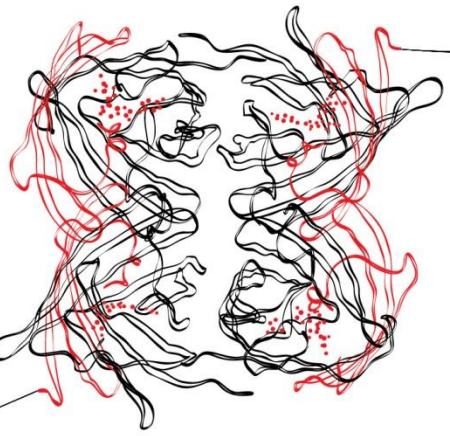
HET METEN VAN CYBERCRIME

Validiteit van de door het CBS gebruikte vragenlijst en alternatieve mogelijkheden



UNIVERSITEIT TWENTE.

Het meten van Cybercrime: Validiteit van de door het CBS gebruikte vragenlijst en alternatieve mogelijkheden

Bachelorscriptie
Rick Verkade

Begeleiders:
Prof. Dr. M. Junger
Dr. A.L. Montoya

Externe begeleiders:
Prof. Dr. F.L. Leeuw – Directeur WODC
Dhr. D. Meuldijk – Hoofd Bureau Veiligheidsmonitor

Universiteit Twente
Enschede, 9 februari 2015

UNIVERSITEIT TWENTE.

Voorwoord

Voor u ligt mijn bachelorscriptie die ingaat op de validiteit van de door het Centraal Bureau voor de Statistiek (CBS) gebruikte methode voor het meten van slachtofferschap van cybercrime. Vanaf het moment dat ik de overstap maakte naar de middelbare school heb ik een bovengemiddelde interesse gehad in de redenen die individuen en groepen hebben voor het plegen van misdaden. Gezien het feit dat criminaliteit uiteraard kan worden gezien als maatschappelijk probleem, en dus aansluit bij een studie Bestuurskunde, was het onderwerp voor mijn bachelorscriptie snel gekozen. Het moest iets met criminaliteit te maken hebben.
Professor Junger kwam al snel met het onderwerp cybercrime, een onderwerp waar ze vanuit de Universiteit Twente onderzoek naar doet. Het onderwerp sprak me direct aan. Dit vooral vanwege het feit dat er nog weinig bekend is met betrekking tot cybercrime en het een relatief nieuw soort criminaliteit is. Waarbij er bij traditionele vormen van criminaliteit al veel onderzocht is, is er op het gebied van cybercrime nog veel te onderzoeken. Vooral het meten van slachtofferschap van cybercrime is nog relatief zeldzaam. Daarom hoop ik door middel van deze bachelorscriptie iets aan de wetenschap toe te voegen op dat gebied.

In dit voorwoord maak ik van de gelegenheid gebruik om professor doctor Marianne Junger te bedanken voor de hulp en begeleiding tijdens dit onderzoek. Mede dankzij haar begeleiding en kritische blik heb ik dit onderzoek kunnen afronden. Tevens bedank ik professor doctor Pieter Hartel en doctor Lorena Montoya voor hun taak als tweede begeleider en het meedenken met het onderzoek.

Ook bedank ik professor doctor Frans Leeuw, directeur van het Wetenschappelijk onderzoek- en documentatiecentrum (WODC), en dhr. Dick Meuldijk, hoofd Bureau Veiligheidsmonitor, voor hun hulp als externe begeleider en voor een inkijkje in hoe de overlegvoering op dergelijk niveau in zijn werk gaat.
Dankzij Jennifer van den Hoven en Ilona Malisse is de dataverzameling tot een goed einde gekomen. Door hun hulp en inzet is het mogelijk geweest een totaal van 225 respondenten te ondervragen. Een aantal dat ik anders niet had kunnen bereiken. Mijn dank daarvoor.
Tevens bedank ik Inés Carvajal voor het controleren van de coderingen bij de omschrijvingen van de respondenten.

Uiteraard bedank ik alle respondenten voor hun medewerking aan het onderzoek. Zonder hun medewerking zijn slachtofferschapsonderzoeken niet mogelijk. Ik bedank hen voor alle eerlijke antwoorden en hun vertrouwen om mij, Jennifer en Ilona in hun huiskamers toe te laten.

Rick Verkade
Enschede, 9 februari 2015

Samenvatting

In deze scriptie wordt onderzoek gedaan naar de vragenlijst uit de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek (CBS), die het slachtofferschap van cybercrime meet. Er zijn aanwijzingen die erop wijzen dat de vragen en begrippen niet voldoende duidelijkheid bieden aan de respondent. Als gevolg hiervan zouden de uitkomsten van het CBS geen valide beeld geven van de daadwerkelijke hoeveelheid slachtoffers van cybercrime. Hierdoor heeft deze studie als doel de validiteit van de vragen met betrekking tot cybercrime, zoals deze zijn gebruikt in de Veiligheidsmonitor van het CBS, te onderzoeken. Dit onderzoek wordt uitgevoerd aan de hand van de volgende hoofdvraag: Hoe verhoudt een nieuwe enquête zich tot de huidige veiligheidsmonitor van het CBS wat betreft het valide meten van cybercrime slachtofferschap? Deze hoofdvraag wordt onderverdeeld in drie deelvragen:

1. *Begrijpt de respondenten de exacte bedoeling van de vraag in de Veiligheidsmonitor en antwoordt hij of zij in overeenstemming met die bedoeling?*
2. *Geven respondenten nog andere cybercrime op bij nadere ondervraging?*
3. *Hoeveel cybercrime lijkt de Veiligheidsmonitor van het CBS te missen?*

De eerste deelvraag wordt beantwoord door het afnemen van de vragenlijst met betrekking tot cybercrime uit de Veiligheidsmonitor van het CBS. Hierdoor kan worden vastgesteld in hoeverre de respondent de vragen en begrippen uit de vragenlijst begrijpt. Wanneer de respondent slachtofferschap rapporteert, wordt er gevraagd naar verdere uitleg over hetgeen er heeft plaatsgevonden. Deze uitleg zal worden vergeleken met de definitie van de gerapporteerde cybercrime en hier zal een score aangehangen worden die het begrip van de respondent aangeeft. Een tweede vragenlijst, genaamd Vragenlijst Universiteit Twente (UT), wordt ontwikkeld en ingezet als vergelijkingsmateriaal. Scoren beide vragenlijsten even goed met betrekking tot het aantal respondenten dat de vragenlijst begrijpt?

Om de tweede en derde vraag te beantwoorden zal opnieuw gebruik worden gemaakt van de Vragenlijst UT. Dit om te onderzoeken of respondenten nog andere cybercrimes rapporteren dan in de vragen van de Veiligheidsmonitor gebeurt. Deze vragenlijst wordt ook gebruikt om te bekijken hoeveel slachtofferschap van cybercrime het CBS lijkt te missen in zijn vragenlijst.

Als antwoord op de eerste deelvraag blijkt dat 21,7% van de slachtoffers de vragen uit de vragenlijst van de Veiligheidsmonitor niet, of niet geheel, begrijpt. 15,9% van de slachtoffers

begrijpt de vragen uit de Vragenlijst UT niet of niet geheel. Uit een chi-kwadraattoets voor de homogeniteit kan worden afgeleid dat er geen significant verschil is tussen beide vragenlijsten met betrekking tot het aantal respondenten dat de vragenlijsten begrijpt.

Als antwoord op de tweede deelvraag blijkt wel blijkt dat er in de Vragenlijst UT extra cybercrimes worden gerapporteerd wanneer hiernaar gevraagd wordt. Met betrekking tot de volgende onderwerpen wordt gerapporteerd in de Vragenlijst UT: Phishing met een vraag naar inloggegevens, het kwijtraken van geld of goederen door online oplichting met truc of op andere wijze, online bedreiging en diefstal van een elektronisch apparaat.

Als antwoord op de derde deelvraag blijkt dat er zowel door de vragenlijst uit de Veiligheidsmonitor, als door de Vragenlijst UT, cybercrimes gemist worden. Dit is onderzocht door het vergelijken van gelijkende cybercrimes uit beide vragenlijsten.

Inhoud

1 Probleemstelling en Vraagstelling

Deze scriptie heeft betrekking op de vragen over slachtofferschap van cybercrime uit de Nederlandse Veiligheidsmonitor van het CBS. De prevalentie slachtofferschap van cybercrime die door middel van deze vragen gemeten wordt, komt niet overeen met de verwachte prevalentie. Een mogelijke oorzaak hiervoor is dat de Veiligheidsmonitor niet voldoende duidelijkheid biedt aan de respondent. Met andere woorden: de vragen over slachtofferschap uit de Nederlandse veiligheidsmonitor, met betrekking tot cybercrime, zouden niet voldoende aansluiten bij het begrip, de kennis en de belevingswereld van de respondent. Een gevolg hiervan is dat er vraagtekens worden gezet bij de validiteit van de uitkomsten van de meting. Dit zijn vraagtekens die leiden tot de hoofdvraag:
Hoe verhoudt een nieuwe enquête zich tot de huidige veiligheidsmonitor van het CBS wat betreft het valide meten van cybercrime slachtofferschap?

Deze vraag wordt onderverdeeld in drie deelvragen:
1. *Begrijpt de respondenten de exacte bedoeling van de vraag in de Veiligheidsmonitor en antwoordt hij of zij in overeenstemming met die bedoeling?*
2. Geven respondenten nog andere cybercrime op bij nadere ondervraging?
3. Hoeveel cybercrime lijkt de Veiligheidsmonitor van het CBS te missen?

1.1 De Veiligheidsmonitor

Het doel van deze studie is een onderzoek naar de validiteit van de vragen met betrekking tot cybercrime, zoals deze zijn gebruikt in de Veiligheidsmonitor (CBS). De Veiligheidsmonitor is een jaarlijks terugkerende bevolkingsenquête, die wordt afgenomen in opdracht van het Ministerie van Veiligheid en Justitie en het Centraal Bureau voor de Statistiek. Door middel van de Veiligheidsmonitor worden zaken als leefbaarheid en overlast in de woonbuurt, onveiligheidsgevoelens en slachtofferschap van veel voorkomende criminaliteit onderzocht. Tevens wordt er gekeken naar het oordeel van de burger over het optreden van de politie en het preventiegedrag (CBS, 2012). Jaarlijks worden deze aspecten gemeten door middel van een gestandaardiseerde vragenlijst. De vragenlijst wordt afgenomen bij personen die woonachtig zijn in Nederland, en ouder zijn dan 15 jaar. Deze worden geselecteerd vanuit één register, namelijk de Gemeentelijke Basisadministratie.

De manier van afnemen van de enquête ligt vast. Allereerst krijgt de geselecteerde respondent een brief thuisgestuurd waarin hem of haar wordt gevraagd via internet de vragenlijst in te vullen. Op het moment dat respondent hier niet op reageert, volgen er nog twee ronden waarin de respondent een schriftelijke vragenlijst krijgt toegestuurd. Indien hier niet op wordt gereageerd, wordt er afgesloten met een telefonische herinnering (CBS, 2012).
In het geval van de Veiligheidsmonitor uit 2012 werden 203080 individuen aangeschreven. De non-response (personen die niet aan de enquête mee willen doen) zorgde ervoor dat de onderzoeksgegevens van 77 989 respondenten zijn verkregen (CBS, 2012).
De Veiligheidsmonitor meet de hoeveelheid slachtofferschap van een groot aantal misdaden van burgers. Slachtofferschap van bedrijven wordt niet onderzocht. Deze studie richt zich enkel op het deel van de Veiligheidsmonitor dat het slachtofferschap van cybercrime meet. Slachtofferschap van bedrijven wordt in deze studie tevens niet onderzocht.

1.2 Aanpak

De eerste deelvraag wordt beantwoord door het afnemen van de vragenlijst met betrekking tot cybercrime uit de Veiligheidsmonitor van het CBS. Hierdoor kan worden vastgesteld in hoeverre de respondent de vragen en begrippen uit de vragenlijst begrijpt. Dit zal worden gedaan door het doorvragen wanneer de respondent slachtofferschap van een cybercrime rapporteert. De uitleg van de respondent zal in dit geval vergeleken worden met de definitie van de gerapporteerde cybercrime en hier zal een score aangehangen worden die het begrip van de respondent aangeeft. Een tweede vragenlijst, genaamd Vragenlijst Universiteit Twente (UT), wordt ontwikkeld en ingezet als vergelijkingsmateriaal. Scoort deze vragenlijst hetzelfde op het gebied van duidelijkheid voor, en begrip bij, de respondent?

Om de tweede en derde vraag te beantwoorden zal opnieuw gebruik worden gemaakt van de Vragenlijst UT. Dit om te onderzoeken of respondenten nog andere cybercrimes rapporteren dan in de vragen van de Veiligheidsmonitor gebeurt. Deze vragenlijst wordt ook gebruikt om te bekijken hoeveel slachtofferschap van cybercrime het CBS lijkt te missen in zijn vragenlijst.

Een verdere uitleg met betrekking tot de aanpak kunt u in hoofdstuk 3 vinden.

2 Relevante literatuur

Dit hoofdstuk is ondermeer gewijd aan de theorie met betrekking tot cybercrime. Tevens komt de theorie met betrekking tot het stellen van vragen op de juiste manier aan bod. Ook richt dit hoofdstuk zich op het valide meten van het slachtofferschap van cybercrime.
Allereerst zal worden uitgelegd wat het begrip cybercrime precies inhoudt en welke verschijningsvormen van cybercrime worden geïdentificeerd.

2.1 Cybercrime

Om het begrip 'cybercrime' geheel duidelijk te maken is het ten eerste van belang aan te geven wat criminaliteit is. Criminaliteit, in alle manifestaties, gaat over het toebrengen van sociaal niet te tolereren schades (Brenner, 2004).

In de literatuur worden verscheidene definities gegeven met betrekking tot het begrip cybercriminaliteit. Enkele definities die zijn ontwikkeld:

- "Cybercrime is elke misdaad die is gefaciliteerd of gepleegd door gebruik van een computer, netwerk of hardware apparaat" (Gordon & Ford, 2006).
- Junger, Montoya en Hartel definiëren cybercrime als het gebruik van Informatie Technologie (IT) voor het plegen van criminele activiteiten tegen personen, eigendommen, organisaties of elektronische communicatienetwerken en informatiesystemen (Montoya Morales, Junger, & Hartel, 2013).
- Ngo en Paternoster (2011) geven aan dat de term over het algemeen refereert aan misdaden die gepleegd worden met gebruik van een computer en computernetwerken, maar misdaden die niet sterk afhankelijk zijn van computergebruik vallen er ook onder.

Zoals te zien is in bovenstaande definities, is er in dit geval consensus over het volgende: Het gebruik van een computer, computernetwerk, of IT in een andere vorm door de dader, is een noodzakelijke voorwaarde voor het classificeren van een misdaad als een cybercrime.

Het gebruik van IT door de dader is voor enkele onderzoekers echter niet voldoende. Computers en netwerken kunnen, naast een gereedschap, ook een doel of plaats delict zijn. Krohn, Lizotte en Hall (2009) definiëren cybercrime dan ook als volgt: "Cybercrime is een term die gebruikt wordt voor het beschrijven van activiteiten waarin computers en netwerken een gereedschap, een doel of een plaats zijn voor criminele activiteiten."

Een uitbreiding komt van Van der Hulst en Neve (2008). Deze auteurs waarschuwen voor een verschil tussen cybercriminaliteit en computercriminaliteit: "Cybercriminaliteit betreft alle criminaliteitsvormen waarbij Informatie- en Communicatie Technologie (ICT) wordt ingezet als instrument. Dit kan het gebruik van ICT ten behoeve van communicatie en logistiek (tussen daders of tussen dader en slachtoffer) zijn, maar ook transacties van gelden en goederen (vrijwillige transacties tussen daders of onvrijwillige transacties tussen dader en slachtoffer).
Computercriminaliteit betreft alle criminaliteitsvormen waarbij ICT behalve instrument ook expliciet doelwit is van de criminele activiteiten. Dit kan zijn het gebruik van ICT om in te breken op netwerken en systemen, om de functionaliteiten van ICT te verstoren, of om geautomatiseerd opgeslagen gegevens te manipuleren (beschadigen, wijzigen, vernietigen)" (Hulst & Neve, 2008).
Het woord 'cybercriminaliteit' kan in dit verband gezien worden als een traditionele misdaad die wordt gepleegd met behulp van een computer. Een voorbeeld hiervan is stalken of het plegen van fraude. Dit terwijl computercriminaliteit zonder een computer niet kan bestaan. Een voorbeeld hiervan is hacken of het plaatsen van virussen op de computer.
Holt en Bossler (2008) geven een soortgelijke uitleg met betrekking tot het onderscheid tussen computercriminaliteit en cybercriminaliteit. Wel geven ze aan dat beide termen door elkaar heen worden gebruikt. " Over the past two decades, criminologists have begun to pay significant attention to the problem of computer and cybercrime. These terms are often used interchangeably…." (Holt & Bossler, 2008).
In deze studie worden de twee termen door elkaar gebruikt.

Om het begrip cybercrime zo goed mogelijk te conceptualiseren is het verstandig één definitie te kiezen die zo allesomvattend mogelijk is. In dit geval is er gekozen voor de definitie van Krohn et al. (2009). Dit omdat deze definitie aangeeft dat computers en netwerken niet alleen een gereedschap of doel van criminele acties kunnen zijn, maar ook als plaats delict gezien kunnen worden. De definitie van cybercrime die deze studie hanteert luidt dus als volgt:
"Cybercrime is een term die gebruikt wordt voor het beschrijven van activiteiten waarin computers en netwerken een gereedschap, een doel of een plaats zijn voor criminele activiteiten" (Krohn, et al., 2009).

2.1.1 Onderverdeling in typen cybercrime

Cybercrime kan onderverdeeld worden in verschillende onderdelen. Hieronder is een onderverdeling te vinden die als een goede aanvulling geldt op de bovenstaande bespreking van de definities.

Zhang, Xiao, Ghaboosi, Zhang en Deng (2012) onderscheiden vijf verschillende onderdelen van cybercrime:

- De computer of het netwerk wordt gebruikt als een gereedschap voor criminele activiteiten. Voorbeelden hiervan zijn het versturen van spammails en copyright overtredingen.
- De computer of het netwerk is het doel van de criminele activiteit. Voorbeelden als toegang forceren zonder toestemming, virussen en hacken worden gegeven.
- Het computernetwerk als de plaats voor criminele activiteiten. Voorbeelden van diefstal, fraude worden door het artikel genoemd.
- Traditionele misdaden die gefaciliteerd worden door computers of de netwerken. Veel traditionele misdaden brengen meer schade toe wanneer er gebruik wordt gemaakt van computers voor de uitvoering ervan. Voorbeelden ervan zijn phishing, identiteitsfraude, kinderpornografie en cyberstalken.
- Andere informatiemisdaden. In de overige categorie vallen volgens de schrijvers de industriële en economische spionage die gezien worden als cybercrimes wanneer ze uitgevoerd worden met behulp van computers of netwerken.

2.1.2 Beschrijving van de bekende vormen van cybercrime

Cybercrime is een zeer breed begrip. Een goede onderverdeling in verschillende vormen van cybercrime komt van het United Nations Office on Drugs and Crime (UNODC). Het UNODC (Malby et al., 2013) onderscheidt de volgende verzameling cybercrimes met bijbehorende definities:

Handelingen tegen de vertrouwelijkheid, integriteit of beschikbaarheid van computerdata of computersystemen:

- Illegale toegang tot een computer

Refereert aan de acties die te maken hebben met het binnendringen in delen van, of de gehele computer, zonder toestemming of reden. Dit kan worden gedaan door bijvoorbeeld het omzeilen van een firewall (beveiligingssysteem). Op deze is het mogelijk om het computersysteem van bijvoorbeeld een bank binnen te dringen (Malby, et al., 2013). Deze vorm van cybercrime wordt ook wel 'hacking' genoemd.

- Illegale toegang, onderschepping of vergrendeling van computerdata

Refereert aan acties die te maken hebben met bovenstaande, met de volgende uitbreiding: Het verkrijgen van data, tijdens het binnendringen van de computer, die niet publiekelijk bekend mag worden. Malby et al. (2013) noemen als voorbeeld een medewerker binnen een bedrijf die bepaalde computerbestanden verkrijgt, kopieert en zonder toestemming meeneemt.

- Illegale tussenkomst in een computersysteem of computer data

Refereert aan acties die het functioneren van een computersysteem hinderen. Tevens houdt deze vorm van cybercrime het beschadigen, verwijderen, afbreken, veranderen of onderdrukken van computerdata zonder toestemming in. Een voorbeeld hiervan is de zogeheten 'Denial-of-service attack'. In dit geval stuurt een dader dermate veel verzoeken naar een bepaalde computer of website, zoals een online-bankieren site. Dit met het gevolg dat het systeem de grote hoeveelheid verzoeken niet meer aankan. Het systeem kan in dit geval ook 'legitieme' verzoeken, van bijvoorbeeld internetbankierende mensen die van goede wil, zijn niet meer verwerken.

- Productie, verspreiding of bezit van gereedschappen die misbruik kunnen maken van iemands computer

Refereert aan acties als het ontwikkelen of verspreiden van hardware of software-programma's die kunnen worden gebruikt bij computer- of internetgerelateerde overtredingen.

