultaten uit onderzoek niet worden vergeleken. Hoogstens – en dan met de nodige terughoudendheid – kan er gesproken worden van bepaalde trends. Wat wel duidelijk is, is dat een niet onaanzienlijk deel van de (Nederlandse) internetgebruikers slachtoffer wordt van cybercrime. Hierbij gaat het zowel om cybercrimes gericht tegen computers en computernetwerken als om traditionele criminaliteit die ook of zelfs geheel in een digitale vorm voorkomt.

Gezien de prevalentie van cybercrime, is representatief longitudinaal onderzoek naar slachtofferschap van cybercrime in Nederland noodzakelijk. Om prioriteiten aan te kunnen brengen in de opsporing, is inzicht nodig in de ernst van de problematiek: welke cybercrimes komen vaak voor en wat zijn de materiële en immateriële gevolgen van slachtofferschap? Daarnaast is inzicht in de modus operandi van de dader behulpzaam bij het inrichten van de aanpak van daders. Behalve cijfers over de omvang en gevolgen van van slachtofferschap cybercrime, is ook inzicht nodig in het profiel van de slachtoffers van elke cybercrime. Wanneer meer bekend is over wie slachtoffer worden van cybercrime, kunnen meer gerichte preventiestrategieën uitgedacht worden. Als derde moet een begin gemaakt worden met het ontwikkelen van theorieën die slachtofferschap van cybercrime verklaren. Hierbij kan uitgegaan worden van bestaande criminologische theorieën, die wellicht door de specifieke kenmerken van internet aangepast moeten worden.

Deze scriptie gaat uitsluitend over de omvang van slachtofferschap cybercrime en bevat enkele beschrijvende statistieken over de gevolgen van slachtofferschap van elke afzonderlijke cybercrime. In de discussie, hoofdstuk 11, wordt ingegaan op de bruikbaarheid van de data die voor dit onderzoek zijn verzameld voor onderzoek naar risicoprofielen en criminologische theorieën.

3 Methode

3.1 Inleiding

In dit hoofdstuk wordt de totstandkoming van de vragenlijst en de dataverzameling voor het slachtofferonderzoek cybercrime verantwoord. Het onderzoek werd aangestuurd door een stuurgroep, bestaande uit een accountmanager van het Programma Aanpak Cybercrime (PAC) en het afdelingshoofd Beleid & Strategie van het Korps Landelijke Politiediensten (KLPD). Tijdens de uitvoering is inhoudelijke ondersteuning geboden door een klankbordgroep bestaande uit medewerkers van het Centraal Bureau voor de Statistiek (CBS), regiopolitie Amsterdam-Amstelland, de noordelijke drie politieregio's, de zuidelijke zes politieregio's, het toenmalige ministerie van Justitie, het ministerie van Binnenlandse Zaken en Koninkrijkrelaties, bureau Intervict, het PAC, het KLPD en de universiteit Tilburg (voorzitter). Het onderzoek is gestart in september 2009 en de dataverzameling is afgerond in juli 2011.

3.2 Design

Om slachtofferschap te meten is het bestuderen van registraties van de politie niet afdoende, immers niet iedereen maakt melding of doet aangifte van slachtofferschap. Uit de Integrale Veiligheidsmonitor (IVM) 2010 van het CBS blijkt dat van offline criminaliteit gemiddeld 35% een melding maakt en 25% aangifte doet. De aangiftebereidheid loopt daarbij sterk uiteen per delict; 5% doet aangifte van seksuele delicten en 80% van inbraak (CBS, 2010). Wat de meldings- en aangiftebereidheid van cybercrime is, weten we niet. Om de werkelijke omvang van slachtofferschap en de aangiftebereidheid van cybercrime te meten moest een onderzoek onder een steekproef van Nederlanders uitgevoerd worden.

Van oudsher werd bevolkingsonderzoek schriftelijk, telefonisch en face-to-face uitgevoerd. Tegenwoordig worden voor veel onderzoek (ook) via internet gegevens verzameld. Er is nog veel discussie gaande tussen onderzoekers over de foutenbronnen die van invloed zijn op de kwaliteit van de uitkomsten van slachtofferenquêtes (zie voor een volledig overzicht Bethlehem, 1999). Volgens Bethlehem (2006) is met name *onderdekking* een groot probleem bij online enquêtes. Mensen die geen internetverbinding hebben kunnen immers niet meedoen met onderzoeken die geheel online worden uitgevoerd. Verder kunnen volgens Bethlehem trekkingsfouten door zelfselectie worden veroorzaakt doordat bij veel online enquêtes de respondenten niet door de onderzoeker worden benaderd, maar participeren via een oproep op internet. De onderzoeker heeft hierdoor weinig invloed op de

representativiteit van de steekproef. Ten slotte zou de non-respons, een probleem dat geldt bij alle onderzoeksmethoden, bij online enquêtes groter kunnen zijn door technische problemen, trage modems en verouderde browsers die de online enquête niet goed kunnen weergeven.

Problemen met trekkingsfouten door zelfselectie is in dit onderzoek ondervangen door de vragenlijst niet geheel digitaal af te nemen. Respondenten zijn a-select uit de Gemeentelijke Basis Administratie (GBA) geselecteerd en hebben per post een uitnodiging ontvangen om een online vragenlijst in te vullen. Er was hier dus geen sprake van zelfselectie. Door respondenten met een uitnodigingsbrief te benaderen, zijn problemen met de onderdekking verkleind. Ook mensen die geen internetverbinding hebben, zijn op deze manier benaderd. Mensen die geen internet gebruiken zijn verzocht toch de vragenlijst over slachtofferschap van cybercrime in te vullen omdat ook zij slachtoffer kunnen worden van cybercrime: hun identiteitsgegevens kunnen offline gestolen worden bij bijvoorbeeld een pinautomaat en online misbruikt worden door er aankopen mee te doen via internet. In de brief werd een telefoonnummer en e-mailadres van het onderzoeksteam genoemd waar mensen zich konden afmelden voor het onderzoek of een papieren vragenlijst op konden vragen. Op deze manier konden mensen zonder internetverbinding toch deelnemen en ontstond zicht op de reden van afmelding.

Voor dit onderzoek is een mix van oude en nieuwe methoden gebruikt; respondenten zijn met een brief benaderd met het verzoek een online vragenlijst in te vullen. De respondenten konden vervolgens de vragenlijst via een website invullen of telefonisch of via e-mail contact opnemen met het onderzoeksteam om zich af te melden voor het onderzoek of om een papieren vragenlijst aan te vragen. Mensen die niet respondeerden hebben een reminder per brief ontvangen, waarin meteen een aankondiging stond dat zij telefonisch zouden worden benaderd. Mensen konden wederom kiezen om de vragenlijst alsnog op internet in te vullen of te bellen of e-mailen. Van de mensen die ook op de reminder niet respondeerden, zijn de telefoonnummers opgezocht. Vervolgens zijn zij gebeld. Tijdens het telefoontje konden mensen kiezen om alsnog zelf de vragenlijst online invullen, een papieren versie te ontvangen, direct telefonisch de vragenlijst af te nemen of deelname te weigeren. Een dergelijke opzet waarin oude en nieuwe methoden worden gecombineerd, lag voor de hand. De IVM is in het najaar van 2008 voor de eerste keer op deze manier uitgevoerd en alle volgende metingen ook. Het CBS heeft het onderzoek parallel ook met de ‘oude methode’ uitgevoerd (CBS, 2008). Afname gebeurde daarbij enkel schriftelijk en mondeling. De verschillen in uitkomsten bleken statistisch significant. Hieruit blijkt weer eens dat geen

enkele methode waterdicht is. Het werkelijke slachtofferschap zal ergens rondom de resultaten van de oude en nieuwe methode liggen.

Expertinterviews

Op basis van een inventarisatie van voorkomende cybercrimes door het WODC (Sikkel, 2010) en de vragenlijst die gebruikt wordt voor de IVM is een topiclist ontwikkeld voor interviews. De interviews hadden twee belangrijke functies: kennisvergaring en behoeftepeiling. Tijdens de interviews is kennis opgedaan over cybercrime en over hoe in een slachtofferonderzoek naar slachtofferschap van cybercrime gevraagd kan worden. Ten tweede is de vraag beantwoord welke cybercrimes prioriteit hebben en welke aspecten van slachtofferschap relevant zijn volgens medewerkers van politie en justitie, zowel op beleids- als uitvoerend niveau. In totaal zijn 16 interviews gehouden met 23 ervaringsdeskundigen bij politie en justitie. De lijst van geïnterviewde personen is opgenomen in bijlage 1.

Politie 2.0

De website politie 2.0 is een 'community opgezet om kennis te delen over de politie, intelligence en het complexe ICT dossier'[27]. Mensen die beroepsmatig bezig zijn met veiligheid en ICT kunnen zich aanmelden voor dit forum en daar berichten of oproepen plaatsen. Er is een oproep geplaatst onder de naam 'wat mag niet ontbreken in een slachtofferonderzoek cybercrime'. Andere leden van het forum hebben hierop gereageerd.

Groepsinterviews

Om helder te krijgen hoe burgers het beste bevraagd kunnen worden naar slachtofferschap van cybercrime zijn twee groepsinterviews gehouden met in totaal 16 burgers. Deze mensen zijn geworven via het consumentenpanel vraaghetdevries.nl. Dit is een panel van ongeveer 1400 Friezen die zes keer per jaar geïnterviewd worden door eerstejaars studenten van instituut Economie en Management van NHL Hogeschool[28].

Interviews gedupeerden marktplaatsfraude

Marktplaats.nl heeft namen van 40 gedupeerden van marktplaatsfraude aangeleverd. Deze gedupeerden zijn telefonisch ondervraagd over hun slachtofferschap.

[27] http://criminaliteitswijzer.ning.com/
[28] http://www.nhl.nl/nhl/1209/kenniscentrum-vraaghetdevriesnl/pid5ae9b41a-abb3-43c2-954d-3668867ad481

3.3 Vragenlijst

Op basis van het rapport van het WODC (Sikkel, 2010), de expertinterviews, de groepsinterviews en de reacties op het forum politie 2.0 is een lijst opgesteld van cybercrimes en aspecten van slachtofferschap die volgens het werkveld de meeste aandacht verdienen. Deze lijst is voorgelegd aan de leden van de klankbordgroep, die in overleg met de onderzoekers de inhoud van de vragenlijst hebben vastgesteld.

De vragenlijst bestond uit:

a. persoonlijke achtergrondkenmerken;
b. beveiligingsniveau meest gebruikte computer thuis;
c. internetgedrag;
d. risicobewustzijn;
e. slachtofferschap (afgelopen 5 jaar en 12 maanden)
    - spam
    - malware
    - marktplaatsfraude
    - voorschotfraude
    - identiteitsfraude
    - stalking
    - smaad/laster
    - bedreiging
    - chantage/afpersing
    - hacking

Wanneer iemand slachtoffer was van één of meer delicten, zijn vragen gesteld over:

a. de modus operandi van de dader
b. internationale component;
c. relatie dader/slachtoffer;
d. reactie slachtoffer inclusief aangiftebereidheid en tevredenheid bij politieoptreden;
e. materiële schade.

De onderwerpen zijn vertaald naar een conceptvragenlijst. Deze vragenlijst is voorgelegd aan de klankbordgroep. Het commentaar is verwerkt en leidde tot een tweede concept. Binnen de klankbordgroep hebben de onderzoekers zich virtueel verenigd in een ‘methodenclub’. Het

tweede concept is besproken met de ‘methodenclub’. De laatste wijzigingen zijn doorgevoerd en de vragenlijst is digitaal gemaakt om te kunnen testen.

De vragenlijst is getest door: alle onderzoekers van het lectoraat cybersafety, familieleden en bekenden van de onderzoekers van lectoraat cybersafety, een aantal medewerkers van NHL Hogeschool, leden van de klankbordgroep, familieleden en bekenden van de leden van de klankbordgroep en enkele studenten. In totaal ongeveer 30 mensen.

Alle bruikbare opmerkingen die door de testers gemaakt zijn, zijn verwerkt. De laatste wijzigingen zijn doorgevoerd en de vragenlijst voor de testmeting is definitief vastgesteld.

3.4 Opzet testmeting

Nadat de vragenlijst is getest door onderzoekers en bekenden, is een grootschalige testmeting opgezet. Het doel van de testmeting was tweeledig. Ten eerste moest inzicht verkregen worden in de omvang en de representativiteit van de respons bij de gebruikte methodiek. Voor het onderzoek is een respons van 10.000 respondenten nagestreefd die op achtergrondkenmerken representatief zijn voor internetters vanaf 15 jaar. Het tweede doel van de test was het inhoudelijk verbeteren van de vragenlijst.

In dit hoofdstuk wordt eerst beschreven hoe de test is verlopen, daarna wordt ingegaan op de respons en representativiteit. Heel kort komt de omvang slachtofferschap in de testmeting aan bod. Na een beschrijving van reacties van respondenten zijn de bevindingen samengevat in conclusies over de methode en conclusies over de vragenlijst.

In de verslaglegging van de testmeting is een significantieniveau van 0.05 gehanteerd. Niet significante verschillen zijn hier en daar wel genoemd, omdat ze van belang geacht worden voor de interpretatie van de testresultaten.

Steekproef testmeting

Er zijn negen gemeenten aangeschreven met het verzoek om een steekproef te leveren ten behoeve van wetenschappelijk onderzoek. Volgens nationale wetgeving is een gemeente verplicht om een steekproef te leveren. Een gemeentelijke verordening om geen steekproeven te leveren is niet toegestaan.

Het CBS heeft de stedelijkheid van gemeenten op basis van omgevingsadressendichtheid opgedeeld in vijf niveaus: zeer sterk, sterk, matig, weinig en niet stedelijk. Op basis van contacten met gemeente Leeuwarden konden we rekenen op een steekproef uit deze gemeente. Gemeente Leeuwarden valt in de categorie ‘sterk stedelijk’. In de overige vier categorieën schreven we elk twee gemeenten aan, verspreid over Nederland.

Vijf van de acht aangeschreven gemeenten reageerden positief en zegden een steekproef toe. Eén gemeente weigerde 'op basis van slechte ervaringen in het verleden'; deze weigering was in strijd met de wetgeving. Twee gemeenten reageerden in het geheel niet. We kozen vier van de vijf gemeenten die positief reageerden, zodat we uit elke stedelijkheidscategorie burgers konden aanschrijven. De gemeenten die meededen aan het onderzoek waren: Leeuwarden, Soest, Zeevang, Hilvarenbeek en Beverwijk.

We ontvingen van drie gemeenten een aselecte steekproef van 500 inwoners en van twee gemeenten een aselecte steekproef van 499 inwoners tussen 15 en 70 jaar. De totale steekproefomvang bedroeg 2.498 burgers.

Digitale vragenlijst testmeting

De vragenlijst was bereikbaar tussen 6 oktober 2010 en 3 januari 2011 op www.cybercrime-onderzoek.nl. De vragenlijst was alleen bereikbaar met een inlogcode. Voor elke respondent is een inlogcode gemaakt die bestond uit een 5 of 6 cijfer-lettercombinatie. Wanneer een respondent de vragenlijst halverwege afbrak, kon deze op een later moment verder op de plaats waar het invullen was gestopt. Als de respondent op het einde van de vragenlijst op 'versturen' klikte, kon daarna niet meer ingelogd worden met de inlogcode. Er was geen voortgangsbalkje zichtbaar omdat de eerste helft van de vragenlijst veel langer duurde om in te vullen dan de tweede helft. Een voortgangsbalkje zou de respondent ontmoedigd hebben. Het online invullen van de vragenlijst duurde gemiddeld 20 minuten, inclusief een facultatief vragenblok over zelfcontrole en impulsiviteit dat door 70% van de respondenten werd ingevuld.

Lay-out testmeting

Aangezien het vaststellen van de omvang en representativiteit van de respons een voornaam doel van de test was, besloten we om de helft van de steekproef namens het KLPD en de helft namens NHL Hogeschool aan te schrijven. De brief in KLPD lay-out was inhoudelijk nagenoeg hetzelfde als de brief in NHL lay-out. De brief in KLPD lay-out was getekend door Timo Kansil, die in NHL lay-out door mijzelf.

Per gemeente zijn aselect 250 burgers geselecteerd die een brief met KLPD lay-out ontvingen, de rest ontving een brief met NHL lay-out. Een uitzondering hierop was gemeente Zeevang, een erg kleine gemeente met 4.500 mensen in de leeftijd 15 t/m 70 jaar, verspreid over ongeveer 2.000 huishoudens. Gemiddeld kreeg één op de vier huishoudens een brief en soms vielen meerdere personen in één huishouden in de steekproef. Aangezien we verwachtten dat het voor burgers verbazing en wantrouwen zou scheppen als het ene gezinslid

een brief met KLPD lay-out en het andere gezinslid een brief met NHL lay-out zou ontvangen, besloten we de inwoners van gemeente Zeevang per straat brieven met dezelfde lay-out te sturen.

Uitnodiging voor online vragenlijst

De uitnodigingsbrieven zijn op naam (voorletters en achternaam) bezorgd. In de brief werd de respondent uitgenodigd mee te doen aan het onderzoek door in te loggen op de website met de unieke code die in de brief stond vermeld. Er stond geen vergoeding tegenover. Na het inloggen op het inlogscherm met neutrale lay-out werd de respondent doorgestuurd naar een website die overeenstemde met de lay-out van de brief. Eerst werd een invulinstructie zichtbaar, daarna kon de vragenlijst ingevuld worden. Aan het einde van de vragenlijst werd gevraagd of de respondent nog een aantal extra vragen wilden invullen ten behoeve van een scriptie. Wanneer een respondent dat weigerde, werd de vragenlijst als 'geheel ingevuld' beschouwd. In de brief werd een e-mailadres en een telefoonnummer genoemd waarmee de respondent een papieren vragenlijst aan kon vragen of zich kon afmelden voor het onderzoek.

Na ruim twee weken werd een reminderbrief gestuurd aan de respondenten die niet hadden gereageerd. De lay-out was voor elke respondent hetzelfde als die van de uitnodigingsbrief. In de reminderbrief is aangekondigd dat de respondent gebeld zou worden indien niet op de reminder werd gereageerd. Ook naar aanleiding van de reminder kon de respondent telefonisch of per e-mail een papieren vragenlijst aanvragen of zich afmelden voor het onderzoek. Wederom tekende Timo Kansil of ikzelf, afhankelijk van de lay-out.

Nabellen

Het was de bedoeling alle respondenten die niet reageerden op de uitnodiging en de reminder telefonisch te benaderen. Aangezien de respons tegenviel en het budget voor nabellen vast stond, hebben we een steekproef van respondenten nagebeld. We schatten in dat we in de beschikbare 75 uren 800 telefoonnummers konden afhandelen. Eerst zochten we de telefoonnummers bij alle overgebleven adressen. Respondenten die in het 'bel me niet' register staan, mogen wel voor wetenschappelijk onderzoek benaderd worden. Burgers kunnen aangeven ook niet voor wetenschappelijk onderzoek benaderd te willen worden, maar slechts een enkeling heeft dit geregistreerd. We vonden van 76% van de adressen telefoonnummers die we mochten gebruiken. Uit de gevonden telefoonnummers trokken we een a-selecte steekproef van 400 respondenten per lay-out. Op een aantal adressen, vooral in Zeevang, werd hetzelfde nummer meerdere keren gevonden omdat er meerdere respondenten op hetzelfde adres woonden.

Het was de telefonisch enquêteurs bekend uit welke steekproef de telefoonnummers afkomstig waren. Zij belden met de welkomsttekst 'Dag meneer of mevrouw <naam>, ik ben <naam> van Breuker Telemarketing, ik bel u namens <KLPD of NHL Hogeschool>. Vervolgens werd de persoon die in het bestand genoemd werd aan de lijn gevraagd. Wanneer meerdere personen uit één huishouden in de steekproef zaten, werden meerdere personen ondervraagd. Elk nummer werd maximaal zes keer gebeld. Alle telefoonnummers zijn afgehandeld in 68,5 uur.

De respondent kon een keuze maken uit:
- zelf alsnog online invullen;
- een papieren vragenlijst aanvragen;
- telefonisch afnemen;
- weigeren.

Gezien de beperkte tijd, instrueerden we de enquêteurs optie 1 te stimuleren, dan optie 2 etc. Wanneer respondenten toezegden de vragenlijst alsnog zelf online in te vullen, konden zij een e-mailadres opgeven. In totaal gaven 141 van de 244 (57,8%) respondenten die toezegden de vragenlijst alsnog online in te vullen een e-mailadres. Geen enkel e-mailadres bleek ongeldig. Zij ontvingen van ons een e-mail met een link naar de vragenlijst en hun persoonlijke inlogcode. Na ongeveer drie weken stuurden we een reminder naar de respondenten die een e-mail hadden gekregen maar nog niet hadden gereageerd. Niemand koos ervoor de vragenlijst telefonisch af te nemen.

Papieren vragenlijsten
Om de respondenten niet af te schrikken met een dik pak papier, week de papieren vragenlijst op één punt af van de online vragenlijst: de vervolgvragen van slachtofferschap werden aan het einde van de vragenlijst één maal gevraagd in plaats van per vorm van slachtofferschap. De respondent kon aangeven van welke vorm van cybercrime hij de laatste keer slachtoffer was en de vragen voor die vorm beantwoorden.

3.5 Respons testmeting

Tabel 3.1 is een weergave van de respons van de 1249 respondenten die met de KLPD lay-out zijn benaderd. Aangezien we slechts een deel van de steekproef telefonisch hebben benaderd, is de totale respons van 28,7% lager dan we mogen verwachten als we de hele steekproef

zouden nabellen. In de rechter kolom is daarom een geëxtrapoleerd overzicht van de respons opgenomen.

Tabel 3.1 overzicht respons KLPD lay-out

Respons KLPD, werkelijk			*respons KLPD geëxtrapoleerd*
Online afname	**N**	**% van 1249**	
Adressen	1.249		1.249
Brieven onbezorgbaar	2	0,2%	2
Deelname eerste mailing	106	8,5%	106
Deelname tweede mailing	152	12,2%	152
Afgemeld telefonisch/mail	11	0,9%	11
Papieren vragenlijst aangevraagd	7	0,6%	7
Totaal afgewerkt	**278**	**22,3%**	278
Geen reactie op online enquête	**971**		971
Telefoonnummers opvragen			
Steekproef van adressen (van 971)	526		971
Telefoonnummers in steekproef	400	76,0%	738
Bereik nabellen	**N**	**% van 400**	
Incorrecte nummers	37	9,3%	68
6 keer niet bereikt	46	11,5%	85
Bereikt	317	79,3%	585
	400		738
Reactie nabellen	**N**	**% van 400**	
Medewerking geweigerd	131	32,8%	242
Toegezegd alsnog online te doen	131	32,8%	242
Telefonisch afgenomen	0	0,0%	0
Papieren vragenlijst aangevraagd	55	13,8%	101
	317	79,3%	585
Respons nabellen	**N**	**% van 400**	
Alsnog zelf online gedaan	68	17,0%	125
Papieren vragenlijsten geretourneerd	32	8,0%	59
	100	25,0%	184

Totale respons	**358**	**28,7%**	
Geëxtrapoleerde respons	**442**		**35,4%**

In de laatste kolom valt te lezen dat de respons op een mailing in KLPD lay-out bij volledig nabellen 35,4% zou zijn geweest. In bijlage 2 valt dezelfde berekening te zien voor de respons op de NHL lay-out. De werkelijk respons op de NHL lay-out bedraagt 175 (14,0%) wat

overeenkomt met een geëxtrapoleerde respons van 20,8%. De respons op de NHL lay-out is lager. In totaal (NHL en KLPD lay-out samen) hebben 533 respondenten de vragenlijst ingevuld wat een respons betekent van 21,3%.

Respons per methode

Om de respons per methode vast te kunnen stellen, moeten we uit gaan van de geëxtrapoleerde respons. In tabel 3.2 is de respons op de KLPD lay-out zien aan de hand van tabel 3.1. Hetzelfde overzicht kan voor de NHL lay-out gemaakt worden op basis van de tabel in bijlage 2.

Tabel 3.2 geëxtrapoleerde respons per methode

methode	**respons van 1249**	**respons% van 1249**
eerste brief	106	24,0%
tweede brief	152	34,4%
online nav nabellen	125	28,3%
respons papieren vragenlijsten	59	13,3%
Totaal	**442**	**100,0%**

Uit tabel 3.2 blijkt dat 58,4% van de respons online is binnengekomen, de rest is verzameld naar aanleiding van het nabellen. We weten niet hoeveel papieren vragenlijsten zijn binnen gekomen naar aanleiding van het bellen of de brief, aangezien alle lijsten tegelijk zijn verzonden en niet iedereen de unieke code op de papieren vragenlijst heeft geschreven. Er zijn echter maar 7 lijsten telefonisch of per e-mail aangevraagd naar aanleiding van de uitnodigingsbrieven.