Malby et all. (2013) geven het volgende voorbeeld: de overtreder die software ontwikkelt die automatisch Denial-of-service aanvallen (zie hierboven) kan uitvoeren.

- Inbreuk op privacy of databeschermingsmaatregelen

Refereert aan acties waarbij van computersystemen gebruik wordt gemaakt om persoonlijke informatie, in strijd met databeschermingsbepalingen, te verkrijgen, verwerken of verspreiden.

Malby et al (2013) geven het voorbeeld van de eigenaar van een webwinkel die de persoonlijke gegevens van klanten uitgeeft, terwijl hij deze eigenlijk geheim had moeten houden.

Computergerelateerde handelingen voor het verkrijgen van persoonlijke winst of toebrengen van persoonlijke schade:

- Computergerelateerde fraude of vervalsing

Refereert aan acties die te maken hebben met het onderbreken van, of het illegaal toegang nemen tot, een computersysteem of bepaalde data. Dit met het doel om op misleidende of oneerlijke wijze geld, of andere economische voordelen, te verkrijgen. Hierbij kan gedacht worden aan iemand die bepaalde software van een bank aanpast, om er op die manier voor te zorgen dat alle financiële overboekingen op zijn rekening worden gestort. Tevens is het bijvoorbeeld mogelijk dat iemand een authentieke mail van een financieel instituut aanpast om op die manier te frauderen. De mail kan vragen naar persoonlijke gegevens van een slachtoffers. Het sturen van mails die vragen naar persoonlijke gegevens, met als doel bijvoorbeeld het frauderen, wordt ook wel 'phishing' genoemd.

- Computer-gerelateerde identiteitsovertredingen

Refereert aan daden die te maken hebben met, het zonder enig recht erop, overdragen, bezitten, of gebruiken van identificatiemiddelen van een ander persoon, die bewaard worden in computerdata. Dit met het doel om deze identificatiemiddelen te gebruiken voor het plegen, of het helpen plegen, van een criminele activiteit. Als voorbeeld noemen Malby et al. (2013) iemand die rijbewijsinformatie van een slachtoffer uit een computersysteem heeft gestolen. Deze informatie kan vervolgens verkocht worden. Ook kan de dader de informatie zelf gebruiken om zijn of haar eigen identiteit te verbergen tijdens het plegen van een misdaad.

- Computer-gerelateerde copyright of handelsmerk overtredingen

Refereert aan het kopiëren van materiaal dat bewaard wordt als computerdata. Dit in overtreding van copyright- of handelsmerkwetten. Malby et al (2013) noemen in dit geval als voorbeeld het verspreiden van een lied waarop copyright rust via een systeem waarmee bestanden worden gedeeld. Dit gebeurt dan zonder toestemming van de copyrighthouder.

- Verzenden van Spam

Refereert aan het gebruik van een computersysteem, om deze vervolgens te gebruiken voor het versturen van berichten aan een groot aantal ontvangers. Dit zonder toestemming of verzoek van die ontvangers.

- Computer-gerelateerde handelingen die persoonlijke schade toebrengen

Refereert aan het gebruik van een computersysteem, om deze vervolgens te gebruiken voor het lastigvallen, pesten, bedreigen, stalken of intimideren van een individu. Malby et al (2013) identificeren verschillende manieren waarop deze persoonlijke schade kan worden toegebracht. De dader kan het slachtoffer bijvoorbeeld beledigende of bedreigende afbeeldingen of berichten sturen. Tevens is het mogelijk om de computer te gebruiken voor het traceren of stalken van een slachtoffer.

- Computer-gerelateerde ‘ dwingende uitnodiging’ of ‘grooming’ van kinderen

Refereert aan het gebruik van een computersysteem om een kind te benaderen, dat de leeftijd voor het toestemmingen in seksuele relaties nog niet heeft bereikt.
Dit heeft als doel het plegen van een seksgerelateerde misdaad. Malby et al (2013) geven als voorbeeld het chatten via internet. In dit geval benadert de overtreder het kind via een internetchat, en doet zich ook voor als een kind. Vervolgens doet de overtreder het voorstel een keer af te spreken, met het misbruiken van het kind als doel. Dit wordt ‘grooming’ genoemd (Malby, et al., 2013).

Computer inhoud gerelateerde handelingen:

- Computer-gerelateerde handelingen die te maken hebben met racisme/haatspreken/vreemdelingenhaat

Refereert aan het gebruik van een computersysteem voor het verspreiden van racistisch materiaal of materiaal dat betrekking heeft op vreemdelingenhaat. Tevens kan het computersysteem gebruikt worden voor het bedreigen of beledigen van individuen of groepen.

- Computer-gerelateerde productie, verspreiding of bezit van kinderpornografie

Refereert aan het gebruik van een computersysteem voor het produceren, creëren, verspreiden, bekijken, ontvangen, bewaren of bezitten van een representatie van een echt of fictief persoon onder de 18, die betrokken is in echte, of gesimuleerde, seksuele handelingen.

- Computer-gerelateerde handelingen als steun voor terroristische overtredingen

Refereert aan acties waarbij een computersysteem wordt gebruikt als steun voor terroristische acties. Het computersysteem kan, volgens Malby et al (2013), worden gebruikt als communicatiemiddel naar het publiek toe. Ook kan de computer worden gebruikt als middel om financiële middelen in te zamelen, die kunnen worden gebruikt voor terroristische acties.

Ook kunnen computers worden gebruikt voor de planning, voorbereiding, onderzoek of organisatie ten behoeve van een terroristische daad.
(Malby, et al., 2013)

Zoals hierboven te zien is, zijn er verschillende vormen van cybercrime bekend. De bovenstaande typologie is dan ook niet compleet. Van alle genoemde vormen zijn immers weer subvormen bekend, die onmogelijk allemaal vermeld kunnen worden. Bovenstaand overzicht geeft dus enkel een indruk van wat er allemaal bekend is op het gebied van cybercrime.

2.2 Vormgeving en afname Vragenlijst UT

Voor het deel van de vragen dat afkomstig is uit de Veiligheidsmonitor hoeft de vraagstelling logischerwijs niet meer bedacht te worden.

Voor de UT-vragenlijst is een goed ontwerp van belang. Een goede vraagstelling, die zorgt voor antwoorden die de omvang van slachtofferschap op een goede manier aangeven, is zeer belangrijker. Hiervoor moeten enkele methodologische problemen en het begrip response error worden voorkomen. In tabel 1 staan enkele problemen en mogelijke oplossingen. De oplossingen met de vermelding 'toegepast' worden gebruikt in dit onderzoek. In de onderstaande paragrafen worden de problemen en oplossingen verder uitgelegd.

Tabel 1 – Problemen en oplossingen bij de ontwikkeling van de vragenlijst.

Afname vragenlijst	**In studie gebruikte oplossingen**
Manier afname vragenlijst	Schriftelijke en mondelinge afname - toegepast
Opzet vragenlijst	
Open- of gesloten vragen	Combinatie van beide - toegepast
Items	Duidelijk, kort, niet negatief geformuleerd, geen bias - toegepast
Response error	
Fouten in het begrijpen	Eenvoudige opzet, duidelijke items, gebruik van situatieschetsen, interviewers in de nabijheid - toegepast
Problemen met betrekking tot herinneren	Stimuleren van het geheugen van de respondent door 'geheugenhulpjes' - toegepast
Het niet-rapporteren van grijze zone incidenten	Respondent aansporen om alles op cybercrime-gebied te rapporteren, onafhankelijk van de dader - toegepast
Schaamte voor het rapporteren.	Vragen meerdere malen op verschillende plek opnemen – niet toegepast in deze studie
Classificeren van antwoorden door onderzoeker	Dicht bij verhaal van de respondent blijven, doorvragen, in de gaten houden van definities - toegepast
Problemen plaatsing incidenten in de tijd	Begrenzing door datumgebruik - toegepast

2.2.1 Manier van afname

Er zijn verschillende manieren denkbaar om een vragenlijst af te nemen bij een respondent. De meest gebruikte manieren zijn een mondeling interview, een telefonisch interview, of een interview via de post/het internet. Elke vorm heeft zijn eigen voor- en nadelen.

Oplossingen toegepast in dit onderzoek

In dit onderzoek wordt gebruik gemaakt van een combinatie van een schriftelijke en mondelinge afname van de vragenlijst. Het schriftelijk deel wordt gebruikt, omdat dit de realiteit beter nabootst. De Nederlandse Veiligheidsmonitor wordt immers ook schriftelijk afgenomen. De respondent leest de vragen dus zelf en schrijft zelf zijn of haar antwoord op.

In sommige gevallen wordt er een deel van de vragenlijst mondeling door de interviewer afgenomen. Dit is het geval wanneer de respondent 'ja' heeft geantwoord op één van de vragen die afkomstig zijn uit de Veiligheidsmonitor. Dit is het deel waarin de respondent gevraagd wordt naar wat er precies gebeurd is. Op deze manier wordt geprobeerd te onderzoeken of de respondent wel begrijpt wat er precies bedoeld is met de vraag. Vervolgens wordt de Vragenlijst UT ook schriftelijk afgenomen bij de respondent.

2.2.2 Opzet vragenlijst

Tevens is het essentieel om de methodologische problemen en de response error tot een minimum te beperken.

- *Open- of gesloten vragen*

Allereerst is het belangrijk een keuze te maken tussen open en gesloten vragen. Elk van de vraagvormen hebben eigen voor- en nadelen.

Open vragen zijn populair bij diepte-interviews (Babbie, 2012). Een nadeel van open vragen is echter dat deze eerst gecodeerd moeten worden voordat ze verwerkt kunnen worden.

De betekenis van het antwoord van de respondent moet dan geïnterpreteerd worden, wat kan leiden tot het verkeerd begrijpen door de onderzoeker, of een zogeheten 'researcher bias' (Babbie, 2012). In dit geval beïnvloedt de onderzoeker onbewust de resultaten van het onderzoek. Tevens is het mogelijk dat er antwoorden door de respondent worden gegeven die irrelevant zijn voor het onderzoek (Babbie, 2012). In dergelijke gevallen meet de onderzoeker niet wat hij of zij van plan was te meten. De validiteit is in dat geval niet hoog.

Gesloten vragen zijn populair in enquêtes (Babbie, 2012). Deze geven meer uniformiteit en zijn makkelijker te verwerken in een computerbestand. Belangrijk is echter wel dat de relevante antwoordmogelijkheden exclusief en uitputtend moeten zijn. Dat wil zeggen dat de antwoordmogelijkheden alle opties moeten behandelen en de respondent moet niet de neiging hebben twee antwoorden te kiezen (Babbie, 2012).

Oplossingen toegepast in dit onderzoek

Om bovenstaande redenen wordt er voor dit onderzoek gekozen voor een combinatie voor gesloten- en open vragen. Gesloten vragen, omdat deze makkelijker te verwerken zijn. Open vragen worden gebruikt vanwege feit dat er diep in wordt gegaan op bepaalde onderwerpen. Tevens kan op deze manier het belang dat de respondent zelf vertelt over hetgeen hij of zij heeft meegemaakt, worden gewaarborgd. Uit gesloten vragen is het lastig op te maken of de respondent de vragen begrijpt. Door de respondent in de open vragen te laten vertellen over wat er bedoeld wordt met een bepaald antwoord, is de bedoeling van de respondent met zijn of haar antwoord duidelijker waar te nemen.

- *Items*

Het is belangrijk om de vraagstelling van de items duidelijk te maken. De onderzoeker zit vaak zo diep in het onderwerp dat hij de neiging heeft zaken sneller duidelijk en simpel te vinden dan de respondent. Dit gezien het feit dat de respondent zich vaak helemaal niet bezig houdt met het onderwerp van het onderzoek.

Korte items zijn het best (Babbie, 2012). Respondenten moeten de vragen snel kunnen lezen en vervolgens gelijk begrijpen zonder het lang te bestuderen. Negatief geformuleerde items kunnen het beste vermeden worden (Babbie, 2012). Over het woordje ‘niet’ in een zin wordt namelijk vaak heen gelezen (Babbie, 2012). Het is beter items en termen met een bias te vermijden. Sommige vragen moedigen mensen aan een bepaald antwoord te geven. Geheel neutrale vragen zonder bias hebben dus de voorkeur. Voorbeeld: “Ben je het ook niet eens met…..” (Babbie, 2012). Deze vraagstelling zal eerder een ‘eens’-antwoord opwekken (Babbie, 2012).

Oplossingen toegepast in dit onderzoek

Bovenstaande aandachtspunten worden allen in dit onderzoek gebruikt.

2.2.3 Response error

Binnen enquêtes kan het begrip ‘response error’ voor problemen zorgen. Een error (afwijking) is te definiëren als het verschil tussen de werkelijke score en een geobserveerde score van een verschijnsel. Elke geobserveerde score bestaat voor een deel uit de daadwerkelijke score (die we willen meten), en voor een deel uit error, oftewel afwijking (Skogan, 1975). In het geval van een response error klopt het antwoord van de respondent (geobserveerde score) dus niet geheel met de daadwerkelijke score, en dit kan mogelijk een bedreiging zijn voor de validiteit van een onderzoek.

Gezien het feit dat dit onderzoek bestaat uit het interviewen van (potentiële) slachtoffers van een misdaad, in dit geval cybercrime, is het mogelijk dat dergelijke afwijkingen ook in deze studie voor komen. Het is dan ook zaak om deze problemen zoveel mogelijk te minimaliseren, om op die manier een resultaat te krijgen dat valide is. Hieronder worden enkele vormen van response error geïdentificeerd die vermeld worden in de literatuur.

- *Fouten in het begrijpen*

Respondenten begrijpen mogelijk de taak die ze zullen gaan ondernemen niet helemaal. Ze kunnen problemen hebben met het begrijpen van het nut van het interview, de misdaden waarop gefocust wordt, of de definities van de incidenten die gebruikt worden (Statistics, Justice, & Programs, 1989).

Oplossingen toegepast in dit onderzoek

Dit probleem wordt geprobeerd te voorkomen door het zo eenvoudig mogelijk opzetten van de vragenlijst. Elk gevraagd onderwerp wordt zo goed en zo eenvoudig mogelijk uiteengezet. Tevens wordt er bij moeilijkere onderwerpen gebruik gemaakt van situatieschetsen. Dit in plaats van een directe vraag naar slachtofferschap. Er wordt bijvoorbeeld niet gevraagd of de respondent slachtoffer is geworden van phishing. In plaats daarvan worden enkele situaties voorgesteld die de respondent overkomen kunnen zijn, en aan te merken zijn als vormen van phishing. Dit maakt herkenning mogelijk makkelijker.

Een voorbeeld hiervan is dat er wordt gevraagd of de respondent, in verschillende situaties op het internet, wel eens gevraagd is naar persoonlijke gegevens. Dit in plaats van de vraag of de respondent slachtoffer is geworden van phishing. Tevens is het een voordeel dat de vragenlijsten in nabijheid van de interviewers worden afgenomen. Bij onduidelijkheden kan de interviewer extra informatie verstrekken aan de respondent. Uiteraard zonder de

respondent te sturen in zijn of haar antwoord. Dit kan immers een vertekening in de resultaten veroorzaken, die een valide en betrouwbare uitkomst verhindert.

- *Problemen met betrekking tot herinneren*

Indien het slachtoffer geïnterviewd wordt, is het de vraag of het slachtofferschap wordt herinnerd. Vervaging van het geheugen is een reëel probleem binnen onderzoek naar slachtofferschap (Skogan, 1975).
In de National Crime Survey, een Amerikaans onderzoek naar slachtofferschap van criminaliteit, kwam dit probleem ook terug.
De volgende auteurs hebben zich beziggehouden met het herontwerp van de National Crime Survey en aan de hand hiervan wordt het probleem verder uitgelegd:
Het Bureau of Justice Statistics (BJS) (1989) nam waar dat het niet-herinneren van slachtofferschap in de meeste gevallen komt doordat het geheugen van de respondent niet voldoende wordt gestimuleerd in het interview of door de vragenlijst. Ook Taylor (1989) onderkent het bestaan van deze problemen met betrekking tot het herinneren van slachtofferschap. Kindermann, Lynch en Cantor (1997) voegen daaraan toe dat de veranderingen die vervolgens werden aangebracht in de National Crime Survey, vooral geïmplementeerd om betere rapportage te krijgen van criminele incidenten. Er moest voor gezorgd worden dat de respondenten zich alle vormen van criminaliteit waarvan ze slachtoffer waren geworden weer konden herinneren, om deze vervolgens te rapporteren. In sommige gevallen bevatte de vragenlijst niet voldoende mogelijkheden om het geheugen van de respondent te stimuleren.

Algemene oplossingen

Naast de beschrijving van het probleem geven bovengenoemde auteurs ook oplossingen voor de herinneringsproblemen. Het geheugen van de respondent kan namelijk gestimuleerd worden door het gebruik van korte aanwijzingen in de vorm van ‘geheugenhulpjes’ (cues).
Dit hield in dat er geheugenhulpjes (cues) in de vragen werden opgenomen die betrekking hadden op het voorkomen van slachtofferschap in verschillende ‘levensterreinen’, zoals bij activiteiten op het werk of in de vrije tijd. Deze korte geheugenhulpjes zorgden ervoor dat het geheugen van de respondent getriggerd werd. Dit werd gedaan door het benoemen van de levenscontext. Het doel van deze verandering in de National Crime Survey was een verhoogde rapportage van slachtofferschap en het beter structureren van de herinnering van de respondent. Dit laatste om ervoor te zorgen cognitieve en culturele verschillen onder

respondenten een kleinere impact zouden hebben op het rapporteren van criminele incidenten (Taylor, 1989). Deze methode is bewezen effectief. In het geval van de National Crime Survey is de hoeveelheid rapportage van slachtofferschap verbeterd (Taylor, 1989). De nieuwe vragenlijst had een antwoordaantal van 0.99 incidenten per respondent terwijl de eerdere versie van de National Crime Survey niet verder kwam dan 0,60. Uiteindelijk zorgde de nieuwe variant met de geheugenhulpjes voor 39% stijging in slachtofferschap rapportage (Statistics, et al., 1989).

Oplossingen toegepast in dit onderzoek

De manier van bevragen door middel van geheugenhulpjes wordt ook toegepast in de vragenlijst die in deze studie wordt gebruikt. Bij vrijwel elke bevraagde vorm van cybercrime worden korte voorbeelden genoemd van situaties waarin de vorm van cybercrime kan voorkomen. Hieronder volgen enkele voorbeelden:

Bij de vragen die betrekking hebben op phishing wordt er in de vorm van drie verschillende leefsituaties (online gaming, gebruik van social network sites en online bankieren) gevraagd of de respondent wel eens gevraagd is naar persoonlijke gegevens. Het begrip 'persoonlijke gegevens' wordt vervolgens ook weer onderverdeeld in wachtwoorden en bankgegevens.

Het is immers mogelijk dat de respondent zich niet direct iets kan voorstellen bij een enkele vraag naar de gevolgen van phishing voor hem of haar. Op het moment dat echter de volgende hulpjes bij de vraag worden toegevoegd, is het mogelijk dat de respondent zich plotseling een incident herinnert met betrekking:

- het plotseling verdwijnen van geld van uw bankrekening of creditcard
- vrienden of familie die klagen over rare mailtjes die ze van u zouden hebben ontvangen
- of andere zaken die mogelijk terug te herleiden zijn naar het feit dat u uw persoonlijke gegevens hebt verstrekt.

- *Het niet-rapporteren van grijze zone incidenten (incidenten met bekenden)*

Zelfs als het slachtoffer zich het slachtofferschap herinnert, wordt dit niet altijd door het slachtoffer gemeld. Respondenten rapporteren problemen of ruzies met vrienden of familie niet graag (Skogan, 1975). Kindermann, Lynch en Cantor (1997) voegen hieraan toe dat respondenten in sommige gevallen onzeker zijn over in hoeverre ze bepaalde incidenten wel moeten melden, aangezien bepaalde incidenten wel bepaalde karakteristieken van een

misdaad bevatten, maar niet voldeden aan het stereotype van een misdaad, zoals bijvoorbeeld misdaden gepleegd door familieleden. Dit worden incidenten in de grijze zone genoemd (Kindermann, et al., 1997). Deze grijze zone incidenten zijn echter belangrijk voor het verkrijgen van een valide beeld van de hoeveelheid criminaliteit.

Het Bureau of Justice Statistics (BJS) (1989) geeft met betrekking tot dit onderwerp aan dat slachtoffers mogelijk bepaalde incidenten, die ze als emotioneel 'lastig' ervaren, niet rapporteren. Deze onderdrukking kan zowel bewust als onbewust plaatsvinden en kan voortkomen uit angst, pijn of schaamte. Van Dijk en Mayhew (1993) geven een zelfde weergave. Ook in dit geval wordt gemeld dat incidenten waarbij familie, vrienden of andere bekenden bij betrokken zijn geweest minder snel gerapporteerd worden door de respondent.
Daarbij komt nog eens dat slachtoffers liever niet over hun eigen slachtofferschap praten en zich soms zelfs niet realiseren dat bepaalde incidenten die ze zich herinneren van belang kunnen zij voor het onderzoek (Van Dijk & Mayhew, 1993), omdat, zoals hiervoor aangegeven, ze bijvoorbeeld niet voldeden aan het stereotype van een misdaad. Met andere woorden: de misdaad wordt in sommige gevallen niet herkend als misdaad. Op het moment dat deze vormen van misdaad niet gerapporteerd worden, geeft dit een onbetrouwbaar en niet-valide beeld van de werkelijkheid.
Dit geldt ook voor incidenten die de respondent zelf beoordeeld als 'niet belangrijk genoeg om te melden' (Skogan, 1975). Incidenten worden in dat geval niet gemeld terwijl er mogelijk wel sprake was van een (cyber-) crimineel incident.

Algemene oplossingen

Ook in de National Crime Survey was er sprake van een onderrapportage van incidenten in de sfeer van familie of vrienden (grijze zone-incidenten). Dit werd opgelost door het geven van geheugenhulpjes (cues – zie hierboven) en aansporingen om incidenten, die misschien niet leken op de stereotype verschijning van een misdaad, toch te melden (Kindermann, et al., 1997).

Oplossingen toegepast in dit onderzoek

In dit onderzoek wordt een dergelijke tactiek op toegepast, echter niet door een subtiele manier van geheugenhulpjes. Bij elke vorm van cybercrime wordt het volgende duidelijke gemaakt: "Het plegen van …… is een misdrijf, ook wanneer de dader(s) familieleden, vrienden of op een andere manier bekenden van u zijn." Dit in de hoop dat de respondent een

bepaald incident toch gaat associëren met het gedrag van vrienden, collega's of bekenden, waar in eerste instantie niet aan gedacht werd.
Zoals gezegd ziet de respondent, in sommige gevallen, bepaalde zaken als niet belangrijk genoeg om te rapporteren (Skogan, 1975). Om deze reden wordt er in de vragenlijst benadrukt dat elk incident, hoe klein ook, gerapporteerd 'moet' worden.

Met betrekking tot het eerder genoemde schaamte effect, wordt er door Smith (1994) aangeraden om vragen met betrekking tot een bepaald onderwerp meerdere malen, op verschillende manieren en op verschillende plekken in de vragenlijst te stellen. Dit helpt slachtoffers bepaalde incidenten te herinneren of mogelijk hebben ze de beslissing om bepaalde zaken niet te rapporteren heroverwogen. Ze kunnen een kosten-batenanalyse hebben gedaan die goed voor de enquête uitpakt (Smith, 1994). Deze methode wordt, in verband met de beperkte ruimte in de vragenlijst, echter niet gebruikt in dit onderzoek.

- *Classificeren van de antwoorden door de onderzoeker*

Nadat de respondenten antwoord hebben gegeven moeten de antwoorden op open vragen vaak nog worden geclassificeerd door de onderzoeker (Skogan, 1975). Was hier nu daadwerkelijk sprake van een phishing aanval of niet? Hier kunnen ook veel fouten uit voorkomen.

Oplossingen toegepast in dit onderzoek
Fouten hierin zijn erg lastig te voorkomen. In dit onderzoek wordt geprobeerd dicht bij het verhaal van de respondent te blijven en door te vragen op hetgeen de respondent bedoelt. Dit zou positief kunnen bijdragen aan het voorkomen van fouten. Dit in combinatie met het in de gaten houden van de definitie van de verschillende cybercrimes, zodat de bovengenoemde fouten voorkomen worden.

- *Problemen met betrekking tot plaatsing van incidenten in de tijd*

Een laatste vorm van afwijking wordt 'forward telescoping' genoemd (Skogan, 1975).
Dit houdt in dat er sprake is van een onjuiste rapportage door de respondent van de data of tijdsperiodes waarin het incident dat het slachtofferschap veroorzaakte plaatsvond (Taylor, 1989). Gebeurtenissen kunnen gerapporteerd worden als 'plaatsgevonden op een later tijdstip' dan werkelijk het geval was (forward telescoping). Het tegengestelde effect hiervan wordt backward telescoping genoemd (Taylor, 1989).

Er wordt bijvoorbeeld gevraagd naar het slachtofferschap uit de afgelopen 12 maanden. Bij forward telescoping plaatst de respondent echter bepaalde gebeurtenissen die vóór de referentieperiode hebben plaatsgevonden (bijvoorbeeld 14 maanden geleden) toch in de referentieperiode. Met andere woorden: Incidenten die niet in de referentieperiode thuishoren, worden daar door de respondenten toch in 'geplaatst'.

Algemene oplossingen

In de National Crime Survey wordt er, als oplossing voor dit probleem, begrensd. In het geval van een longitudinaal onderzoek als de National Crime Survey (een studie waarin in dit geval steeds dezelfde respondenten elke zes maanden worden geïnterviewd) wordt data van het nieuwste interview, waarin bijvoorbeeld een misdaad wordt gerapporteerd, gecheckt tegen de incidenten die in het vorige interview zijn gerapporteerd.

Dit om te bekijken of het wel degelijk een nieuwe misdaad betreft of dat de respondent in kwestie hetzelfde incident in het huidige interview opnieuw rapporteert (Taylor, 1989).

De veiligheidsmonitor, die met behulp van deze studie verbeterd moet worden, selecteert echter steeds nieuwe respondenten. Dit is de reden dat deze vorm van begrenzing niet mogelijk is.

Oplossingen toegepast in dit onderzoek

In dit onderzoek worden tijdsperiodes echter wel begrensd door middel van datumgebruik. In de huidige veiligheidsmonitor wordt gevraagd naar incidenten van de afgelopen twaalf maanden. Een begrip dat losjes gehanteerd kan worden. Een begrenzing in de vorm van een datum werkt mogelijk beter. In dit geval respondenten 'mogen' respondenten enkel alle incidenten die ná die datum hebben plaatsgevonden rapporteren. Dit is een bedachte oplossing die mogelijk een positief effect teweeg brengt en in dit onderzoek getest zal worden.

3 Research design en aanpak

Hieronder kunt u vinden op welke deze studie, en de vragenlijst, is vormgeven.

3.1 Research design

De eerste deelvraag wordt beantwoord door het afnemen van de vragenlijst met betrekking tot cybercrime uit de Veiligheidsmonitor van het CBS. Om de validiteit van deze vragenlijst te bepalen, wordt onderzocht in hoeverre de respondent de vraagstelling en de begrippen uit de vragenlijst daadwerkelijk begrijpt. Dit wordt gedaan door de vragenlijst voor te leggen aan de respondent en door te vragen wanneer de respondent slachtofferschap van cybercrime rapporteert. Indien de respondent aangeeft slachtoffer te zijn geworden van één of meer van de 4 cybercrimes uit de veiligheidsmonitor, wordt er doorgevraagd. Wat is de respondent precies overkomen? Vervolgens zal er een uitleg van de respondent volgen over hetgeen hij of zij heeft meegemaakt.
Indien de respondent bijvoorbeeld aangeeft slachtoffer te zijn geworden van identiteitsfraude, zal zijn of haar uitleg vergeleken worden met de definitie van identiteitsfraude. Indien de omschrijving van de respondent geheel overeenkomt met de definitie van de cybercrime die hij of zij gerapporteerd heeft, wordt dit beoordeeld met het cijfer 2. Indien de omschrijving van de respondent gedeeltelijk overeenkomt met de definitie van de cybercrime, wordt dit beoordeeld met het cijfer 1. Indien de omschrijving van de respondent niet overeenkomt met de definitie van de cybercrime, wordt dit beoordeeld met het cijfer 0. Vervolgens wordt het aantal van elk cijfer bekeken. Op deze manier is het mogelijk om overzichtelijk weer te geven in hoeverre de vragenlijst begrepen wordt door de respondent.

Tevens wordt er een alternatieve vragenlijst samengesteld, genaamd vragenlijst Universiteit Twente (UT). Deze wordt ook aan de respondent voorgelegd en getest op het valide meten van het slachtofferschap van cybercrime. Er wordt getest in hoeverre deze vragenlijst duidelijkheid biedt aan de respondent. Dit enkel met betrekking tot de vragen over phishing, online oplichting met financiële schade en het kwijtraken van geld op het internet. De methode om te testen in hoeverre de respondent de vragenlijst begrijpt is gelijk aan de methode die is gebruikt bij de vragen uit de Veiligheidsmonitor. Er wordt naar verdere uitleg gevraagd wanneer de respondent slachtofferschap rapporteert.

Vervolgens wordt er een vergelijking gemaakt tussen beide vragenlijst met betrekking tot de hoeveelheid begrip die beide vragenlijsten hebben opgeleverd. Door middel van een chi-kwadraattoets voor de homogeniteit kan worden aangegeven of er een significant verschil bestaat tussen het begrip van de respondent voor de vragenlijst van de Veiligheidsmonitor en het begrip van de respondent voor de Vragenlijst UT.

De verwachting is dat er wel verschil zit in de hoeveelheid begrip per vragenlijst en dat de Vragenlijst UT beter scoort op dit onderwerp. Dit door de toepassing van de theorie met betrekking tot de ontwikkeling van goede vragenlijsten (Paragraaf 2.2) bij het ontwerp van deze vragenlijst. Om de chi-kwadraattoets uit te voeren worden de volgende nul- en alternatieve hypothese gesteld:

H0: de hoeveelheid begrip van de respondent is hetzelfde voor de vragenlijst uit de Veiligheidsmonitor en de Vragenlijst UT
HA: de hoeveelheid begrip van de respondent is niet hetzelfde voor de vragenlijst uit de Veiligheidsmonitor en de Vragenlijst UT

De tweede deelvraag wordt beantwoord door middel van de Vragenlijst UT. De onderwerpen in de Vragenlijst UT wijken namelijk af van die van de Veiligheidsmonitor. Hierdoor is het mogelijk te bekijken welke cybercrimes de respondenten rapporteren bij deze nadere ondervraging.

De derde deelvraag wordt beantwoord door de hoeveelheid gemeten slachtofferschap uit twee gelijkende vraagstellingen uit beide vragenlijsten te vergelijken. Hieruit kan worden afgeleid hoeveel elke vragenlijst lijkt te missen. Allereerst worden cyberpesten (Veiligheidsmonitor) en online bedreiging (Vragenlijst UT) met elkaar vergeleken. De volgende vragen werden gesteld:

- Cyberpesten (Veiligheidsmonitor): Heeft u in de afgelopen 12 maanden via internet wel eens te maken gehad met roddel, getreiter, pesten, stalken, chantage of bedreiging? Let op: het gaat hierbij alleen om uzelf, niet om iemand anders uit uw huishouden!

- Online bedreiging (Vragenlijst UT): In het geval van online bedreiging wordt het slachtoffer bedreigd via de digitale weg, bijvoorbeeld via internet, e-mail of mobiele telefoon. Het bedreigen via de digitale weg komt vaak voor, en is helaas niet ongewoon. Bedreiging is een misdrijf, ook wanneer de dader(s) familieleden, vrienden of op een andere manier bekenden van u zijn.
  Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, via de digitale weg bedreigd?

Het is belangrijk op te merken dat de vraagstelling van de Veiligheidsmonitor een stuk breder meet dan de vraagstelling uit de Vragenlijst UT. In het laatste geval wordt enkel online bedreiging gemeten, terwijl de Veiligheidsmonitor ook roddel, getreiter, pesten, stalken, chantage en bedreiging meet.

Vervolgens worden koop-verkoopfraude (Veiligheidsmonitor) en online oplichting met financiële schade (Vragenlijst UT) met elkaar te vergeleken. Het begrip 'Geld kwijt via het internet' uit de Vragenlijst UT wordt niet opgeteld bij online oplichting met financiële schade. Dit omdat hetgeen de respondent rapporteert bij 'Geld kwijt via het internet' niet altijd kan worden gezien als daadwerkelijke oplichting. Het optellen van deze begrippen zou in dat geval tot een niet-valide beeld leiden.
De volgende vragen werden gesteld:

- Koop-verkoopfraude (Veiligheidsmonitor): Bent u zelf of iemand anders in uw huishouden in de afgelopen 12 maanden bij het kopen of verkopen van goederen of diensten wel eens opgelicht, bijv. doordat gekochte goederen niet geleverd werden of niet betaald werd voor geleverde diensten?
- Online oplichting met financiële schade (Vragenlijst UT): Er zijn meerdere manieren te bedenken waarop iemand u via het internet of e-mail geld of goederen afhandig kan maken. Hieronder noem ik een aantal situaties waarop u 'ja' kunt antwoorden wanneer deze situatie op u van toepassing is. Noemt u ook alle kleine dingen die u mogelijk onbelangrijk zou kunnen vinden. Bent u in de afgelopen 12 maanden wel eens geld of goederen kwijtgeraakt doordat iemand u met een bepaalde truc of 'slimmigheid' via het internet of e-mail heeft opgelicht?

Het is belangrijk op te merken dat de vraagstelling van de Vragenlijst UT een stuk breder meet dan de vraagstelling uit de Veiligheidsmonitor. In het laatste geval wordt enkel koop-verkoopfraude gemeten, terwijl de Vragenlijst UT alle vormen van online oplichting met financiële schade meet.
Interessant is om te kijken hoe de respondenten reageren op deze twee vragen. Rapporteren ze bij beide vragen dezelfde hoeveelheid slachtofferschap?

Tenslotte is het mogelijk om een onderzoek te doen naar het slachtofferschap van phishing. Wat hebben de mensen, die in de Vragenlijst UT aangeven hun gegevens te hebben ingevuld tijdens een phishing-poging, geantwoord op de vragen uit de Veiligheidsmonitor? Indien dit feit in de vragen in de Veiligheidsmonitor niet naar voren komt, blijkt dat dit slachtofferschap daadwerkelijk door de Veiligheidsmonitor gemist wordt.

3.2 Respondenten

Het trekken van een aselecte steekproef behoorde niet tot de mogelijkheden. In deze studie werd gewerkt met 3 interviewers die de respondenten op verschillende plaatsen benaderden met de vraag of ze wilden meewerken aan een kort onderzoek van ongeveer 10 minuten. De selectie is niet als random aan te merken. Een vertekening is in dit geval dan ook niet geheel uit te sluiten. Het is immers mogelijk dat enkel de respondenten, die vaak slachtoffer zijn geworden van een cybercrime, ervoor kiezen om mee te werken. Het doel van deze studie is echter het vergelijken binnen respondenten, en in mindere mate het meten van de prevalentie. Een vertekening is hierdoor minder erg.
Voor het onderzoek zijn op de volgende plaatsen vragenlijsten afgenomen:

- Op huisadressen in Hengelo, Nijmegen, Giesbeek en Wolfheze. Hierbij werd er gebruik gemaakt van een random-walk methode, een manier om op random wijze respondenten te selecteren (Childinfo). Deze methode werd aangepast aan de studie. Door middel van een genummerde adressenlijst van de betreffende plaats en een random getallen-generator op het internet werden straten uitgekozen waar geïnterviewd werd. Vervolgens werden in de regel vier huizen bezocht. Wanneer de respondent niet open deed ging de onderzoeker verder, om vervolgens op een later moment één keer terug te keren naar de woning. Indien de deur werd geopend, werd eerst bekeken of er sprake was van een persoon boven de 18. Indien dit niet het geval was, werd er gevraagd naar een meerderjarige in het huishouden en werd deze

meerderjarige geïnterviewd. Mocht er geen volwassene aanwezig zijn op dat moment, werd er gevraagd door te geven dat de interviewer aan de deur was geweest en hij of zij op een later moment zou terugkomen. Indien medewerking geheel geweigerd werd, werd de respondent overgeslagen en een ander huis in de straat gekozen als vervanger.

- Op de hogeschool in Nijmegen en de Universiteit Twente werden respondenten in kantines en op studentwerkplekken zonder speciale selectie benaderd met de vraag te participeren. De benadering was niet random aangezien er voor de datacollectie geen plan was opgesteld om respondenten op een willekeurige wijze te benaderen. Elke potentiële respondent werd simpelweg aangesproken. Wanneer de respondent ervoor koos niet mee te doen werd hij of zij vervangen door een andere respondent. Uiteraard werden ook hier enkel meerderjarigen ondervraagd.

Interviewers hadden de keuze met betrekking tot welke manier van interviews afnemen er het meest werd gebruikt. Er werd doorgegaan met interviewen tot een totaal van 75 respondenten per interviewer werd bereikt.

3.3 Meetinstrument

Zoals al eerder is aangegeven is er, wat betreft het meetinstrument, sprake van een korte vragenlijst die schriftelijk, en voor een klein deel mondeling, wordt afgenomen. Voor een exemplaar van de vragenlijst verwijs ik u naar bijlage 1.

3.3.1 De apparaten en het online zijn van de respondent

Allereerst worden enkele vragen gesteld over de apparaten die de respondent in zijn of haar bezit heeft. Maakt de respondent gebruik van een computer, laptop, tablet en/of mobiele telefoon en hebben deze verbinding met het internet, of niet?

Vervolgens worden enkele vragen gesteld over de manier waarop, en de frequentie waarmee de respondent zich op het internet bevindt. De vragen lopen uiteen van het checken van de e-mail tot het online gokken. De frequenties lopen uiteen van ‘elke dag’ tot ‘nooit’.

3.3.2 De schriftelijke vragen over cybercrime uit de Veiligheidsmonitor van het CBS

Op dit moment worden de vragen uit de Veiligheidsmonitor van het CBS gesteld. De volgende concepten met bijbehorende definities komen aan bod:

- Identiteitsfraude: Identiteitsfraude is het opzettelijk gebruiken van gestolen of vervalste identiteitspapieren. De naam en identiteit van een ander wordt misbruikt om strafbare feiten te plegen (Politie, 2014). De auteurs van de Veiligheidsmonitor (CBS, 2012) hanteren de volgende definitie: "Gebruik zonder toestemming van persoonsgegevens voor financieel gewin."
- Online koop- of verkoopfraude: In het geval van online koop- of verkoopfraude wordt de koper of verkoper van goederen of diensten, opgelicht door de andere partij. Dit kan gebeuren via sites als Marktplaats, eBay of andere verkoop- of veilingssites. De auteurs van de Veiligheidsmonitor (CBS, 2012) hanteren de volgende definitie: "het (ver)kopen van goederen of diensten zonder die te leveren of te betalen."
- Hacking: In het geval van hacken wordt er ingebroken in het computersysteem zonder toestemming van de gebruiker (Ramesh & Maheswari, 2012) (Yanping Zhang, et al., 2012) en vaak met kwade bedoelingen. De auteurs van de Veiligheidsmonitor (CBS, 2012) hanteren de volgende definitie: "Het ongeoorloofd binnendringen op iemands computer."
- Cyberpesten: Het pesten via de digitale weg. Mogelijk via het internet of een andere elektronisch communicatiemiddel, zoals e-mail, social networks (met als voorbeeld Facebook en Twitter), sms, WhatsApp, internetfora of op een andere digitale manier.

Naast de vraag naar eventueel slachtofferschap komen er ook nog vragen aan bod met betrekking tot de frequentie van slachtofferschap en het slachtoffer.

3.3.3 Mondeling deel van de vragenlijst

Indien de respondent aangeeft slachtoffer te zijn geworden van één of meer van de voorgaande cybercrimes, is er hier ruimte om door te vragen. Er wordt gevraagd wat er zich precies heeft afgespeeld. Dit deel is essentieel voor de latere analyse. Hieruit zal later blijken in hoeverre de respondent de vragen van de Veiligheidsmonitor van het CBS daadwerkelijk begrepen heeft.

3.3.4 Tweede deel schriftelijke vragen

Vervolgens wordt er verdergegaan met de Vragenlijst UT. Hierin worden de volgende concepten met bijbehorende definitie bevraagd:

- Phishing: In het geval van phishing wordt het slachtoffer door middel van frauduleuze e-mails en websites verleid tot het geven van bankrekeningnummers, wachtwoorden en andere persoonlijke informatie aan de dader. Deze e-mails en websites lijken vaak afkomstig van betrouwbare organisaties, zoals een bank of een andere betrouwbare instantie. Dit zijn ze echter niet (Yue Zhang, Egelman, Cranor, & Hong, 2006) (Yue Zhang, Hong, & Cranor, 2007).

  Vragen worden gesteld aan de hand van verschillende vormen van phishing:

  - Phishing naar inloggegevens voor online bankieren
  - Phishing naar social network site inloggegevens
  - Phishing naar inloggegevens voor online bankieren
  - Phishing naar inloggegegevens voor een school- of werkaccount
- Online oplichting met financiële schade door middel van truc of slimmigheid: oplichting via de digitale weg. Dit begrip is ruimer dan koop- en verkoopfraude. Dit gezien het feit dat de vragen met betrekking tot dit onderwerp alle vormen van fraude via de digitale weg meten. Tevens wordt er in dit onderdeel gemeten of de respondent wel eens geld is kwijt geraakt op het internet.
- Online bedreiging: In het geval van online bedreiging wordt het slachtoffer bedreigd via de digitale weg. Mogelijk via het internet of een andere elektronisch communicatiemiddel, zoals e-mail, social networks (met als voorbeeld Facebook en Twitter), sms, WhatsApp, internetfora of op een andere digitale manier. Het begrip van de respondent over dit onderwerp wordt verder niet gecheckt. Enkel de prevalentie wordt gemeten.
- Diefstal of verlies van elektronische apparatuur: in dit geval is er sprake van diefstal of verlies van een materieel goed (bijvoorbeeld een smartphone, computer of laptop). Toch is dit onderwerp van belang gezien de hoeveelheid informatie die op dergelijke apparatuur te vinden is. De informatie hierop, die mogelijk verkegen wordt na de diefstal, geldt als het cyber-element van deze misdaad. Het begrip van de respondent over dit onderwerp wordt verder niet gecheckt. Enkel de prevalentie wordt gemeten.