Non-completes

Een aantal respondenten heeft de vragenlijst halverwege afgebroken. We hebben de vragenlijst als ‘complete’ behandeld, wanneer alle vragen die bij het slachtofferonderzoek horen, zijn beantwoord; dus tot de vraag ‘wilt u nog extra vragen invullen voor de scriptie?’

In totaal hebben 530 respondenten de website bezocht. Wanneer we die 530 respondenten op 100% zetten, blijkt dat 97,9 procent (519 respondenten) de vragenlijst hebben gestart en 91,5 procent (485 respondenten) de vragenlijst tot aan de facultatieve vragen hebben afgemaakt. Ook hier zien we verschil tussen respondenten die een KLPD-envelop (93,1%) en respondenten die een NHL-envelop (88,3%) ontvingen, het verschil is net niet significant (tweezijdig, P=0.07).

In totaal hebben 45 respondenten de website bezocht, maar de vragenlijst niet (helemaal) ingevuld. Twaalf van de 45 respondenten hebben het introductiescherm weg

geklikt en zijn niet begonnen aan de vragenlijst. De vraag naar postcode en geslacht is de eerste pagina na de introductiepagina. Daar haakten nog eens 7 respondenten af. Daarna volgt nog een aantal vragen naar achtergrondkenmerken (tot aan de vraag 'hoe vaak internet u'). Daar zijn in totaal 6 respondenten afgehaakt. De meerderheid van de respondenten die afhaakten (25 van de 45) zijn niet bij de vragen over cybercrime aangekomen. Daarna zien we de afhakers verspreid over meerdere vragen. De vraag waar nog 6 respondenten afhaakten, is de matrix waarin gevraagd wordt naar het internetgedrag van de respondent.

Redenen om niet deel te nemen

Tijdens het nabellen hebben 131 respondenten met de KLPD lay-out en 179 respondenten met een NHL lay-out deelname geweigerd. Dat is een totaal van 310 weigeringen. De respondenten is gevraagd waarom zij niet aan het onderzoek wilden deelnemen (zie tabel 3.3). Zij konden meerdere redenen opgeven. Er was geen significant verschil in de reden van weigering tussen de verschillende lay-outs.

Tabel 3.3: reden om medewerking te weigeren

Reden	**Aantal van 310**	**% van 310**
ik gebruik (bijna) geen internet/computer (vindt zichzelf geen doelgroep)	34	11,6
ik heb nog nooit iets meegemaakt op internet (vindt zichzelf geen doelgroep)	13	4,4
andere reden waarom men zichzelf geen doelgroep vindt	3	1,0
ik vind het niet veilig om mee te doen aan dit onderzoek (privacy, hacken)	13	4,4
ik heb geen tijd / geen zin / ik doe nooit mee aan onderzoek	208	70,7
respondent is niet in staat (gehandicapt, verhuisd, geen Nederlands etc)	14	4,8
anders	10	3,4
geen antwoord	20	6,8

Uit tabel 3.3 blijkt dat het merendeel van de respondenten (70,7%) als reden aangeeft nooit mee te doen met onderzoek of er gewoon geen zin in te hebben. Nog eens 4,8% geeft geen reden en/of gooit de hoorn er op. 17,0% geeft aan zichzelf geen doelgroep te vinden voor het onderzoek. 4,4% geeft aan het onderzoek niet te vertrouwen.

3.6 Representativiteit testmeting

Om de representativiteit van de respondenten in kaart te brengen zijn *stedelijkheid gemeente, leeftijd, geslacht, etniciteit, werksituatie, opleidingsniveau* en *internetgebruik* van de respondenten vergeleken met de Nederlandse bevolking van 15 t/m 70 jaar.

Stedelijkheid gemeente

We trokken een steekproef van 5 gemeenten in Nederland, uit elke stedelijkheidsgraad zoals die is vastgesteld door het CBS een gemeente. De steekproef wijkt op stedelijkheid daarom af van de populatie, zoals te zien is in tabel 3.4.

Tabel 3.4 stedelijkheid steekproef in vergelijking met landelijk beeld.

	steekproef	Nederland
Stedelijkheid	**%**	**%**
zeer sterk stedelijk	20,0%	19,4%
sterk stedelijk	20,0%	27,9%
matig stedelijk	20,0%	19,5%
weinig stedelijk	20,0%	21,7%
niet stedelijk	20,0%	11,5%
	100,0%	100,0%

In de steekproef woonde 40% in een weinig of niet stedelijk gebied (Hilvarenbeek en Zeevang). Wanneer we een landelijk representatieve steekproef nemen, woont 33,2% in een weinig of niet stedelijk gebied.

Respons per gemeente

In tabel 3.5 valt te lezen wat de respons is per gemeente en per lay-out.

Tabel 3.5 Respons per gemeente en lay-out

		KLPD		NHL		Totaal	
gemeente	**Stedelijkheid**	**N**	**%**	**N**	**%**	**N**	**%**
Beverwijk	zeer sterk stedelijk	66	18,5	31	17,8	97	18,3
Leeuwarden	sterk stedelijk	71	19,9	43	24,7	114	21,5
Soest	matig stedelijk	54	15,1	29	16,7	83	15,6
Hilvarenbeek	weinig stedelijk	85	23,8	32	18,4	117	22,0
Zeevang	niet stedelijk	81	22,7	39	22,4	120	22,6
Totaal		357		174		531	

De respons is niet evenredig over de gemeenten verdeeld. Het verschil in respons tussen de gemeenten is niet significant (p=0,053), maar te verwachten is wel dat de respons in stedelijke gebieden lager is dan in weinig of niet stedelijke gebieden. Het verschil in respons tussen

gemeenten naar lay-out is niet significant (p=0.552). Toch valt hier te zien dat de respons in Leeuwarden hoger uitvalt door een relatief hoge respons op de NHL lay-out wat niet verwonderlijk is, aangezien NHL Hogeschool gevestigd is in Leeuwarden en daar een hoge naamsbekendheid heeft.

Wanneer we een aselecte steekproef van Nederlanders trekken voor de nulmeting, zullen inwoners van weinig en niet stedelijke gebieden in de respons oververtegenwoordigd zijn.

Leeftijd

De mediaan en het gemiddelde van de populatie is ongeveer 43 jaar[29]. De gemiddelde leeftijd van mensen die n.a.v. het nabellen alsnog zelf online invullen is onder KLPD'ers significant lager dan onder alle andere groepen (tabel 3.6). De respondenten die de vragenlijst op papier invulden zijn niet significant ouder dan degenen die het online invulden, maar dit is vooral te verklaren door het kleine aantal respondenten dat de vragenlijst op papier invulden. Vermoedelijk zal hun leeftijd in de nulmeting wel significant hoger zijn.

Tabel 3.6 gemiddelde leeftijd per methode

bron data	**Gemiddelde**	**N**	**Std. Deviatie**
klpd online brief	44,75	259	16,507
Klpd online telefonisch	34,70	67	15,511
klpd papier	51,09	32	13,874
nhl online brief	47,36	105	14,841
Nhl online telefonisch	41,17	54	14,075
nhl papier	56,25	16	9,754
Totaal	44,37	533	16,134

Uit tabel 3.7 blijkt dat de leeftijdscategorie 20 t/m 39 is ondervertegenwoordigd onder respondenten die reageerden op de KLPD brief. De leeftijdscategorieën 15 t/m 19 jaar en 50 t/m 70 jaar is oververtegenwoordigd. Jongere mensen reageren vaker op een telefonische herinnering, ouderen op de brief.

[29] CBS 2010: http://statline.cbs.nl/statweb.

Tabel 3.7 leeftijd KLPD-respondenten

	Observed N	Expected N	Residual
15 t/m 19	45	30,1	14,9
20 t/m 24	25	30,0	-5,0
25 t/m 29	27	29,6	-2,6
30 t/m 34	21	29,6	-8,6
35 t/m 39	21	35,0	-14,0
40 t/m 44	40	38,5	1,5
45 t/m 49	32	38,2	-6,2
50 t/m 54	31	34,9	-3,9
55 t/m 59	36	32,1	3,9
60 t/m 64	35	31,7	3,3
65 t/m 70	44	27,1	16,9
Totaal	357		

Aangezien vooral jonge mensen op de telefonische herinnering reageren en deze methode ondervertegenwoordigd is omdat we maar een deel van de mensen telefonisch hebben benaderd, valt te verwachten dat de leeftijd in de nulmeting lager zou liggen en er dus een betere leeftijdsverdeling zal zijn.

Geslacht

Van alle respondenten is 47,4% man. In de populatie is 50,3% man[30]. Het verschil is niet significant.

Etniciteit

Van 11,7% van de respondenten is de etniciteit 'niet Nederlands'. Dit betekent dat de respondent zelf en/of minstens één van de ouders niet in Nederland geboren zijn. In de populatie is dit ongeveer 20%[31]. Allochtonen zijn dus ondervertegenwoordigd in de respons.

Betaald werk

In het derde kwartaal van 2010 woonden er in Nederland 7,5 miljoen personen van 15 tot 65 jaar die betaald werk verrichtten voor twaalf uur of meer per week. Dit betekent dat tweederde van de 15 tot 65 jarigen tot de werkzame beroepsbevolking behoorde[32]. Wanneer

[30] CBS 2010: http://statline.cbs.nl/statweb.
[31] Supra 47, noot 30.
[32] Supra 47, noot 30.

we de leeftijdscategorie 65 t/m 70 jaar buiten beschouwing laten, blijkt 81,1% van de respondenten werk te hebben van 12 uur of meer. Dat is significant hoger dan in de populatie.

Opleidingsniveau
Wanneer we alleen de respondenten tussen 25 en 64 jaar beschouwen, kunnen we zien dat het aandeel hoogopgeleide respondenten representatief is voor Nederland. In Nederland is van deze leeftijdsgroep 32% hoog opgeleid[33]; onder de respondenten in deze leeftijdsgroep is dat 35%.

Gebruik internet
Om de representativiteit van de respondenten op het gebied van internet te bepalen, vergeleken we kerncijfers met cijfers van het CBS[34] (tabel 3.8).

Tabel 3.8 internetgebruik.

	Respondenten	**Landelijk**
gebruikt internet nooit of zelden;	2,4% en 2,1 %	
geen pc met internetverbinding in het huishouden;	1,0%	6,0% (CBS, 2009)
breedbandaansluiting	78%	bijna 80% (CBS)
gebruik internetbankieren;	88%	90% (2009, 25+)
83% heeft in de afgelopen 12 maanden goederen via internet gekocht;	83%	74% van de internetgebruikers (2009)
afgelopen 12 maanden iets via internet verkocht.	42%	

De respondenten hebben vaker een pc met internetverbinding thuis en zijn actievere webshoppers dan de gemiddelde Nederlander. Hierbij moet opgemerkt worden dat de cijfers van het CBS uit 2009 zijn en het aantal webshoppers nog steeds groeit. Het is lastig deze cijfers goed met elkaar te vergelijken vanwege een afwijkende vraagstelling.

Slachtofferschap
Om te kunnen berekenen of de lay-out van invloed is op de omvang van slachtofferschap, is eerst vastgesteld hoe hoog het slachtofferschap was in de test. Slachtofferschap van financiële delicten is daarbij gedefinieerd als het aanwezig zijn van schade, al dan niet vergoed door derden (bank, verzekering). Tabel 3.9 is een overzicht.

[33] Supra 47, noot 30.
[34] Supra 47, noot 30.

Tabel 3.9 slachtofferschap cybercrime

Cybercrime	**N slachtoffers**	**% slachtoffers**
Financiële schade door malware	11	2,1%
Product betaald, niet geleverd	8	1,5%
Nepproduct geleverd	6	1,1%
Geleverd, niet betaald gekregen	2	0,4%
Identiteitsfraude	4	0,8%
Voorschotfraude	0	0%
Datingsitefraude	2	0,4%
Totaal financiële fraude	*21*	*3,9%*
Stalking	4	0,8%
Smaad/laster	1	0,2%
Bedreiging	4	0,8%
Afpersing /chantage	1	0,2%
Totaal relationele delicten	*7*	*1,3%*

Er blijken 21 unieke slachtoffers van financieel economische criminaliteit te zijn (exclusief schade door malware) en 7 unieke slachtoffers van relationele delicten. Cyberstalking en -bedreiging komen twee keer in combinatie voor, één keer ook nog in combinatie met afpersing.

Het is denkbaar dat slachtoffers eerder reageren op een verzoek tot deelname aan een onderzoek met een KLPD lay-out. Tabel 3.10 is een kruistabel tussen slachtofferschap en lay-out.

Tabel 3.10 slachtofferschap financiële cybercrime naar lay-out

		lay-out		
		klpd	**nhl**	**Totaal**
geen slachtoffer	N	341	171	512
	%	95,3%	97,7%	96,1%
slachtoffer	N	17	4	21
	%	4,7%	2,3%	3,9%
Totaal	N	358	175	533
	%	100,0%	100,0%	100,0%

Het verschil in slachtofferschap van financiële delicten is niet significant (p=0.126 (1-zijdig)), toch is het toevalspercentage zo klein (12,6%), dat we bij de interpretatie van de resultaten van de nulmeting wel rekening moeten houden met een oververtegenwoordiging van slachtoffers als we kiezen voor een KLPD lay-out. Alle 7 unieke slachtoffers van relationele delicten komen uit de KLPD steekproef.

3.7 Conclusies representativiteit testmeting

- De respons is onder inwoners van weinig en niet stedelijke gebieden hoger dan onder inwoners van meer stedelijke gebieden. We zullen hiervoor moeten corrigeren in de nulmeting.
- Jongeren tot 20 jaar en burgers van 50 t/m 70 jaar zijn oververtegenwoordigd, vooral burgers van 30 t/m 39 jaar zijn ondervertegenwoordigd. In de nulmeting zal deze verdeling naar verwachting beter zijn, maar een correctie zal wellicht nodig zijn.
- Allochtonen zijn ondervertegenwoordigd, dat zal wellicht een correctie vergen.
- Mensen met betaald werk van 12 uur of meer zijn oververtegenwoordigd, dat zal wellicht een correctie vergen.
- Wat geslacht en opleidingsniveau betreft zijn de respondenten in deze pilot representatief. In de nulmeting moet worden bezien of hierop toch een correctie nodig is.
- Voor internetgebruik zullen we proberen één of twee vragen toe te voegen in de nulmeting zoals het CBS deze ook stelt in hun metingen om de representativiteit te kunnen toetsen.
- De ondervertegenwoordigde groep 30 t/m 39 jaar is gevoelig voor een telefonisch rappèl. Ouderen reageren eerder op de brief. Andere achtergrondvariabelen hebben geen significante invloed op het al dan niet reageren op elke methode.

3.8 Reacties van respondenten

Tijdens de afnameperiode van het onderzoek konden respondenten contact opnemen met de onderzoekers via een speciaal ingesteld telefoonnummer en e-mailadres om een papieren vragenlijst aan te vragen, om medewerking te weigeren of vragen te stellen over bijvoorbeeld het inloggen.

- 10 respondenten hebben een papieren versie aangevraagd per telefoon/e-mail;
- 6 respondenten hebben gebeld/gemaild omdat zij problemen hadden met inloggen (zij bleken www.cybercrime-onderzoek.nl in te typen in de zoekbalk);
- 4 respondenten meldden zich af omdat zij de verbinding niet veilig vonden of bang waren dat het onderzoek zelf een hackpoging was;
- 6 respondenten meldden zich af omdat ze zich geen doelgroep vonden (gehandicapt, geen internetgebruiker);

- 3 respondenten belden om te checken of het onderzoek wel echt was en om te vragen hoe wij aan het adres gekomen waren.

Ook tijdens het nabellen zijn vragen en opmerkingen gekomen van respondenten. Burgers weten niet dat zij wel gebeld mogen worden voor wetenschappelijk onderzoek als zij geregistreerd zijn in het bel-me-niet register. Ook ontstond er bij sommige respondenten woede over het feit dat hun gemeente 'zomaar' hun adres verstrekt voor onderzoek. Dit zijn echter incidenten en mijns inziens niet te voorkomen.

3.9 Conclusies van de testmeting

Naar aanleiding van de testmeting kunnen de volgende conclusies getrokken worden:

- De gehanteerde aanpak resulteerde in een respons van 35,4% met een KLPD lay-out en 20,8% met een NHL lay-out.
- Van de respons op de KLPD lay-out komt 58% online binnen n.a.v. de brief, 28% online n.a.v. de telefonische herinnering en 13% op papier.
- De brief heeft meer effect op oudere mensen, het telefoontje op jongere mensen.
- Ongeveer 75% van de mensen die niet meewerken aan het onderzoek doen dat uit gebrek aan interesse, 20% vindt zichzelf geen doelgroep en 5% twijfelt aan de veiligheid van het onderzoek zelf.
- De respons wijkt op stedelijkheid, leeftijd, etniciteit en arbeidssituatie significant af van de populatie, maar niet dusdanig dat er niet teruggewogen kan worden met de achtergrondgegevens van het CBS.
- Wat betreft internetgebruik lijken er ook verschillen te bestaan tussen respons en populatie, maar die kunnen niet helder vastgesteld worden op basis van de testresultaten.
- 17 van de 21 slachtoffers van financiële delicten komen uit de KLPD steekproef en alle 7 slachtoffers van relationele delicten.
- De vragen over identiteitsfraude moeten herzien worden. De vragen over relationele fraude kunnen wellicht samengenomen worden.
- De aangiftebereidheid is in de test 14,3%.

Naar aanleiding van deze conclusies zijn aanpassingen doorgevoerd in de vragenlijst en in de uitvoering.

3.10 Aanpassingen naar aanleiding van de testmeting

Aanpassingen in de vragenlijst

- Het was lastig om slachtofferschap van identiteitsfraude vast te stellen n.a.v. de verzamelde data in de testmeting. De vraagstelling is aangepast.
- Slachtofferschap van voorschotfraude (erfenissen, loterijen e.d.) kwam niet voor onder de respondenten in de testmeting. Voorschotfraude via datingsites 2 keer. Deze vormen zijn samengevoegd onder de hoofdvorm 'voorschotfraude'.
- In totaal zijn er 7 unieke slachtoffers van relationele delicten (1,3%). Twee slachtoffers gaven aan van meerdere vormen van relationele delicten slachtoffer te zijn geweest, in beide gevallen door dezelfde dader. In het onderzoek zijn voor alle vormen van relationele delicten slachtofferschap, de relatie met de dader en de modus operandi gevraagd, maar zijn de materiële schade en de aangiftebereidheid één keer gevraagd, ook als het slachtoffer van meerdere relationele delicten slachtoffer werd.
- Omdat het CBS op basis van een unieke CBS-code de data verrijkt met allerlei achtergrondkenmerken zoals inkomen en sociaal economische status, konden we in het onderzoek volstaan met veel minder achtergrondkenmerken. Vragen over achtergrondkenmerken zijn naar het einde van de vragenlijst verplaatst.
- Matrixen met meer dan zes stellingen, zijn over meerdere pagina's verdeeld.
- Verder zijn er naar aanleiding van opmerkingen van respondenten en op basis van voortschrijdend inzicht kleine wijzigingen doorgevoerd. Ook zijn antwoordcategorieën weggelaten die nooit aangevinkt werden.

De vragenlijst die is gebruikt voor het onderzoek is opgenomen in bijlage 3.

Aanpassingen in de uitvoering

- Ondanks dat er aanwijzingen zijn dat een brief met KLPD lay-out meer slachtoffers trekt dan een neutrale lay-out, is vanwege de gewenste hoge respons toch gekozen voor een KLPD lay-out. De overweging hierbij was dat als na de nulmeting overgegaan wordt op een nieuwe methode om de omvang te meten (bijvoorbeeld een module in de IVM), er sowieso een methodebreuk op zou treden.
- Voor de nulmeting is een aselecte steekproef van Nederlanders genomen om eventuele invloeden van de regio waarin de respondent woont zo klein mogelijk te maken. De steekproef is aangeleverd door het CBS.

- Voor de nulmeting is geen bovengrens in leeftijd gesteld, maar zijn Nederlanders vanaf 15 jaar aangeschreven, in overeenstemming met de IVM.
- Nederlanders van 15 jaar zijn via hun ouders aangeschreven, omdat tot 16 jaar een informed consent wettelijk verplicht is.
- De volgende responsverhogende maatregelen zijn genomen:

  Communicatie:

  - de vragenlijst is bereikbaar gemaakt via de website www.politie.nl/klpd/internetonderzoek. De woordvoerder van het KLPD heeft een persbericht over het onderzoek verspreid en deze ook op de website van de politie geplaatst. Op de website is informatie geplaatst over de betrokken partijen en een link naar de website van lectoraat cybersafety waar het onderzoek beschreven staat;
  - in de uitnodigingsbrief is de privacywaarborg die door het CBS gebruikt wordt, opgenomen (bijlage 4);
  - het onderzoek is gepresenteerd als een onderzoek naar (on)veiligheid in de digitale wereld en niet als een slachtofferonderzoek: de woorden ‘slachtoffer’ en ‘cybercrime’ zijn in de brief en op de website niet gebruikt en komen pas halverwege de vragenlijst voor het eerst voor;
  - de layout van de brief is geprofessionaliseerd.

  Vindbaarheid van het inlogscherm: nogal wat respondenten bleken www.cybercrime-onderzoek.nl in te typen in de zoekbalk van bijvoorbeeld Google tijdens de testmeting. De website van de politie is goed vindbaar, ook via Google. Op elke deelpagina van de politiewebsite werd in grote, rode letters ‘internetonderzoek’ vermeld, wat linkte naar het inlogscherm. Door het grote aantal bezoekers van het onderzoek, was het inlogscherm na enkele dagen tevens de eerste hit wanneer men het webadres intypte in Google. Er zijn geen telefoontjes gekomen van respondenten die het inlogscherm niet konden vinden.

  Technische beveiliging: er is een https-verbinding gebruikt voor het onderzoek.

4 Respons en representativiteit onderzoek

4.1 Steekproef onderzoek

Het CBS leverde een steekproef uit de landelijke GBA voor het onderzoek. De steekproef was voorzien van een unieke inlogcode om ervoor te zorgen dat alleen mensen uit de steekproef de vragenlijst konden invullen. Verder leverde het CBS een CBS-code mee, zodat de data na afloop van het onderzoek verrijkt konden worden met gegevens uit het Sociaal Statistische Bestand (SSB) en de GBA en zodat het bestand gewogen kon worden door het CBS. Een mooie bijkomstigheid is dat op deze manier van alle 21.800 genodigden inzichtelijk gemaakt kan worden 1. of en hoe zij respondeerden, 2. wie zij zijn en 3. of zij slachtoffer werden van cybercrime. Dit kan leiden tot een mooie methodologische rapportage.

4.2 Respons onderzoek

Er zijn 283 ouders aangeschreven (bijlage 5) met het verzoek hun kind van 15 jaar een online vragenlijst te laten invullen. In totaal vulden 158 jongeren van 15 jaar de vragenlijst in (55,8%). Daarnaast zijn 21.517 Nederlanders van 16 jaar en ouder uitgenodigd met een brief (bijlage 4). Van hen respondeerden 10.122 (47,0%). De totale respons was 10.280, wat een respons betekent van 47,2 procent.

Er zijn vragenlijsten online ingevuld door de respondenten zelf en door telefonisch enquêteurs. In tegenstelling tot in de testfase was er tijdens het onderzoek voldoende budget om alle mensen die niet respondeerden op de uitnodigingsbrief en de reminderbrief na te bellen en om tijdens het nabellen te sturen op telefonische afname. Respondenten konden ook een papieren vragenlijst aanvragen. In de volgende paragrafen wordt de aanpak en respons per methode beschreven.

Respons op uitnodigingsbrieven

De uitnodigingsbrieven zijn verstuurd op 15 april 2011. De brieven zijn gedrukt op KLPD briefpapier en ondertekend met een digitale handtekening van de korpschef R. Bik. In de brief is de respondent verzocht te surfen naar www.politie.nl/klpd/internetonderzoek en daar in te loggen met een unieke inlogcode. In de brief werden een telefoonnummer en emailadres vermeld waarmee de respondent zich af kon melden voor het onderzoek of waarmee een papieren vragenlijst aangevraagd kon worden. De respondent kon zichzelf ook via een link op de politiewebsite afmelden voor het onderzoek of een papieren vragenlijst aanvragen.

Op 6 mei 2011 zijn de reminderbrieven gestuurd naar alle respondenten die niet reageerden op de uitnodigingsbrief. In de reminderbrief werd aangekondigd dat de respondent telefonisch benaderd zou worden als er geen reactie kwam in de vorm van deelname of een weigering.

Uit tabel 4.1 blijkt dat 2.887 mensen uit de steekproef naar aanleiding van de eerste uitnodigingsbrief en 2.723 naar aanleiding van de reminderbrief naar de genoemde website gingen en de vragenlijst in zijn geheel invulden (in totaal 25,7% van de steekproef). Ook reageerden 1.346 mensen door zich telefonisch of via de website af te melden voor het onderzoek (6,2%), dit gebeurde voor het grootste deel telefonisch n.a.v. de tweede brief. Nog eens 306 mensen vroegen telefonisch of via de website een papieren vragenlijst aan. In totaal waren 73 respondenten niet bereikbaar met de brief omdat TNT de brief niet kon bezorgen of omdat de bewoners van het adres aangaven dat de genoemde persoon niet (meer) woonachtig was op dat adres en de brief terugstuurden. 35 respondenten ondernamen meerdere acties. Zij vroegen bijvoorbeeld een papieren vragenlijst aan én melden zich af voor het onderzoek, of vulden de vragenlijst online in. Er waren uiteindelijk geen respondenten die zowel online als op papier hebben gerespondeerd.

Tabel 4.1: online respons n.a.v. uitnodigingsbrieven

	N	**%**
Eerste brief	21.800	100,0%
Respons 1e brief	2.887	13,2%
Respons 2e brief	2.723	12,5%
Onbezorgbaar	73	0,3%
Afgemeld n.a.v. brieven	1.346	6,2%
Papieren vragenlijst aangevraagd	306	1,4%
Overlap afhandeling	35	0,2%
Adressen over voor nabellen	*14.500*	*66,5%*

Met de twee uitnodigingsbrieven is in totaal 33,5 procent van de steekproef afgehandeld en er bleven nog 14.500 adressen over.

Telefonisch bereik

Van de overgebleven 14.500 adressen werden telefoonnummers gezocht door EMD Data BV. Zij beschikken hiervoor over een geautomatiseerd zoeksysteem. Er werd gezocht op naam en op adres naar zowel vaste als mobiele nummers. Een zoekactie kon dus nul, een of twee nummers opleveren. Nadat alle telefoonnummers eenmaal waren gebeld, is van Nederlanders

in de steekproef waarbij geen nummer werd gevonden of waarvan het gevonden nummer onjuist bleek, nogmaals gezocht naar telefoonnummers via bureau Companen. Er werd in totaal bij 82,4 procent van de namen minstens één telefoonnummer gevonden.

Alle telefoonnummers zijn gebeld door enquêteurs van bureau Companen in de periode 23 mei tot en met 2 juli 2011. Van de overgebleven personen in de steekproef waarvan minstens één nummer werd gevonden, bleek in 13,0 procent van de gevallen geen correct nummer te zijn gevonden. Nog eens 7,9 procent van de personen werd niet bereikt in minimaal negen belpogingen. Van 1,5 procent van de overgebleven personen bleek de inlogcode niet meer bruikbaar. De telefoonnummers werden vrij snel na het verzenden van de reminderbrief gezocht om tijd te besparen, deze respondenten hebben de vragenlijst zelf nog online ingevuld in de tijd dat de telefonische afname werd voorbereid of zij hebben zich in die periode afgemeld voor het onderzoek. In totaal werd 59,2 procent van de personen die niet reageerden op de uitnodigingsbrieven telefonisch bereikt (tabel 4.2).

Tabel 4.2 Telefonisch bereik

	N	**% van totaal**	**% van overgebleven steekproef**
Adressen over voor nabellen	14.500	66,5%	100,0%
Telefoonnummers gezocht	14.496	66,5%	100,0%
Telefoonnummers gevonden	11.946	54,8%	82,4%
Onjuist nummer	1.889	8,7%	13,0%
Inlogcode niet bruikbaar	333	1,5%	2,3%
Niet bereikt in 9 pogingen	1.144	5,2%	7,9%
Telefonisch bereikt	8.580	39,4%	59,2%

Respons op telefonische benadering

Uit tabel 4.3 blijkt dat van de 14.500 overgebleven personen in de steekproef 8.580 personen telefonisch werden bereikt. Van hen was 44,3 procent bereid de vragen uit de vragenlijst telefonisch te beantwoorden, echter 0,3 procent brak de vragenlijst halverwege af. Dit betekent dat 44,0 procent van de bereikte personen telefonisch heeft meegewerkt aan het onderzoek, wat overeenkomt met 17,3 procent van de steekproef. Van de bereikte personen weigerde 42,0 procent alle medewerking, 7,6 procent zegde toe de vragenlijst zelf nog online te zullen invullen en 1,4 procent vroeg de enquêteur een papieren vragenlijst op te sturen.

Tabel 4.3 Respons telefonische benadering

	N	**% van totaal**	**% van telefonisch bereikt**
Telefonisch bereikt	8.580	39,4%	100,0%
Telefonische respons	3.777	17,3%	44,0%
Weigering	3.606	16,5%	42,0%
Toezegging zelf alsnog online	652	3,0%	7,6%
Overig geen respons	374	1,7%	4,4%
Papieren vragenlijst aangevraagd	122	0,6%	1,4%
Halverwege afgebroken	55	0,3%	0,6%
Overlap afhandeling	6	0,0%	0,1%
	8.580		

Totale respons

Tabel 4.4 is een overzicht van de totale respons. De brieven leidden tot 5.610 volledig ingevulde vragenlijsten, in totaal 25,7 procent van de steekproef. Telefonisch werden 3.777 respondenten ondervraagd, 17,3 procent van de steekproef.

In totaal werden 428 papieren vragenlijsten verstuurd, 306 n.a.v. de uitnodigingsbrieven (tabel 4.1) en nog eens 122 n.a.v. het nabellen (tabel 4.3). In totaal werden 248 van deze vragenlijsten ingevuld geretourneerd (57,9%) wat overeenkomt met 1,1 procent van de steekproef. Tijdens het nabellen gaven 652 personen uit de steekproef aan zelf de vragenlijst nog online in te zullen vullen; 221 van hen hebben dit ook gedaan (33,9%). Dit komt overeen met 1,0 procent van de steekproef.

Op twee manieren is ‘overige respons’ ontstaan. In de periode van het nabellen zijn er respondenten geweest die de vragenlijst zelf invulden, voordat zij gebeld werden. Aangezien de telefonisch enquêteurs in dezelfde software werkten als de respondenten zelf, is niet terug te halen hoeveel dit er precies zijn geweest. Ten tweede bleek na de dataverzameling dat een aantal enquêtes niet volledig waren ingevuld, maar waren blijven steken bij het eindscherm of bij de facultatieve vragen. Als de vragen ingevuld waren tot en met de laatste verplichte vraag, zijn de enquêtes toch meegenomen als respons. De ‘overige respons’bestond in totaal uit 424 vragenlijsten (1,9% van de steekproef).

Tabel 4.4 Overzicht opbouw totale respons

Respons	**N**	**% van totaal**	**% van respons**
Respons 1e brief	2.887	13,2%	28,1%
Respons 2e brief	2.723	12,5%	26,5%
Telefonische respons	3.777	17,3%	36,7%
Papieren respons	248	1,1%	2,4%
Online respons n.a.v. bellen	221	1,0%	2,1%
Overige respons*	424	1,9%	4,1%
Totale respons	**10.280**	**47,2%**	**100,0%**

4.3 Representativiteit

Van 10.280 respondenten gebruiken 1.117 respondenten (10,9%) nooit internet. De rapportage is gebaseerd op de 9.163 respondenten die wel internet gebruiken. In de rapportage wordt dan ook gesproken over prevalentie als percentage van 'internetters'.

Het CBS heeft de data verrijkt met gegevens uit de GBA en het SSB. Vervolgens heeft het CBS weegfactoren berekend over alle 10.280 respondenten op dezelfde manier als dat het CBS dat voor de Integrale Veiligheidsmonitor doet.

4.4 Analyse

Wanneer uitspraken gedaan worden over alle internetters, zijn resultaten gewogen weergegeven. Dit geldt voor de prevalentie van slachtofferschap onder internetters en voor de bivariate analyses, waarin gemeten wordt of slachtoffers op persoonlijke achtergrondkenmerken afwijken van niet-slachtoffers. Vervolganalyses zijn ongewogen uitgevoerd, omdat met een (vaak kleine) deelpopulatie gerekend wordt, die op achtergrondkenmerken afwijkt van de gehele populatie. Een respondent die bijvoorbeeld veel schade heeft ondervonden van een delict en een relatief hoge weegfactor heeft (omdat hij tot een ondervertegenwoordigde groep behoort) kan in zijn eentje een grote invloed uitoefenen op de resultaten en daardoor een vertekend beeld schetsen.

Er is een significantieniveau van 0.05 gehanteerd.

5 Malware en hacken

5.1 Malware

Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op uw computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, trojan horses, wormen en spyware.

Malware, prevalentie

De bestrijding van malware (en daarmee van cybercrime) is er bij gebaat dat gebruikers opmerken dat hun computer is besmet. Aan respondenten is bovenstaande definitie van malware voorgelegd. Vervolgens is gevraagd zij in de twaalf maanden voorafgaand aan het onderzoek gemerkt hebben dat er malware op hun computer aanwezig was.

Van alle internetgebruikers heeft 16,7 procent in de afgelopen twaalf maanden malware opgemerkt op de computer thuis (met een 95 procent betrouwbaarheidsinterval is dat tussen de 15,9 en 17,5 procent). Het percentage internetters wiens computer in die periode met malware was geïnfecteerd, ligt vermoedelijk hoger omdat niet alle malware door de gebruiker zal zijn opgemerkt.

Malware, modus operandi

Aan de respondenten die malware hebben opgemerkt, is gevraagd hoe deze malware op hun computer terecht is gekomen. Daarbij waren meerdere antwoorden mogelijk. Uit tabel 5.1 blijkt dat bijna vier op de tien respondenten die malware hebben opgemerkt, niet weten hoe deze op hun computer terecht is gekomen (38,4%). Ruim een kwart heeft de malware naar eigen zeggen via e-mail ontvangen, ook ruim een kwart via een link op een website en ruim een vijfde via een download.

De respondenten die ‘anders’ antwoordden, hadden vervolgens de mogelijkheid zelf in te typen hoe de malware op hun computer terecht is gekomen. Het vaakst (33 keer) is een bepaalde toepassing (bijvoorbeeld Skype, Limewire) of website genoemd. Een aantal keer is een externe gegevensdrager zoals een usb-stick genoemd.

Malware, schade

Uit tabel 5.2 blijkt dat van de mensen die malware hebben opgemerkt, 16,1 procent financiële schade heeft geleden. Dat betekent dat 2,7 procent van alle internetters financiële schade heeft

geleden door malware, bijvoorbeeld omdat de PC moest worden gerepareerd. Van de internetters met schade door malware wist 78,2 procent ook de hoogte van het schadebedrag te noemen. Meer dan de helft van de bekende schades bedraagt 100 euro of minder, maar ook 7,9 procent van de schades bedraagt 501 euro of meer. Van de respondenten die malware hebben opgemerkt, is 11,9 procent bestanden of software kwijtgeraakt, wat overeenkomt met 2,0 procent van de internetters.

Tabel 5.1: manier waarop malware naar eigen zeggen op de computer terecht is gekomen (meerdere antwoorden mogelijk, ongewogen)

	Aantal *	**% van slachtoffers (n=1.512)**
Weet ik niet	581	38,4
Via een link op een website	399	26,4
Via een e-mail	385	25,5
Via een download	321	21,2
Anders	64	4,2
Via een msn-bericht	54	3,6
Via een twitterbericht	2	0,1

* omdat er per slachtoffer meerdere antwoorden mogelijk zijn is het totaal in deze kolom groter dan het aantal slachtoffers.

Tabel 5.2: schade door malware (ongewogen)

Euro	**Aantal**	**% van slachtoffers (n=1.512)**	**% van bekende schade**	**% van internetters (n=xx)**
Geen/wel schade				
Geen schade	1.246	82,4		
Onbekend	23	1,5		
Schade	243	16,1		2,7
Omvang schade				
Onbekend				0,8
1 – 100			57,4	1,2
101 – 200			20,5	0,4
201 – 500			14,2	0,3
501 – 1000			6,8	0,1
1001 of meer			1,1	0,0

Malware, wie merken het op?

Om te weten te komen welke internetgebruikers malware opmerken, voeren we bivariate analyses uit (tabel 5.3). Uit deze analyses blijkt dat mannen vaker malware opmerken dan vrouwen en dat mensen met een betaalde baan van minstens twaalf uur per week vaker

malware opmerken dan mensen met minder betaald werk. Dan is er nog een verschil tussen de verschillende opleidingsniveaus en tussen de verschillende leeftijdscategorieën. Tabel 3.3 wijst er op dat hoger opgeleiden vaker malware opmerken dan lager opgeleiden en dat internetters in de leeftijdscategorie 35-54 jaar dat vaker doen dan jongere of juist oudere internetters.

Tabel 5.3: malware opgemerkt naar achtergrondkenmerken (gewogen)

Heeft u malware opgemerkt op uw computer?	**% ja**
Geen opleiding	8,8
Basisonderwijs	14,6
LBO	10,7
VMBO/MAVO	14,4
HAVO/VWO	17,5
MBO	17,3
HBO	19,5
WO	19,0
$\chi^2(7)$	*54,70***
15-24	16,7
25-34	17,4
35-44	20,0
45-54	19,6
55-64	13,5
65+	9,4
$\chi^2(5)$	*78,87***
< 12 uur betaald werk p.w.	14,1
12+ uur betaald werk p.w.	18,1
$\chi^2(1)$	*25,40***
Geen partner[35]	16,3
Partner	17,1
$\chi^2(1)$	*1,07*
Autochtoon	16,6
1e generatie	17,1
2e generatie, 1 ouder	18,5
2e generatie, beide ouders	14,3
$\chi^2(3)$	*2,45*
Man	19,6
Vrouw	13,6
$\chi^2(1)$	*59,86***
Totaal	**16,7**

* p<0.05, ** p<.0.01

[35] Alleenstaand, verweduwd of gescheiden volgens de gemeentelijke basisadministratie.

Malware, conclusies

16,7 procent van de ondervraagde internetters heeft in de afgelopen twaalf maanden gemerkt dat er malware op hun computer stond; 2,7 procent van de internetters heeft hierdoor financiële schade geleden en 2,0 procent van de internetters is bestanden en/of software kwijtgeraakt door malware. Vooral hoogopgeleiden, mannen, mensen tussen 35 en 54 jaar en mensen met een betaalde baan merken malware op.

5.2 Hacken

Leukfeldt e.a. (2010) vonden in hun studie op basis van 665 politiedossiers dat hacken verbanden heeft met een groot aantal andere vormen van criminaliteit en vaak een middel is om andere delicten te plegen. Om die reden is het slachtofferschap van hacken in onze studie op verschillende manieren gemeten. Er is direct gevraagd of iemand gehackt is, met onderstaande drie stellingen waarop de respondent met ja of nee kon antwoorden.

1. Iemand heeft zonder uw toestemming uw webpagina en/of profiel (Hyves, Facebook, etc) veranderd (defacing).
2. Iemand heeft ingebroken in uw computer en gegevens vernietigd, veranderd of gestolen.
3. Iemand heeft ingebroken in uw e-mail of zonder toestemming op uw e-mailaccount ingelogd.

Daarnaast is bij identiteitsdiefstal en stalking gevraagd of hacken onderdeel was van de modus operandi van de dader.

Hacken, prevalentie

In totaal is 4,3 procent van de respondenten die internet gebruiken in de twaalf maanden voorafgaande aan het onderzoek slachtoffer geworden van één of meerdere van de bovengenoemde vormen van hacken. Met een betrouwbaarheid van 95 procent is tussen 3,9 en 4,7 procent van de internetters slachtoffer geworden van hacken: 1,5 procent is slachtoffer geworden van *defacing* (het zonder toestemming wijzigen van een website of profielpagina), van 0,7 procent van de respondenten is de computer gehackt, van 2,9 procent is een e-mailaccount gehackt en bij 0,3 procent van de respondenten hackte de dader de computer of veranderde de dader een website of profiel als modus operandi van stalking en/of identiteitsdiefstal.

Hacken, risicogroepen

Om te weten te komen welke internetgebruikers een grotere kans lopen om gehackt te worden, voerden we een bivariate analyse uit (tabel 5.4).

Tabel 5.4: slachtofferschap hacken naar achtergrondkenmerken (gewogen, bivariaat)

	Defacing	**Hacken PC**	**Hacken e-mail**	**Hacken als M.O.**	**Totaal hacken**
Geen opleiding	1,2	1,8	1,3	0,0	2,9
Basisonderwijs	3,3	1,1	5,0	0,2	7,8
LBO	0,1	0,4	1,9	0,2	2,1
VMBO/MAVO	2,0	1,0	2,1	0,6	4,0
HAVO/VWO	2,4	1,1	4,4	0,5	6,7
MBO	1,3	0,4	2,8	0,1	3,9
HBO	1,5	0,6	2,6	0,3	3,7
WO	0,9	0,5	3,3	0,1	4,5
$\chi^2(7)$	*33,53***	*13,24*	*23,99***	*9,41*	*42,50***
15-24	4,7	1,3	5,9	0,7	10,1
25-34	1,7	0,7	4,9	0,3	5,9
35-44	0,7	0,6	1,8	0,2	2,8
45-54	1,0	0,6	1,6	0,3	2,5
55-64	0,6	0,6	1,9	0,4	2,6
65+	0,2	0,3	1,2	0,0	1,4
$\chi^2(5)$	*140,11***	*11,98**	*105,91***	*11,05*	*195,60***
<12 uur betaald werk p.w.	1,9	0,6	2,5	0,4	4,1
12+ uur betaald werk p.w.	1,3	0,7	3,1	0,3	4,3
$\chi^2(1)$	*5,36**	*0,52*	*2,27*	*0,53*	*0,26*
Geen partner	2,3	0,7	3,9	0,4	5,9
Partner	0,7	0,6	1,8	0,2	2,5
$\chi^2(1)$	*39,93***	*0,21*	*36,32***	*3,15*	*68,74***
Autochtoon	1,3	0,6	2,8	0,3	4,0
1e generatie	2,4	1,3	2,6	0,0	4,7
2e generatie, 1 ouder	1,6	0,8	4,1	0,6	6,0
2e generatie, beide ouders	3,2	1,2	4,1	0,0	5,9
$\chi^2(3)$	*12,48***	*8,83**	*4,55*	*5,47*	*7,07*
Man	1,5	0,8	2,8	0,2	4,2
Vrouw	1,5	0,6	2,9	0,4	4,3
$\chi^2(1)$	*0,98*	*0,99*	*0,08*	*3,33*	*0,11*
Totaal	**1,5**	**0,7**	**2,9**	**0,3**	**4,3**

* p<0.05, ** p<.0.01

Hieruit blijkt (kolom 'totaal hacken') dat internetters zonder partner eerder slachtoffer worden van hacken dan internetters met partner. Dan is er net als bij het opmerken van malware nog een verschil tussen de verschillende opleidingsniveaus en tussen de verschillende

leeftijdscategorieën. Tabel 5.4 wijst er op dat vooral internetters in de leeftijdscategorie van 15-24 jaar slachtoffer worden van hacken evenals internetters die als hoogst genoten opleiding het basisonderwijs hebben. Internetters in de leeftijdgroep 15-24 jaar worden naar verhouding vaak slachtoffer van hacken en dat zijn vanwege die leeftijd ook de personen die nog geen hogere opleiding hebben afgerond en niet in een huishouden samenleven met een partner.

Hacken, conclusies

Van alle internetters wordt 4,3 procent slachtoffer van hacken. Het hacken van een e-mailaccount komt het vaakst voor. Internetters zonder partner worden eerder slachtoffer van hacken dan internetters met partner. Verder wijzen de bevindingen er op dat vooral internetters in de leeftijdscategorie van 15-24 jaar slachtoffer worden van hacken evenals internetters die als hoogst genoten opleiding het basisonderwijs hebben.

6 Financiële delicten

6.1 Fraude via veiling- en verkoopsites

6.1.1 Betaald maar niet geleverd

Van alle internetgebruikers die aan het onderzoek mee hebben gedaan, heeft 73,2 procent in de afgelopen twaalf maanden minstens één aankoop gedaan via internet. Voor de producten wordt door bijna 80 procent betaald met iDEAL, bijna de helft betaalt door geld over te maken via internetbankieren en ruim een derde betaalt met creditcard. Ruim 6 procent betaalt (ook) contant (tabel 6.1).

Tabel 6.1: manier waarop wordt betaald voor producten die via internet worden gekocht (ongewogen, meerdere antwoorden mogelijk)

	Aantal	**% van kopers**
iDEAL	5.295	79,3
Internetbankieren	3.323	49,8
Creditcard via internet	2.342	35,1
PayPal	995	14,9
Offline via de bank (acceptgiro/overschrijven)	977	14,6
Automatische machtiging	840	12,6
Contant	405	6,1
Anders	68	1,0
Weet niet/wil niet zeggen	46	0,7

Betaald maar niet geleverd, prevalentie

We legden de groep 'kopers' de volgende vraag voor:

> Heeft u een product of een dienst via internet gekocht en tenminste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is, omdat de verkoper u heeft opgelicht?

Van de kopers heeft 3,1 procent in de twaalf maanden voorafgaande aan het onderzoek wel eens betaald voor een product dat nooit geleverd werd. Dit komt overeen met 2,4 procent van alle internetgebruikers die zijn ondervraagd. Met een betrouwbaarheid van 95 procent wordt tussen 2,1 en 2,7 procent van de internetters jaarlijks slachtoffer van deze vorm van fraude. Dit percentage komt overeen met de uit het LISS-panel afkomstige bevinding van Van Wilsem (2010b), dat 2,5 procent van de Nederlandse internetgebruikers in 2007 op deze

manier was opgelicht. Van de slachtoffers van deze vorm van fraude werd 11,4 procent twee keer en nog eens 4,0 procent drie keer slachtoffer in de afgelopen twaalf maanden.

Betaald maar niet geleverd, modus operandi

In 37,7 procent van de gevallen werd de fraude gepleegd met consumentenartikelen, in 26,5 procent van de gevallen met elektronica. Verder werd er veel gefraudeerd met dvd's, films, boeken, games, speelgoed, verzamelitems en vakanties.

Het contact met de fraudeur kwam in 45,6 procent van de gevallen tot stand via een online handelsite waar particulieren onderling kopen en verkopen, in 23,0 procent via een (geregistreerde) webwinkel en in 21,6 procent op een andere manier.

In 19,2 procent van de gevallen (n=34) verliep het contact met de verkoper via het buitenland: acht keer via China, zeven keer via de VS, vijf keer via Duitsland, drie keer via België, drie keer via Engeland en nog een aantal landen allemaal één keer. Leukfeldt e.a. (2010) vonden op basis van politiedossiers dat bij e-fraude in 14,5 procent van de gevallen de dader opereerde vanuit het buitenland.

Betaald maar niet geleverd, materiële schade

Van de slachtoffers heeft 85,3 procent financiële schade geleden. Van de 29 slachtoffers die geen financiële schade hebben ondervonden van de fraude geeft bijna de helft (dertien) aan dat zij het geld uiteindelijk terug hebben gekregen van de verkoper. Hoe de anderen (zestien) het geld hebben teruggekregen is niet bekend.

In tabel 6.2 valt te lezen dat van de mensen die een schadebedrag konden noemen, bijna driekwart maximaal 100 euro schade had en dat 5,2 procent van de slachtoffers meer dan 500 euro schade had.

Betaald maar niet geleverd, risicogroepen

Om te weten te komen welke internetgebruikers een grotere kans lopen om slachtoffer te worden van deze fraudevorm, voerden we een bivariate analyse uit (tabel 6.3). Hieruit blijkt (kolom drie) dat internetters zonder partner eerder slachtoffer worden dan internetters met partner, en dat internetters met twaalf uur of meer betaald werk eerder slachtoffer worden dan internetters met minder of geen betaald werk. Dan is er net als bij malware en hacken nog een verschil tussen de verschillende opleidingsniveaus en tussen de verschillende leeftijdscategorieën. Tabel 6.3 wijst er op dat internetters van 55 jaar en ouder relatief weinig slachtoffer worden. Bij opleidingsniveau wijzen de bevindingen niet zo duidelijk in een

bepaalde richting. Het lijkt er op dat hoger opgeleiden vaker slachtoffer worden van fraude ('betaald maar niet geleverd') met uitzondering van WO'ers die juist minder vaak slachtoffer worden dan alle andere internetters, inclusief HBO'ers.