3.3.5 Kenmerken respondent

Vervolgens wordt er geëindigd met enkele vragen met betrekking tot de leeftijd, het beroep en de opleiding van de respondent.

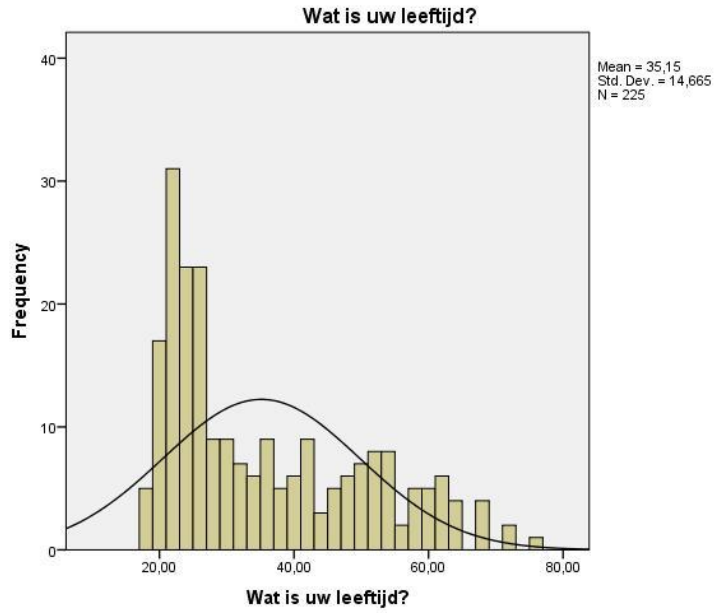
4 Resultaten

In dit hoofdstuk wordt bekend gemaakt welke resultaten er zijn gevonden. Allereerst wordt de steekproef beschreven. Vervolgens wordt er uitgeweid over de hoeveelheid slachtofferschap die er in deze studie door de respondenten is gerapporteerd. Vanaf paragraaf 4.3 wordt er onderzocht in hoeverre de respondent de exacte bedoeling van de vragen in de Veiligheidsmonitor begrijpt en antwoordt in overeenstemming met die bedoeling. Tevens wordt het begrip van de respondent met betrekking tot de vragen uit de Veiligheidsmonitor vergeleken met het begrip voor de vragenlijst UT. Tenslotte wordt er in paragraaf 4.4 onderzocht of de respondenten nog andere cybercrime opgeven in de Vragenlijst UT en hoeveel het CBS lijkt te missen.

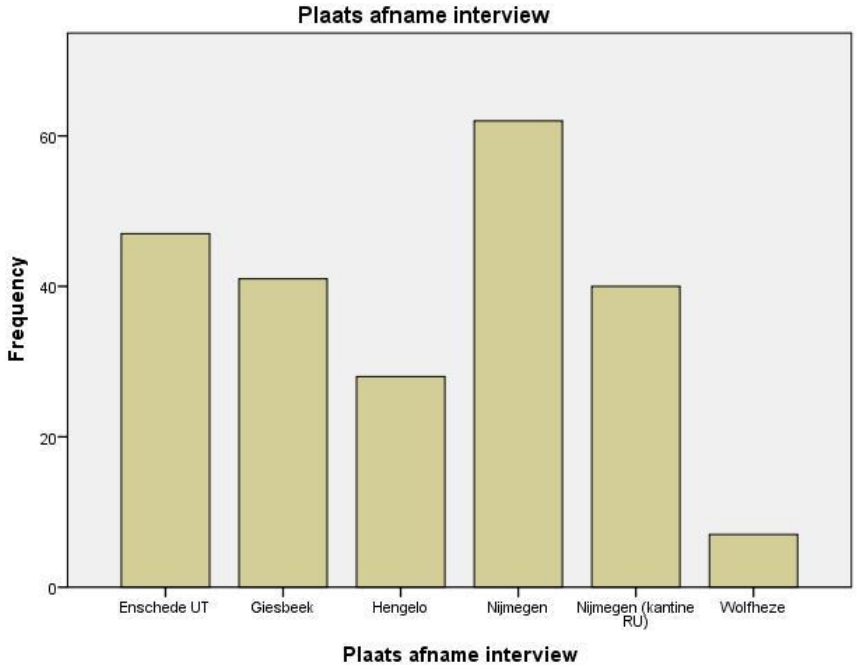
4.1 Steekproef

In totaal is er sprake van een steekproef van 225 respondenten, bestaande uit 117 mannen en 108 vrouwen. De leeftijden zijn niet geheel normaal verdeeld. Er is sprake van een grote piek bij de lagere leeftijdscategorieën (20 t/m 25 jaar oud). Dit is mogelijk het gevolg van het feit dat veel vragenlijsten op hogescholen en universiteiten zijn afgenomen. De vragenlijsten zijn afgenomen in Nijmegen, Hengelo, Giesbeek en Wolfheze. Tevens zijn er Vragenlijsten afgenomen op de Universiteit Twente in Enschede en Radboud Universiteit in Nijmegen.

Tabel 2 – Verdeling leeftijden respondenten in dit onderzoek



Tabel 3 – Verdeling woonplaatsen respondenten in dit onderzoek



4.2 Prevalentie cybercrime

De volgende hoeveelheid cybercrimes is gemeld door de respondenten. Tabel 4 is als volgt onderverdeeld:

Alle cybercrimes uit het onderzoek zijn in de tabel benoemd, onderverdeeld in de vragenlijst uit de Veiligheidsmonitor en de Vragenlijst UT. Vervolgens wordt het aantal respondenten dat de cybercrime heeft gerapporteerd vermeld. Het aantal respondenten dat de cybercrime heeft meegemaakt, wordt tevens weergegeven in een percentage van het totaal aantal respondenten. Er is een onderverdeling gemaakt in ‘respondent zelf’ en ‘respondent & huishouden’. Dit omdat de respondent in de vragenlijst van de Veiligheidsmonitor kan aangeven of hij of zij zelf slachtoffer is geworden van een cybercrime, of dat het gehele huishouden slachtoffer is geworden.

Tabel 4 - Prevalentie cybercrime gemeld door de respondenten

	Respondent & huishouden (a)	Respondent zelf (b)	Phishing, heeft gegevens ingevuld (c)	Respondent & huishouden (d)	Respondent zelf (e)	Phishing, heeft gegevens ingevuld [1] (f)
	Absolute aantallen			In %		
Vragen afkomstig uit de Veiligheidsmonitor van het CBS	**225**	**225**	**225**	**100**	**100**	**100**
A. Identiteitsfraude	14	11	-	6,2	4,9	-
B. Koop-verkoop fraude	13	4	-	5,8	1,78	-
C. Hacking	18	12	-	8	5,3	-
D. Cyberpesten	6	6	-	2,7	2,7	-
Totaal	**51**	**33**	-	**22,7**	**14.7**	-
Vragen afkomstig uit de Vragenlijst UT					**(b/225)x100**	**(c/b)x100**
E. E-mail van 'bank' met link om in te loggen (phishing)	-	55	1	-	24,4	1,8 (N=55)
F. Gevraagd om inlog social network site account (phishing)	-	11	1	-	4,9	9,1 (N=11)
G. Gevraagd om inlog online gaming account (phishing)	-	13	1	-	5,8	7,7 (N=13)
H. Gevraagd om inlog werk-/schoolaccount (phishing)	-	8	4	-	3,6	50,0 (N=8)
I. Geld/goederen kwijt door oplichting met truc of slimmigheid op internet	-	7	-	-	3,1	-
J. Geld/goederen op andere wijze kwijt op het internet	-	8	-	-	3,6	-
K. Online bedreiging	-	8	-	-	3,6	-
L. Laptop gestolen	-	2	-	-	1,1	-
M. Mobiele telefoon gestolen	-	8	-	-	4,3	-
N. Laptop en mobiele telefoon gestolen	-	1	-	-	0,5	-
Totaal cybercrime	-	**121**	**7**	-	-	-
Totaal Veiligheidsmonitor + Totaal Vragenlijst UT cybercrime	-	**154**	-	-	-	-

[1] basis is aantal respondenten dat phishing-mails heeft ontvangen

4.3 Analyse van het begrip van de respondent met betrekking tot de concepten

Hieronder volgt een analyse van het begrip van de respondent met betrekking tot de vragen en cybercrimes uit de vragenlijsten. Het begrip van de respondent is gemeten zoals is aangegeven in paragraaf 3.1 (Research design). Allereerst wordt de vragenlijst uit de Veiligheidsmonitor geanalyseerd. Vervolgens wordt dezelfde aanpak toegepast op de Vragenlijst UT. Als afsluiting wordt een vergelijking gemaakt tussen het begrip van de respondent voor beide vragenlijsten.

4.3.1 Analyse van het begrip van de vragen uit de Veiligheidsmonitor

Hierop volgt de analyse van het begrip van de respondent met betrekking tot de vragen die afkomstig zijn uit de Veiligheidsmonitor.

36 van de 46 respondenten hebben een volledig begrip van de vragen uit de Veiligheidsmonitor. Ze begrijpen wat er precies gevraagd wordt in de enquête, herkennen de situatie uit hun eigen leven, en antwoorden naar aanleiding hiervan ‘ja’ bij de vraag over de cybercrime die hem of haar is overkomen. Tevens leggen ze uit wat hen overkomen is op een manier die overeen komt met de definitie van de betreffende cybercrime. Een voorbeeld hiervan is de uitleg van een respondent die koop-verkoopfraude rapporteerde: “Vader van respondent wou kaartjes bestellen voor een concert van André Rieu aangezien dit goedkoper was dan via de normale kanalen. Kaarten zijn nooit aangekomen.” Deze uitleg komt overeen met de definitie van koop-verkoopfraude, zoals gesteld door het CBS.

Bij 5 van de 46 respondenten is dit in mindere mate het geval. Ze hebben een gedeeltelijk begrip van wat er met de vragen bedoeld wordt. Ze rapporteren een misdaad die sterk lijkt op de misdaad die gevraagd wordt in het onderzoek. Toch komt dit niet geheel overeen. Een voorbeeld hiervan is de volgende rapportage van een respondent die identiteitsfraude rapporteerde: “Mail gekregen dat iemand vanuit het buitenland gmail account probeerde binnen te komen. wachtwoord veranderd en verder niks aan de hand.” De respondent krijgt in dit geval score 1. Om het account binnen te komen is het wachtwoord van de respondent nodig. Op zich is het voor te stellen dat de respondent denkt dat iemand die een account binnen probeert te komen, zich voordoet als de eigenaar van het account. Toch heeft de respondent de vraag niet goed begrepen.

Er is hier geen gebruik gemaakt van gestolen of vervalste identiteitspapieren en er zijn ook geen aanwijzingen om aan te nemen dat er een poging is gedaan met financieel motief. Aan de andere kant worden de naam en de identiteit van de eigenaar van het account (de respondent in kwestie) wel misbruikt. Een gedeeltelijk correcte rapportage dus. Het is echter aannemelijker dat er hier sprake is van hacking.

Bij 4 van de 46 respondenten komt hun beschrijving van hetgeen ze overkomen is in het geheel niet overeen met de definitie van de gevraagde cybercrimes uit het onderzoek. De respondenten rapporteren in dit geval een compleet andere cybercrime dan de crime waarom gevraagd werd. Dit indiceert dat de respondenten in kwestie de vraag niet begrepen hebben. Een voorbeeld hiervan is de uitleg van een respondent die hacking rapporteert: "Mail van bank met de vraag of ik wilde inloggen terwijl de bank hier nooit om vraagt." In dit geval is er sprake van phishing en heeft de respondent de vraag, of het begrip hacking, niet goed begrepen en als gevolg hiervan niet goed gerapporteerd. Hetgeen de respondent uitlegt komt immers niet overeen met de definitie van hacking.

Bij 1 van de 46 respondenten was het door onvolledigheid van het antwoord niet mogelijk om een score te bepalen.

In tabel 5 worden de resultaten samengevat. U kunt hier het begrip van de respondent voor de hele vragenlijst uit de Veiligheidsmonitor, en per type cybercrime, vinden.

Tabel 5 – Begrip vragenlijst Veiligheidsmonitor. Totaal en per cybercrime.

Score	**Aantal score**	**Percentage score**
Score 2	36	78,3
Score 1	5	10,9
Score 0	4	8,7
Geen score	1	2,2
Totaal	**46**	**100**

Identiteitsfraude	-Van de respondenten die identiteitsfraude hebben meegemaakt, rapporteerde 57,1% geheel in overeenstemming met de definitie
	-Van de respondenten die identiteitsfraude hebben meegemaakt, rapporteerde 28,6% **niet geheel** in overeenstemming met de definitie
	-Van de respondenten die zeiden identiteitsfraude te hebben meegemaakt, rapporteerde 7,1 % **niet** in overeenstemming met de definitie
	-Van de respondenten die zeiden identiteitsfraude te hebben meegemaakt, gaf 7,1% **niet** voldoende verdere informatie
Koop-verkoopfraude	-Van de respondenten die zeiden verkoopfraude te hebben meegemaakt, rapporteerde 91,7% geheel in overeenstemming met de definitie
	-Van de respondenten die zeiden verkoopfraude te hebben meegemaakt, rapporteerde 8,3% **niet** in overeenstemming met de definitie
Hacking	-Van de respondenten die zeiden hacking te hebben meegemaakt, rapporteerde 80% geheel in overeenstemming met de definitie
	-Van de respondenten die zeiden hacking te hebben meegemaakt, rapporteerde 6,7% **niet geheel** in overeenstemming met de definitie
	-Van de respondenten die zeiden hacking te hebben meegemaakt, rapporteerde 13,3 % **niet** in overeenstemming met de definitie
Cyberpesten	-Van de respondenten die zeiden cyberpesten te hebben meegemaakt, rapporteerde 100% geheel in overeenstemming met de definitie

4.3.2 Analyse van het begrip van de vragen uit de Vragenlijst UT

Eenzelfde analyse die uitgevoerd is bij de vragenlijst van de Veiligheidsmonitor, is ook uitgevoerd voor de vragenlijst die speciaal voor deze studie is ontwikkeld.

74 van de 88 respondenten hebben een volledig begrip van de vragen die specifiek voor deze studie zijn ontwikkeld. Ze begrijpen wat er precies gevraagd wordt in de enquête, herkennen de situatie uit hun eigen leven, en antwoorden naar aanleiding hiervan 'ja' bij de vraag over de cybercrime die hem of haar is overkomen. Tevens leggen ze uit wat hen overkomen is op een manier die overeen komt met de definitie van de betreffende cybercrime. Een voorbeeld hiervan is de uitleg van een respondent die phishing heeft gerapporteerd: "Mails van "bank" van een ander adres die vragen om persoonsgegevens in te voeren en op te sturen. Niet op ingegaan." Deze uitleg komt overeen met de definitie van phishing.

Bij 6 van de 88 respondenten is dit in mindere mate het geval. Ze hebben een gedeeltelijk begrip van wat er met de vragen bedoeld wordt. Ze rapporteren een misdaad die sterk lijkt op de misdaad die gevraagd wordt in het onderzoek. Toch komt dit niet geheel overeen. Een voorbeeld hiervan is de uitleg van een respondent die phishing rapporteert: "Normale situatie om op de desbetreffende accounts te komen." De respondent heeft gedeeltelijk correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze en criminele wijze, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar de score 1.

Bij 1 van de 88 respondenten komt de beschrijving van hetgeen hen/haar overkomen is in het geheel niet overeen met de definitie van de gevraagde cybercrimes uit het onderzoek. De respondent rapporteert in dit geval een compleet andere cybercrime dan de crime waarom gevraagd werd. Dit indiceert dat de respondent in kwestie de vraag niet begrepen heeft. Een voorbeeld hiervan is de uitleg van een respondent die phishing rapporteert: "Via linkedin verzoek om connectie te maken met iemand die respondent niet kende, niet op gereageerd." Er is hier geen sprake van phishing. De connectie kan ook per ongeluk verzonden zijn. Tevens kan er sprake zijn van de mogelijkheid dat de respondent de verzender niet kent, maar de verzender de respondent wel. Er wordt in dit geval niet aan de definitie van phishing voldaan. Daarom de score 0.

Bij 7 van de 88 respondenten was het door onvolledigheid van het antwoord niet mogelijk om een score te bepalen. Deze respondent is voorzien van een streepje (-) in tabel 4.

In tabel 6 worden de resultaten samengevat. U kunt hier het begrip van de respondent voor de hele vragenlijst uit de Veiligheidsmonitor, en per type cybercrime, vinden.

Tabel 6 – Begrip vragenlijst UT. Totaal en per cybercrime.

Score	**Aantal score**	**Percentage score**
Score 2	74	84,1
Score 1	6	6,8
Score 0	1	1,1
Geen score	7	8,0
Totaal	**88**	**100**

Phishing	-Van de respondenten die zeiden phishing te hebben meegemaakt, rapporteerde 81,8% geheel in overeenstemming met de definitie
	-Van de respondenten die zeiden phishing te hebben meegemaakt, rapporteerde 7,8% **niet geheel** in overeenstemming met de definitie
	-Van de respondenten die zeiden phishing te hebben meegemaakt, rapporteerde 1,3% **niet** in overeenstemming met de definitie
	-Van de respondenten die zeiden phishing te hebben meegemaakt, gaf 9,1% **niet** voldoende verdere informatie
Online oplichting	-Van de respondenten die zeiden online oplichting te hebben meegemaakt, rapporteerde 100% geheel in overeenstemming met de definitie
Geld kwijt via internet	-Van de respondenten die zeiden geld kwijt te zijn geraakt via internet, rapporteerde 100% geheel in overeenstemming met de definitie

4.3.3 Vergelijking tussen het begrip van beide vragenlijsten

De chi-kwadraat toets met formule $X^2 = \sum \frac{(Observed - Expected)^2}{Expected}$ met alfa = 0,05 geeft:

(X^2 = 7.03, df = 3, p = 0.05<p<0.10)

Tabel 7 - Aantal scores per vragenlijst. In geobserveerde en verwachte waarden

Vragenlijst/Score	**2**		**1**		**0**		**Geen score**		**Totaal**
	Obs	**Exp**	**Obs**	**Exp**	**Obs**	**Exp**	**Obs**	**Exp**	
Veiligheidsmonitor	36	37,76	5	3.78	4	1.72	1	2.75	46
Vragenlijst UT	74	72.24	6	7.22	1	3.28	7	5.25	88
Totaal	110		11		5		8		134

Gezien het feit dat de p-waarde groter is dan de alfa van 0,05 is er niet voldoende bewijs om de nulhypothese te verwerpen. De hoeveelheid begrip van de respondenten voor beide vragenlijsten is hetzelfde.

4.4 Vergelijking Veiligheidsmonitor en Vragenlijst UT

Hieronder wordt aangegeven in hoeverre de Veiligheidsmonitor van het CBS cybercrimes lijkt te missen. Er is onderzocht welke cybercrimes wel bij de vragen van de Vragenlijst UT zijn gerapporteerd, maar niet bij de vragen van de Veiligheidsmonitor. Hetzelfde wordt ook omgekeerd gedaan.

4.4.1 Cyberpesten en online bedreiging

Tabel 8 – Vergelijking Cyberpesten (Veiligheidsmonitor) en Online bedreiging (Vragenlijst UT)

		Cyberpesten (Veiligheidsmonitor)		**Totaal**
		Nee	Ja	
Online bedreiging (vragenlijst UT)	Nee	215 98,2% 99,5%	1 16,7% 0,5%	216 96,0% 100,0%
	Ja	4 1,8% 50,0%	4 66,7% 50,0%	8 3,6% 100,00%
	Weet niet	0 0,0% 0,0%	1 16,7% 100,0%	1 0,4% 100,0%
Totaal		219 100,0% 97,3%	6 100,0% 2,7%	225 100,0% 100,0%

Uit tabel 7 blijkt dat 2,7% van de respondenten cyberpesten van de Veiligheidsmonitor rapporteren, terwijl dit bij Online bedreiging uit de Vragenlijst UT 3,6% is.

Op de vraag van de Veiligheidsmonitor is 6 keer slachtofferschap gerapporteerd. Hier tegenover staat dat 4 van deze respondenten, of 66,7%, hun slachtofferschap ook hebben gerapporteerd bij de vragen met betrekking tot online bedreiging. Op deze vraag uit de Vragenlijst UT is in totaal 8 keer positief gereageerd. Uit de data blijkt dat de Vragenlijst UT één cybercrime heeft gemist die wel bij de vragen uit de Veiligheidsmonitor werd gerapporteerd.

Tevens zijn vier verschillende online bedreigingen wel gemeld zijn bij de vraag in de Vragenlijst UT, maar niet gemeld bij de ruimer gestelde vraag van de Veiligheidsmonitor. De vraag uit de Veiligheidsmonitor heeft dus 4 cybercrimes gemist die wel onder vraagstelling van de Veiligheidsmonitor vallen.