Tabel 6.2: schade door marktplaatsfraude; gekocht maar niet geleverd (ongewogen)

Euro	**Aantal**	**% van slachtoffers (n=204)**	**% van bekende schade**	**% van internetters (n=xx)**
Geen/wel schade				
Geen schade	29	14,2		
Onbekend	1	0,5		
Schade	174	85,3		xx
Omvang schade				
Onbekend				0,0
1 - 100			74,1	1,6
101 – 200			16,1	0,4
201 – 500			4,6	0,1
501 - 1000			2,9	0,1
1001 of meer			2,3	0,0

Betaald maar niet geleverd, actie van het slachtoffer

Van de 204 slachtoffers ondernam 11,3 procent niets naar aanleiding van de oplichting (tabel 6.4). Het merendeel van de slachtoffers probeerde zijn of haar geld terug te krijgen. Manieren waarop slachtoffers proberen geld terug te krijgen zijn het blijven benaderen van de verkoper (56,4%), via de eigen bank of de bank van de oplichter (respectievelijk 19,6 en 5,9%). Ook zocht 36,8 procent van de slachtoffers na de oplichting informatie over de oplichter via internet. 19,6 procent van de slachtoffers nam contact op met de politie (zie verder hfst 7).

Andere acties van slachtoffers zijn het op andere wijze terug proberen te krijgen van geld, bijvoorbeeld via PayPal of een creditkaartmaatschappij, of proberen te voorkomen dat de oplichter meer slachtoffers maakt. Dat laatste bijvoorbeeld door een advertentie met waarschuwende tekst over de oplichter op de verkoopsite te zetten, hoge biedingen te doen op de advertenties van de oplichter of de oplichter te beschrijven op websites als opgelicht.nl.

Tabel 6.3: Slachtofferschap fraude via veiling- of verkoopsite naar achtergrondkenmerken (bivariaat)

	Aankopen gedaan via internet (% internetgebruikers, gewogen)	**Slachtoffer fraude via veiling- of verkoopsite niet geleverd (% internetgebruikers, gewogen)**	**Slachtoffer fraude via veiling- of verkoopsite niet geleverd (% kopers, ongewogen)**
Geen opleiding	37,1	1,8	4,8
Basisonderwijs	49,5	1,1	2,9
LBO	54,9	2,3	3,7
VMBO/MAVO	60,6	1,8	2,6
HAVO/VWO	75,1	2,6	3,2
MBO	76,6	2,9	3,7
HBO	83,3	3,0	3,2
WO	89,0	1,0	1,3
$\chi^2(7)$	*808,65***	*19,98***	*13,03*
15-24	71,2	2,8	4,0
25-34	85,2	3,2	3,6
35-44	83,2	2,9	3,2
45-54	76,2	2,8	3,6
55-64	66,2	1,5	2,2
65+	47,2	0,5	1,0
$\chi^2(5)$	*629,38***	*30,59***	*17,32***
<12 uur betaald werk p.w.	60,0	1,8	2,9
12+ uur betaald werk p.w.	80,7	2,7	3,1
$\chi^2(1)$	*461,95***	*7,85***	*0,42*
Geen partner*	73,1	2,8	3,7
Partner	73,3	2,0	2,6
$\chi^2(1)$	*0,08*	*6,81***	*7,58***
Autochtoon	75,0	2,4	3,0
1^e generatie	62,3	2,5	3,5
2^e generatie, 1 ouder	73,9	2,2	3,2
2^e generatie, beide ouders	62,1	2,0	3,9
$\chi^2(3)$	*88,40***	*0,35*	*0,55*
Man	74,6	2,5	3,1
Vrouw	71,1	2,3	3,0
$\chi^2(1)$	*10,43***	*0,18*	*0,09*
Totaal	**73,2**	**2,4**	**3,1**

* p<0.05, ** p<.0.01

Tabel 6.4: actie van slachtoffers fraude via veiling- of verkoopsite, betaald maar niet geleverd (ongewogen)

	Aantal	**% van slachtoffers (n=204)**
Geprobeerd geld terug te krijgen door de verkoper te blijven benaderen	115	56,4
Melding gemaakt bij de online handelsite of webwinkel	80	39,2
Op internet gezocht naar informatie over de verkoper	75	36,8
Geprobeerd geld terug te krijgen via mijn bank	40	19,6
Contact opgenomen met de politie	40	19,6
Andere actie	26	12,7
Niets	23	11,3
Geprobeerd geld terug te krijgen via de bank van de verkoper	12	5,9

Betaald maar niet geleverd, conclusies

2,4 procent van alle internetgebruikers werd slachtoffer van e-fraude in de vorm van 'wel betaald maar niet gekregen'. De bevindingen wijzen er op dat internetters van 55 jaar en ouder relatief weinig slachtoffer worden en dat hoger opgeleiden vaker slachtoffer worden, met uitzondering van WO'ers.

In 19,2 procent van alle gevallen liep het contact met de verkoper via het buitenland. Met andere woorden: in een vijfde van al deze zaken opereert de dader vanuit of via het buitenland. Als de politie meer aangiften van dit soort criminaliteit krijgt, zal haar werkaanbod dus verder internationaliseren.

6.1.2 Verkocht maar geen betaling ontvangen

Van alle internetters heeft 32,8 procent in de twaalf maanden voorafgaand aan het onderzoek een product of dienst verkocht via internet. We legden deze internetters de volgende stelling voor:

Heeft u als particulier een product of dienst verkocht via internet, maar geen geld ontvangen van de koper terwijl u het product of de dienst wel geleverd heeft, omdat de koper u heeft opgelicht?

Verkocht maar geen betaling ontvangen, prevalentie

Van de internetters die een product hebben verkocht, heeft 1,0 procent in de afgelopen twaalf maanden een product of dienst geleverd waarvoor nooit een betaling is ontvangen. Dit komt overeen met 0,3 procent van alle internetgebruikers. Met een betrouwbaarheid van 95 procent ontvangt jaarlijks tussen 0,2 en 0,4 procent van de internetters geen geld voor een verkocht product of dienst.

Van de slachtoffers werd 8,0 procent twee keer slachtoffer van deze vorm van fraude in de afgelopen twaalf maanden (2 van de 25). Aangezien het aantal slachtoffers van deze vorm van fraude in dit onderzoek klein is (n=25), gebruiken we in de rest van dit hoofdstuk ongewogen aantallen in plaats van percentages. De resultaten moeten met enige voorzichtigheid geïnterpreteerd worden.

Verkocht maar geen betaling ontvangen, modus operandi

De producten waarmee gefraudeerd wordt, zijn zeer uiteenlopend; acht keer ging het om consumentenartikelen, vier keer om elektronica, twee keer om diensten en verder om een paardendeken, speelgoed, een timesharehuisje, etc.

In zeventien van de 25 gevallen kwam het contact tot stand doordat de fraudeur reageerde op een advertentie van het slachtoffer, vier keer reageerde het slachtoffer op een advertentie van de oplichter en vier keer kwam het contact op een andere manier tot stand, namelijk via de website van het slachtoffer, e-mail en telefoon.

In zeven van de 25 gevallen bevond de koper zich in het buitenland. Twee keer in Italië, een keer in China, een keer in België, een keer in Spanje, een keer in Engeland en een keer is onbekend in welk land.

Verkocht maar geen betaling ontvangen, materiële schade

Van de 25 slachtoffers weten 22 de omvang van de schade te noemen. De meesten hebben schades tot 100 euro, een klein aantal heeft schades van meer dan 1.000 euro (tabel 6.5).

Tabel 6.5: schade door fraude via veiling- of verkoopsite; verkocht maar geen betaling ontvangen (ongewogen)

Euro	**Aantal**
Geen/wel schade	
Geen schade	0
Onbekend	3
Schade	22
Omvang schade	
1 - 100	15
101 – 200	1
201 – 500	4
501 - 1000	0
1001 of meer	2

Verkocht maar geen betaling ontvangen, actie van het slachtoffer

Van de 25 slachtoffers proberen er vijftien het geld terug te krijgen (tabel 6.6). Dertien slachtoffers deden dat door het blijven benaderen van de koper, twee slachtoffers probeerden geld terug te krijgen via de bank van de oplichter. Verder maakten zes slachtoffers een melding bij de handelssite of webwinkel waar de oplichting plaatsvond en zochten zeven slachtoffers naar informatie over de koper. Vier slachtoffers deden helemaal niets en twee namen contact op met de politie. Bij 'andere actie' geven slachtoffers aan dat de oplichter niet reageerde op contactverzoeken van het slachtoffer.

Tabel 6.6: actie van slachtoffer (n=25)

Actie	**Aantal**
Niets	4
Melding bij de betreffende handelssite of webwinkel	6
Geprobeerd geld terug te krijgen door de verkoper te benaderen	13
Geprobeerd geld terug te krijgen via mijn bank	0
Geprobeerd geld terug te krijgen via de bank van de verkoper	2
Op internet gezocht naar informatie over de verkoper	7
Contact opgenomen met de politie	2
Andere actie	4

Verkocht maar geen betaling ontvangen, conclusies

Van alle internetters heeft 32,8 procent in de twaalf maanden voorafgaand aan het onderzoek een product of dienst verkocht via internet, waarvan 1,0 procent minstens eenmaal geen

betaling ontving voor een opgestuurd product of geleverde dienst. Dit komt overeen met 0,3 procent van de internetgebruikers.

Vijftien van de 25 slachtoffers leden minder dan 100 euro schade, twee slachtoffers namen contact op met de politie.

6.2 Identiteitsfraude

In de vragenlijst gebruikten we de volgende omschrijving:

> 'Identiteitsfraude houdt in dat iemand zonder uw toestemming uw persoonlijke of financiële gegevens gebruikt om er zelf geld aan te verdienen. Iemand pint bijvoorbeeld van uw rekening, koopt producten op uw naam of vraagt officiële documenten aan op uw naam. Meestal is identiteitsfraude een gevolg van diefstal van identiteitsgegevens, maar het kan ook zijn dat u zelf de identiteitsgegevens heeft verstrekt.'

Eerst is gevraagd of iemand slachtoffer is geworden van identiteitsfraude, dus los van de vraag of dat online of offline was. Van alle ondervraagde internetters is 0,9 procent slachtoffer geworden van identiteitsfraude. Vervolgens stelden we vast of ICT van wezenlijk belang was voor de uitvoering van het delict, en we dus kunnen spreken van cybercrime. Dat deden we door na te gaan hoe de fraudeur de identiteitsgegevens heeft bemachtigd en door na te gaan of de fraudeur internet heeft gebruikt om de fraude te plegen. We spreken hierna van de cybercrime identiteitsfraude (kortweg 'identiteitsfraude') indien:

- de fraudeur de identiteitsgegevens met ICT heeft bemachtigd (identiteitsdiefstal door middel van bijvoorbeeld skimming of phishing), en/of:
- de fraudeur internet heeft gebruikt om de fraude te plegen.

In totaal zijn van de internetters die mee hebben gedaan aan het onderzoek 18 internetters alleen slachtoffer geworden van identiteitsdiefstal, 22 alleen van identiteitsfraude en 23 van zowel identiteitsdiefstal als identiteitsfraude. Er zijn dus in totaal 63 slachtoffers van identiteitsfraude waaronder 41 slachtoffers van identiteitsdiefstal. De rest van dit hoofdstuk gaat over de 63 internetters die slachtoffer zijn geworden van één of beide hierboven beschreven delicten.

Van alle respondenten die internet gebruiken, geeft 0,8 procent (n=63) aan dat zij in de twaalf maanden voorafgaande aan het onderzoek weten dat zij slachtoffer zijn geworden van identiteitsfraude. Met 95 procent betrouwbaarheid is tussen 0,6 en 1,0 procent van de internetters hiervan slachtoffer geworden. Het slachtofferpercentage ligt in werkelijkheid

waarschijnlijk hoger omdat respondenten niet altijd weten of hun identiteitsgegevens *via ICT* zijn bemachtigd en omdat ze niet altijd weten of de fraude *via internet* is gepleegd.

Hierna kijken we eerst apart naar de 41 slachtoffers van identiteitsfraude die aangaven dat de dader de identiteitsgegevens met ICT heeft bemachtigd (kortweg: 'identiteitsdiefstal'). Daarna presenteren we een analyse over alle 63 slachtoffers van identiteitsfraude.

Identiteitsdiefstal, prevalentie

Aan de respondenten die aangaven slachtoffer te zijn geworden van identiteitsfraude is gevraagd op welke manier de fraudeur de identiteitsgegevens heeft verkregen. Vervolgens zijn respondenten waarbij de identiteit gestolen was met behulp van ICT, aangemerkt als slachtoffers van identiteitsdiefstal. Het blijkt dat in de twaalf maanden voorafgaande aan het onderzoek van 0,5 procent van de internetters slachtoffer is geworden van identiteitsdiefstal (n=41). Met 95 procent betrouwbaarheid is tussen 0,4 en 0,6 procent van de internetters afgelopen jaar slachtoffer geworden van identiteitsdiefstal.

Identiteitsdiefstal, modus operandi

Aan respondenten zijn zeven manieren voorgelegd waarop ICT zou kunnen zijn gebruikt bij het plegen van de identiteitsdiefstal (tabel 6.7). Er waren meerdere antwoorden mogelijk, een vijfde van de respondenten heeft meer dan één antwoord aangekruist waaruit blijkt dat het slachtoffer niet altijd zeker weet hoe de identiteitsdiefstal is gepleegd. Skimming is wat volgens de slachtoffers het meest voorkomt als modus operandi voor het verkrijgen van de identiteitsgegevens (31,7%). Verder geeft 31,7 procent van de slachtoffers aan gegevens zelf te hebben ingevuld op een website voor een loterij of enquête en heeft 19,5 procent gegevens ingevuld op een gehackte website.

Van de 41 slachtoffers van identiteitsdiefstal, weten (zeven) of vermoeden (vier) slachtoffers (26,8%) wie de dader is. In vijf gevallen is het een bekende, in drie gevallen iemand die men niet persoonlijk kent, in twee gevallen een ex-partner en in één geval iemand van het werk.

Identiteitsfraude, materiële schade

We kijken nu naar alle 63 slachtoffers van identiteitsfraude. Er is materiële schade geleden door 60,3 procent van de slachtoffers, voordat een deel van de schade eventueel was vergoed. De bedragen lopen uiteen van 1 tot 112.500 euro. Meer dan een derde van de slachtoffers met schade heeft meer dan duizend euro schade geleden (tabel 6.8).

Tabel 6.7: manier waarop de identiteitsgegevens zijn gestolen (ongewogen)

	Aantal	**% van slachtoffers**
Skimming	13	31,7
Gegevens ingevuld voor loterij, enquête etc	11	26,8
Hacking en/of virus	8	19,5
Gegevens ingevuld op gehackte website	8	19,5
Persoonlijke gegevens zijn op een website geplaatst	6	14,6
Gegevens verstrekt n.a.v. verzoek via e-mail	2	4,9
Phishing	1	2,4

Tabel 6.8: schade door identiteitsfraude (ongewogen)

Euro	**Aantal**	**% schade**
Geen/wel schade		
Geen schade	25	39,7
Schade	38	60,3
Omvang schade		
1 - 100	6	15,8
101 – 200	4	10,5
201 – 500	6	15,8
501 - 1000	8	21,1
1001 of meer	14	36,8

Van tien van de 38 slachtoffers met schade (26,3%), is de schade niet vergoed. Vier van die tien keer betrof de schade 35 euro of minder. De andere schades die niet vergoed zijn, waren schades van 250, 800, 3.000, 5.000, 10.000 en 20.000 euro. In negentien gevallen is de schade vergoed door de bank. Wie de andere negen schades heeft vergoed, is niet gevraagd in de vragenlijst en dus onbekend.

Identiteitsfraude, risicogroepen

Het blijkt dat internetters met 12 uur of meer betaald werk meer kans lopen om slachtoffer te worden van identiteitsfraude dan andere internetters (tabel 6.9).

Tabel 6.9: slachtofferschap id-fraude naar achtergrondkenmerken (gewogen, bivariaat)

	Slachtoffer identiteitsfraude (% internetgebruikers)
Geen opleiding	0,0
Basisonderwijs	0,2
LBO	0,6
VMBO/MAVO	0,7
HAVO/VWO	0,9
MBO	0,7
HBO	0,9
WO	1,0
$\chi^2(7)$	*5,30*
15-24	0,5
25-34	0,9
35-44	1,0
45-54	0,6
55-64	0,8
65+	0,7
$\chi^2(5)$	*3,63*
< 12 uur betaald werk p.w.	0,4
12+ uur betaald werk p.w.	0,9
$\chi^2(1)$	*6,71***
Geen partner	0,9
Partner	0,6
$\chi^2(1)$	*2,23*
Autochtoon	0,7
1e generatie	0,8
2e generatie, 1 ouder	1,4
2e generatie, beide ouders	0,8
$\chi^2(3)$	*3,04*
Man	0,9
Vrouw	0,6
$\chi^2(1)$	*3,15*
Totaal	**0,8**

* p<0.05, ** p<.0.01

Identiteitsfraude, actie van het slachtoffer

Uit tabel 6.10 blijkt dat naar aanleiding van de slachtofferschap van identiteitsdiefstal en/of –fraude 33,3 procent probeerde het geld terug te krijgen via de bank, 15,6 procent nam contact op met de politie en 11,1 procent deed niets.

In de categorie ‘andere actie’ beschrijven de slachtoffers verschillende acties. Twaalf slachtoffers hebben contact opgenomen met het medium waarmee of waarop de

identiteitsfraude werd gepleegd. Vier slachtoffers werden door het bedrijf waarbij was gefraudeerd ingelicht. Drie slachtoffers wijzigden inloggegevens zodat de oplichter daar geen gebruik meer van kan maken. Drie slachtoffers probeerden de dader zelf te benaderen.

Tabel 6.10: actie van slachtoffer (n=63)

Actie	**Aantal**	**%**
Andere actie	34	54,0
Geprobeerd geld terug te krijgen via de bank	21	33,3
Contact opgenomen met de politie	12	15,6
Niets	7	11,1
Geprobeerd geld terug te krijgen via de verzekering	2	3,2
Gewend tot het meldpunt identiteitsfraude	1	1,6
Gewend tot website / vereniging van gedupeerden	0	0,0

Identiteitsfraude, conclusies

Van 0,5 procent van de internetters zijn identiteitsgegevens gestolen met behulp van ICT. In totaal is 0,9 procent van de internetters slachtoffer geworden van identiteitsfraude. Volgens de respondenten zijn hun identiteitsgegevens het vaakst via skimming bemachtigd. Ook vulden respondenten hun gegevens vaak zelf in op een website of een online formulier.

Zes op de tien slachtoffers leden financiële schade, waarvan ruim een derde duizend euro of meer. Tien van de 63 slachtoffers leden schade die niet werd vergoed. Een derde van de slachtoffers nam naar aanleiding van het incident contact op met hun bank. Twaalf van de 63 slachtoffers (19,0%) namen (ook) contact op met de politie.

6.3 Voorschotfraude

We hanteerden in de vragenlijst de volgende definities:

‘Voorschotfraude is een vorm van internetfraude. Kern van voorschotfraude is dat slachtoffers een voorschot moeten betalen om een groot bedrag te ontvangen. Het gaat dan bijvoorbeeld om een zogenaamde erfenis, investering of loterij.’

Een specifieke vorm van voorschotfraude is dat meestal buitenlandse oplichters via contact- of datingsites het vertrouwen van mensen winnen. Vervolgens vragen zij geld voor een ontmoeting of om zogenaamde persoonlijke problemen van zichzelf of hun familie op te lossen.

Vervolgens is gevraagd of de respondent is opgelicht door geld over te maken. Van de 9.163 ondervraagde internetters, zijn achttien internetters slachtoffer geworden van voorschotfraude (vier maal via een datingsite, veertien maal op een andere manier), dit komt overeen met 0,2 procent van de ondervraagde internetters. Bij voorschotfraude hebben we aangemerkt dat iemand pas slachtoffer is als er ook daadwerkelijk schade is geleden.

Voorschotfraude, materiële schade

De schades lopen uiteen van 7 tot 8.000 euro. In meer dan de helft van de gevallen is de schade hoger dan 500 euro (tabel 6.11).

Tabel 6.11: schade door voorschotfraude (ongewogen)

Euro	**Aantal**
1 - 100	11
101 – 200	2
201 – 500	1
501 - 1000	0
1001 of meer	4

Voorschotfraude, actie van het slachtoffer

Zes slachtoffers bleven de oplichter(s) benaderen om zo hun geld terug te krijgen. Vier slachtoffers deden niets. Eén slachtoffer nam contact op met de politie (tabel 6.12).

Tabel 6.12: actie van slachtoffer (n=18)

Actie	**Aantal**
Niets	4
Op internet gezocht naar informatie over de fraude	4
Contact met lotgenoten gezocht	2
Fraudeur blijven benaderen	6
Rechtshulp gezocht	2
Contact opgenomen met de politie	1
Andere actie	3

Voorschotfraude, conclusies

Voorschotfraude komt niet vaak voor. Slechts 0,2 procent van de ondervraagde internetters werd hiervan slachtoffer. Dat zijn in totaal achttien slachtoffers. Door het geringe aantal slachtoffers is het niet mogelijk om generaliserende conclusies te trekken.

7 Delicten in de persoonlijke sfeer

7.1 Stalking

Stalking, prevalentie

Om te meten of een respondent slachtoffer is geworden van stalking, gebruikten we onderstaande definitie:

Stalking (belaging) is het bewust herhaaldelijk lastigvallen en achtervolgen van een persoon met de bedoeling die persoon iets te laten doen óf hem/haar bang te maken. Stalking kan plaatsvinden door steeds dezelfde handeling of verschillende handelingen, zoals volgen en bespieden, bedreigingen uiten, ongewenst opbellen of het beschadigen van (digitale) eigendommen.

Vervolgens is gevraagd of de respondent hiervan slachtoffer is geworden in de afgelopen twaalf maanden. Het blijkt dat van alle internetters 1,3 procent slachtoffer werd van stalking in de twaalf maanden voorafgaande aan het onderzoek. In 82,9 procent van de gevallen werd (ook) ICT gebruikt om te stalken. Dit betekent dat in de twaalf maanden voorafgaande aan het onderzoek 1,1 procent van de internettende respondenten slachtoffer werd van *cyber*stalking (n=92). Met een zekerheid van 95 procent wordt tussen 0,9 en 1,3 procent van de internetters jaarlijks slachtoffer van cyberstalking.

Stalking, modus operandi

We hebben de slachtoffers gevraagd welke middelen de stalker(s) gebruikte(n) om te stalken. Het slachtoffer kon daarbij meerdere antwoorden aankruisen. De stalker gebruikt gemiddeld meer dan twee van de genoemde middelen (tabel 7.1). Het ongewenst sturen van e-mailberichten (52,2%), het sturen van berichten via de mobiele telefoon (46,7%) en het ongewenst sturen van chatberichten (44,6%) worden het meest ingezet.

Vervolgens is gevraagd of het slachtoffer weet wie de stalker was (tabel 7.2). In 62,0 procent van de gevallen weet het slachtoffer wie de dader is. Als het slachtoffer ‘andere bekende’ aankruiste is niet gevraagd hoe het slachtoffer de dader kende. Het is in die gevallen dan ook niet bekend of de dader en het slachtoffer elkaar in real life kenden of uitsluitend via internet.

Tabel 7.1: middelen van cyberstalkers (ongewogen)

Middelen van cyberstalkers	**Aantal**	**% slachtoffers**
Ongewenste e-mail	48	52,2
Bericht via mobiele telefoon	43	46,7
Ongewenst chatbericht	41	44,6
Anders via internet	28	30,4
Gênante foto's, verhalen via internet	19	20,7
Ingebroken in e-mail	12	13,0
Veranderingen profiel, webpagina's	8	8,7
Ingebroken in computer	5	5,4
Totaal middelen	**204**	
Totaal aantal slachtoffers	**92**	**100**

Tabel 7.2: relatie dader-slachtoffer cyberstalking (ongewogen)

Relatie dader-slachtoffer	**Aantal**	**% slachtoffers**
Onbekende dader	35	38,0
Ex-partner	18	19,6
Collega	7	7,6
Buurtgenoot	6	6,5
Familielid	4	4,3
Andere bekende	25	27,2
Totaal	**92**	**100**

Stalking, materiële schade

Tien van de 92 slachtoffers (10,9%) hebben materiële schade geleden door de stalking, vier slachtoffers weten daarbij ook de hoogte van de schade te noemen: 20, 50, 1.000 en 15.000 euro.

Stalking, risicogroepen

Om te weten te komen welke internetgebruikers slachtoffer worden van stalking, voeren we een bivariate analyse uit (tabel 5.3). Hieruit blijkt dat internetters zonder partner eerder slachtoffer worden dan internetters met partner. Dan is er (evenals bij malware, hacken en e-fraude) nog een verschil tussen de verschillende opleidingsniveaus en tussen de verschillende leeftijdscategorieën. Tabel 7.3 wijst er op dat internetters in de leeftijd van 15-24 jaar en internetters die alleen (nog) het basisonderwijs hebben afgerond vaker slachtoffer zijn van stalking dan andere internetters.

Tabel 7.3: slachtofferschap cyberstalking naar achtergrondkenmerken (gewogen, bivariaat)

	Slachtoffer cyberstalking (% internetgebruikers)
Geen opleiding	0,0
Basisonderwijs	2,2
LBO	0,3
VMBO/MAVO	1,8
HAVO/VWO	1,2
MBO	1,3
HBO	0,9
WO	0,5
$\chi^2(7)$	*21,51***
15-24	2,5
25-34	0,9
35-44	0,8
45-54	1,1
55-64	0,8
65+	0,5
$\chi^2(5)$	*35,96***
<12 uur betaald werk p.w.	1,4
12+ uur betaald werk p.w.	1,0
$\chi^2(1)$	*3,50*
Geen partner	1,6
Partner	0,7
$\chi^2(1)$	*16,29***
Autochtoon	1,1
1e generatie	0,9
2e generatie, 1 ouder	1,6
2e generatie, beide ouders	1,6
$\chi^2(3)$	*2,01*
Man	1,1
Vrouw	1,1
$\chi^2(1)$	*0,01*
Totaal	**1,1**

*p<0.05, **p<0.01

Stalking, actie van het slachtoffer

Het merendeel van de slachtoffers onderneemt geen actie naar aanleiding van de stalking (58,7%). Bijna eenderde (30,4%) nam contact op met de politie. Andere slachtoffers namen contact op met de huisarts (3,3%), slachtofferhulp (2,2%) of met het Riagg (1,1%) (tabel 7.4).

Daarnaast geeft 17,4 procent van de slachtoffers aan met andere instanties contact te hebben opgenomen. Meest genoemde instanties zijn KPN (3,3%), school (3,3%) of Hyves

(2,2%). Verder namen slachtoffers contact op met allerlei verschillende organisatie zoals Tros Radar, de burgemeester en een woningbouwcoöperatie.

Tabel 7.4: actie van slachtoffer (n=92)

Actie	**Aantal**	**%**
Niets	54	58,7
Contact opgenomen met de politie	28	30,4
Contact opgenomen met de huisarts	3	3,3
Contact opgenomen met Slachtofferhulp	2	2,2
Contact opgenomen met het Riagg	1	1,1
Contact opgenomen met Stichting Anti Stalking	0	0,0
Contact opgenomen met Vereniging van lotgenoten	0	0,0
Contact opgenomen met Schadefonds Geweldsmisdrijven	0	0,0
Contact opgenomen met Stichting M. (Meld Misdaad Anoniem)	0	0,0
Contact opgenomen met een andere instantie	16	17,4

Stalking, conclusies

1,1 procent van de internetters wordt jaarlijks slachtoffer van *cyber*stalking. Slachtoffers zijn jonge internetters tussen 15 en 25 jaar, internetters met als hoogst genoten opleiding het basisonderwijs, en internetters zonder partner. De dader gebruikt uiteenlopende manieren om het slachtoffer te stalken, waarbij e-mail, mobiele telefoon en chatprogramma's het meest gebruikt worden. In meer dan de helft van de gevallen is de dader een bekende van het slachtoffer. Bijna één op de drie slachtoffers stapt naar de politie.

7.2 Bedreiging

Bedreiging, prevalentie

Om te meten of een respondent slachtoffer is geworden van bedreiging is eerst onderstaande definitie gegeven:

> Bedreiging is het dreigen met - in de meeste gevallen - fysiek geweld of de dood tegen een persoon of zijn/haar eigendommen.

Vervolgens is gevraagd of de respondent hiervan slachtoffer is geworden in de afgelopen twaalf maanden. Van alle internetters werd 1,2 procent slachtoffer van bedreiging, waarbij in 54,8 procent van de gevallen (ook) gebruik werd gemaakt van internet om de bedreigingen te uiten. Dit betekent dat 0,7 procent van de ondervraagde internetters in de twaalf maanden voorafgaande aan het onderzoek slachtoffer werd van *cyber*bedreiging (n=54). Met een

betrouwbaarheid van 95 procent wordt tussen 0,5 en 0,9 procent van de internetters jaarlijks slachtoffer van cyberbedreiging. Van de 54 slachtoffers werden 40 slachtoffers (74,1%) vaker dan één keer bedreigd in de twaalf maanden voorafgaande aan het onderzoek. Het is niet bekend of dat meerdere keren door dezelfde dader was of door verschillende daders.

Bedreiging, modus operandi

We hebben de slachtoffers van cyberbedreiging gevraagd welke middelen de dader heeft ingezet om de bedreigingen te uiten. Het slachtoffer kon daarbij meerdere antwoorden aankruisen. Uit tabel 7.5 blijkt dat gemiddeld bijna twee middelen worden ingezet om de bedreigingen te uiten. Het blijkt dat alle genoemde middelen door ongeveer vier van de tien daders gebruikt worden om hun slachtoffer te bedreigen.

Tabel 7.5: middelen van cyberbedreiger (ongewogen)

Middel van cyberbedreiger	**Aantal**	**% slachtoffers**
Mobiele telefoon	24	44,4
Chatbericht	23	42,6
E-mail	21	38,9
Profielsite	21	38,9
Andere manier via internet	8	14,8
Totaal aantal slachtoffers	**54**	**100**

Vervolgens is gevraagd of het slachtoffer weet wie hem/haar bedreigd heeft. In 72,0 procent van de gevallen weet het slachtoffer wie de dader is. Als het slachtoffer ‘andere bekende’ aankruiste is niet gevraagd hoe het slachtoffer de dader kende. Het is dan ook niet bekend of de dader en het slachtoffer elkaar in real life kenden of uitsluitend via internet. Als het slachtoffer aangaf te weten wie hem/haar heeft bedreigd, konden meerdere antwoorden aangekruist worden; twee slachtoffers hebben dat ook gedaan (tabel 7.6).

Tabel 7.6: relatie dader-slachtoffer cyberbedreiging (ongewogen)

Relatie dader-slachtoffer	**Aantal**	**% slachtoffers**
Andere bekende	20	37,0
Onbekende dader	15	28,0
Ex-partner	10	18,5
Buurtgenoot	4	7,4
Collega	4	7,4
Familielid	2	3,7
Partner	1	1,9
Totaal aantal slachtoffers	**54**	**100**

Als laatste is gevraagd ‘Denkt u dat de oorzaak van de bedreiging gelegen is in het feit dat u tot een bepaalde groep behoort (bijvoorbeeld etnische minderheid, seksuele voorkeur of publieke functie zoals politieagent of politicus)?’ Twee derde (n=36) van de slachtoffers behoort naar eigen zeggen niet tot een dergelijke groep (tabel 7.7). Van de achttien slachtoffers die wel tot een dergelijke groep behoren zegt de helft (negen) dat de oorzaak inderdaad daarin gelegen is en nog eens vier zeggen dat dit misschien zo is.

Tabel 7.7: oorzaak cyberbedreiging (ongewogen)

	Aantal	**% slachtoffers**
Behoort niet tot een bepaalde groep	36	66,7
Tot een bepaalde groep behoren is niet de oorzaak	5	9,3
Tot een bepaalde groep behoren is misschien de oorzaak	4	7,4
Tot een bepaalde groep behoren is de oorzaak	9	16,7
Totaal	**54**	**100**

Bedreiging, materiële schade

Vier van de 54 slachtoffers hebben materiële schade geleden door de bedreiging, twee van hen wisten ook de hoogte van de schade te noemen: 1.000 en 12.000 euro.

Bedreiging, risicogroepen

Om te weten te komen welke internetgebruikers slachtoffer worden van bedreiging, voeren we een bivariate analyse uit. Uit tabel 7.8 valt af te leiden dat – vergelijkbaar met wat we eerder zagen bij malware, hacken, e-fraude en cyberstalking – vooral internetters tussen 15 en 24 jaar, internetters die alleen (nog) het basisonderwijs hebben afgerond, die minder dan 12 uur per week betaald werk verrichten en internetters zonder partner vaker slachtoffer worden van cyberbedreiging dan andere internetters.

Uit een onderzoek naar slachtofferschap van traditionele en cyberbedreiging door Van Wilsem (2011) onder ruim 6.000 huishoudens in Nederland bleek eveneens dat gemiddeld minder dan 1 procent van de internetters slachtoffer wordt van bedreiging, maar dat dit percentage onder internetters tot 25 jaar aanzienlijk hoger ligt, namelijk boven de 5 procent.

Tabel 7.8: slachtofferschap cyberbedreiging naar achtergrondkenmerken (gewogen, bivariaat)

	Slachtoffer cyberbedreiging (% internetgebruikers)
Geen opleiding	0,6
Basisonderwijs	1,7
LBO	0,4
VMBO/MAVO	1,1
HAVO/VWO	1,1
MBO	0,6
HBO	0,5
WO	0,2
$\chi^2(7)$	*18,80***
15-24	2,2
25-34	0,7
35-44	0,5
45-54	0,3
55-64	0,1
65+	0,2
$\chi^2(5)$	*63,50***
Geen of minder dan 12 uur betaald werk	1,0
12 uur per week of meer betaald werk	0,5
$\chi^2(1)$	*7,14**
Geen partner	1,0
Partner	0,4
$\chi^2(1)$	*10,48***
Autochtoon	0,7
1e generatie	0,8
2e generatie, 1 ouder	0,4
2e generatie, beide ouders	1,6
$\chi^2(4)$	*3,90*
Man	0,6
Vrouw	0,7
$\chi^2(1)$	*0,27*
Totaal	**0,7**

Bedreiging, actie van het slachtoffer

Er zijn 54 slachtoffers van bedreiging. 38,9 procent onderneemt geen actie naar aanleiding van dit delict (tabel 7.9) en 27,8 procent neemt contact op met de politie. Daarnaast geeft 37,0 procent van de slachtoffers aan een andere actie te hebben ondernomen. Meest genoemde acties zijn ‘de dader benaderen om zo de bedreigingen te laten stoppen’ (11,1%), ‘contact opnemen met de verantwoordelijke van het medium waarop de bedreiging werd geuit’ (9,3%)

en ‘contact opnemen met de school van de dader’ (5,6%). Andere slachtoffers ontliepen de verdachte, ‘lachten de dader uit’ of namen contact op met de ouders of met Jeugdzorg.

Tabel 7.9: actie van slachtoffer (n=54)

Actie	**Aantal**	**%**
Niets	21	38,9
Contact opgenomen met de politie	15	27,8
Andere actie	20	37,0
Totaal aantal slachtoffers	**54**	**100**

Bedreiging, conclusies

0,7 procent van de internetters is slachtoffer geworden van cyberbedreiging. Ongeveer drie kwart van deze respondenten is vaker dan één keer bedreigd. Eenzelfde percentage weet wie de dader van de bedreiging is. Mensen die worden bedreigd zijn meestal internetters tussen de 15 en 24 jaar, die alleen (nog) het basisonderwijs hebben afgerond, die minder dan 12 uur werk per week verrichten en die geen partner hebben. Dat is een patroon dat vergelijkbaar is met hetgeen we vonden bij malware, hacken, e-fraude en cyberstalking. Vier respondenten hebben financiële schade geleden als gevolg van de bedreiging.

7.3 Smaad, laster, belediging

Smaad, laster, belediging, prevalentie

*Cyber*smaad is het opzettelijk aantasten van iemands eer of goede naam door hem te beschuldigen van een bepaald feit (of dat nu waar is of niet) via ICT, met het doel aan dit feit bekendheid te geven. De aantasting kan mondeling, bij geschrift of bij afbeelding plaatsvinden. *Cyber*laster is het plegen van cybersmaad of cybersmaadschrift, terwijl de dader weet dat het feit waarvan hij het slachtoffer beschuldigt niet waar is. De grens tussen belediging, smaad en laster is vaak lastig te trekken. Gemeenschappelijk aan deze delicten is de opzettelijke aanranding van de eer of goede naam.

Om te meten of de respondent slachtoffer is geworden van smaad of laster via digitale middelen zijn de onderstaande stellingen voorgelegd waarop de respondent kon antwoorden met ‘ja’ of ‘nee’.

Iemand heeft zonder uw toestemming een gênante webpagina en/of gênant profiel (Hyves, Facebook, etc) over u gemaakt.
Iemand heeft zonder uw toestemming verhalen, roddels, filmpjes of foto's over u verspreid via e-mail of internet.

Van de internetters antwoordt 3,4 procent 'ja' op één of beide van bovenstaande stellingen (n=9.163). Met een betrouwbaarheid van 95 procent overkomt jaarlijks tussen 3,0 en 3,8 procent van de internetters minstens één van beide situaties. In de stellingen ontbreekt echter de vraag naar de opzettelijkheid van de dader, waardoor er niet per definitie sprake is van een delict.[36] In deze paragraaf spreken we dan ook niet van slachtofferschap. Wanneer een respondent 'ja' heeft geantwoord op één of beide stellingen, zeggen we in deze paragraaf dat de respondent is beledigd. Dit houdt dus in dat het om smaad, laster en/of belediging gaat.

Belediging, risicogroepen

Om te bepalen welke internetters vaker te maken krijgen met de verspreiding van beledigende teksten, filmpjes en/of foto's over henzelf voerden we een bivariate analyse uit (tabel 7.10). Uit deze analyse valt op te maken dat vooral internetters in de leeftijdsgroep van 15-24 jaar via internet worden beledigd. Het betreft ook vaak internetters die als hoogst afgeronde opleiding de basisschool of middelbare school hebben, geen partner hebben en minder dan 12 uur per week betaald werk. Opvallend is dat eerste generatie allochtonen en allochtonen waarvan beide ouders in het buitenland zijn geboren significant vaker een belediging rapporteren.

Met uitzondering van die laatste bevinding zien we hier dus een patroon dat we ook zagen bij malware, hacken, e-fraude, cyberstalking en bedreiging.

[36] Het is bovendien door het slachtoffer niet (altijd) te achterhalen of er überhaupt sprake is van opzettelijkheid.

Tabel 7.10: belediging naar achtergrondkenmerken (gewogen, bivariaat)

	Belediging (% internetgebruikers)
Geen opleiding	4,1
Basisonderwijs	6,3
LBO	1,1
VMBO/MAVO	3,1
HAVO/VWO	6,3
MBO	3,0
HBO	2,3
WO	4,4
$\chi^2(7)$	*64,59***
15-24	8,0
25-34	4,1
35-44	2,8
45-54	2,6
55-64	1,5
65+	0,5
$\chi^2(5)$	*150,20***
<12 uur betaald werk p.w.	3,9
12+ uur betaald werk p.w.	3,1
$\chi^2(1)$	*4,29**
Geen partner	4,8
Partner	1,9
$\chi^2(1)$	*61,02***
Autochtoon	3,1
1e generatie	5,0
2e generatie, 1 ouder	3,4
2e generatie, beide ouders	4,8
$\chi^2(3)$	*10,98**
Man	3,2
Vrouw	3,6
$\chi^2(1)$	*1,38*
Totaal	**3,4**

*p<0.05, **p<0.01

Belediging, conclusies

Van de internetters is 3,4 procent wel eens beledigd. Het blijkt dat voornamelijk jonge internetters zijn beledigd, internetters die basisschool of middelbare school als hoogst afgeronde opleiding hebben, die minder dan 12 uur per week een betaalde baan hebben en internetters die geen partner hebben.

8 Meervoudig Slachtofferschap

8.1 Bepalen van meervoudig slachtofferschap

Jaarlijks wordt 8,5 procent van de internetters slachtoffer van een of meer vormen van de door ons onderzochte delicten met een digitale component. Er is een groep slachtoffers die vaker dan één keer slachtoffer wordt. Deze groep is interessant omdat interventies gericht op deze groep meer effect kunnen hebben dan interventies gericht op andere internetters. Zij zijn met een kleine groep immers slachtoffer van een relatief groot deel van de delicten.

In de victimologie wordt onderscheid gemaakt tussen herhaald slachtofferschap en meervoudig slachtofferschap. Herhaald slachtofferschap betekent dat een respondent vaker dan één keer slachtoffer is geworden van hetzelfde delict in een periode van twaalf maanden. Meervoudig slachtofferschap betekent dat een respondent in zo'n periode van verschillende delicten slachtoffer is geworden. Van deze laatste groep slachtoffers is hier de vraag wie zij zijn. Bij het vaststellen of een respondent meervoudig slachtoffer is laten we malware buiten beschouwing omdat het enkel om het opmerken daarvan gaat. Hacken als MO laten we eveneens buiten beschouwing omdat een slachtoffer dat gehackt wordt om bijvoorbeeld de identiteitsgegevens te stelen feitelijk maar eenmalig slachtoffer is. Respondenten die slachtoffer zijn van identiteitsdiefstal en identiteitsfraude, maar verder van geen ander delict zijn als enkelvoudig slachtoffer gerekend, omdat identiteitsdiefstal uitsluitend als voorbereidingshandeling voor identiteitsfraude is gevraagd en niet als los delict. Smaad, laster en belediging laten we buiten beschouwing omdat er door de brede vraagstelling in het onderzoek geen sprake hoeft te zijn van een delict.

Een respondent is in dit onderzoek als meervoudig slachtoffer van delicten met een digitale component aangemerkt als hij slachtoffer was van twee of meer van de delicten:

1. Hacken, *defacing*: een profielpagina of website is ongevraagd gewijzigd;
2. Hacken, mail gehackt: iemand heeft zonder toestemming ingebroken of ingelogd op het mailaccount van de respondent;
3. Hacken, pc gehackt: iemand heeft ingebroken in de computer en gegevens vernietigd, veranderd of gestolen;
4. Fraude via veiling of verkoopsites, betaald maar niet geleverd;
5. Fraude via veiling of verkoopsites, verkocht, maar geen betaling ontvangen;
6. Identiteitsdiefstal: de identiteit van de respondent is met behulp van ICT gestolen;
7. Identiteitsfraude: de identiteit van de respondent is met behulp van ICT misbruikt voor financieel gewin;

8. Voorschotfraude: de respondent heeft aan een contact op internet een geldbedrag betaald als voorschot voor een niet-bestaande investering;
9. Stalking: de respondent is gestalkt met behulp van ICT-middelen;
10. Bedreiging: de respondent is bedreigd met behulp van ICT-middelen;

8.2 Prevalentie en risicogroepen

Van de slachtoffers wordt 17,6 procent slachtoffer van twee of meer verschillende delicten, wat overeenkomt met 1,5 procent van de internetters (tabel 8.1).

Tabel 8.1: meervoudig slachtofferschap (gewogen, percentages van internetters)

Geen slachtoffer	91,5
Enkelvoudig slachtoffer	7,0
Meervoudig slachtoffer	1,5

Uit tabel 8.2 blijkt dat internetters zonder partner een grotere kans hebben om meervoudig slachtoffer te worden. Verder is slachtofferschap ook niet toevallig verdeeld over de verschillende groepen leeftijden. De tabel wijst er op dat vooral in de leeftijdsgroep van 15-34 jaar het percentage meervoudig slachtoffers hoog is. Het accent op jongere leeftijdsgroepen zagen we eerder in voorgaande hoofdstukken. Ook in een analyse van politiedossiers zagen we dat cybercrime lijkt samen te gaan met jongeren (Leukfeldt e.a., 2010; Leukfeldt & Stol, 2011). In een verdiepende analyse zijn jongere internetters dus een groep die speciale aandacht verdient.

Tabel =8.2: Meervoudig slachtofferschap naar achtergrondkenmerken (gewogen, bivariaat

	Meervoudig slachtoffer (% internetgebruikers)
Geen opleiding	1,2
Basisonderwijs	2,2
LBO	0,4
VMBO/MAVO	1,8
HAVO/VWO	1,5
MBO	1,6
HBO	1,6
WO	0,9
$\chi^2(7)$	*11,74*
15-24	3,1
25-34	2,3
35-44	1,1
45-54	1,0
55-64	0,6
65+	0,5
$\chi^2(5)$	*53,21***
Geen of minder dan 12 uur betaald werk	1,5
12 uur per week of meer betaald werk	1,4
$\chi^2(1)$	*0,07*
Geen partner	2,0
Partner	0,9
$\chi^2(1)$	*18,22***
Autochtoon	1,3
1e generatie	1,9
2e generatie, 1 ouder	1,4
2e generatie, beide ouders	3,2
$\chi^2(3)$	*7,41*
Man	1,3
vrouw	1,6
$\chi^2(1)$	*2,01*
Totaal	**1,5**

*p<0.05, **p<0.01

8.3 Meervoudig slachtofferschap: conclusies

Op jaarbasis wordt 8,5 procent van de internetters slachtoffer van één of meerdere delicten met een digitale component waarover dit onderzoek gaat. Meervoudig slachtofferschap wil zeggen dat een internetter slachtoffer wordt van meer dan één van deze delicten. 1,5 procent van de internetters in ons onderzoek is meervoudig slachtoffer. Vooral in de leeftijdsgroep van 15-34 jaar het percentage meervoudig slachtoffers hoog. Ook internetters zonder partner zijn naar verhouding vaak slachtoffer.

9 Politie

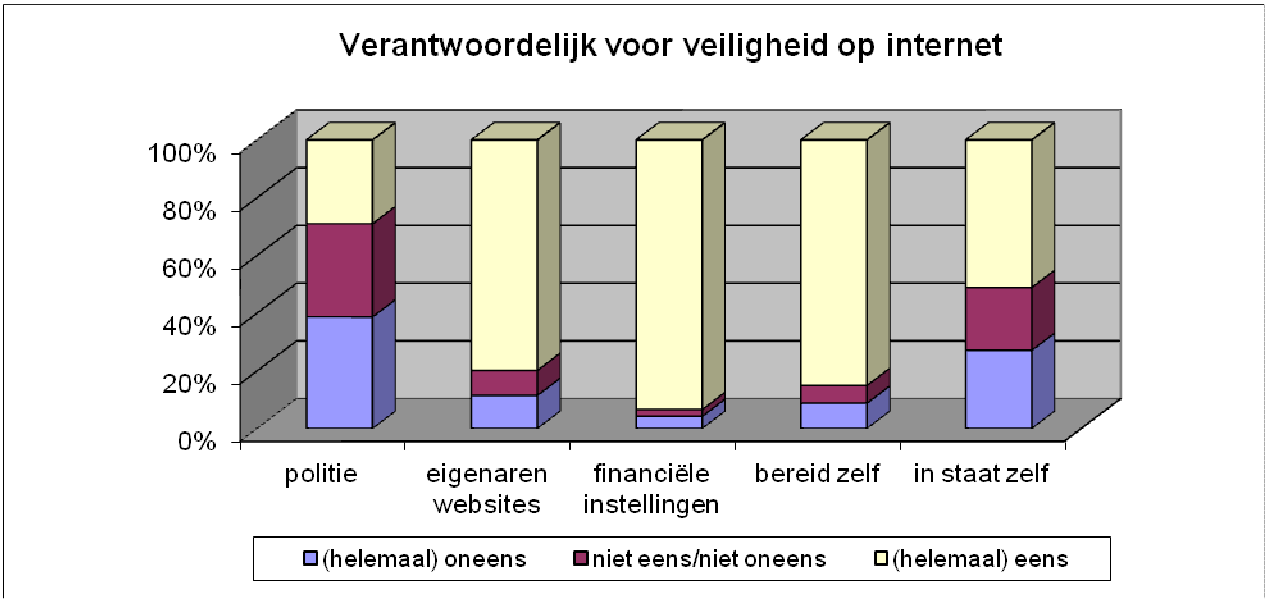
Dit hoofdstuk gaat over de rol van politie in relatie tot delicten met een digitale component, gezien door ogen van internetters. Vinden zij dat de politie verantwoordelijk is voor hun veiligheid in de digitale wereld? En als een slachtoffer aangifte doet van een delict met een digitale component, neemt de politie dan een aangifte op? En is de burger tevreden over de reactie van de politie?

9.1 Verantwoordelijkheid

Vinden burgers de politie de aangewezen organisatie om de veiligheid op internet te waarborgen? Er zijn immers ook andere actoren die verantwoordelijkheid (kunnen) dragen, bijvoorbeeld de financiële instellingen (in het geval van het digitale betalingsverkeer), eigenaren van websites, internet service providers of de internetters zelf.