4.4.2 Vergelijking koop-verkoopfraude en oplichting via het internet

Tabel 9 – Vergelijking Koop-verkoopfraude (Veiligheidsmonitor) en Oplichting met financiële schade (Vragenlijst UT)

		Koop-verkoopfraude (Veiligheidsmonitor)		**Totaal**
		Nee	Ja	
Online oplichting met financiële schade (vragenlijst UT)	Nee	208 98,1% 95,4%	10 76,9% 4,6%	218 96,9% 100,0%
	Ja	4 1,9% 57,1%	3 23,1% 42,9%	7 3,1% 100,0%
Totaal		212 100,0% 94,2%	13 100,0% 5,8%	225 100,0% 100,0%

Uit tabel 8 blijkt dat 5,8% van de respondenten koop-verkoopfraude van de Veiligheidsmonitor rapporteren, terwijl dit bij Online oplichting met financiële schade uit de Vragenlijst UT 3,1% is.

Op de vraag van de Veiligheidsmonitor is 13 keer slachtofferschap gerapporteerd. Hier tegenover staat dat 3 van deze respondenten, of 23,1%, hun slachtofferschap ook hebben gerapporteerd bij de vragen met betrekking tot online oplichting met financiële schade. Op deze vraag uit de Vragenlijst UT is 7 keer positief gereageerd.
Uit de data blijkt dat de Veiligheidsmonitor 4 cybercrimes heeft gemist die wel bij de vragen uit de Vragenlijst UT werd gerapporteerd. De Vragenlijst UT heeft daarentegen 10 cybercrimes gemist die wel door bij de vragenlijst uit de Veiligheidsmonitor werden gerapporteerd

4.5 Phishing en de Veiligheidsmonitor

In totaal rapporteren zeven respondenten dat ze hun gegevens hebben ingevuld wanneer ze daar door iemand om gevraagd zijn. De respondenten in kwestie zouden dus op een phishing-poging in kunnen zijn gegaan. Het is nu de vraag in hoeverre dit feit ook weergegeven wordt in de vragen uit de Veiligheidsmonitor. De volgende verduidelijkende quotes werden opgetekend uit de mond van de respondenten die phishing hadden gerapporteerd en staan vermeld in tabel 9. Tevens wordt vermeld van welke phishing-variant er sprake is en welk slachtofferschap de respondent in kwestie bij de vragen uit de Veiligheidsmonitor heeft gerapporteerd.

Tabel 10 - Hebben respondenten die op een phishing-poging zijn ingegaan ook slachtofferschap bij de Veiligheidsmonitor gerapporteerd?

Respondentnummer	**Phishingvariant (Vragenlijst UT)**	**Uitleg respondent**	**Crime gerapporteerd bij Veiligheidsmonitor?**
490007420	Phishing bankaccount	Mails van bank en game account ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	ID-FRAUDE/HACKING: Partner heeft inloggegevens ingevoerd na ontvangen van phishing mail. Na 1 dag achter gekomen dat dit van een andere afzender kwam. Bank op de hoogte gesteld, codes account veranderd en aangifte gedaan. Ook mails ontvangen vanuit eigen mailaccount waarin advertenties stonden ondertekend met eigen naam. wachtwoord mailaccount veranderd daarna niet meer voorgekomen.
210005521	Social network account	Normale situatie om op de desbtreffende accounts te komen	Geen rapportage
700000431	Phishing Online game	Geen toelichting	Geen rapportage
50000311	Phishing werkaccount	Het gaat altijd om vragen van vrienden die iets op mijn account willen doen.	Geen rapportage
440000311	Phishing werk-/schoolaccount	Informatie gegeven aan vrienden die zich voor mij (in mijn naam) hebben ingelogd om me voor een les in te schrijven.	HACKING: kreeg mail dat Google account mogelijk gehackt was. Dit omdat telefoonnummer van Google account veranderd scheen te zijn toen de respondent Facebook op de mobiel had gedownload. Verder geen zekerheid. Respondent snapt het zelf ook niet helemaal – Lijkt onafhankelijk van phishing
190005521	Phishing werk-/schoolaccount	Inloggegevens voor schoolsysteem geleend aan een oud-klasgenootje. Zij kon niet meer in het systeem en had bepaalde informatie nodig. Via deze manier is dit gelukt.	Geen rapportage
210005521	Phishing werk-/schoolaccount	Normale situatie om op de desbtreffende accounts te komen	Geen rapportage

Zoals te zien is in tabel 9 is er waarschijnlijk enkel in het eerste geval (respondent 490007420) sprake van phishing-poging met criminele opzet. De respondent in kwestie geeft in zijn toelichting echter aan niet op de phishing mails in te zijn gegaan. Toch rapporteert hij bij de vragen van de Veiligheidsmonitor, weliswaar onder het label Identiteitsfraude/hacking, zelf in te zijn gegaan op een phishing poging. Deze phishing-actie wordt dus zowel door de vragenlijst van de Veiligheidsmonitor, als door de Vragenlijst UT, opgemerkt.

In de andere gevallen is er waarschijnlijk geen sprake van phishing met criminele of frauduleuze opzet. Het hacking-slachtofferschap dat respondent 440000311 bij de vragen van de Veiligheidsmonitor rapporteert, lijkt onafhankelijk van het afgeven van zijn gegevens aan zijn vrienden. Hier lijkt eerder sprake van vriendschappelijk contact met wederzijdse dienst (respondent 50000311, 440000311, 190005521) of een respondent die de vraag heel letterlijk heeft genomen en ‘het inloggen’ ziet als een vraag om gegevens (respondent 210005521). Eén respondent (700000431) geeft geen nadere toelichting.

5 Conclusie en discussie

In dit onderzoek werd onderzocht hoe een nieuwe enquête zich verhoudt tot de huidige veiligheidsmonitor van het CBS wat betreft het valide meten van cybercrime slachtofferschap. Daartoe is een gelegenheidssteekproef geselecteerd van 225 respondenten aan wie de cybercrime vragenlijst uit de Veiligheidsmonitor en de Vragenlijst UT zijn voorgelegd. Aan de hand van de uitleg van de respondent is bepaald in hoeverre hij of zij de exacte bedoeling van de vragen in de Veiligheidsmonitor begrijpt en heeft geantwoord in overeenstemming met die bedoeling. Allereerst wordt er ingegaan op deze kwestie. Vervolgens wordt het begrip van de respondent met betrekking tot de vragen van de Veiligheidsmonitor vergeleken met het begrip van de respondent met betrekking tot de Vragenlijst UT. Als laatst wordt er bekeken wat respondenten rapporteren bij nadere ondervraging en wat het CBS lijkt te missen

Het begrijpen van de vragen uit de Veiligheidsmonitor van het CBS

De eerste vraag uit dit onderzoek luidt als volgt: Begrijpt de respondenten de exacte bedoeling van de vraag in de Veiligheidsmonitor en antwoordt hij of zij in overeenstemming met die bedoeling? Om deze vraag te beantwoorden zijn de vragen uit de Veiligheidsmonitor afgenomen en werd er doorgevraagd wanneer een respondent slachtofferschap rapporteert. Aan de hand van deze uitleg van de respondent werd vervolgens beoordeeld of de respondent de vraag begrepen heeft. Hetzelfde werd gedaan voor de Vragenlijst UT. een vergelijking tussen beide vragenlijsten op dit gebied werd tevens uitgevoerd.

Uit dit onderzoek blijkt dat 78,3% van de slachtoffers de vragen uit de vragenlijst van de Veiligheidsmonitor volledig begrijpt. De slachtoffers in kwestie begrijpen wat er gevraagd wordt en herkennen de cybercrimes die genoemd worden. Hetgeen ze vertellen over wat hen overkomen is, komt overeen met de cybercrime die ze gerapporteerd hebben. Hieruit volgt dat dit bij 21,7% van de slachtoffers niet of minder het geval is.

Hiervan begrijpen 10,9% van de slachtoffers gedeeltelijk wat er met de vragen bedoeld wordt. Ze vertellen over een misdaad die sterk lijkt op de misdaad die ze gerapporteerd hebben in het onderzoek. Toch komen beide niet geheel overeen. Bij 8,7% van de slachtoffers komt de beschrijving van hetgeen hen overkomen is geheel niet overeen met de cybercrime die gerapporteerd is. Dit deel van de slachtoffers begrijpt de vraagstelling of de genoemde cybercrime in de vraagstelling geheel niet. Bij de restcategorie van 2,2% procent was het geven van een score niet mogelijk omdat de slachtoffers in kwestie geen verdere uitleg hebben gegeven over hetgeen hem of haar overkomen is.

Er is een onderscheid aan te merken in het begrijpen van de vragen door de respondent per type cybercrime. Het percentage slachtoffers dat de vragen met betrekking tot koop-verkoopfraude en cyberpesten volledig begreep is hoog, respectievelijk 91,7% en 100% procent van de slachtoffers begreep de vragen met betrekking tot deze cybercrimes volledig. Bij hacking en vooral bij identiteitsfraude liggen deze cijfers een stuk lager. De vragen met betrekking tot hacking worden maar door 80% van de slachtoffers volledig begrepen, correct beantwoord en van correcte uitleg voorzien. Dit terwijl het percentage slachtoffers dat de vragen met betrekking tot identiteitsfraude volledig begrijpt, en in overeenstemming met de definitie van identiteitsfraude uitleg geeft, slechts 57,1% is.

Zoals blijkt uit bovenstaande data is er een verschil tussen de cybercrimes, met betrekking tot het percentage respondenten dat de vragen erover geheel begrijpt. Het is niet met zekerheid te verklaren hoe deze verschillen veroorzaakt zijn. Vermoedelijk heeft dit weinig te maken met de manier waarop de vraag gesteld is. Het verschil zou sneller verklaard kunnen worden door de kennis die het slachtoffer al bezit voordat hij of zij de vragenlijsten invult. Begrippen als pesten en fraude bestaan al sinds mensenheugenis en bijna elk individu zal zich een beeld kunnen vormen van dergelijke delicten. Sinds enkele jaren zijn deze misdaden verplaatst naar het wereldwijde web, maar de essentie van fraude of pesten is nog steeds hetzelfde. De respondent begrijpt deze begrippen als gevolg hiervan mogelijk goed. Hoe anders is dit bij begrippen als hacking en identiteitsfraude. Het gebruik van computers en internet is van groot belang voor het plegen van deze misdaden en deze misdaden zijn als vrij nieuw aan te merken. Mogelijk heeft de respondent als gevolg hiervan minder kennis van dergelijke misdaden die ergens op een computer, in een minder tastbare wereld plaatsvinden.

Het feit dat er met betrekking tot identiteitsfraude enkel in 57,1% van de gevallen correct is gerapporteerd, geeft aan dat de rapportage van deze misdaad geen valide beeld geeft van de werkelijkheid. Wanneer het begrip van het slachtoffer niet zou zijn getest, maar de resultaten simpelweg als waar zouden zijn aangenomen, zou dit een bedreiging kunnen zijn voor de validiteit van het onderzoek. Als gevolg hiervan zou het niet mogelijk zijn om te meten wat er precies gemeten moet worden.

Het begrijpen van de vragen uit de Vragenlijst UT

Bij de Vragenlijst UT lijken de percentages in eerste instantie hoger. 84,1% van de slachtoffers begrijpt wat er gevraagd wordt en herkent de cybercrimes die genoemd worden. Tevens leggen deze slachtoffers, in overeenstemming met de definitie van de cybercrime die gerapporteerd is, uit wat hem of haar overkomen. Bij 15,9% van de slachtoffers is dit dus niet of in mindere mate het geval.

Hiervan begrijpt 6,8% van de slachtoffers de vragen die hem gesteld worden gedeeltelijk. Dit bleek uit het feit dat de slachtoffers in kwestie verhalen vertelden die wel leken te passen bij de cybercrimes die ze rapporteerden, maar uiteindelijk niet overeen kwamen. In 1,1% van de gevallen begreep het slachtoffer de vragen en/of gevraagde cybercrimes geheel niet. Ze rapporteerden in dit geval bepaalde cybercrimes, maar uit de verhalen van deze slachtoffers bleek dat ze iets anders hadden meegemaakt. 8,0% van de slachtoffers kregen geen score omdat ze niet, of niet voldoende, duidelijk hadden gemaakt wat hen overkomen is.

Ook in dit geval verschillen de percentages sterk per cybercrime. Bij phishing rapporteert 81,8% van de slachtoffers in overeenstemming met de definitie van phishing. Hieruit blijkt dat deze slachtoffers volledig begrijpen wat hen gevraagd wordt en het duidelijk is voor het slachtoffer wat phishing inhoudt. In het geval van Online oplichting met financiële schade en de variabele ‘geld kwijt via internet’ is dit percentage zelfs 100%.

In dit geval liggen de percentages hoger dan bij de vragenlijst van de Veiligheidsmonitor. Ook hier is er echter een onderscheid op te merken tussen phishing en de andere gemeten cybercrimes. Bij de cybercrime phishing wordt er minder correct gerapporteerd dan bij de andere cybercrimes die bevraagd werden. Mogelijk is dezelfde verklaring voor dit verschil van toepassing als bij de vragen van de Veiligheidsmonitor. De kennis die de respondent ‘vooraf’ van phishing had is mogelijk minder dan de kennis die de respondent heeft van een online vorm van het aloude oplichting.

Vergelijking van het begrijpen van de vragenlijsten door de respondent

Door middel van een chi-kwadraattoets voor de homogeniteit kan worden aangegeven of er een significant verschil bestaat tussen het begrip van de slachtoffers voor de vragenlijst van de Veiligheidsmonitor en het begrip van de slachtoffers voor de Vragenlijst UT. Uit de uitkomst van deze test blijkt dat er, ondanks het uitvoerige ontwerpproces van de Vragenlijst UT, geen significant verschil is tussen het begrip van het slachtoffer voor beide vragenlijsten.

Dit is niet volgens de verwachting. De verwachting was dat de Vragenlijst UT beter zou scoren op dit punt. Dit door de toepassing van uitgebreide theorie met betrekking tot het ontwerpen van goede vragenlijsten. Dit kan er op duiden dat het ontwerpproces geen effect heeft gehad of dat de Vragenlijst van de Veiligheidsmonitor technisch op gelijk niveau ontworpen is.

Rapportage Vragenlijst UT

De tweede deelvraag luidt als volgt: Geven respondenten nog andere cybercrime op bij nadere ondervraging? Dit is het geval. Zoals uit Tabel 4 blijkt rapporteren respondenten ook slachtofferschap op de onderwerpen uit de Vragenlijst UT, te weten:

- Phishing met een vraag naar inloggegevens van het online bankaccount, social networksite-account, online gaming site-account en werk- of schoolaccount.
- Geld of goederen kwijt door online oplichting met truc of slimmigheid
- Het, op een andere wijze, kwijtraken van geld of goederen op het internet
- Online bedreiging
- Laptop gestolen
- Mobiele telefoon gestolen

Missen de vragenlijsten slachtofferschap van cybercrime?

De derde deelvraag uit dit onderzoek luidt als volgt: Hoeveel cybercrime lijkt de Veiligheidsmonitor van het CBS te missen? Als antwoord werden de vragenlijsten uit de Veiligheidsmonitor en de Vragenlijst UT met elkaar vergeleken. Uit deze vergelijking bleek dat er door beide vragenlijsten cybercrimes gemist worden.

Bij de vergelijking tussen cyberpesten (Veiligheidsmonitor) en Online bedreiging (Vragenlijst UT) werd er door de Vragenlijst UT 1 geval van slachtofferschap gemist dat wel bij de Veiligheidsmonitor werd gerapporteerd. Dit is niet vreemd. De vragen van de Veiligheidsmonitor meten immers ruimer. Dat wil zeggen, er worden meer soorten pesten op het internet bevraagd, terwijl de Vragenlijst UT enkel online bedreiging bevraagt. Opvallender is het feit dat vier verschillende online bedreigingen wel gemeld zijn bij de Vragenlijst UT, maar niet gemeld zijn bij de ruimer gestelde vragen van de Veiligheidsmonitor. De vragenlijst van de Veiligheidmonitor heeft dus 4 cybercrimes gemist die wel onder de vraagstelling vallen.

Een verklaring hiervoor is niet met zekerheid te geven. Mogelijk heeft het uitgebreide ontwerpproces van de Vragenlijst UT bijgedragen aan het feit dat er meer slachtofferschap gerapporteerd is en/of was de vraag van de Veiligheidsmonitor niet van voldoende kwaliteit. Tevens is het mogelijk dat de positie van de vraag een effect heeft gehad. De vraag van de Veiligheidsmonitor werd als eerst gesteld en de vraag uit de Vragenlijst UT als tweede. Het meest waarschijnlijk lijkt echter de verklaring dat de respondenten die slachtoffer zijn geworden van een vorm van online bedreiging, vooral specifiek 'op zoek' zijn naar deze misdaad in de vragenlijst. Mogelijk voelen ze zich niet voldoende aangesproken door het begrip cyberpesten.

Uit een vergelijking tussen koop-verkoopfraude (Veiligheidsmonitor) en online oplichting met financiële schade (Vragenlijst UT) blijkt het volgende:
Op de vraag van het CBS is 13 keer slachtofferschap gerapporteerd. Drie van deze slachtoffers, of 23,1%, hebben hun slachtofferschap ook gerapporteerd bij de vragen met betrekking tot online oplichting met financiële schade. Het genoemde percentage is lager dan verwacht. Uit onderzoek is tevens gebleken dat de vragenlijst van de Veiligheidsmonitor 4 cybercrimes heeft gemist die wel bij de vragen uit de Vragenlijst UT werd gerapporteerd. Daarentegen blijkt uit de data dat de Vragenlijst UT 10 cybercrimes heeft gemist die wel door bij de vragenlijst uit de Veiligheidsmonitor werden gerapporteerd. Dit is bijzonder te noemen. De verwachting was dat de Vragenlijst UT meer rapportage van slachtofferschap zou genereren. Dit door het uitgebreide ontwerpproces en de ruimere vraagstelling met betrekking tot het onderwerp.
De mogelijke oorzaak voor het feit dat er bij de Vragenlijst UT minder slachtofferschap is gerapporteerd kan zijn dat er gesproken wordt van Online oplichting met financiële schade. Indien het slachtoffer geen of weinig financiële schade heeft ondervonden van de oplichting of fraude, kan dit ervoor zorgen dat de respondent in kwestie zich niet aangesproken voelt bij de vraag uit de Vragenlijst UT en ervoor kiest niet te rapporteren.

In totaal hebben zeven respondenten gerapporteerd dat ze hun persoonlijke gegevens hebben ingevuld wanneer er om gevraagd werd. Uit de uitleg van de respondent blijkt dat er van ze zeven incidenten, er enkel één keer sprake was van een daadwerkelijke phishing-poging met crimineel en frauduleuze opzet. In de andere gevallen was er geen sprake van een criminele opzet. Dit incident is door de respondent ook gerapporteerd in de vragen van de

Veiligheidsmonitor. De vragen van de Veiligheidsmonitor zijn er dus in geslaagd om het criminele en frauduleuze incident te identificeren.
De andere zes niet-frauduleuze gevallen werden niet gerapporteerd bij de vragen uit de Veiligheidsmonitor. Dit is een gunstig resultaat. De Veiligheidsmonitor identificeert enkel de criminele en frauduleuze incidenten en geeft dus, op dit gebied, een valide beeld van de hoeveelheid cybercrime.
Concluderend kan gesteld worden dat er geen significant verschil is gevonden tussen de twee vragenlijsten op het gebied van de hoeveelheid begrip van de respondent voor de vragen en de onderwerpen. Wel viel het op dat er tijdens de nadere ondervraging door middel van de Vragenlijst UT extra slachtofferschap van cybercrime is gerapporteerd door de respondent.
Tevens heeft het onderzoek uitgewezen dat zowel de Vragenlijst UT als de vragenlijst van de Veiligheidsmonitor een bepaalde hoeveelheid slachtofferschap missen. Positief opvallend is dat de vragenlijst van de Veiligheidsmonitor er goed in is geslaagd enkel het daadwerkelijke slachtofferschap van phishing uit de rapportages van phishing te filteren.

Beperkingen

De benadering van de respondenten zou in vervolgonderzoek beter op een random wijze kunnen plaatsvinden. Het benaderen van de huishoudens was als gedeeltelijk random te zien. Het aanspreken van potentiële respondenten op de hogeschool Nijmegen en Universiteit Twente is echter geheel niet als random te kwalificeren. Bij een volgend onderzoek is een meer random aanpak te adviseren. Dit zou er immers voor kunnen zorgen dat de resultaten meer representatief zijn voor de Nederlandse bevolking.

Dit is nu niet het geval. Het feit dat een groot deel van de respondenten studeert aan de Universiteit Twente of de Hogeschool Nijmegen kan immers leiden tot een vertekening van de resultaten. Op dergelijke instellingen zijn over het algemeen veel jongeren en hoger opgeleiden te vinden. Het feit dat veel respondenten met een hogere opleiding bezig zijn, kan leiden tot mindere representativiteit van de resultaten. Het is immers mogelijk dat hoger opgeleide individuen vaker of juist minder vaak slachtoffer van cybercrime zijn. Tevens is het mogelijk dat jongeren vaker gebruik maken van internet. Dit zou tevens de slachtofferschapspercentages kunnen vergroten.