In figuur 9.1 zijn de antwoorden te zien op de vraag wie de veiligheid op internet moet waarborgen. Volgens internetters zijn vooral de financiële instellingen (93,4%) en de eigenaren van websites (79,9%) verantwoordelijk voor de veiligheid op internet. Van alle ondervraagde internetters geeft 85,1 procent aan dat zij ook zelf bereid zijn iets aan hun veiligheid op internet te doen. Ruim een kwart van de internetters (27,1%) acht zichzelf echter niet goed in staat de eigen veiligheid te waarborgen. Bijna drie op de tien internetters (29,0%) vindt dat (ook) de politie een verantwoordelijkheid heeft in het waarborgen van de veiligheid op internet.

Figuur 9.1: verantwoordelijkheid voor de veiligheid op internet volgens burgers



9.2 Relatie politie-publiek

Contact met politie

In hoofdstuk 3 tot en met 5 is per delict, waar het ging over de reactie van de slachtoffers, beschreven met welke organisaties slachtoffers contact opnemen. In deze paragraaf gaan we nader in op het politiecontact.

Gemiddeld over alle delicten neemt 13,4 procent van de slachtoffers contact op met de politie. Tabel 9.1 toont dat dit percentage relatief hoog is bij stalking en bedreiging (respectievelijk 30,4 en 27,8%). Daarna volgt oplichting op een veiling- of verkoopsite (19,6%). Het aandeel slachtoffers dat contact met de politie opneemt is klein bij een hack (in dit geval hacken van een computer of e-mailaccount of *defacing*) en voorschotfraude (respectievelijk 4,1 en 5,6%).

Tabel 9.1: contact met politie n.a.v. slachtofferschap, ongewogen

	Aantal unieke slachtoffers	**Respondenten die minstens 1 keer contact opnamen (n)**	**(%)**
Hacken (direct gevraagd)	339	14	4,1
Betaald maar niet geleverd	204	43	21,1
Verkocht maar niet betaald	25	2	8,0
Voorschotfraude	18	1	5,6
Identiteitsfraude en/of -diefstal	63	12	15,6
Stalking	92	28	30,4
Bedreiging	54	15	27,8
Belediging	274	25	9,1
Totaal	**876**	**117**	**13,4**

Reactie van de politie

We vroegen de slachtoffers wat de reactie van de politie was naar aanleiding van dit contact. Mogelijke antwoorden waren:

1. de politie heeft een aangifte opgenomen en heeft de dader opgespoord of geprobeerd op te sporen;
2. de politie heeft een aangifte opgenomen en is bezig met het opsporen van de dader;
3. de politie heeft een aangifte opgenomen, verder niets meer van gehoord;
4. de politie heeft een melding opgenomen, maar geen aangifte;
5. de politie gaf advies, maar nam geen melding of aangifte op;
6. de politie zei dat zij niets kon doen;
7. de politie nam de melder niet serieus;

8. andere reactie politie.

Om nadere uitspraken te kunnen doen over de reactie van de politie hebben we drie elkaar uitsluitende categorieën gedefinieerd over het politieoptreden:

1. de politie nam een aangifte op (antwoord 1, 2 en/of 3),
2. de politie nam een melding op of gaf advies (antwoord 4 of 5, en niet antwoord 1, 2 of 3),
3. de politie ondernam geen strafrechtelijke actie (antwoord 6, 7 of 8 en niet antwoord 1, 2, 3, 4 of 5).

We vroegen op drie plaatsen in de vragenlijst naar de reactie van de politie, waardoor we ten aanzien van drie groepen delicten gegevens hebben over de reactie van de politie:

- wanneer de respondent contact had opgenomen met de politie omdat hij/zij slachtoffer was geworden van één of beide vormen van fraude via veiling- en/of verkoopsites;
- omdat er contact was geweest naar aanleiding van voorschotfraude en/of identiteitsfraude;
- omdat er contact was geweest met de politie naar aanleiding van stalking, bedreiging, belediging, *defacing*, het hacken van de pc en/of het hacken van een e-mailaccount.

Tabel 9.2 geeft weer welke politiereacties de respondenten rapporteerden bij de drie groepen delicten met een digitale component.

Tabel 9.2: reactie van de politie (ongewogen)

Reactie	**Aangifte opgenomen**		**Melding of advies**		**Geen strafrechtelijke actie**	
	Aantal	%	Aantal	%	Aantal	%
Fraude via veiling- of verkoopsites	26	57,8	7	15,6	12	26,7
Voorschotfraude en identiteitsfraude	7	53,8	3	23,1	3	23,1
Stalking, bedreiging, *defacing*, pc gehackt, mail gehackt of belediging	18	28,6	33	52,4	12	19,0

Wanneer een respondent contact opnam met de politie vanwege fraude via veiling- of verkoopsites, nam de politie in 57,8 procent van de gevallen een aangifte op. Bij voorschotfraude / identiteitsfraude in 53,8 procent van de gevallen, en bij hacken, een

persoonlijk delict of belediging in 28,6 procent van de gevallen. In het laatste geval wordt vaker een melding opgenomen of advies gegeven (52,4%).

Tevredenheid over reactie politie

We keken ook of de slachtoffers tevreden waren over de reactie van de politie. Slachtoffers konden hun tevredenheid aangeven op een vijfpuntschaal, van zeer ontevreden (1) tot zeer tevreden (5). De tevredenheid over het politieoptreden is op dezelfde drie plaatsen gevraagd als de reactie van de politie en kan daarom niet met zekerheid aan één delict worden toegeschreven. We geven daarom de tevredenheid weer voor de drie clusters van delicten (tabel 9.3). De gemiddelde tevredenheid over het politieoptreden bij fraude via veiling- of verkoopsites is een 2,7. De afhandeling bij voorschotfraude en/of identiteitsmisbruik scoort een 3,4 en de afhandeling van delicten in de persoonlijke sfeer of belediging een 3,0.

Tabel 9.3: tevredenheid van slachtoffers over reactie van de politie

	Gemiddelde tevredenheid	**Aangifte opgenomen**	**Geen aangifte opgenomen**	**Significantie**
Fraude via veiling- of verkoopsites	2,7	3,2	2,0	(n=45, p<0.001)
Voorschotfraude, identiteitsfraude en/of -diefstal	3,4	4,0	2,7	(n=13, p=0.083)
Stalking, bedreiging, defacing, pc gehackt, mail gehackt of belediging	3,0	3,6	2,8	(n=63, p=0.022)

Omdat de tevredenheid van het slachtoffer te maken kan hebben met de reactie van de politie hebben we gekeken of de tevredenheid verschilt tussen slachtoffers waarvan de politie wel of geen aangifte opnam. We zien bij fraude via verkoop- en veilingsites en bij hacken en delicten in de persoonlijke sfeer dat slachtoffers waarvan de politie een aangifte opnam, tevredener zijn dan slachtoffers waarbij de politie geen aangifte opnam. Het aantal slachtoffers dat naar de politie stapte vanwege voorschotfraude en/of identiteitsmisbruik is klein, waardoor het verschil tussen een 4,0 en een 2,7 niet significant is.

Rol politie, conclusie

29,0 procent van de internetters vindt dat de politie een verantwoordelijkheid heeft in het waarborgen van de veiligheid op internet. De meeste verantwoordelijkheid leggen de respondenten echter bij financiële instellingen en eigenaren van websites.

Het percentage slachtoffers dat contact opneemt met de politie is niet hoog: het varieert van tussen 4,1 (hacken) en 30,4 (stalking) procent, gemiddeld 13,4 procent. De reactie van de politie op verschillende meldingen van slachtoffers wisselt. Bij fraude via veiling- of verkoopsites en bij voorschotfraude en identiteitsfraude, neemt de politie in ruim de helft van de gevallen een aangifte op. Bij hacken en delicten in de persoonlijke sfeer ligt dat met 28,6 procent beduidend lager. Slachtoffers waarbij wel een aangifte is opgenomen zijn beduidend meer tevreden over het politieoptreden dan slachtoffers waarbij dit niet is gebeurd.

10 Conclusies

10.1 Slachtofferschap

Kerncijfers slachtofferschap

In de inleiding van dit onderzoek presenteerden we de cijfers uit de spaarzame onderzoeken die er zijn met betrekking tot de omvang van delicten met een digitale component. Op basis van die cijfers was de verwachting dat het slachtofferschap daarvan aanzienlijk is. Wat prevalentie betreft laat dit slachtofferonderzoek zien dat in de twaalf maanden voorafgaande aan de vragenlijst 8,5 procent van alle internetters slachtoffer was van een of meerdere vormen van de hier bevraagde delicten met een digitale component (tabel 10.1). In de tabel zijn eveneens de prevalentiecijfers van de afzonderlijke delicten gepresenteerd. Indien smaad/laster als delict zou worden meegerekend is het percentage 10,6 procent. Tot slot heeft 16,7 procent malware op zijn/haar computer opgemerkt.

Als kerncijfers voor criminaliteitsbeleid komt uit ons onderzoek naar voren dat, gezien op jaarbasis, van alle Nederlandse internetgebruikers:

- 4,3 procent slachtoffer wordt van hacken;
- 3,5 procent slachtoffer wordt van e-fraude (fraude via een advertentie- of veilingsite, identiteitsfraude, voorschotfraude);
- 1,2 procent slachtoffer wordt van een delict in de persoonlijke sfeer.

Niet alle delicten met een digitale component zijn in ons onderzoek bevraagd. Daarvan zijn er simpelweg te veel.[37] Delicten die niet aan de orde kwamen, zijn bijvoorbeeld handel in valse goederen, afpersing en chantage. Slachtofferschap van delicten met een digitale component ligt in totaal dus waarschijnlijk in werkelijkheid hoger dan het in tabel 10.1 genoemde totaalpercentage.

[37] Zie bijvoorbeeld de Handreiking voor delicten met een digitale component waarin alleen al 28 delicten worden behandeld (Leukfeldt,, Kentgens, Frans, Toutenhoofd, Stol, & Stamhuis, 2012.)

Tabel 10.1: prevalentie slachtofferschap van delicten met een digitale component

Delict	Prevalentie (% internetters)	Betrouwbaarheidsinterval (95%)
Hacken, defacing	1,5	1,3 – 1,7
Hacken, pc gehackt	0,7	0,5 – 0,9
Hacken, mail gehackt	2,9	2,6 – 3,2
Hacken, als MO	0,8	0,6 – 1,0
Hacken, totaal	*4,3*	*3,9 – 4,7*
Betaald maar niet geleverd	2,4	2,1 – 2,7
Verkocht maar niet betaald	0,3	0,2 – 0,4
Identiteitsdiefstal en/of -fraude	0,8	0,6 – 1,0
Voorschotfraude	0,2	0,1 – 0,3
Financiële delicten, totaal	*3,5*	*3,1 – 3,9*
Stalking	1,1	0,9 – 1,3
Bedreiging	0,7	0,5 – 0,9
Persoonlijke delicten, totaal	*1,5*	*1,3 – 1,7*
Delicten totaal, excl. malware en smaad/laster/belediging	*8,5*	*7,9 – 9,1*
Smaad, laster, belediging	3,4	3,0 – 3,8
Delicten totaal,excl. malware en incl. smaad, laster, belediging	*10,6*	*10,0 – 11,2*
Malware opgemerkt	16,7	15,9 – 17,5

Meervoudig slachtofferschap

Meervoudig slachtofferschap betekent dat iemand slachtoffer is van meer dan één soort delict. Van alle internetters is 1,5 procent meervoudig slachtoffer van de door ons bevraagde vormen van delicten met een digitale component. Vooral in de leeftijdsgroep 15-34 jaar is het percentage meervoudig slachtoffers hoog.

Factoren die een rol spelen bij slachtofferschap

Leeftijd is een factor die bij meerdere delicten met een digitale component een rol speelt. Jonge mensen (onder de 35 jaar) zijn vooral slachtoffer van hacken. Internetters tussen de 15 en 24 jaar zijn vaak slachtoffer van stalking en bedreiging. Ook worden jonge internetters vaak beledigd. Andere kenmerken van internetters die naar verhouding vaak slachtoffer worden, zijn: alleen lagere school of middelbare school als hoogst genoten opleiding, minder dan 12 uur per week betaald werk hebben en geen partner hebben. We vermoeden dat dit kenmerken zijn die samengaan met een jonge leeftijd. In dat geval resteert vooral leeftijd als risicofactor voor slachtofferschap (en dan vermoedelijk eerder nog weer aan leeftijd verbonden kenmerken zoals internetgedrag en risicobewustzijn).

Etniciteit speelt een kleine rol bij slachtofferschap van delicten met een digitale component. Alleen bij belediging zien we hier een significant verschil. Eerste generatie allochtonen en allochtonen waarvan beide ouders in het buitenland zijn geboren, rapporteren significant vaker een belediging.

Internationalisering

Bij oplichtingen waarbij slachtoffers werden opgelicht doordat zij voor een goed of dienst hadden betaald maar deze niet kregen geleverd (2,4% van alle internetgebruikers) liep in een vijfde van de gevallen het contact met de verkoper volgens het slachtoffer via het buitenland (19,2%). Leukfeldt e.a. (2010) concludeerden dit ook voor e-fraudes op basis van hun analyse van politiedossiers. Gezien de aard van het delict: fraudes via veiling- en verkoopsites voor relatief lage bedragen, zal het werkaanbod van de politie verder internationaliseren.

10.2 Rol van de politie

Rol politie voor waarborgen veiligheid in cyberspace

De meeste respondenten achten financiële instellingen en eigenaren van websites verantwoordelijk voor de veiligheid op internet. Niet meer dan 29,0 procent van de internetters vindt dat de politie daarin een verantwoordelijkheid heeft.

Contact met de politie

Er zijn gewogen 786 slachtoffers. Van hen namen er 117 minstens één keer contact op met de politie, oftwel 14,9 procent Dat percentage is lager dan het percentage dat in de IVM wordt gemeten gemiddeld over de daarin bevraagde offline delicten. Alleen het *aangifte*percentage is daar al significant hoger (26,3%); het *meldings*percentage voor offline delicten is met 34,5 procent nog weer hoger (CBS, 2012). Met andere woorden, het dark number voor delicten met een digitale component is aanzienlijk groter dan het dark number voor klassieke criminaliteit. Een deel van de verklaring daarvoor vinden we ongetwijfeld in de bevinding dat internetters niet meteen aan de politie denken als hen wordt gevraagd wie verantwoordelijk is voor de veiligheid op internet. Internetters zien eerder financiële instellingen en eigenaren van websites daarvoor verantwoordelijk (par. 7.1).

Bij delicten met een digitale component liggen de percentages bij de politie gemelde delicten tussen de 4,1 (hacken) en 30,4 (stalking) procent (gemiddeld 14,9%). De reactie van de politie op verschillende meldingen van slachtoffers wisselt. In ruim de helft van de gevallen van fraude via veiling- of verkoopsites en van voorschotfraude en identiteitsfraude

neemt de politie een aangifte op. Bij hacken en delicten in de persoonlijke sfeer ligt het aangiftepercentage met 28,6 procent significant lager.

Tevredenheid over de politie

De gemiddelde tevredenheid van slachtoffers over de politie is afhankelijk van de delictsoort. De afhandeling van fraude via verkoopsites scoort een 2,7 op een schaal van 1 tot 5, de afhandeling van identiteitsfraude en voorschotfraude een 3,4 en van persoonlijke delicten een 3,0. Van de slachtoffers waarbij de politie een aangifte heeft opgenomen is een groter deel tevreden over het politieoptreden dan slachtoffers waarbij dit niet is gebeurd. Wellicht dat zij zich serieuzer genomen voelen en daardoor de reactie van de politie positiever beoordelen.

11 Discussie

Inleiding

In deze scriptie staan de uitkomsten van het eerste landelijke slachtofferonderzoek naar cybercrime onder een representatieve steekproef van Nederlandse burgers van 15 jaar en ouder. Het onderzoek is uitgevoerd in opdracht van het Korps Landelijke Politiediensten (KLPD) en gefinancierd door het Programma Aanpak Cybercrime (PAC), een versterkingsprogramma van de politie. Aanleiding voor het onderzoek was het ontbreken van sturingsinformatie over cybercrime.

In het onderzoek komen de volgende vormen van cybercrime aan bod: verspreiden van malware en hacken; fraude via veiling- en verkoopsites, identiteitsfraude en voorschotfraude en; cyberstalking, -bedreiging, smaad, laster en belediging. Dit zijn delicten gericht tegen computers en computernetwerken, financiële delicten en delicten in de persoonlijke sfeer. De keuze voor deze vormen van cybercrime is ingegeven door professionals uit de politiepraktijk. Ander vormen van cybercrime, zoals het produceren en distribueren van kinderpornografisch materiaal op internet, blijven buiten beschouwing (zie voor een overzicht van cybercrimes Gordon & Ford, 2006; Leukfeldt, e.a., 2010; Wall, 2007). Ook valt te verwachten dat door de snel veranderende techniek nieuwe vormen van cybercrime zullen ontstaan. Dit onderzoek geeft dus geen beeld van slachtofferschap van álle vormen van cybercrime in Nederland.

Onderzoek naar slachtofferschap van cybercrime vergeleken

Een vergelijking van de uitkomsten uit dit onderzoek met data uit ander onderzoek is lastig: er is nog nauwelijks onderzoek verricht naar slachtofferschap van cybercrime en daarnaast verschillen de al dan niet op nationale strafrechtelijke bepalingen gebaseerde definities en operationalisaties van de verschillende vormen van cybercrime. Ten aanzien van sommige vormen van cybercrime geldt bovendien dat in ander onderzoek geen onderscheid gemaakt wordt tussen de conventionele en digitale vormen van een delict. Dit geldt bijvoorbeeld voor stalking (zie Sommer, 2009; Parsons-Pollard, & Moriarty, 2008). Wel is het mogelijk om in te schatten welke vormen van cybercrime het meest prevalent of schadelijk zijn.

Uit het onderzoek is gebleken dat in de twaalf maanden voorafgaande aan het onderzoek 16,7 procent van de internetters malware heeft opgemerkt op zijn computer, waarvan 16,1 procent ook financiële schade heeft ondervonden. In ruim 40 procent van de gevallen bedroeg de schade meer dan honderd euro. Van alle ondervraagde internetters is 4,3 procent op één of meerdere manieren gehackt. Hierbij moet wel de kanttekening worden

geplaatst dat een internetgebruiker lang niet altijd weet of zijn of haar computer geïnfecteerd is met malware of dat de computer is gehackt. Voor de verspreiding van malware en bepaalde technieken van hacken geldt bovendien dat er in ander onderzoek mogelijk sprake is van een overrapportage (zie Anderson, e.a., 2012), omdat de data over de verspreiding van malware veelal afkomstig zijn van bedrijven die belang hebben bij de verkoop van beveiligingssoftware (zie Wall, 2007).

Van alle internetters is 3,5 procent slachtoffer geworden van één of meer van de onderzochte financiële delicten. De schade als gevolg van oplichting via veiling- en verkoopsites bedraagt in bijna driekwart van de gevallen minder dan honderd euro, maar in vijf procent van de gevallen is de schade groter dan 500 euro. Bij identiteitsfraude is de geleden schade beduidend hoger: in ruim een derde van de gevallen gaat het om meer dan duizend euro. Deze schades worden vergoed door banken, maar uiteindelijk wordt de rekening linksom of rechtsom betaald door de consument. Ook voorschotfraude gaat doorgaans gepaard met grote financiële schade, maar de omvang van voorschotfraude is relatief klein.

Van de persoonlijke delicten cyberstalking en bedreiging via internet is 1,5 procent van de respondenten slachtoffer geworden. Bij deze delicten is sprake van geen of weinig materiële schade.

Ter vergelijking enkele klassieke offline delicten: in 2012 werd 3,5 procent van de Nederlandse burgers slachtoffer van bedreiging, 1,7 procent van zakkenrollerij en 1,5 procent van inbraak (CBS, 2012). Over schadebedragen van deze delicten is niets bekend. De uitkomsten zijn lastig te vergelijken omdat zowel dit onderzoek als het onderzoek naar offline criminaliteit niet alle delicten omvat. Ook is niets bekend over verplaatsingseffecten van de offline naar de online wereld. Slachtofferpercentages van 4,3 procent (hacken) en 3,5 procent (financiële delicten) zijn echter aanzienlijke percentages, waardoor deze vormen van criminaliteit wel de nodige aandacht verdienen in slachtofferonderzoek.

Problemen bij de uitvoering van het slachtofferonderzoek cybercrime

Het is lastig de verschillende cybercrimes zo te operationaliseren, dat daadwerkelijk gemeten wordt of de internetgebruiker slachtoffer is geworden van een delict zoals beschreven in het wetboek van strafrecht én waarbij de vragen voor alle internetgebruikers begrijpelijk zijn. Bij de vraag 'is uw computer gehackt' of 'is uw mail gehackt', zal niet elke internetter er meteen aan denken dat wanneer iemand de inloggegeven kent en deze vervolgens zonder toestemming gebruikt, er *de jure* al sprake is van hacken. Ook identiteitsdiefstal is lastig te operationaliseren. Ten eerste is onduidelijk welke persoonsgegevens vallen in de categorie 'identiteitsgegeven' en ten tweede weet lang niet elke Nederlander welke persoonsgegevens een identiteitsgegeven genoemd kunnen worden. De definities van de persoonlijke delicten stalking en bedreiging, gebaseerd op de strafrechtelijke omschrijving, bevatten dusdanig veel elementen, dat ook niet van elke Nederlander verwacht kan worden in te kunnen schatten of er daadwerkelijk sprake was van een delict. Eén respondent heeft bijvoorbeeld op basis van de geven definitie het versturen van spam als stalking aangemerkt.

Het is bovendien lastig om complex deviant gedrag te duiden in termen van afzonderlijke cybercrimes. Uit onderzoek blijkt dat bepaalde cybercrimes naast een zelfstandig delict ook een middel kunnen zijn om andere delicten, al dan niet online, te kunnen plegen. Voorbeelden zijn hacken en identiteitsdiefstal. Een hacker kan bijvoorbeeld de identiteit van een persoon stelen met het uiteindelijke doel om deze persoon te bedreigen ((Leukfeldt, e.a., 2010; Van Wilsem, 2012). Uit internationaal onderzoek komt bovendien naar voren dat de grens tussen intimidatie, bedreiging en stalking moeilijk is aan te geven (Ashcroft, 2001) en dat de grens tussen seksuele delicten en stalking diffuus is (Duntley & Buss, 2012).

Zelfrapportage-onderzoek is bij uitstek de manier om het *dark number* van delicten te meten. Het *dark number* is dan dat deel van criminaliteit dat niet zichtbaar is in statistieken omdat het niet aangegeven wordt bij de politie. In het geval van malware, hacken en identiteitsfraude is echter sprake van een extra *dark number*, omdat respondenten zelf ook niet weten dat ze slachtoffer zijn geworden.

Bruikbaarheid van de resultaten

Dit onderzoek geeft een globaal beeld van de omvang en schade van slachtofferschap van cybercrime. Er is een beeld geschetst van de modus operandi van daders en de acties die

slachtoffers nemen naar aanleiding van de gebeurtenissen. Dit biedt de politiepraktijk en beleidsmakers aanknopingspunten voor prioritering en (preventie)beleid.

De toekomst van slachtofferonderzoek cybercrime in Nederland

Omdat dit het eerste landelijke onderzoek naar slachtofferschap van cybercrime is, is dit onderzoek te beschouwen als een nulmeting. In het voorjaar van 2013 zal het CBS een deel van deze vragen herhalen als onderdeel van de IVM en wordt daarmee een begin gemaakt met monitoring. De vragenlijst is echter voor verbetering vatbaar en het is denkbaar dat de lijst van cybercrimes en de operationalisering van de cybercrimes in de komende jaren verandert. De delicten passen inhoudelijk ook niet goed bij de huidige Integrale Veiligheidsmonitor.

Aangezien er nog steeds een *dark number* bestaat bij de delicten malware, hacken en identiteitsfraude, kunnen wellicht betere manieren gevonden worden om deze fenomenen te monitoren dan een slachtofferonderzoek. Om te weten te komen hoeveel computers zijn besmet met malware, kan een steekproef van computers technisch onderzocht worden. Het meten van de omvang van slachtofferschap van hacken is een hachelijke onderneming: het is een koepelbegrip en hacken is vaak een voorbereidingshandeling voor andere delicten. Om slachtofferschap van hacken tegen te gaan, is informatie over de modus operandi van daders essentieel en het is maar zeer de vraag of slachtofferschap van hacken als op zichzelf staand delict wel gemeten moet worden. Informatie over de aard en omvang van identiteitsfraude kan beter in samenwerking met banken verzameld worden. Aangezien de schade van identiteitsfraude hoog is en vergoed wordt door banken, is het aannemelijk dat slachtoffers hiervan altijd melding zullen maken bij banken.

Het meten van oplichting via fraude- en verkoopsites levert weinig problemen op met de operationalisering en internetters weten ook of zij hiervan slachtoffer zijn geworden. Het betreft hier kleine criminaliteit en past daarom ook inhoudelijk goed in de IVM. Op dit moment wordt niet naar slachtofferschap van offline oplichtingen gevraagd in de IVM. Wanneer het CBS vragen over offline oplichting op zou nemen, dan zou dat wellicht interessante vergelijkingen kunnen opleveren.

Prevalentie van voorschotfraude zou via de IVM gemeten kunnen worden. Op dit moment komt het weinig voor, maar het is bekend dat daders hiervan hun slachtoffers in steeds wisselende landen zoeken en daarom is monitoring relevant.

De operationalisering van de persoonlijke delicten stalking en bedreiging is lastig, daarbij is de online en offline variant van deze delicten sterk verweven. In de IVM is op dit moment geen aandacht voor deze delicten. Monitoring van slachtofferschap van deze delicten

zou dan ook in beide varianten opgenomen moeten worden in de IVM óf er kunnen vragen naar de modus operandi van daders van deze delicten opgenomen worden in onderzoek dat zich specifiek richt op stalking en/of bedreiging.

Uit deze inventarisatie blijkt dat vooral slachtofferschap van cybercrime in ruime zin, dus de (kleine) criminaliteit waarbij het gebruik van technologie onderdeel is van de modus operandi van de dader, geschikt is om via slachtofferonderzoek te meten. Het is dan ook niet aan te raden een monitoringsinstrument te ontwikkelen om 'slachtofferschap cybercrime' te monitoren. Om meer sturingsinformatie over de rol van internet bij criminaliteit te verkrijgen is het aan te raden goed te gaan kijken naar bestaande monitoringsinstrumenten en daar (meer) aandacht te gaan besteden aan de rol van internet.

Aanbevelingen voor verder onderzoek

Het verdient aanbeveling om toekomstig onderzoek naar (verklarende factoren voor) slachtofferschap van cybercrime te plaatsen binnen een theoretisch kader. Uit de literatuur blijkt dat de routineactiviteitentheorie en de zelfcontroletheorie het meest voor de hand liggen. Onderzoekers hebben de routineactiviteitentheorie als uitgangspunt genomen om slachtofferschap van verschillende vormen van cybercrime nader te duiden: malware (Bossler & Holt, 2009), intimidatie (*harassment*) (Holt & Bossler, 2009), fraude via online veilingsites (Conradt, 2012; Nikitkov, Stone, Miller, 2011; Van Wilsem, 2010b), *phishing* (Hutchings & Hayes, 2009) en cyberstalking (Reyns, Henson, & Fisher, 2011). Door Yar (2005) worden er echter kritische kanttekeningen geplaatst bij de toepasbaarheid van de routineactiviteitentheorie in een digitale omgeving, dus mogelijk moeten hypotheses gefundeerd in deze theorie een digitale variant krijgen of worden uitgebreid naar de online omgeving. Ook de zelfcontroletheorie – een theorie die in eerste instantie is bedoeld om daderschap van criminaliteit te verklaren – is in verband gebracht met slachtofferschap van cybercrime: hacking (Bossler, & Burruss, 2010), intimidatie (Holt, Bossler, & May, 2011; Ngo & Paternoster, 2011), fraude via online veilingsites (Van Wilsem, 2010b) en phishing (Ngo & Paternoster).

De data die voor dit onderzoek zijn gebruikt, bevatten gegevens over internetgedrag, het beveiligingsniveau van de computer en over risicobewustzijn. Bij ruim de helft van de respondenten is tevens een vragenlijst afgenomen waarmee zelfcontrole wordt gemeten. Wanneer nieuwe hypotheses zijn geformuleerd, kan deze dataset gebruikt worden om een begin te maken met het toetsen van de toepasbaarheid van bestaande theorieën op cybercrime. Met de bestaande data kan een multiple regressiemodel gebouwd worden dat per cybercrime

risicofactoren in kaart brengt. De uitkomst van deze modellen kan gebruikt worden om preventiebeleid te ontwikkelen.

In de gebruikte vragenlijst zijn ook vragen gesteld over de immateriële gevolgen van slachtofferschap. Deze data kunnen gebruikt worden om in kaart te brengen of en hoe slachtofferschap van cybercrime van invloed is op het vertrouwen dat internetters hebben in onder andere internet, de rechtstaat en de mensheid als geheel.

Literatuur

Aa, S. van der, & Kunst, M.J.J. (2009). The prevalence of stalking in the Netherlands. *The International Review of Victimology 16*(4), 35-50.

Ahmed, T., & Oppenheim, C. (2006). Experiments to identify the causes of spam. *Aslib Proceedings : New Information Perspectives*, *58*(3), 156-178.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of yberstalking among college students. *Brief Treatment and Crisis Intervention, 5,* 279-289.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J. G., Levi, Moore, T., & Savage, S. (2012). *Measuring the Cost of Cybercrime*. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf. Laatst geraadpleegd op 26 augustus 2012.

Arneklev, B.J., Grasmick, H.G., Tittle, C.R., & Bursik Jr., R.J. (1993). Low self-control and imprudent behavior. *Journal of Quantitative Criminology*, *9*, 225-247.

Ashcroft, J. (2001). *Stalking and Domestic Violence*. Washington DC: United States Department of Justice.

AusCERT (2008). *AusCERT Home Users Computer Security Survey*. http://www.auscert.org.au/userservey. Laatst geraadpleegd op 25 augustus 2012.

AWPG (2010). *Phishing Activity Trends Report, 3rd Quarter, 2009*. www.anti-phishing.org. Laatst geraadpleegd op 29 augustus 2012.

AWPG (2012). Global Phishing Survey: Trends and Domain. Name Use in 2H2011. Period July - . December 2011. www.anti-phishing.org. Laatst geraadpleegd op 29 augustus 2012.

Baum, K., Catalano, S., Rand, M., & Rose, K. (2009). *Stalking victimization in the United States.* Washington, DC: U.S. Department of Justice.

Bethlehem, J. G. (1999). Cross-sectional Research. In H.J. Ader en G.J. Mellenbergh (Red.) *Research Methodology in the Social Behavioural and Life Science*. London: Sage Publications.

Bethlehem, J. G. (2006). *Representativiteit van web-surveys – Een illusie?* Voorburg: Centraal Bureau voor de Statistiek.

Bijleveld, C.C.J.H. (2005). *Methoden en technieken van onderzoek in de criminologie*. Den Haag: Boom Juridische Uitgevers.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family.* Westport: Praeger Publishers.

Bocij, P. (2006). *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals*. Westport, CT: Praeger Publishers.

Boerman, F., Grapendaal, M., & Mooij, A. (2008). *Nationaal Dreigingsbeeld 2008: Georganiseerde Criminaliteit*. Rotterdam: Thieme MediaCenter.

Bossler, A. M., & Burruss, G. W. (2010). The general theory of crime and computer hacking: Low selfcontrol hackers? In T. J. Holt & B. Schell (Eds.), *Corporate hacking and technology-driven crime: Social dynamics and implications* (pp. 57-81). Hershey: IGI Global.

Bossler, A.M., & Holt, T.J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Boutellier, H. (2008). Solidariteit en slachtofferschap: De morele betekenis van criminaliteit in een postmoderne cultuur. Amsterdam: Amsterdam University Press.

Bradley, T. (2010). How to Stop 11 hidden security threats and how to stop them. PCWorld. http://www.pcworld.com/article/187199/how_to_stop_11_hidden_security_threats.html. Laatst geraadpleegd op 28 augustus 2012.

Britz, M.T. (2008). *Computer Forensics and Cyber Crime: An Introduction*. Upper Saddle River, NJ: Prentice Hall.

Burton Jr., V.S., Cullen, F.C., Evans, T.D., Fiftal Alarid, L., & Dunaway, R.G. (1998). Gender, self-control, and crime. *Journal of Research in Crime and Delinquency*, *35*, 123-147.

Butler, D. A., Kift, S. M. , & Campbell, M. A. (2010). Cyber bullying in schools and the law : is there an effective means of addressing the power imbalance? *eLaw Journal*, *16*(1), 84-114.

Butler, D., Kift, S., & Campbell (2009), M. Cyber Bullying In Schools and the Law: Is There an Effective Means of Addressing the Power Imbalance? *eLaw Journal*, *16*(1), 84-114.

Capeller, W. (2001). Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies, 10*, 229-42.

CBS (2008). *Veiligheidsmonitor Rijk 2008. Landelijke Rapportage.* Voorburg/Heerlen: Centraal Bureau voor de Statistiek.

CBS (2009). *De digitale economie 2009*. Voorburg/Heerlen: CBS. http://www.cbs.nl/NR/rdonlyres/E87BCAE8-8F0E-4F43-90FE-B44F3D513E8A/0/2009p34pub.pdf. Laatst geraadpleegd op 1 september 2012.

CBS (2010). *Veiligheidsmonitor Rijk 2010. Landelijke Rapportage.* Voorburg/Heerlen: Centraal Bureau voor de Statistiek.

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law*, *24*(2), 229-251.

Chawki, M. (2009). Nigeria Tackles Advance Fee Fraud. *Journal of Information, Law and Technology 1*.

Choi, K. (2008). Computer crime vixtimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308-333.

Chu, B., Holt, T.J., & Joon Ahn, G. (2010). *Examining the Creation, Distribution, and Function of Malware On-Line*. NCJ 230111 Grant Report. Prepared for the National Institute of Justice. https://www.ncjrs.gov/pdffiles1/nij/grants/230111.pdf. Laatst geraadpleegd op 28 augustus 2012.

Clarke, R. V. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods*. Police Research Series, paper 112. London: Home Office.

CMI (2010). *Jaarrapportage 2009*. Den Haag: CMI.

Cohen, F. (1987). Computer Viruses: Theory and Experiments. *Computers and Security*, *6*, 22-35.

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

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory. *American Sociological Review, 46*(5), 505-524.

Conradt, C. (2012). Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case. *International Journal of Cyber Criminology*, *6* (1): 912–923.

Coupe, T., & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology, 44*, 431-464.

D'Ovidio, R., & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin, 73,* 10-17.

Dignan, J. (2005). Understanding Victims And Restorative Justice. Maidenhead: Open University Press.

Dijk, J.J.M. van (1997). Het victimologisch perspectief in verleden, heden en toekomst. Tijdschrift voor Criminologie, 39(4), 292-309.

Dion, M. (2010). Advance Fee Fraud Letters as Machiavellian/Narcissistic Narratives. *International Journal of Cyber Criminology*, *4*(1&2), 630-642.

Drapkin, I., & Viano, E. (Eds.) (1974-1975). Victimology: A new focus (Vols. 1-5). Lexington, MA: Heath.

Duntley, J.D., & Buss, D.M. (2012). The Evolution of Stalking. *Sex Roles*, *66*,311-327.

Easterbrook, F.H. (1996). Cyberspace and the law of the horse. *University of Chicago Legal Forum 207*.

eBay Inc. (2010). eBay Inc. form 10-K (form 10-K). San Jose, CA: eBay Inc. http://www.zonebourse.com/EBAY-INC-4869/pdf/211170/eBay%20Inc_SEC-Filing-10K.pdf. Laatst geraadpleegd op 29 augustus 2012.

EECFT (2011). EECFT European Cybercrime Survey. http://www.poste.it/salastampa/CYBER_CRIME.pdf. Laatst geraadpleegd op 29 augustus 2012.

European Commission (2007). *Towards a general policy on the fight against cyber crime.* COM(2007) 267 final. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.

Evans, T.D., Cullen, F.T., Burton Jr., V.S., Dunaway, R.G., & Benson, M.L. (1998). The social consequences of self-control: testing the general theory of crime. *Criminology*, *35*, 475-504.

Fafinski, S. (2010). Mapping and Measuring Cybercrime, Position Paper. In *Oxford Internet Institute Forum Mapping and Measuring Cybercrime* (pp. 75-78). University of Oxford, Oxford Internet Institute. http://www.oii.ox.ac.uk/events/details.cfm?id=337. Laatst geraadpleegd op 26 augustus 2012.

Fatah, E.A. (2000). Victimology: Past, Present and Future. *Criminology*, *33*(1), 17-46.

Federal Trade Commission (2011). *Consumer Sentinel Network Data Book for January–December, 2010*. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf. Laatst geraadpleegd op 1 september 2012.

Felson, M. (1998). *Crime and everyday life*. Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2002). Routine Activities and Crime Prevention in the Developing Metropolis. In S. Cote (Ed.). *Criminological Theories: Bridging the Past to the Future* (pp. 297-304). Thousand Oakes, CA: Sage Publishers.

Felson, M., & Clarke, R.V. (1998). *Opportunity makes the thief: practical theory for crime prevention*. London: Home Office.

Ferwerda, H. (2008). Theorie over criminaliteit. In W. Ph. Stol & A. Ph. van Wijk (Red.) *Inleiding criminaliteit en opsporing* (pp.23-35). Den Haag: Boom Juridische Uitgevers.

Ferwerda, H.B. (2004). *Huiselijk geweld: de voordeur op een kier. Omvang, aard en achtergronden in 2004 op basis van landelijke politiecijfers*. Arnhem: A&O Beke.

Forde, D. R., & Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly*, *14*, 265-294.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston, MA: Addison-Wesley.

Galetsas, A. (2007). *Statistical Information on Network Security*. European Commission Information Society and Media Directorate-General. Brussels: European Commission.

Garland, D. (2002). Of Crimes and Criminals: The Development of Criminology in Britain. In M. Maguire, R. Morgan, & R. Reiner (Eds). *The Oxford Handbook of Criminology*. Oxford: Oxford University Press.

Geest, E. van (2006). *Van herkenning tot aangifte. Handleiding cybercrime*. Den Haag: Govcert.nl.

Gibbs, J.J., Giever, D, & Martin, J.S. (1998). Parental management and self-control: an empirical test of Gottfredson's and Hirschi's general theory. *Journal of research in Crime and Delinquency*, *35*, 40-70.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

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

Govcert.nl (2010). *Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010*. http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/dienstverlening/kennis-en-publicaties/trendrapporten/trendrapport-2010/trendrapport-2010/govcert%3AdocumentResource/govcert%3Aresource. Laatst geraadpleegd op 25 augustus 2012.

Grabosky, P. N. (2001). Virtual Criminality: Old Wine in New Bottles? *Social and Legal Studies*, *10*, 243-249.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. In D. Wall (Ed.) *Crime and the Internet* (pp. 23-45). London: Routledge.

Grasmick, H.G., Tittle, C.R., Bursik, R.J., & Arneklev, B.J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, *30*, 5-29.

Groenhuijsen, M.S. (2008b). Slachtoffers van misdrijven in het recht en in de victimologie. Verslag van een intellectuele zoektocht. *Delikt en Delinkwent*, *38*(2), 121-145.

Groenhuisen, M.S. (2008a). Naar een eigenstandig academisch statuut van de victimologie. In M. Moering, M. de Lange, & A. Franken (Ed.). *Constante waarden: Liber Amicorum prof. Mr. Constantijn Kelk* (pp. 101-111). Den Haag: Boom Juridische uitgevers.

Hackworth, A. (2005). *Spyware*. Carnegie Mellon University. www.cert.org. Laatst geraadpleegd op 26 augustus 2012.

Halbert, D. (1997). Discourses of danger and the computer hacker. *The Information Society*, *13*, 361-74.

Hindelang, M. J., Gottfredson, M. R., & Gaffalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger.

Hinduja, S. & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, *29*(2), 129-156.

Hoekman, J., & Dirkzwager, C. (2009). Virtuele diefstal: hoe gegevens toch weer goederen werden. *Computerrecht*, 4, 158-161.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*, 1-25.

Holt, T.J., & Graves, D.C. (2A Qualitative Analysis of Advance Fee Fraud E-mail Schemes. *International Journal of Cyber Criminology*, *1*(1), 137-154.

Holt, T.J., Bossler, A.M., & May, D.C. (2011). Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance. *American Journal of Criminal Justice*. http://news.msu.edu/media/documents/2011/06/963e40c7-08ff-411d-af16-fe7563496f89.pdf. Laatst geraadpleegd op 9 september 2012.

Holtfreter, K., Reisig, M.D., & Pratt, T.C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*, 189-220.

House of Commons Science and Technology Committee (2012). *Malware and Cybercrime: Twelfth Report of Session 2010-12*. HC 1537London: The Stationary Office Limited.

Hulst, R.C., van der, & Neve, R.J.M. (2008). *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders*. Den Haag: WODC.

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice*, *20*(3), 433–452.

Internet Crime Complaint Center (2009). *2008 Internet Crime Report*. Washington: IC3.

Internet Crime Complaint Center (2011). *2010 Internet Crime Report*. Washington: IC3.

Jaishankar, K., Shariff, S., & Ramdoss, S. (2008). Pedophilia, Pornography, and Stalking: Analyzing Child Victimization on the Internet. In F. Schmallenger, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 28-42). Upper Saddle River NJ: Prentice Hall.

James, D., & Philip, M. (2012). A Novel Anti Phishing Framework Based on Visual Cryptography. *International Journal of Distributed and Parallel Systems*, *3*(1), 207-218.

Jansen, J. (te verwachten). Financieel-economische criminaliteit. In J. Kerstens & W. Ph. Stol (Red.) *Jeugd & Cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren*. Den Haag: Boom Juridische uitgevers.

Javelin Strategy & Research (2012). *2011 Identity Fraud Survey Report: Consumer Version*, February 2012.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *Sociological Review, 46*(4), 757-780.

Joutsen, M. (1998). The internationalization of victimologie. In H.-D. Schwind, E. Kube, & H.-H. Kuehne (Eds.). Criminology on the threshold of the 21st century (pp. 353-365). Berlin: De Gruyter.

Kambil, A., & Heck, E. V. (2002). *Making markets*. Boston, MA: Harvard Business School Press.

Kapersky, E. V. (2003). *The classification of computer viruses.* Bern: Metropolitan Network BBS Inc.. http://www.avp.ch/avpve/classes/classes.stm. Laatst geraadpleegd op 23 augustus 2012.

Karmen, A. (1990). *Crime Victims: An Introduction to Victimology*. Belmont, CA: Wadsworth Publishing.

Kennedy, L.W., & Sacco, V.F. (1998). *Crime victims In context*. Los Angeles: Roxbury Publishing Company.

Kerckvoorde, J. van (1995). *Een maat voor het kwaad?* Leuven: Universitaire Pers Leuven.

Kerstens, J., & Stol, W. Ph. (Red.). (te verwachten). *Jeugd & Cybersafety: Online slachtoffer- en daderschap onder Nederlandse jongeren*. Den Haag: Boom Juridische uitgevers.

Kokswijk, J. van, & Lodder, A. (2008). *Virtuele werelden en regulering*. Den Haag: Rathenau Instituut.

Koops, B-J. (2010). The Internet and its Opportunities for Cybercrime. In M. Herzog-Evans (Ed.). *Transnational criminology Manual*, *Vol. 1* (pp. 735-774). Nijmegen: Wolf Legal Publishers.

Koops, B-J. (2012). De dynamiek van cybercrimewetgeving in Europa en Nederland. *Justitiële Verkenningen*, 38(1), 9-24.

Kowalski, M. (2002). Cyber-Crime: Issues, Data Scources, and Feasibility of Collecting Police-Reported Statistics. In S.C.C.C.f.J. Statistics (Eds.). (pp.31). http://dsp-psd.pwgsc.gc.ca/Collection/Statcan/85-558-X/85-558-XIE2002001.pdf. Laatst geraadpleegd op 20 augustus 2012.

Langton, L., & Planty, M. (2010). *Victims of Identity Theft, 2008*. Washington: Bureau of Justice Statistics.

Lauritsen, J.L. (2005). Social and Scientific Influences on the Measurement of Criminal Victimization. *Journal of Quantitative Criminology*, *17*,3.

Lessig, L. (1999). The law of the horse: what cyberlaw might teach. *Harvard Law Review*, *113*, 501.

Leukfeldt, E.R., M.M.L. Domenie, M.M.L., & Stol, W. Ph. (2010) *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische Uitgevers.

Leukfeldt, E.R., & Stol, W.Ph. (2011) *Internetoplichters uitgelicht. E-fraudeurs en klassieke fraudeurs vergeleken*. De Bilt / Leeuwarden: Programma Aanpak Cybercrime / NHL Hogeschool.

Leukfeldt, R., Kentgens, A., Frans, B., Toutenhoofd, M. Stol, W. Ph., & Stamhuis, E. (2012). *Alledaags politiewerk in een gedigitaliseerde wereld. Handreiking voor delicten met een digitale component*. Den Haag: Boom Lemma Uitgevers.

Lissenberg, E. (1997). Overheid en slachtoffers. Aantasting van een geweldsmonopolie? *Tijdschrift voor Criminologie*, 39,(4), 310-321.

Lissenberg, E. (2001). Definities van criminaliteit. In E. Lissenberg, S. van Ruller, R. van Swaaningen (Red.) *Tegen de regels 4. Een inleiding in de criminologie* (pp. 39-50). Nijmegen: Ars Aequi Libri.

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. *Berkeley Technology Law Journal*, *20*, 259-300.

McAfee Labs (2011). *McAfee Threats Report: Third Quarter 2011*. www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2011.pdf. Laatst geraadpleegd op 25 augustus 2012.

McKinnon, R. (1997). Virtual rape. *Journal of Computer Mediated Communication*, *2*(4). Xx

McLennan, G., Pawson, J., & Fitzgerald, M. (1980). Crime and Society: Readings in History and Theory. London: Routledge.

Messner, S. F., & Blau, J. R. (1987). Routine Leisure Activities and Rates of Crime: A Macro-Level Analysis. *Social Forces, 65*(4), 1035-1052.

Messner, S. F., Zhou, L., Lening, Z., & Jianhong, L. (2007). Risks of Criminal Victimization in Contemporary Urban China: An Application of Lifestyle/Routine Activities Theory. *Justice Quarterly, 24*, 496-522.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context : toward an integrated theory of offenders, victims, and situations*. Albany: State University of New York Press.

Miethe, T. D., Stafford, M. C., & Long, J. S. (1987). Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories. *American Sociological Review, 52*(2), 184-194.

Moitra, S.D. (2005). Developing Policies for Cybercrime: Some Empirical Issues. *European Journal of Crime, Criminal Law and Criminal Justice, 13*(3), 435-464.

Morris, S. (2004). *The future of nectarism now: Part 1 – threats and challenges. UK home office online report nr. 6 2/04, 2004*. www.homeoffice.gov.uk/rds/pdf04/rdsolr6204.pdf. Laatst geraadpleegd op 2 september 2012.

Moszkowicz, Y. (2009). Een kritische noot bij de 'Runescape'- en 'Habbohotel'-uitspraken: een illusive is geen goed. *Strafblad*, *7*(5), 495-503.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures. *Criminology, 36*, 829-857.

Nazario, J. (2003). *Defense and detection strategies against Internet worms.* Norwood, MA: Artech House.

Newman, G.R. (2009). Cybercrime. In M.D. Krohn, A.J. Lizotte, & G. Penly Hall (Eds.). *Handbook on Crime and Deviance* (pp. 551-584). New York: Springer Publishers.

Newman, G.R., & Clarke, R.V. (2003). *Superhighway Robbery: Preventing e-commerce crime*. Cullompton: Willan Publishing.

Newman, O. (1972). *Defensible Space*. New York, NY: Macmillan.

Ngo, F.T., & Paternoster, R. (2011). Cybercrime victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nikitkov, A.N., Stone, D.N., & Miller, T.C. (2011). Tracing the Birth and Evolution of Mundane Online Crime: Routine Activity Theory (RAT), Management Control Systems, and the Sustainable Online Auction Con. Under Review. http://www.business.umt.edu/Libraries/LaurieToomey/dan_stone_paper.sflb.ashx. Laatst geraadpleegd op 9 september 2012.

Parker, D.B. (1973). *Computer Abuse*. Palo Alto.

Parsons-Pollard, N., & Moriarty, L. J. (2008). Cyberstalking: What's the big deal? In L. J. Moriarty (Ed.), *Controversies in Victimology* (pp. 1031-13). Cincinnati, OH: Anderson.

Pauwels, L., & Pleysier, S. (2008). Crime Victims and Insecurity in Belgium and the Netherlands. In R. Zauberman (Ed.), *Victimization and Insecurity in Europe. A Review of Surveys and their Use* (pp. 39-64). Brussel: VUBPress.