Een derde eigenschap van de gebruikte vorm van onderzoek, die als beperking kan worden gezien, is het feit dat de antwoorden van de respondent gescoord zijn door de onderzoeker.

Dit is geen objectieve bezigheid. De mening van de onderzoeker komt hier aan te pas en het referentiekader van de betreffende onderzoeker kan ervoor zorgen dat de codering hiernaar gekleurd is. Dit is in dit onderzoek opgelost door de data en de coderingen te laten checken door een tweede onderzoeker.

Aanbevelingen

Uit de resultaten blijkt dat respondenten in bepaalde gevallen de vragen en cybercrimes uit de vragenlijsten van de Veiligheidsmonitor en Vragenlijst UT niet volledig begrijpen. Vooral met betrekking tot de onderwerpen identiteitsfraude, hacking en phishing zou een voorlichtingscampagne mogelijk positieve effecten teweeg kunnen brengen. Het is immers voor te stellen dat een individu dat meer kennis bezit over deze onderwerpen, minder snel slachtoffer zal worden. Aan de andere kant is het echter ook zo dat het CBS moet zorgen voor een Veiligheidsmonitor die door iedereen volledig te begrijpen is. Een Veiligheidsmonitor met duidelijke vragen en heldere begrippen. Hier is nog winst op te behalen.

Een interessant vervolgonderzoek zou het analyseren van de exacte oorzaken voor het verschil tussen het begrip van de respondent voor de verschillende cybercrimes kunnen zijn. Waarom wordt de ene cybercrime beter begrepen dan de andere?
Een tweede vervolgonderzoek zou het analyseren van de oorzaken voor de verschillen tussen beide delen van de vragenlijst kunnen zijn. Wat zijn de exacte oorzaken voor het feit dat de ene vragenlijst hoger scoort dan de andere, op het percentage respondenten dat de vragenlijst volledig begrijpt?

Tevens is het naar mijn idee verstandig verder onderzoek te doen naar hoe de hoeveelheid slachtofferschap van cybercrime het best gemeten kan worden. In de literatuur is nog erg weinig tot niets te vinden over:

- Welke methode het best gebruikt kan worden (testen van de apparaten van respondenten of toch een ‘ouderwetse’ vragenlijst?)
- Hoe een vragenlijst op het gebied van cybercrime door zoveel mogelijk respondenten volledig begrepen wordt

Het zoeken naar nieuwe methoden voor het meten van slachtofferschap is mijns inziens een belangrijk onderwerp van onderzoek. In een tijd waarin mensen steeds meer apparatuur gebruiken, is het mogelijk tijd voor een vernieuwing op het gebied van

slachtofferschaponderzoek. Het onderzoeken van de mogelijkheden voor het rapporteren van slachtofferschap via speciale apps is zeer de moeite waard. Een dergelijke vinding bespaart mankracht, tijd, en dus geld. Doordat de app op het apparaat van het slachtoffer is geïnstalleerd is het mogelijk om de app extra informatie te laten verzamelen door middel van bijvoorbeeld een scan. Uiteraard is dit momenteel nog toekomstmuziek. Maar in een tijd waarin de technologie zo snel vooruitsnelt, is het mogelijk tijd om de vragenlijst te vervangen voor een modernere vinding die zijn nut kan bewijzen in de nabije toekomst.

Tevens is het interessant de vragenlijst verder uit te breiden. Welke crimes worden nog meer gemist in de gebruikte vragenlijsten? Zijn er nog andere cybercrimes die vaak voorkomen in het dagelijks leven van de respondent?

Referenties

Babbie, Earl. (2012). *The practice of social research*: CengageBrain. com.

Brenner, Susan W. (2004). Cybercrime Metrics: Old Wine, New Bottles? *Va. JL & Tech., 9*, 13-13.

CBS. (2012). *Veiligheidsmonitor 2012*. Centraal Bureau voor de Statistiek i.s.m. Ministerie van Veiligheid en Justitie.

Childinfo. *Multiple-Indicator Survey Handbook: Conducting the fieldwork*.

CRIME, UNITED NATIONS OFFICE ON DRUGS AND. (2013). Comprehensice Study on Cybercrime.

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

Holt, Thomas J, & Bossler, Adam M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25.

Hulst, R.C. van der, & Neve, R.J.M. (2008). High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie *Onderzoek en Beleid*: Wetenschappelijk Onderzoek- en Documentatiecentrum.

Kindermann, Charles, Lynch, James, & Cantor, David. (1997). *Effects of the redesign on victimization estimates*: US Department of Justice, Bureau of Justice Statistics Washington, DC.

Krohn, Marvin D, Lizotte, Alan Jeffrey, & Hall, Gina Penly. (2009). *Handbook on crime and deviance*: Springer.

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime. Wenen.

Montoya Morales, AL, Junger, M, & Hartel, PH. (2013). How'Digital'is Traditional Crime?

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

Politie. (2014). Identiteitsfraude Retrieved 5 maart, 2014, from http://www.politie.nl/onderwerpen/identiteitsfraude.html

Ramesh, P, & Maheswari, D. (2012). *Survey of cyber crime activities and preventive measures.* Paper presented at the Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology.

Skogan, Wesley G. (1975). Measurement problems in official and survey crime rates. *Journal of Criminal Justice, 3*(1), 17-31.

Smith, Michael D. (1994). Enhancing the quality of survey data on violence against women: A feminist approach. *Gender & Society, 8*(1), 109-127.

Statistics, Bureau of Justice, Justice, US Dept of, & Programs, Office of Justice. (1989). Redesign of the National Crime Survey.

Taylor, Bruce M. (1989). *New directions for the national crime survey*: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Van Dijk, Jan JM, & Mayhew, Patricia. (1993). Criminal victimisation in the industrialised world: Key findings of the 1989 and 1992 international crime surveys. *Research Bulletin, 28*, 4-13.

Zhang, Yanping, Xiao, Yang, Ghaboosi, Kaveh, Zhang, Jingyuan, & Deng, Hongmei. (2012). A survey of cyber crimes. *Security and Communication Networks, 5*(4), 422-437.

Zhang, Yue, Egelman, Serge, Cranor, Lorrie, & Hong, Jason. (2006). *Phinding phish: Evaluating anti-phishing tools*.

Zhang, Yue, Hong, Jason I, & Cranor, Lorrie F. (2007). *Cantina: a content-based approach to detecting phishing web sites.* Paper presented at the Proceedings of the 16th international conference on World Wide Web.

I Bijlage 1
Vragenlijst onderzoek

Onderzoek cybercriminaliteit – Universiteit Twente

Versie 2 mei 2014

Goedendag meneer/mevrouw, ik ben Rick/Jennifer/Ilona en ik ben verbonden aan de Universiteit Twente/Hogeschool Arnhem-Nijmegen en het bureau Veiligheidsmonitor.

Wij doen onderzoek naar cybercrime. Zou ik u enkele vragen mogen stellen? Het onderzoek duurt ongeveer 15 minuten. U zou ons hier zeer mee helpen.

Mijn vragen aan u hebben betrekking op criminaliteit. In Nederland vindt er jaarlijks een onderzoek van het Centraal Bureau voor de Statistiek plaats naar slachtofferschap van misdaad. De vragenlijst die nu voor u ligt, geldt als aanvulling op dit onderzoek.

De vragenlijst bestaat uit 3 fases:
1) Ik leg u eerst enkele schriftelijke vragen voor.
2) Vervolgens zal ik heel kort doorvragen op hetgeen u ingevuld heeft.
3) Als laatste leg ik u nog enkele andere schriftelijke vragen voor.

Alle antwoorden die u geeft worden vertrouwelijk behandeld en zullen niet naar u terug te herleiden zijn.

Naam enquêteur: ……..

Geslacht:……..

Respondent-ID nummer: ……

Datum:……

Tijd:……

Plaats:…….

Deel I Schriftelijke vragen

Gebruik van apparatuur en internet

1a) Maakt u gebruik van de volgende apparaten, en kunt u aangeven of die een internetverbinding hebben? Kruis alstublieft het rondje aan dat bij uw keuze past.

Vaste computer	○ Ja	○ Ja, tevens met internet-verbinding	○ Nee
Laptop	○ Ja	○ Ja, tevens met internet-verbinding	○ Nee
Tablet (bijv. iPad)	○ Ja	○ Ja, tevens met internet-verbinding	○ Nee
Mobiele Telefoon	○ Ja	○ Ja, tevens met internet-verbinding	○ Nee

1b) In onderstaande tabel zou ik graag van u willen weten hoe vaak u elke activiteit op uw apparaat uitvoert. Zet alstublieft een kruis in het hokje dat het beste past bij de aantal keren dat u een activiteit uitvoert.

	Elke dag	4 tot 6 dagen **in de week**	1 tot 3 dagen **in de week**	Enkele keren **per maand**	Minder dan één keer **per maand**	Nooit
Het lezen en afhandelen van uw e-mail	5	4	3	2	1	0
Surfen op het internet (nieuwssites, YouTube, Uitzendinggemist.nl)	5	4	3	2	1	0
Het spelen van online games (World of Warcraft of andere spellen online)	5	4	3	2	1	0
Online gokken	5	4	3	2	1	0
Het bezoeken van social network sites (bijvoorbeeld facebook, Twitter, Google+, Myspace, LinkedIn)	5	4	3	2	1	0
Online bankieren	5	4	3	2	1	0
Online kopen of verkopen (bijv. op Marktplaats of eBay)	5	4	3	2	1	0
Het online kopen bij webwinkels (bol.com, Zalando, Booking.com)	5	4	3	2	1	0
Downloaden van muziek, films of computerspellen	5	4	3	2	1	0

Hier volgen enkele vragen met betrekking tot cybercrime:

11 | IDENTITEITSFRAUDE

11a **Allereerst identiteitsfraude. Hierbij wordt zonder toestemming gebruik gemaakt van iemand zijn/haar persoonlijke gegevens voor financieel gewin, bijv. voor het opnemen of overmaken van geld, het afsluiten van leningen of het opvragen van officiële documenten. Daders kunnen op verschillende manieren aan de persoonlijke gegevens zijn gekomen, bijv. door het onderscheppen van de post, het kopiëren van bankpasgegevens bij een pinautomaat of via het internet.**

Is dit u zelf of iemand anders in uw huishouden in de afgelopen 12 MAANDEN wel eens overkomen?

- ☐ Ja
- ☐ Nee ..... ga verder naar vraag **12a** pagina 27

11b **Hoe vaak gebeurde dit in totaal in de afgelopen 12 maanden?**

☐ 1 keer ☐ 2 keer ☐ 3 keer ☐ 4 keer ☐ 5 keer of vaker

De volgende vragen gaan alleen over de LAATSTE keer dat dit gebeurde.

11c **Is dit de laatste keer u zelf overkomen, iemand anders in uw huishouden of beide?**
Bij beide kunt u bijv. denken aan gekopieerde bankpasgegevens van een gezamenlijke rekening of een gehackte computer waarbij van meerdere personen gegevens zijn ontvreemd.

- ☐ Zelf
- ☐ Iemand anders in huishouden
- ☐ Beide: zowel zelf als iemand anders in huishouden

12 | KOOP- EN VERKOOPFRAUDE

12a **Bent u zelf of iemand anders in uw huishouden in de afgelopen 12 MAANDEN bij het kopen of verkopen van goederen of diensten wel eens opgelicht, bijv. doordat gekochte goederen niet geleverd werden of niet betaald werd voor geleverde diensten?**

- ☐ Ja
- ☐ Nee ..... ga verder naar vraag **13a** pagina 29

12b **Hoe vaak gebeurde dit in totaal in de afgelopen 12 maanden?**

☐ 1 keer ☐ 2 keer ☐ 3 keer ☐ 4 keer ☐ 5 keer of vaker

De volgende vragen gaan alleen over de LAATSTE keer dat dit gebeurde.

12c **Is dit de laatste keer u zelf overkomen, iemand anders in uw huishouden of beide?**
Bij beide kunt u bijv. denken aan gezamenlijke aan- of verkopen.

- ☐ Zelf
- ☐ Iemand anders in het huishouden ..... ga verder naar vraag **13a** pagina 29
- ☐ Beide: zowel zelf als iemand anders in het huishouden

13 | HACKEN

13a **Is het in de afgelopen 12 MAANDEN wel eens voorgekomen dat iemand met kwade bedoelingen heeft ingebroken of ingelogd op een computer, emailaccount, website of profielsite (bijv. hyves, facebook, twitter) van uzelf of iemand anders in uw huishouden?**

- ☐ Ja
- ☐ Nee ..... ga verder naar vraag **14a** pagina 31

13b **Hoe vaak gebeurde dit in totaal in de afgelopen 12 maanden?**

☐ 1 keer ☐ 2 keer ☐ 3 keer ☐ 4 keer ☐ 5 keer of vaker

De volgende vragen gaan alleen over de LAATSTE keer dat dit gebeurde.

13c **Is dit de laatste keer u zelf overkomen, iemand anders in uw huishouden of beide?**
Bij beide kunt u bijv. denken aan een computer die door meerdere personen in het huishouden werd gebruikt of een gezamenlijk emailaccount.

- ☐ Zelf
- ☐ Iemand anders in huishouden ..... ga verder naar vraag **14a** pagina 31
- ☐ Beide: zowel zelf als iemand anders in huishouden

-

14 | CYBERPESTEN

14a **Heeft u ZELF in de afgelopen 12 MAANDEN via internet wel eens te maken gehad met roddel, getreiter, pesten, stalken, chantage of bedreiging?**
Let op: het gaat hierbij alleen om uzelf, niet om iemand anders in uw huishouden!

- ☐ Ja
- ☐ Nee ..... ga verder naar blok **5** pagina 33

14b **Hoe vaak gebeurde dit in totaal in de afgelopen 12 maanden?**

☐ 1 keer ☐ 2 keer ☐ 3 keer ☐ 4 keer ☐ 5 keer of vaker

De volgende vragen gaan alleen over de LAATSTE keer dat dit gebeurde.

DEEL II
HET VOLGENDE DEEL WORDT INGEVULD DOOR DE INTERVIEWER

- Precies plaatsgevonden – voor elk genoemd incident:
- schrijf de naam v.h. ''delict'' op + het verhaal/de uitleg

……

……

……

……

……

……

……

……

……

……

……

……

……

……

……

Deel III Schriftelijke vragen

Vervolgens vraag ik u te vergeten dat u al eerder een lijst heeft ingevuld.
Nu volgen opnieuw enkele schriftelijke vragen. Het de bedoeling dat u zo precies mogelijk de vragen beantwoordt, *ook al had u sommige zaken al eerder gemeld.*

1) Phishing

Bij phishing wordt u door middel van frauduleuze e-mails en/of websites verleid tot het geven van uw bankrekeningnummers, wachtwoorden en andere persoonlijke informatie aan de dader.
- Deze e-mails en websites lijken vaak afkomstig van betrouwbare organisaties, zoals bijvoorbeeld uw bank of uw werk, maar zijn dit niet.
- Het plegen van phishing aanvallen is een misdrijf, ook wanneer de dader(s) familieleden, vrienden of op een andere manier bekenden van u zijn.

1 A) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens gevraagd naar de inloggegevens van uw ONLINE BANKREKENINGACCOUNT?

- Ja
- Nee (Ga naar vraag 1B)
- Ik heb geen online bankrekening account (Ga naar vraag 1B)
- Weet niet (Ga naar vraag 1B)

Hoe vaak hebt u dergelijke vragen in de afgelopen 12 maanden ontvangen?

Vul in: ……

Hebt u de gevraagde gegevens, in één of meerdere gevallen, verstrekt?

- Ja, vul in: hoe vaak……
- Nee
- Weet niet

1 B) Heeft u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens een e-mail gekregen die van uw bank leek, en waarin u gevraagd werd op een link te klikken, om vervolgens in te loggen met uw wachtwoord?

- Ja
- Nee (Ga naar vraag 1C)
- Ik heb geen online bankrekening account (Ga naar vraag 1C)
- Weet niet (Ga naar vraag 1C)

Hoe vaak hebt u dergelijke e-mails in de afgelopen 12 maanden ontvangen?

Vul in: ……

Hebt u de gevraagde gegevens, in één of meerdere gevallen, verstrekt?

- Ja, vul in: hoe vaak……
- Nee
- Weet niet

1 C) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens gevraagd naar de inloggegevens van uw SOCIAL NETWORK ACCOUNT (bijvoorbeeld Facebook, Twitter, MySpace of Google+)?

- Ja
- Nee (Ga naar vraag 1D)
- Ik heb geen Social Network account (Ga naar vraag 1D)
- Weet niet (Ga naar vraag 1D)

Hoe vaak hebt u dergelijke vragen in de afgelopen 12 maanden ontvangen?

Vul in: ……

Hebt u de gevraagde gegevens, in één of meerdere gevallen, verstrekt?

- Ja, vul in: hoe vaak……
- Nee
- Weet niet

1 D) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens gevraagd naar de inloggegevens van uw ONLINE GAMING ACCOUNT? Met online gaming bedoel ik alle spelletjes die u op internet speelt, zoals World of Warcraft, Runescape of Habbohotel.

- Ja
- Nee (Ga naar vraag 1E)
- Ik heb geen online gaming account (Ga naar vraag 1E)
- Weet niet (Ga naar vraag 1E)

Hoe vaak hebt u dergelijke vragen in de afgelopen 12 maanden ontvangen?

Vul in: ……

Hebt u de gevraagde gegevens, in één of meerdere gevallen, verstrekt?

- Ja, vul in: hoe vaak……
- Nee
- Weet niet

1 E) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens gevraagd naar de inloggegevens van uw ACCOUNT OP HET NETWERK VAN UW WERK OF SCHOOL?

- Ja
- Nee
- Ik heb geen werk- of schoolaccount
- Weet niet

Hoe vaak hebt u dergelijke vragen in de afgelopen 12 maanden ontvangen?

Vul in: ……

Hebt u de gevraagde gegevens, in één of meerdere gevallen, verstrekt?

- Ja, vul in: hoe vaak……
- Nee
- Weet niet

Vraag 1F en 1G vult u in als u hierboven **'ja'** hebt geantwoord op één van de vragen. Indien u dergelijke vragen naar persoonlijke gegevens **geen** enkele keer hebt ontvangen kunt u doorgaan naar **vraag 2**.

1 F) Kunt u nog wat toelichting geven over de incidenten die u hierboven heeft vermeld? U kunt dan bijvoorbeeld denken aan de manier waarop er werd gevraagd naar uw gegevens?

……

……

……

……

……

……

1 G) Indien u uw gegevens heeft verstrekt, heeft dat merkbare gevolgen gehad? U kunt dan bijvoorbeeld denken aan

- **het plotseling verdwijnen van geld van uw bankrekening of creditcard**
- **vrienden of familie die klagen over rare mailtjes die ze van u zouden hebben ontvangen**
- **of andere zaken die mogelijk terug te herleiden zijn naar het feit dat u uw persoonlijke gegevens hebt verstrekt.**

Omschrijft u alstublieft zo uitgebreid mogelijk welke gevolgen het verstrekken van de gegevens heeft gehad.

……

……

……

……

……

……

……

……

2) Online oplichting met financiële schade

Er zijn meerdere manieren te bedenken waarop iemand u via het internet of e-mail geld of goederen afhandig kan maken. Hieronder noem ik een aantal situaties waarop u 'ja' kunt antwoorden wanneer deze situatie op u van toepassing is. Noemt u ook alle kleine dingen die u mogelijk onbelangrijk zou kunnen vinden.

2 A) Bent u in de afgelopen 12 maanden wel eens GELD OF GOEDEREN KWIJTGERAAKT doordat iemand u met een bepaalde truc of 'slimmigheid' via het internet of e-mail heeft opgelicht?

- o Ja
- o Nee (Ga naar vraag 2B)
- o Weet ik niet (Ga naar vraag 2B)

Zo ja, hoe vaak is dit u in de afgelopen 12 maanden overkomen?

Vul in: ……

Wat is er toen precies gebeurd en welk trucje hebben de daders gebruikt om u op te lichten? Licht alstublieft zo uitgebreid mogelijk toe wat er gebeurd is.

.....

……

……

……

2 B) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, wel eens op een andere manier GELD OF GOEDEREN KWIJTGERAAKT OP HET INTERNET?

- Ja
- Nee (Ga naar vraag 3A)
- Weet ik niet (Ga naar vraag 3A)

Zo ja, hoe vaak is dit u in de afgelopen 12 maanden overkomen?

Vul in: ……

Wat is er toen precies gebeurd en hoe komt het dat u geld op het internet bent kwijtgeraakt? Licht alstublieft zo uitgebreid mogelijk toe wat er gebeurd is.

.....

……

……

……

3) ONLINE BEDREIGING

In het geval van online bedreiging wordt het slachtoffer bedreigd via de digitale weg, bijvoorbeeld via internet, e-mail of mobiele telefoon. Het bedreigen via de digitale weg komt vaak voor, en is helaas niet ongewoon.
Bedreiging is een misdrijf, ook wanneer de dader(s) familieleden, vrienden of op een andere manier bekenden van u zijn.

3 A) Bent u in de afgelopen 12 maanden, dus na mei/juni 2013, via de digitale weg bedreigd?

- o Ja
- o Nee (Ga naar vraag 4A)
- o Weet ik niet (Ga naar vraag 4A)

Zo ja, hoe vaak is dit u in de afgelopen 12 maanden overkomen? (Als u het niet heel precies weet: Geef een schatting)

Vul in: ……

Hoe heeft de online bedreiging plaatsgevonden?

a) Social media (Facebook, Twitter, Google+),	o Ja	o Nee
b) Chatboxen	o Ja	o Nee
c) Skype	o Ja	o Nee
d) Internetberichten, bijvoorbeeld op forums	o Ja	o Nee
e) SMS	o Ja	o Nee
f) Whatsapp	o Ja	o Nee
g) E-mail.	o Ja	o Nee

h) Anders, namelijk.....

Wat is uw relatie met de dader? vul in: ……

4) Nog iets anders vervelends meegemaakt op internet/via email/ …?

4 A) Heeft nog IETS ANDERS MEEGEMAAKT in dezelfde trant, bijv. slechte ervaringen op internet of diefstal van uw gegevens o.i.d. tijdens de afgelopen 12 maanden?

……
……

4 B) Is een van de apparaten waarmee u online bent wel eens GESTOLEN of bent u het KWIJTGERAAKT tijdens de afgelopen 12 maanden?

Gestolen:	**1** Vaste computer	**2** Laptop	**3** Tablet (bijv. iPad)	**4** Mobiele Telefoon	**5** anders
Kwijtgeraakt	**1** Vaste computer	**2** Laptop	**3** Tablet (bijv. iPad)	**4** Mobiele Telefoon	**5** anders

4 C) Heeft u hier gevolgen van ondervonden (behalve de diefstal zelf)?
……
……
……

5) Deelnemers onderzoek

Tevens zou ik u graag nog enkele algemene vragen willen stellen:

5 A) Wat is uw leeftijd? ……..

5 B) Voert u betaald werk uit? Wat voor werk?

……

5 C) Wat is uw hoogst genoten opleiding?

		Afgerond	Mee bezig
a	Basis onderwijs – lager onderwijs	○ Ja	○ Ja
b	VMBO – mavo	○ Ja	○ Ja
c	MBO	○ Ja	○ Ja
d	HAVO	○ Ja	○ Ja
e	HBO	○ Ja	○ Ja
f	VWO	○ Ja	○ Ja
g	Universiteit	○ Ja	○ Ja

h) Anders, namelijk.....

5 D) Wat voor werk doet u?

a	Fulltime werk	○ Ja
b	Parttime werk	○ Ja
c	Werkzoekende (werkloos)	○ Ja
d	Huisvrouw/huisman	○ Ja
e	Gepensioneerd	○ Ja
f	Ziektewet	○ Ja
g	Student	○ Ja

h) Anders, namelijk.....

Dit is het einde van de vragenlijst. Hebt u nog opmerkingen die u kwijt wilt of vragen die u wilt stellen?

Hartelijk dank voor het invullen.

II Bijlage 2 – Analyse antwoorden op CBS-vragen

In tabel 10 ziet u allereerst het respondentnummer dat tijdens het interview door de interviewers is genoteerd. Vervolgens wordt de score vermeld die aangeeft in hoeverre de respondent de vragen lijkt te begrijpen. De uitleg van de respondent komt hier na. Welke cybercrime heeft hij of zij gerapporteerd, en hoe legt de respondent uit wat hem of haar precies overkomen is? Vervolgens wordt er vermeld hoe de onderzoeker tot de score (0, 1 of 2) is gekomen.

In de zesde kolom van de tabel (genaamd ‘Daadwerkelijk’) wordt weergegeven van welke crime het slachtoffer daadwerkelijk slachtoffer is geworden. Indien de respondent een andere crime rapporteert, dan hij of zij beschreven heeft, welke cybercrime beschrijft de respondent dan?

Tabel 11 - Scoringstabel over het begrip van de respondent met betrekking tot cybercrime vragen uit de Veiligheidsmonitor

Respondent	Crime	Score	Verhaal	Uitleg score	Daad-werkelijk
130501110	A. ID-fraude	2	ID-FRAUDE/HACKING: Mevrouw zegt dat het een combinatie is van ID-fraude en hacking. Haar echtgenoot zag in de website van ABN AMRO een derde edentifier. Echtgenoot heeft toen de bank gebeld. Mevrouw heeft verder geen verdere uitleg of info en snapt het zelf ook niet volledig. Wel weet ze dat als echtgenoot erop geklikt zou hebben en door was gegaan, ze geld kwijt waren geraakt. Er zat(quote): "Een film over alle gegevens van de echtgenoot". Gelukkig op tijd onderschept.	Op het gebied van identiteitsfraude krijgt deze respondent een score 2. De respondent lijkt correct gerapporteerd te hebben in overeenstemming met de definitie. Er werd immers zonder toestemming gebruik gemaakt van persoonlijke gegevens (waarschijnlijk wachtwoorden) voor financieel gewin. Er werd een poging gedaan om de identiteit van de respondent, op het gebied van bankzaken aan te nemen. Ondanks dat het hier een poging betreft, gaan we hier toch uit van een score 2 omdat de respondent de identiteitsfraude goed heeft herkend.	Identiteits-fraude
510000311	A. ID-fraude	1	ID-FRAUDE: Anouk (de zangeres) had een foto geplaatst van het vriendinnetje van de respondent met een discriminerende tekst tegenover negers erbij. Dit inzake de zwarte pietendiscussie. Naam van vriendinnetje is niet gebruikt, enkel de foto. (Schijnt op RTV oost site te staan - Niet gevonden - RV).	Met betrekking tot de ID-fraude krijgt deze respondent score 1. De respondent lijkt gedeeltelijk correct gerapporteerd te hebben. Er is zonder toestemming gebruikt van de identiteit van een persoon. In dit geval gaat het echter enkel om de foto en niet om daadwerkelijke persoonsgegevens of identiteitspapieren. Daarbij komt nog eens dat er in dit geval geen aanwijzingen zijn voor een financieel motief. Er is dus gedeeltelijk aan de definitie van identiteitsfraude voldaan, , maar waarschijnlijker is het dat er sprake is van cyberpesten.	Cyberpesten
560000311	A. ID-fraude	1	ID-FRAUDE: Mail gekregen dat iemand vanuit het buitenland gmail account probeerde binnen te komen. wachtwoord veranderd en verder niks aan de hand	De respondent krijgt in dit geval score 1. Om het account binnen te komen is het wachtwoord van de respondent nodig. Op zich is het voor te stellen dat de respondent denkt dat iemand die een account binnen probeert te komen, zich voordoet als de eigenaar van het account. Toch heeft de respondent de vraag niet goed begrepen. Er is hier geen gebruik gemaakt van gestolen of vervalste identiteitspapieren en er zijn ook geen aanwijzingen om aan te nemen dat er een poging is gedaan met financieel motief. Aan de andere kant worden de naam en de identiteit van de eigenaar van het account (de respondent in kwestie) wel misbruikt. Een gedeeltelijk correcte rapportage dus. Hacking is echter aannemelijker	Combi van Identiteits-Fraude en hacking
580000311	A. ID-fraude	2	ID-FRAUDE: e-mails van Blizzard dat World of warcraft account niet online verkocht mocht worden. Anders zou het account geblokkeerd worden. Respondent speelt zelf echter geen World of warcraft	De respondent krijgt in dit geval score 2. Blizzard heeft in dit geval blijkbaar informatie ontvangen dat er een account werd verkocht door een individu die de naam van de respondent gebruikt. In zekere zin is er dus zeker sprake van het gebruik van persoonsgegevens zonder toestemming en, in dit geval ook, voor financieel gewin. Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude

670000311	A. ID-fraude	2	ID-FRAUDE: Er was opeens 190 euro van de creditcard van de respondent afgeschreven. De respondent heeft deze betaling zelf niet uitgevoerd. Het geld is vergoed door de bank. De betaling was uitgevoerd bij een wielrenzaak die de respondent niet kent. Respondent heeft een nieuwe creditcard gekregen	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van identiteitsfraude gerapporteerd. Er is immers zonder toestemming gebruik gemaakt van (gestolen of vervalste) persoonsgegevens van de respondent (bankgegevens) voor, in dit geval, financieel gewin. De naam en identiteit zijn gebruikt voor het plegen van strafbare feiten. . Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude
680000311	A. ID-fraude	2	ID-FRAUDE - Respondent had het huis van een meisje overgenomen en was ook voornemens het Ziggo contract over te nemen. Bij het Ziggo contract zat echter ook een gratis IPad. De vorige bewoner wou deze echter niet afstaan. Respondent vond dit prima maar wou dan wel gecompenseerd worden voor de IPad, als hij zelf een abonnement afsloot zou deze er immers wel bij zitten en nu bij overname van het abonnement van de vorige bewoner niet. Er werd echter geen compensatie aanbod gedaan en de overname ging niet door. Vorige bewoner van het huis had echter toch Ziggo gebeld om overname van contract door te geven, echter zonder medeweten van de respondent. Vorige bewoner kreeg het echter toch voor elkaar om rekeningnummer en naam op haar Ziggo contract te wijzigen naar dat van de respondent.	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van identiteitsfraude gerapporteerd. Er is immers zonder toestemming gebruik gemaakt van (gestolen of vervalste) persoonsgegevens van de respondent (naam en rekeningnummer) voor, in dit geval, financieel gewin. De naam en identiteit zijn gebruikt voor financieel gewin zonder toestemming van de respondent. Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude
40002420	A. ID-fraude	1	ID-FRAUDE: Wordt regelmatig gebeld over het invullen van een enquête, via deze telefoongesprekken wordt weer reclame aangeboden en gezegd dat mevrouw van alles gewonnen heeft. Mevrouw zegt deze enquête nooit te hebben ingevuld	Deze respondent krijgt score 1. Op zich komt hetgeen dat de respondent zegt geheel overeen met de definitie van identiteitsfraude van het CBS. Er wordt hier immers gebruik gemaakt van de persoonlijke gegevens van de respondent voor financieel gewin. De omschrijving van de respondent komt echter niet overeen met de omvangrijkere definitie van de politie. Hoewel de respondent de omschrijving van het CBS goed heeft begrepen, denk ik toch dat er hier geen sprake is van identiteitsfraude. De kans dat dergelijke aanbiedingen een gevolg zijn van identiteitsfraude is onwaarschijnlijk. De kans is groter dat er hier sprake is van een vorm van fraude via de telefoon.	Mogelijk Telefoonfraude
180005521	A. ID-fraude	-	ID-FRAUDE/CYBERPESTEN: Bankpas fraude, praat er liever niet over.	Zonder verdere uitleg is het lastig een score te bepalen. Op zich is het niet onmogelijk dat bankpasfraude onder Id-fraude past. Bij skimming wordt er bijvoorbeeld gebruik gemaakt van een kopiepas en een afgekeken pincode. Persoonlijke gegevens die worden gebruikt voor financieel gewin. De overeenkomst met cyberpesten is niet duidelijk.	-
310005521	A. ID-fraude	1	ID-FRAUDE/HACKING: Moeder kreeg een brief per post binnen dat er een account aangemaakt was met haar gegevens.	Op het gebied van ID-fraude krijgt deze respondent een 1. Er is immers zonder toestemming gebruik gemaakt van de persoonlijke gegevens van de moeder. Het is echter niet duidelijk of er ook financieel gewin in het spel was, of dat de gegevens gebruikt zouden worden voor het plegen van strafbare feiten.	Identiteits-fraude

490007420	A. ID-fraude	2	ID-FRAUDE/HACKING: Partner heeft inloggegevens ingevoerd na ontvangen van phishing mail. Na 1 dag achter gekomen dat dit van een andere afzender kwam. Bank op de hoogte gesteld, codes account veranderd en aangifte gedaan. Ook mails ontvangen vanuit eigen mailaccount waarin advertenties stonden ondertekend met eigen naam. wachtwoord mailaccount veranderd daarna niet meer voorgekomen.	De respondent krijgt een 2 aangezien meneer de identiteitsfraude goed heeft herkend. In de basis is er hier sprake van een phishing mail waar de echtgenote op in is gegaan. De gevolgen hiervan, zoals het versturen van mails onder de identiteit van de respondent zijn te aan te merken als identiteitsfraude. Dit gezien het feit dat er zonder toestemming gebruik wordt gemaakt van de persoonlijke gegevens van de respondent. in dit geval echter ook weer zonder financieel motief, althans, dat lijkt in eerste instantie het geval.	Identiteits-fraude
70000431	A. ID-fraude	2	ID-FRAUDE: Mijn creditcard gegeven gebruikt om producten te kopen. Deze had ik ingevuld voor onlinepokeren	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van identiteitsfraude gerapporteerd. Er is immers zonder toestemming gebruik gemaakt van (gestolen of vervalste) persoonsgegevens van de respondent (creditcardnummer) voor, in dit geval, financieel gewin. De naam en identiteit zijn gebruikt voor financieel gewin zonder toestemming van de respondent. Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude
100000431	A. ID-fraude	2	ID-FRAUDE: Nadat ik geld had opgenomen bij geldautomaat is mijn rekening helemaal leeg getrokken. Politie zei dat dit vaker voorkwam de laatste tijd. Blijkbaar was er een apparaatje op de pinautomaat die mijn rekening en pincode onthield en zo konden ze hem leeg trekken.	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van identiteitsfraude gerapporteerd. In dit geval is de respondent slachtoffer van skimming en dit kan resulteren in identiteitsfraude. Er is immers zonder toestemming gebruik gemaakt van (door middel van skimming gestolen) persoonsgegevens van de respondent (rekeningnummer en pincode) voor, in dit geval, financieel gewin. Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude
120000431	A. ID-fraude	0	ID-FRAUDE: mail van bank met de vraag of ik wilde inloggen terwijl de bank hier nooit om vraagt.	Deze respondent krijgt score 0. Hier is duidelijk sprake van phishing. Op geen enkele wijze komt de beschrijving van de respondent overeen met de definitie van identiteitsfraude, behalve wanneer de respondent bedoelt dat de identiteit van de bank vervalst wordt. Hier is geen zekerheid over.	Phishing
430008430	A. ID-fraude	2	ID-FRAUDE: Creditcard gegevens zijn gebruikt in een hotel waar ik nooit ben geweest. Ik was hier natuurlijk voor verzekerd waardoor ik werd gebeld omdat er ineens hele hoge bedragen vanuit het buitenland werden geboekt. Geen idee hoe ze aan mijn gegevens zijn gekomen.	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van identiteitsfraude gerapporteerd. Er is immers zonder toestemming gebruik gemaakt van (gestolen of vervalste) persoonsgegevens van de respondent (creditcardgegevens) voor, in dit geval, financieel gewin. Er is hier dus inderdaad sprake van identiteitsfraude volgens de definitie. Het lijkt erop dat de respondent de vraag goed begrepen, de kenmerken van identiteitsfraude heeft waargenomen en begrepen, en hier vervolgens naar heeft gerapporteerd.	Identiteits-fraude
100000311	B. Koop-Verkoopfraude	2	KOOP-VERKOOP: Computerspel gekocht. Zou er extra collectors-software bij krijgen. Echter niet ontvangen. Spel heette Elder Scrolls Online.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude

410000311	B. Koop-verkoopfraude	2	KOOP- VERKOOP: Spelletje via Marktplaats niet geleverd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
460000311	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Vader van respondent wou kaartjes bestellen voor een concert van André Rieu aangezien dit goedkoper was dan via de normale kanalen. Kaarten zijn nooit aangekomen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
500000311	B. Koop-verkoopfraude	2	KOOP VERKOOP: 1 euro dingetje (UV filter) dat nooit is aangekomen. Besteld via eBay	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
750000311	B. Koop-verkoopfraude	2	KOOP-VERKOOP: broertje van de respondent had via marktplaats een Wii gekocht. Deze is betaald, maar is nooit aangekomen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
110003721	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Via marktplaas.nl een paar schoenen gekocht van een particuliere verkoper, waarde 30 euro. Nooit geleverd, daarna ook geen contact meer gekregen met verkoper.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
290005521	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Vader via marktplaats een tv. van 1000+ euro gekocht bij een particulier, deze is nooit geleverd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
340005521	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Via marktplaas.nl een buitenkachel gekocht van een particuliere verkoper, waarde 200 euro. Nooit geleverd, daarna ook geen contact meer gekregen met verkoper.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
440006420	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Via markplaats.nl een tas gekocht van een particuliere verkoper, waarde 30 euro. Tas nooit ontvangen, geprobeerd contact te zoeken met verkoper maar niet meer gelukt. Klacht ingediend bij Marktplaats	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
80000431	B. Koop-verkoopfraude	2	KOOP-VERKOOP: Via marktplaats iets opgestuurd maar nooit geld ontvangen. Ik kon de koper op geen enkele manier meer bereiken.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
390682430	B. Koop-verkoopfraude	2	KOOP-VERKOOP: kaartje gekocht via het internet (marktplaats) en persoon wilde pas kaartje mailen als ik bewijs had dat ik had betaald. Ik heb het geld overgeschreven maar daarna nooit het kaartje gehad en contact hield direct op.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de koop- verkoopfraude klopt geheel met de definitie. Er is immers iets gekocht wat niet geleverd is door de leverancier.	Koop-verkoop fraude
620000431	B. Koop-verkoopfraude	0	KOOP-VERKOOPFRAUDE: Ik wilde huurtoeslag aanvragen en vond via Google een site die dit regelde tegen een kleine betaling. Ik heb dit ingevuld en ontdekte een paar minuten later dat je dit zelf kunt doen en dit helemaal geen geld kost dan. Ik heb meteen op de mail gereageerd en de aanvraag geannuleerd. Het geld heb ik toen terug gekregen	In dit geval krijgt de respondent score 0. Er is hier geen sprake van fraude. de respondent deed zelf de bestelling en het bedrijf was voornemens de service te leveren. De respondent heeft de aangeboden service echter zelf afbesteld en besloten de huurtoeslag zelf aan te vragen, in plaats van te kiezen voor uitbesteding. Aangezien het geld netjes is teruggeven, is er geen sprake van fraude.	Geen Cybercrime plaatsgevonden

130501110	C. Hacking	1	ID-FRAUDE/HACKING: Mevrouw zegt dat het een combinatie is van ID-fraude en hacking. Haar echtgenoot zag in de website van ABN AMRO een derde edentifier. Echtgenoot heeft toen de bank gebeld. Mevrouw heeft verder geen verdere uitleg of info en snapt het zelf ook niet volledig. Wel weet ze dat als echtgenoot erop geklikt zou hebben en door was gegaan, ze geld kwijt waren geraakt. Er zat(quote): "Een film over alle gegevens van de echtgenoot". Gelukkig op tijd onderschept.	Op het gebied van hacking krijgt deze respondent score 1. De respondent lijkt gedeeltelijk correct gerapporteerd te hebben. Er zijn in dit geval inderdaad persoonlijk gegevens gebruikt voor financieel gewin. De cybercriminelen hebben immers (gedeeltelijke) toegang gehad tot de bankrekening van de echtgenoot van de respondent. Het probleem bestaat echter uit de manier waarop de gegevens verkregen zijn. De respondent rapporteert hacking, maar geeft tegelijk aan niet helemaal te snappen wat er precies heeft plaatsgevonden. De mogelijkheid dat de persoonlijke gegevens niet door hacking zijn verkregen, maar door bijvoorbeeld ‘niet-opgemerkte’ phishing mails, mag daarom niet worden uitgesloten. De kans is dus aanwezig dat er in dit geval een vorm van hacking is gerapporteerd die in werkelijkheid niet heeft plaatsgevonden. Onderzoek van de computer van de respondent geeft mogelijk uitsluitsel, maar dit maakt geen deel uit van de schriftelijke vragenlijst.	Niet zeker/ Niet te bepalen
340659110	C. Hacking	2	HACKING: Facebook: Broer van de respondent was in India. Kon niet inloggen op Facebook. Kreeg een mail van Facebook om verificatie van identiteit. Er bleek namelijk dat er iemand vanuit Estland op het account van de broer van de respondent probeerde in te loggen. Hotmail: dezelfde broer van de respondent kon niet meer inloggen op Hotmail. Reden onbekend. Door twee stappen verificatie (schijnt via mobiele telefoon te gebeuren) kon de respondent alweer inloggen.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben, in overeenstemming met de definitie. Dit ondanks het feit dat het hier een poging tot hacking betreft in plaats van een daadwerkelijk ‘ongeoorloofd binnendringen of inbreken’.	Hacking
440000311	C. Hacking	2	HACKING: kreeg mail dat Google account mogelijk gehackt was. Dit omdat telefoonnummer van Google account veranderd scheen te zijn toen de respondent Facebook op de mobiel had gedownload. Verder geen zekerheid. Respondent snapt het zelf ook niet helemaal	Deze respondent krijgt score 2. De respondent lijkt gedeeltelijk in eerste instantie enkel gedeeltelijk overeenstemming met de definitie gerapporteerd te hebben. Er kunnen immers verschillende redenen zijn die een verandering van telefoonnummer op Facebook. Er hoeft niet per se sprake te zijn van hacking. Dit is de respondent echter niet aan te rekenen. De respondent rapporteert immers exact wat de mail van Google hem of haar mededeelde. De respondent herkende het begrip en de omschrijving van hacking dus goed en rapporteerde in overeenstemming met wat Google hem of haar verteld heeft.	Hacking
490000311	C. Hacking	2	HACKING: Virus op computer van een huisgenoot dat alle informatie van de computer had afgehaald. Huisgenoot van de respondent heeft vervolgens alle wachtwoorden moeten wijzigen uit veiligheid	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben, in overeenstemming met de definitie. Er heeft in dit geval namelijk daadwerkelijk iemand ‘ongeoorloofd binnengedrongen en ingebroken’. Dit met kwade bedoelingen, aangezien alle bestanden verwijderd zijn.	Hacking
510000311	C. Hacking	2	HACKING: "vriendinnen" van zusje van de respondent hebben geprobeerd in te breken op het Facebook account van het zusje.	Op het gebied van hacking krijgt deze respondent een score 2. Er is geheel in overeenstemming gerapporteerd. Ondanks het feit dat het enkel een poging betreft, is er toch sprake van het binnendringen in, of het inbreken in, een computersysteem zonder toestemming van de eigenaar.	Hacking
650000311	C. Hacking	2	HACKING: E-mail van Facebook, "je probeerde in te loggen van uit de Emiraten. Klopt dit?". Indien dit niet het geval is moest de respondent extra maatregelen nemen , zoals het instellen van extra veiligheidsvragen.	De respondent krijgt in dit geval score 2. Er is geheel in overeenstemming met de definitie van hacking gerapporteerd. Ondanks het feit dat het enkel een poging betreft, is er toch sprake van het binnendringen in, of het inbreken in, een computersysteem zonder toestemming van de eigenaar.	Hacking