Pauwels, L., & Pleysier, S. (2009). Self-report studies in Belgium and the Netherlands. In R. Zauberman (Ed.), *Victimization and Insecurity in Europe. A Review of Surveys and their Use* (pp. 51-76). Brussel: VUBPress.

Pease, K. (2001). Crime futures and foresight: Challenging criminal behaviour in the information age. In D. Wall (Ed.) *Crime and the internet*. London: Routledge.

Philips, F., & Morrissey, G. (2004). Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet. *Convergence, 10***,** 66-79.

Piquero, A. R., & Tibbetts, S. (1996). Specifying the direct and indirect effects of low self control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly*, *13*, 481-510.

Piquero, A.R., MacDonald, J., Dobrin, A., Daigle, L., & Cullen, F. (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology*, *21*, 55-71.

Polakowski, M. (1994). Linking self- and social control with deviance: illuminating the structure underlying a general theory of crime and its relation to deviant activity. *Journal of Quantitative Criminology*, *10*, 41-78.

Pratt, T. C., & Cullen, F. T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*, 931-964.

Regeerakkoord (2010). *Vrijheid en Verantwoordelijkheid*. Regeerakkoord VVD-CDA, Rapport 30 september 2010. http://www.kabinetsformatie2010.nl/pdf/dsc9a1a.pdf?c=getobject&s=obj&objectid=127493. Laatst geraadpleegd op 23 augustus 2012.

Reno, J. (1999). *Cyberstalking: A new challenge for law enforcement and industry*. Washington, DC: U.S. Department of Justice. http://www.justice.gov/criminal/cybercrime/cyberstalking.htm. Laatst geraadpleegd op 4 september 2012.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12,* 99-118.

Reyns, B.W., Henson, B., & Fisher, B.S. (2011). Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theorie to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*, 1149-1169.

Rock, P. (1994). *Victimology*. Dartmouth: Aldershot.

Ross, G., & Smith, R. (2011). Risk factors for advance fee fraud victimisation. *Trends & Issues in Crime and Criminal Justice* no. 420. Canberra: Australian Institute of Criminology. http://www.aic. gov.au/ publications/ current%20series/ tandi/401-420/tandi420.aspx. Laatst geraadpleegd op 3 september 2012.

Ryan, J.J.C.H., & Jefferson, T. (2003). *The Use, Misuse, and Abuse of Statistics in Information Security Research*. Proceedings of the 23rd ASEM National Conference, ASEM 15-18 October 2003.

Ryan, W. (1971). *Blaming the Victim*. New York: Pantheon Books.

Sampson, R. J., & Wooldredge, J. D. (1987). Linking the micro- and macro-level dimensions of lifestyle-routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology, 3*(4), 371-393.

Schiller, C. A., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C. & Cross, M. (2007). *Botnets: The killer web app*. Rockland, Ma: Syngress Publishing.

Schneider, H.J. (2001). Victimological Developments in the World During the Past Three Decades (I): A Study of Comparative Criminology. International Journal of Offender Therapy and Comparative Criminology, 45(4), 449-468.

Schoenmakers, Y.M.M., Vries Robbé, E., de, & Wijk, A. Ph., van (2009). *Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak.* Den Haag: Reed Business.

Schreck, C. J., Wright, R. A., & Miller, J. M. (2002). A study of individual and situational antecedents of violent victimization. *Justice Quarterly*, *19*, 159-180.

Schreck, C.J. (1999). Criminal victimization and low self-control: An extension and test of a general theory of crime. *Justice Quarterly*, *16*, 633-654.

Schreck, C.J., Stewart, E.A., & Fisher, B.S. (2006). Self-control, victimization, and their influence on risky life styles: A longitudinal analysis using panel data. *Journal of Quantitative Criminology*, *22*, 319-350.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13,* 627-640.

Sikkel, D. (2010). *Voorbereiding nulmeting cybercrime en financieel-economische criminaliteit*. Leidschendam: WODC.

Skibell, R. (2002). The myth of the computer hacker. *Information, Security and Society, 5*, 336-356.

Skoudis, E., & Zeltzer, L. (2004). Malware: Fighting Malicious Code 3. Upper Saddle River: Prentice Hall Professional Technical Reference.

Smith, R. G., Holmes, M. N., and Kauffman, Ph. (1999). *Trends and issues in crime and criminal justice No. 121: Nigerian Advance Fee Fraud.* Australian Institute of Criminology. http://www.aic.gov.au/publications/tandi/ti121.pdf. Laatst geraadpleegd op 2 september 2012

Sommer, P. (2009). *Literature Review on Internet Crime for National Audit Office*. London: LSE.

Spano, R., & Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology, 70*, 414-437.

Spitzberg, B. (2002). The Tactical Topography of Stalking Victimization and Management. *Trauma, Violence and Abuse*, *3*(4),261-288.

Spitzberg, B. H., & Hoobler, G. (2002). Cyberstalking and the technologies of interpersonal terrorism. *New Media & Society, 4,*71-92.

Sproule, S., & Archer, N. (2006). *Defining Identity Theft – A Discussion Paper*. McMaster eBusiness ResearchCentre (MeRC), McMaster University. http://www.business.mcmaster.ca/idtdefinition/IDT%20Discussion%20Paper%20Revision%20from%20Sue%20Sproule%20April%206%2006.pdf. Laatst geraadpleegd op 1 september 2012.

Sterling, B. (1992). The *hacker crackdown: Law and disorder on the electronic frontier*. London: Viking.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*, 159-181.

Stewart, E.A., Elifson, K.W., & Sterk, C.E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly*, *21*, 159-181.

Stol, W.Ph., & Treeck, R.J., van (2001). *Criminaliteitsbestrijding in cyberspace – vanuit Nederland. Handboek Politiediensten*. Diegem (B): Kluwer Editorial, 3-40.

Stol, W.Ph., Leukfeldt, E.R., & Klap, H. (2012) Cybercrime en politie. Een schets van de Nederlandse situatie anno 2012. *Justitiële Verkenningen*, *38*(1) 25-39.

Sutherland, E. H., & Cressey, D. (1960). Principles of Criminology. Philadelphia: Lippincott.

Symantec Corporation (2012). Symantec Internet security threat report. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf. Laatst geraadpleegd op 23 augustus 2012.

Szor, P. (2005). *The art of computer virus research and defense.* Upper Saddle River, NJ: Addison Wesley.

Tanfa, D.Y. (2006). *Advanced fee fraud* [Thesis]. University of South Africa. http://uir.unisa.ac.za/bitstream/handle/10500/2304/thesis.pdf?sequence=1. Laatst geraadpleegd op 2 september 2012.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). *Digital crime and digital terrorism.* Upper Saddle River, NJ: Pearson Prentice Hall.

Tewksbury, R. & Mustaine, E. (2000). Routine activities and vandalism: A theoretical and empirical study. *Journal of Crime & Justice, 23*, 81-110.

Vanderveen, G.N.G. (2004). Meten van veiligheid. In E.R. Muller (Red.), *Veiligheid; studies over inhoud, organisatie en maatregelen* (pp. 71-122). Alphen aan den Rijn: Kluwer.

Versteegh, P., & Heuvel, J., van de (2007). Is de nieuwe veiligheidsmonitor grappig? *Secondant*, *6*, 44-47.

Vries, U.R.M.Th. de, Tigchelaar, H., Linden, M. van der & Hol, A.M. (2007). *Identiteitsfraude: een afbakening. Een internationale begripsvergelijking en analyse van nationale strafbepalingen*. Utrecht: Universiteit Utrecht. Disciplinegroep

Rechtstheorie. Departement Rechtsgeleerdheid, Universiteit Utrecht en WODC, Ministerie van Justitie.

Wall, D. S. (2007). *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Wall, D.S.(2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1), 45-63.

Wallis Consulting (2007). *Community attitudes to privacy*. http://www.privacy.gov.au/publications/rcommunity07.pdf. Laatst geraadpleegd op 1 september 2012.

Williams, F. P., & McShane, M. D. (1999). *Criminological theory*. Upper Saddle River, NJ: Prentice Hall.

Williams, M. (2006). *Virtually Criminal*. Abingdon: Routledge.

Wilsem, J. van (2010a). Digitale en traditionele bedreiging vergeleken. Een studie naar risicofactoren van slachtofferschap. *Tijdschrift voor Criminologie*, *1*, 73-87.

Wilsem, J. van (2012). Slachtofferschap van identiteitsfraude: een studie naar aard, omvang en risicofactoren van slachtofferschap. *Justitiële verkenningen*, *38*(1), 97-107.

Wilsem, J., van (2010b). Gekocht, maar niet gekregen. Slachtoffers van online oplichting nader onderzocht. *Tijdschrift voor Veiligheid*, *9*(4). 16-29.

Wilsem, J., van (2011). *Typologizing identity fraud. A Dutch study of unauthorized cash withdrawal from bank accounts*. Lezing tijdens congres van Internationaal Academy for Investigative Psychology, 31 maart 2011. Amsterdam: VU.

Wilson, J.K. (Ed.) (2009). The Praeger Handbook of Victimology. Santa Barbara, CA: ABC-CLIO.

Wittbrood, K., & Nieuwbeerta, P. (2006). Een kwart eeuw stijging in geregistreerde criminaliteit. Vooral meer registratie, nauwelijks meer criminaliteit. Tijdschrift voor criminologie, *48*, 227-242.

Wittebrood, K. (2006). Slachtoffers van criminaliteit: Feiten en achtergronden. Den Haag: SCP.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Society of Criminology*, 2, 407-427.

Yucedal, B. (2010). Victimization in cyberspace: an application of routine activity and lifestyle exposure theories. PHD Kent State University. http://etd.ohiolink.edu/send-pdf.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984. Laatst geraadpleegd op 23 augustus 2012.

Zijderveld, A.C., Cleiren, C.P.M., & Du Perron, C.E. (2005). Het opstandige slachtoffer: genoegdoening in strafrecht en burgerlijk recht. Deventer: Kluwer.

Bijlagen

Bijlage 1 lijst geïnterviewde personen

- Simon van de Geer, beleid, ministerie van justitie
- Wim Wensink, meldpunt identiteitsfraude
- René Hesseling (analyse en research) en Ruud Elderhorst (teamchef digitale expertise), Haaglanden
- Erik Boerboom (Wnd Teamchef FO – Digitaal) en Gerard Hofstede (financiële ondersteuning), Flevoland
- Rob van Dalen, KLPD / NR
- Nural Orucu (meldpunt cybercrime), Peter Zinn (THTC), Rob van Dalen (NR), KLPD
- Chantal Malfeyt, Jurist Marktplaats
- Brigitte Bloem en Cees Schep, team fraude, KLPD
- Jolanda Boorsma, zeden, Amsterdam-Amstelland
- Majolein Viersma (dig. rechercheur) en Barend Frans (team kwaliteitsimpuls intake en opsporing), Amsterdam-Amstelland
- Stef Cusiel en Hans Doevendans, digitale opsporing NRE
- John van Kesteren, Intervict, UvT
- Hans Pijnenburg, BR Zuidoost
- Lodewijk van Zwieten, OvJ hightechcrime, landelijk parket
- Bureau Veiligheidsmonitor, Dick Meuldijk
- (Rienk Eisma, afstudeerder politieacademie)

Bijlage 2 respons testmeting NHL lay-out

Respons NHL, werkelijk			geëxtrapoleerd
Online afname	**N**	**% van 1249**	
Adressen	1.249		1.249
Brieven onbezorgbaar	2	0,2%	2
Respons eerste mailing	38	3,0%	38
Respons tweede mailing	64	5,1%	64
Geweigerd telefonisch/mail	2	0,2%	2
Papieren vragenlijst aangevraagd	3	0,2%	3
Totaal afgewerkt	**109**	**8,7%**	**109**
Adressen over na online enquête	**1.140**		**1.140**
Telefoonnummers opvragen			
Steekproef van adressen	526		1.140
Telefoonnummers in steekproef	399	75,9%	865
Bereik nabellen	**N**	**% van 399**	
Incorrecte nummers	38	9,5%	82
6 keer niet bereikt	37	9,3%	80
Bereikt	324	81,2%	702
	399		865
Reactie nabellen	**N**	**% van 399**	
Medewerking geweigerd	179	44,9%	388
Alsnog toegezegd	113	28,3%	245
Telefonisch afgenomen	0	0,0%	0
Papieren vragenlijst aangevraagd	55	13,8%	119
	347	87,0%	752
Respons nabellen	**N**	**% van 399**	
Alsnog zelf online gedaan	57	14,3%	124
Papieren vragenlijsten geretourneerd	16	4,0%	35
	73	18,3%	158

Totale respons	**175**	**14,0%**	**260**
			20,8%

Bijlage 3 vragenlijst onderzoek

(apart pdf-bestand)

Bijlage 4 brief onderzoek (geprint op KLPD briefpapier)

Korps Landelijke Politiediensten
p.a. Postbus 1080
8900 CB Leeuwarden

Leeuwarden, 15 april 2011

<Aanhef1> <initialen> <naam>
<straatnaam> <huisnummer>
<postcode> <Woonplaats>

Betreft: onderzoek naar (on)veiligheid in de digitale wereld

Geachte <aanhef2> <naam>,

Met deze brief nodigen wij u uit om deel te nemen aan het landelijke onderzoek naar (on)veiligheid in de digitale wereld. Digitalisering heeft Nederlanders de afgelopen jaren veel nieuwe mogelijkheden geboden. Via internet kan iedereen winkelen, contacten onderhouden, bankieren, muziek luisteren, informatie zoeken enzovoorts. De digitale wereld kent echter net als de 'gewone wereld' ook onveilige situaties.

Om te weten te komen hoe Nederlanders gebruikmaken van de digitale wereld en omgaan met onveilige situaties op internet voeren de Open Universiteit Nederland (OU) en lectoraat Cybersafety van NHL Hogeschool dit onderzoek uit. Het Korps Landelijke Politiediensten (KLPD) heeft opdracht gegeven voor het onderzoek. Het ministerie van Veiligheid en Justitie, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Centraal Bureau voor de Statistiek (CBS) zijn nauw bij het onderzoek betrokken.

Waarom ontvangt u deze uitnodiging?
Natuurlijk kunnen niet alle inwoners van Nederland ondervraagd worden, daarom heeft het CBS voor dit onderzoek een steekproef getrokken uit de bevolkingsadministratie van Nederlandse gemeenten. Uw naam is in deze steekproef naar voren gekomen.

Hoe kunt u meewerken?
Wij vragen u een vragenlijst in te vullen over (on)veiligheid in de digitale wereld. Het invullen van de vragenlijst kost ongeveer 15 minuten tijd. De vragen gaan over uw gebruik van digitale mogelijkheden, hoe u omgaat met onveilige situaties op internet en over mogelijke incidenten die u heeft meegemaakt in de digitale wereld. Ook als u geen gebruik maakt van internet of geen incidenten heeft meegemaakt, zijn uw antwoorden belangrijk voor het onderzoek! U kunt de vragenlijst via internet invullen of op papier.

Om de vragenlijst via internet in te vullen moet u het volgende doen:
- Open uw webbrowser (bijvoorbeeld Internet Explorer, FireFox of Google Chrome);
- Type 'www.politie.nl/klpd/internetonderzoek' in de adresbalk van uw webbrowser (boven in uw scherm);
- U komt nu op de website van de politie;
- U klikt op de link 'vragenlijst invullen'. U wordt dan via een beveiligde verbinding naar de vragenlijst doorgestuurd. U kunt deze beveiligde verbinding herkennen aan de beginletters 'https' in plaats van 'http';
- U kunt inloggen met deze inlogcode: **<inlogcode>**;
- Na het inloggen krijgt u verdere informatie over het invullen van de vragenlijst.

Als u de vragenlijst niet via internet kunt of wilt invullen, kunt u een papieren vragenlijst aanvragen via het telefoonnummer 058-2511700, via een e-mail naar internetonderzoek@klpd.politie.nl, of via de website www.politie.nl/klpd/internetonderzoek. Als u niet mee wilt werken, kunt u zich op deze manieren ook afmelden voor het onderzoek; u wordt dan voor dit onderzoek niet meer benaderd.

Privacy
Bij dit onderzoek is uw privacy volledig gewaarborgd. Uw persoonsgegevens worden na afloop van het onderzoek vernietigd. Als de internetvragenlijst is gesloten, worden de antwoorden opgeleverd aan het CBS en is de CBS privacy waarborging van toepassing. U leest hierover meer onderaan deze pagina.

Ten slotte
Indien u vragen heeft over het onderzoek, de waarborging van uw privacy of als u problemen heeft bij het invullen van de vragenlijst dan kunt u contact opnemen met het onderzoeksteam. Dit kan via een e-mail naar internetonderzoek@klpd.politie.nl of via telefoonnummer 058-2511700. Het onderzoeksteam is bereikbaar van maandag tot en met vrijdag tussen 09:00 en 17:00 uur. Meer informatie over het onderzoek is te lezen op www.politie.nl/klpd/internetonderzoek.

Bij voorbaat hartelijk dank voor uw medewerking.

Met vriendelijke groet,

<handtekening Ruud Bik>

R.G.C. Bik
Korpschef Korps Landelijke Politiediensten

CBS privacy waarborging

Bij al onze onderzoeken is uw privacy gewaarborgd. Dit is een verplichting van het CBS die in een speciale wet is vastgelegd. Om uw gegevens te beveiligen heeft het CBS tal van maatregelen getroffen. Zo is er een strenge geheimhoudingsplicht voor alle medewerkers, op straffe van rechtsvervolging. Gegevens over mensen worden zo snel mogelijk gescheiden van de namen en adressen. De gegevens worden verwerkt met goed beveiligde computersystemen waartoe onbevoegden geen toegang hebben. De wet garandeert dat uw gegevens alleen voor statistische doeleinden worden gebruikt. Geen enkele instelling kan toegang opeisen tot de gegevens die het CBS verzamelt. In de statistische informatie die het CBS naar buiten brengt, zijn persoonlijke gegevens nooit te herkennen.

Het CBS verzamelt niet alleen zelf gegevens maar krijgt ook veel bestanden van andere instellingen. Bijvoorbeeld de gegevens van de bevolkingsadministraties, de centra voor Werk en inkomen (UWV WERKbedrijven), de sociale diensten en de salarisadministraties van veel bedrijven. Wij combineren automatisch de informatie die u zelf in dit onderzoek geeft met informatie die we van andere instellingen krijgen. Met deze gecombineerde informatie stelt het CBS statistieken samen over Nederland en werken we zo zuinig mogelijk.

Bijlage 5 brief onderzoek voor personen van 15 jaar (geprint op KLPD briefpapier)

Korps Landelijke Politiediensten
p.a. Postbus 1080
8900 CB Leeuwarden

Leeuwarden, 15 april 2011

Aan de ouder(s)/verzorger(s) van: <initialen> <naam>
<straatnaam> <huisnummer>
<postcode> <Woonplaats>

Betreft: onderzoek naar (on)veiligheid in de digitale wereld

Geachte <aanhef2> <naam>,

Met deze brief nodigen wij uw kind uit om deel te nemen aan het landelijke onderzoek naar (on)veiligheid in de digitale wereld. Digitalisering heeft Nederlanders de afgelopen jaren veel nieuwe mogelijkheden geboden. Via internet kan iedereen winkelen, contacten onderhouden, bankieren, muziek luisteren, informatie zoeken enzovoorts. De digitale wereld kent echter net als de 'gewone wereld' ook onveilige situaties.

Om te weten te komen hoe Nederlanders gebruikmaken van de digitale wereld en omgaan met onveilige situaties op internet voeren de Open Universiteit Nederland (OU) en lectoraat Cybersafety van NHL Hogeschool dit onderzoek uit. Het Korps Landelijke Politiediensten (KLPD) heeft opdracht gegeven voor het onderzoek. Het ministerie van Veiligheid en Justitie, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Centraal Bureau voor de Statistiek (CBS) zijn nauw bij het onderzoek betrokken.

Waarom ontvangt u deze uitnodiging?
Natuurlijk kunnen niet alle inwoners van Nederland ondervraagd worden, daarom heeft het CBS voor dit onderzoek een steekproef van Nederlanders getrokken. In deze steekproef is de naam van uw kind naar voren gekomen. Wij nemen geen vragenlijsten af bij kinderen jonger dan 16 jaar zonder de toestemming van de ouder(s) of verzorger(s). Daarom verzoeken wij u met deze brief dit kind een vragenlijst in te laten vullen.

Hoe kan uw kind meewerken?
Wij vragen u uw kind een vragenlijst in te laten vullen over (on)veiligheid in de digitale wereld. Het invullen van de vragenlijst kost ongeveer 15 minuten tijd. De vragen gaan over het gebruik van digitale mogelijkheden, hoe uw kind omgaat met onveilige situaties op internet en over mogelijke incidenten die uw kind heeft meegemaakt in de digitale wereld. Ook als uw kind geen gebruik maakt

van internet of geen incidenten heeft meegemaakt, zijn de antwoorden belangrijk voor het onderzoek! Uw kind kan de vragenlijst via internet invullen of op papier.

Om de vragenlijst via internet in te vullen moet uw kind het volgende doen:
- Open de webbrowser (bijvoorbeeld Internet Explorer, FireFox of Google Chrome);
- Type 'www.politie.nl/klpd/internetonderzoek' in de adresbalk van de webbrowser (boven in het scherm);
- U komt nu op de website van de politie;
- U klikt op de link 'vragenlijst invullen'. U wordt dan via een beveiligde verbinding naar de vragenlijst doorgestuurd. U kunt deze beveiligde verbinding herkennen aan de beginletters 'https' in plaats van 'http';
- U kunt inloggen met deze inlogcode: **<inlogcode>**;
- Na het inloggen krijgt u verdere informatie over het invullen van de vragenlijst.

Als uw kind de vragenlijst niet via internet kan of wil invullen, kan een papieren vragenlijst aangevraagd worden via het telefoonnummer 058-2511700, via een e-mail naar internetonderzoek@klpd.politie.nl of via de website www.politie.nl/klpd/internetonderzoek. Als u niet wilt dat uw kind meewerkt, kunt u zich op deze manieren ook afmelden voor het onderzoek; u wordt dan voor dit onderzoek niet meer benaderd.

Privacy

Bij dit onderzoek is de privacy van u en uw kind volledig gewaarborgd. De persoonsgegevens van uw kind worden na afloop van het onderzoek vernietigd. Als de internetvragenlijst is gesloten, worden de antwoorden opgeleverd aan het CBS en is de CBS privacy waarborging van toepassing. U leest hierover meer onderaan deze pagina.

Ten slotte

Indien u vragen heeft over het onderzoek, de waarborging van de privacy of als uw kind problemen heeft bij het invullen van de vragenlijst dan kan contact opgenomen worden met het onderzoeksteam. Dit kan via een e-mail naar internetonderzoek@klpd.politie.nl of via telefoonnummer 058-2511700. Het onderzoeksteam is bereikbaar van maandag tot en met vrijdag tussen 09:00 en 17:00 uur. Meer informatie over het onderzoek is te lezen op www.politie.nl/klpd/internetonderzoek.

Bij voorbaat hartelijk dank voor uw medewerking.

Met vriendelijke groet,

<handtekening Ruud Bik>

R.G.C. Bik
Korpschef Korps Landelijke Politiediensten

CBS privacy waarborging

Bij al onze onderzoeken is uw privacy gewaarborgd. Dit is een verplichting van het CBS die in een speciale wet is vastgelegd. Om uw gegevens te beveiligen heeft het CBS tal van maatregelen getroffen. Zo is er een strenge geheimhoudingsplicht voor alle medewerkers, op straffe van rechtsvervolging. Gegevens over mensen worden zo snel mogelijk gescheiden van de namen en adressen. De gegevens worden verwerkt met goed beveiligde computersystemen waartoe onbevoegden geen toegang hebben. De wet garandeert dat uw gegevens alleen voor statistische doeleinden worden gebruikt. Geen enkele instelling kan toegang opeisen tot de gegevens die het CBS verzamelt. In de statistische informatie die het CBS naar buiten brengt, zijn persoonlijke gegevens nooit te herkennen.

Het CBS verzamelt niet alleen zelf gegevens maar krijgt ook veel bestanden van andere instellingen. Bijvoorbeeld de gegevens van de bevolkingsadministraties, de centra voor Werk en inkomen (UWV WERKbedrijven), de sociale diensten en de salarisadministraties van veel bedrijven. Wij combineren automatisch de informatie die u zelf in dit onderzoek geeft met informatie die we van andere instellingen krijgen. Met deze gecombineerde informatie stelt het CBS statistieken samen over Nederland en werken we zo zuinig mogelijk.