740000311	C. Hacking	2	HACKING: respondent kwam op website die er grimmig uitzag. Respondent bekeek toen de bronpagina. Toen bleek dat een Javascript bovenaan de pagina een plug in installeerde. Deze plug in bleek de door de respondent bezochte websites door te sturen naar een derde partij voor marketing doeleinden. Virusscanner gebruikt en alleen Bitdefender kreeg het voor elkaar om de plug in te verwijderen	De respondent krijgt in dit geval score 2. Het is echter niet geheel duidelijk of er ook iemand is binnengedrongen in, of heeft ingebroken in, de computer van de respondent. Toch is aan te nemen dat het plaatsen van bestanden (plug in) op de computer ook aan te merken is als binnendringen, en dus hacking. Uiteraard enkel als dit zonder toestemming gebeurt. Er is dus geheel in overeenstemming met de definitie van hacking gerapporteerd.	Hacking
60002420	C. Hacking	0	HACKING: Mails van "nep" bank vragen naar gegevens. Niets mee gedaan	Deze respondent krijgt score 0. Hier is duidelijk sprake van phishing. Op geen enkele wijze komt de beschrijving van de respondent overeen met de definitie van hacking. Er is namelijk niet binnengedrongen in de computer.	Phishing
260005521	C. Hacking	2	HACKING: Game account gehackt door email waarin naar inloggegevens werd gevraagd.	Deze respondent krijgt score 2. Het is immers mogelijk dat het game account gehackt werd nadat de respondent per ongeluk reageerde op een phishing mail. Indien het account daarna, door middel van de verkregen gegevens gehackt werd, heeft de respondent de vraag goed begrepen en correct gerapporteerd	Phishing
490007420	C. Hacking	2	ID-FRAUDE/HACKING: Respondent rapporteert zowel identiteitsfraude als hacking. Partner heeft inloggegevens ingevoerd na ontvangen van phishing mail. Na 1 dag achter gekomen dat dit van een andere afzender kwam. Bank op de hoogte gesteld, codes account veranderd en aangifte gedaan. Ook mails ontvangen vanuit eigen mailaccount waarin advertenties stonden ondertekend met eigen naam. wachtwoord mailaccount veranderd daarna niet meer voorgekomen.	Hacking heeft er in dit geval mee te maken dat de daders, zonder toestemming, zijn binnengedrongen in het email account van de respondent. ook dit is goed herkend door de respondent. dus ook met betrekking tot hacking een score 2.	Hacking
540007420	C. Hacking	2	HACKING: Partner kreeg mails vanuit eigen account toegestuurd met reclame advertenties	Respondent krijgt score 2. Er is in dit geval zonder toestemming van de gebruiker ingebroken of binnengedrongen in het mailaccount van de respondent	Hacking
580008420	C. Hacking	2	HACKING: Vanuit email account e-mails verstuurd naar vrienden/bekenden met reclame erin. Geen toestemming voor gegeven. E-mails waren ondertekend met naam van respondent.	Respondent krijgt score 2. Er is in dit geval zonder toestemming van de gebruiker ingebroken of binnengedrongen in het mailaccount van de respondent	Hacking
210017430	C. Hacking	2	HACKING: Iemand IP adres gebruikt.Kreeg bericht met beschuldiging gebruik kinderporn en geld brengen naar pompstation anders politie erbij. Politie gebeld en virusscanner erop gezet.	De respondent krijgt score 2. Blijkbaar heeft iemand zonder toestemming van de respondent besloten de computer van de respondent binnen te dringen. Dit om vervolgens de respondent te chanteren. Op zich zou er ook nog aan identiteitsfraude gedacht kunnen worden, aangezien de persoonlijke gegevens (IP-adres), zonder toestemming van de respondent, gebruikt zijn voor financieel gewin.	Hacking (mogelijk tevens ID-fraude)
320068430	C. Hacking	2	HACKING: Ik kon niet inloggen in mijn mail omdat iemand daar al op ingelogd was maar ik zag vervolgens niets raars toen ik het wachtwoord had verandert.	Respondent krijgt score 2. Er is in dit geval zonder toestemming van de gebruiker ingebroken of binnengedrongen in het mailaccount van de respondent	Hacking
680000431	C. Hacking	0	HACKING: Ik kreeg een pop-up waarin naar mijn creditcardgegevens werd gevraagd omdat ik extra vliegpunten had verdient en ze dezen wilde bijschrijven.	Deze respondent krijgt score 0. Hier is duidelijk sprake van phishing. Op geen enkele wijze komt de beschrijving van de respondent overeen met de definitie van hacking. Er is namelijk niet binnengedrongen in de computer.	Phishing
630000311	D. Cyberpesten	2	CYBERPESTEN:Respondent geeft aan te zijn gestalked via e-mail en whatsapp door een ex-relatie. Meerdere keren e-mail adres en telefoonnummer veranderd. Af en toe echter nog steeds last.	De respondent krijgt in dit geval score 2. Stalken is een overtreffende trap in pestend gedrag. Tevens gebeurde het stalken middels internet. Het lijkt erop dat de respondent de vraag goed begrepen en de kenmerken van cyberpesten heeft waargenomen en begrepen.	Cyberpesten

100003721	D. Cyberpesten	2	CYBERPESTEN: Aantal nare mails ontvangen van familie leden	De respondent krijgt in dit geval score 2. Het sturen van nare e-mails kan worden gezien als pestend gedrag. Tevens gebeurde dit middels het internet. Het lijkt erop dat de respondent de vraag goed begrepen en de kenmerken van cyberpesten heeft waargenomen en begrepen.	Cyberpesten
470006420	D. Cyberpesten	2	CYBERPESTEN: Mails ontvangen van vervelende aard van een aantal familieleden. contact met deze mensen was/is niet goed, sinds kort benaderen ze hem via email.	De respondent krijgt in dit geval score 2. Het sturen van nare e-mails kan worden gezien als pestend gedrag. Tevens gebeurde dit middels het internet. Het lijkt erop dat de respondent de vraag goed begrepen en de kenmerken van cyberpesten heeft waargenomen en begrepen.	Cyberpesten
110000431	D. Cyberpesten	2	CYBERPESTEN: Dreigen met plaatsen van foto´s en stalken, constant contact blijven zoeken ookal reageerde ik niet meer.	De respondent krijgt in dit geval score 2. Stalken en dreigen kunnen worden gezien als een overtreffende trap in pestend gedrag. Tevens gebeurde het stalken en dreigen middels internet. Het lijkt erop dat de respondent de vraag goed begrepen en de kenmerken van cyberpesten heeft waargenomen en begrepen.	Cyberpesten
100000311	D. Cyberpesten	2	CYBERPESTEN: uit woede of vanwege verlies. Het staat de dader niet aan wat er gebeurt. Wordt geuit in de chat van het spel. VB: "We zullen wel eens zien hoe stoer je bent als ik voor je deur sta".	De respondent krijgt in dit geval score 2. De omschrijving van cyberpesten is geheel overeenkomstig met de definitie. Er is sprake van een bedreiging via internet. Een bedreiging is te zien als een overtreffende vorm van pesten.	Cyberpesten

III Bijlage 3 - Analyse antwoorden op vragen uit dit onderzoek

In tabel 11 ziet u allereerst het respondentnummer dat tijdens het interview door de interviewers is genoteerd. Vervolgens wordt de score vermeld die aangeeft in hoeverre de respondent de vragen lijkt te begrijpen. De uitleg van de respondent komt hier na. Welke cybercrime heeft hij of zij gerapporteerd, en hoe legt de respondent uit wat hem of haar precies overkomen is? Vervolgens wordt er vermeld hoe de onderzoeker tot de score (0, 1 of 2) is gekomen.

In de zesde kolom van de tabel (genaamd 'Daadwerkelijk') wordt weergegeven van welke crime het slachtoffer daadwerkelijk slachtoffer is geworden. Indien de respondent een andere crime rapporteert, dan hij of zij beschreven heeft, welke cybercrime beschrijft de respondent dan?

Tabel 12 - Scoringstabel over het begrip van de respondent met betrekking tot cybercrime vragen Vragenlijst UT

Respondent	Crime	Score	Verhaal	Uitleg score	Daad-werkelijk
10077110	Phishing	2	Phishing: Via een mail. door een 'bank' (niet de mijne) werden inloggegevens gevraagd. Deze mail doorgestuurd naar deze bank, daarna mail weggegooid.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
30410110	Phishing	2	Phishing: Bij Rabobank en SNS bank via mail	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
40410110	Phishing	2	Phishing: Western Union Amerika. De vraag was (via mail - RV) of ik mijn creditkaart wou activeren anders zou die (het saldo - RV) worden verlaagd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
50000311	Phishing	1	Phishing: Het gaat altijd om vragen van vrienden die iets op mijn account willen doen.	Er was in dit geval geen sprake van een crime, maar de respondent heeft wel correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	Geen crime
60000311	Phishing	-	Phishing: E-mail op studentmail	Niet genoeg info van de respondent om een score te bepalen	Niet te bepalen
70000311	Phishing	2	Phishing: Spam-mail, ziet er wel professioneel uit, maar als je twee seconden langer kijkt dan zie je dat zo'n mail nep is en gaat deze de ton in.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
100000311	Phishing	2	Phishing: BANK: Nagemaakte layout van ABN Amro. Vroegen om een beveiligingsupdate af te ronden. SOCIAL NETWORK: Mail van een onbekende dat ze contact willen leggen en je moet klikken op een linkje. Geen layout, niet professioneel. GAMING: mails van Blizzard (world of Warcraft) die nagemaakt worden. 7 dagen gratis spelen en dan inloggen op nagemaakt site.	Deze respondent krijgt score 2. De respondent lijkt in alle 3 de gavellen correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
130501110	Phishing	2	Phishing: Via e-mail. Vaak in slecht Nederlands, soms	Deze respondent krijgt score 2. De respondent lijkt correct	Phishing

			van een andere bank waar we geen rekening hebben. Paar keer heel goed nagemaakt met logo e.d.	gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	
180174110	Phishing	2	Phishing: Respondent heeft iets anders meegemaakt wat hij niet in de vragen terug vond komen: "Bij het inloggen op wetransfer.com maakte ik een spelfout en kwam op een site terecht waarbij ik werd gewaarschuwd dat het een phishig site kon zijn." Respondent heeft vervolgens weggeklikt. ?	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De respondent rapporteerde jn overeenstemming met hetgeen zijn computer hem vertelde. De vraag is of de computer daadwerkelijk gelijk had. Dit is niet meer te achterhalen	Phishing
240566110	Phishing	2	Phishing: Tekst, weinig gelijkenis met echte websites	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
250521110	Phishing	2	Phishing: Mail "via/van" bank (RABO). Mail doorgestuurd naar betreffende bank + specifiek mailadres	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
260566110	Phishing	2	Phishing: Mail van ING --> Vertaalmachine	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
270480110	Phishing	2	Phishing: Professioneel, adres in balk niet betrouwbaar. Bank: ABN. SNS: Facebookmail, afkomstig van facebookmail.com (dus niet facebook zelf). Vroegen om wachtwoord te wijzigen (respondent vertelde dit, maar schreef het zelf niet op ivm haast - RV)	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
280480110	Phishing	1	Phishing: een collega vroeg naar het wachtwoord van mijn werkaccount bij het MST. Per account ben je verantwoordelijk voor je eigen acties, iemand die op mijn account zit tekent dus onder mijn naam.	Er was in dit geval geen sprake van een crime, maar de respondent heeft wel correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	Geen crime
290480110	Phishing	2	Phishing: veel mails zijn met 'vertaalmachine nederlands'	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om	Phishing

				persoonlijke informatie van het slachtoffer.	
300480110	Phishing	2	Phishing: van ABN AMRO	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
320000311	Phishing	2	Phishing: Zowel ingame, als via e-mail met phishing link	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
330000311	Phishing	-	Phishing: WOW (World of warcraft - RV) account meuk, nooit gedaan	Niet genoeg info van de respondent om een score te bepalen	Niet te bepalen
350659110	Phishing	2	Phishing: E-mail zag er professioneel uit. Ik trap er niet in. Rabobank had al eerder gewaarschuwd voor dit soort zaken.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
410000311	Phishing	2	Phishing: Mail leek afkomstig van de Rabobank. Was duidelijk niet het geval. Was sprake van zeer slecht Nederlands in de mail	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
420000311	Phishing	-	Phishing: Respondent heeft verder geen aanvulling (RV)	Niet genoeg info van de respondent om een score te bepalen	Niet te bepalen
440000311	Phishing	1	Phishing: Informatie gegeven aan vrienden die zich voor mij (in mijn naam) hebben ingelogd om me voor een les in te schrijven.	Er was in dit geval geen sprake van een crime, maar de respondent heeft wel correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	Geen crime
480000311	Phishing	2	Phishing: Een kopie van de huisstijl van een game developer die door de spam filter via e-mail binnen is gekomen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (game developer), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
500000311	Phishing	2	Phishing: Goedlijkende mail. Beon bekijken/soundbox kom je er dan wel achter	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt	Phishing

				geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	
510000311	Phishing	2	Phishing: In een e-mail met link naar een officieel uitziende ING-website om het wachtwoord opnieuw in te vullen 'ter bescherming'.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (ING), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
540000311	Phishing	2	Phishing: 1B) van de ING bank 1E) door een bekende op eduroan netwerk	Deze respondent krijgt in beide gevallen score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (ING en een andere bekende), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
560000311	Phishing	2	Phishing: Ik kreeg een link gestuurd waarop ik mijn account gegevens kon invullen, maar heb dit uiteraard niet gedaan. Het was vrij duidelijk dat dit om oplichting ging.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
570000311	Phishing	2	Phishing: In misleidende e-mails en advertenties/voorgestelde berichten op Facebook	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (in dit geval ook via zo'n organisatie), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
580000311	Phishing	-	Phishing: Vaak inactiviteit op een bepaald spel maar Blizard zei: account online verkopen ofzo	Niet genoeg info van de respondent om een score te bepalen	Niet te bepalen
600000311	Phishing	2	Phishing: bankemails komen wekelijks binnen meestal van een willekeurige kant	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
610000311	Phishing	2	Phishing: the question was included in advertisements for costly download services	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
630000311	Phishing	-	Phishing: Respondent heeft verder geen aanvulling - RV	Niet genoeg info van de respondent om een score te bepalen	Niet te bepalen
650000311	Phishing	2	Phishing: De mail was geschreven in een soort Zuid-Afrikaans / Turks-Nederlands	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt	Phishing

				geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	
660000311	Phishing	2	Phishing: MAil met daarin de opmerking dat er iets mis was met mn bankaccount en dat ik moest klikken op de volgende link	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
670000311	Phishing	2	Phishing: Vaak krijg je een mailtje met een vreemde domeinnaam en met slecht geschreven e-mails	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
690000311	Phishing	2	Phishing: Via slecht vertaalde mailtjes wordt er gevraagd om in te loggen, maar ik klik nooit op die links	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
700000311	Phishing	2	Phishing: de vraag werd gesteld via standaard phishing mails (overduidelijk nep)	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
710000311	Phishing	2	Phishing: ik kreeg een mail van de bank op mijn persoonlijke e-mail. Ik heb er niet op geklikt omdat het tegenwoordig wel duidelijk is dat zoiets niet door de banken opgestuurd wordt.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
730000311	Phishing	2	Phishing: per mail gevraagd om gegevens te verstrekken. niet moeilijk te herkennen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
750000311	Phishing	2	Phishing: Incidenten via de EA-site. Er wordt gevraagd onder de naam van EA (gameproducent) naar inloggegevens van de gameaccounts van de spelers die goed scoren in de games. Dit omdat ze van EA (gameproducent) leuke extraatjes schijnen te krijgen omdat ze zulke goede spelers zijn.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (EA), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
10001420	Phishing	2	Phishing: Er werd gevraagd om een conectie op linkedin te maken. Volgende dag verzoek om tijdelijk 18.000.000 euro op bankrekening te laten storten. Niet op ingegaan	De respondent krijgt in dit geval score 2. Er kan hier namelijk zeker sprake zijn van phishing. Indien de respondent zou toestemmen zal er naar waarschijnlijkheid op frauduleuze wijze naar de persoonlijke bankgegevens en mogelijk kopieën van bankgegevens gevraagd gaan	Phishing

				worden. Mogelijk is het een zoektocht naar het witwassen van geld of het doorsluizen van crimineel geld. Dit is echter niet meer na te gaan. Tevens lijkt het mij niet aannemelijk om dit via Linkedin te doen.	
20001420	Phishing	2	Phishing: Mail met banklogo, maar ander adres in het engels met een link erin waarop gevraagt wordt te klikken.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
50002420	Phishing	2	Phishing: Mail ontvangen die lijkt op een mail van de bank, met een link naar een ander adres waar wordt gevraagd in te loggen.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
60002420	Phishing	2	Phishing: Mails van "bank" van een ander adres die vragen om persoonsgegevens in te voeren en op te sturen. Niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
70002420	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
90003721	Phishing	-	Phishing: Voor spelletje op telefoon werd er om gegevens gevraagd, hierdoor waren er extra "levens" te verdienen	Niet genoeg info van de respondent om een score te bepalen. Het is niet zeker of er inderdaad sprake is van phishing, aangezien het niet zeker is of deze vraag naar gegevens met frauduleuze redenen gesteld is.	8 Niet te bepalen
100003721	Phishing	2	Phishing: Mails ontvangen die van bank leken, vragen om inlogggevens. Ook werd in deze mails gewaarschuwd voor het blokkeren van de rekening of het afschrijven van een aanzienlijk bedrag bij geen gehoor, gegevens niet verstrekt. Bank ingelicht over mails	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
120003721	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
180005521	Phishing	2	Phishing: Mail ontvangen waarin naar inloggegevens werd gevraagd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
190005521	Phishing	1	Phishing: Inloggegevens voor schoolsysteem geleend aan	Er was in dit geval geen sprake van een crime, maar de respondent	Geen crime

			een oud-klasgenootje. Zij kon niet meer in het systeem en had bepaalde informatie nodig. Via deze manier is dit gelukt.	heeft wel deels correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	
210005521	Phishing	1	Phishing: Normale situatie om op de desbetreffende accounts te komen	Er was in dit geval geen sprake van een crime, maar de respondent heeft wel deels correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	Geen crime
220005521	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
230005521	Phishing	2	Phishing: Via persoonlijke mail een mail ontvangen die van bank leek, meteen weggegooid. Sms bericht ontvangen of ze op een bepaalde site wilde inloggen, was een engelstalig bericht.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
240005521	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
250005521	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
260005521	Phishing	-	Phishing: Krijgt vaak mails over oude world of warcraft account, negeert deze altijd.	Niet genoeg info van de respondent om een score te bepalen. Hoeft niet per se phishing te zijn.	Niet te bepalen
310005521	Phishing	2	Phishing: Een email van "nep" ING waarin gevraagd werd om in te loggen voor verificatie	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
340005521	Phishing	2	Phishing: Er wordt regelmatig via mail gevraagd naar gegevens van banken waar hij geen rekeningen heeft lopen/ Eemalig vanuit eigen bank. Stuurt mails door naar phishing meldpunten.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
360005521	Phishing	2	Phishing: Een mail gerkregen waarbij stond dat er een derde partij was gesignaleerd in de account. Daarom was	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt	Phishing

			besloten detoegang tot het account te beperken. Om weer toegang te krijgen moest ingelogd worden via een link in de mail	geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	
390005521	Phishing	2	Phishing: Mails van bank ontvangen met link om in te loggen, van een ander adres, niet op ingegaan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
750011420	Phishing	2 en 0	Phishing: 1: Mail met link van "bank" niet op gedrukt, meteen weggegooid. 2: Via linkedin verzoek om connectie te maken met iemand die respondent niet kende, niet op gereageerd	Deze respondent krijgt in het eerste geval score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer. In het geval 2 krijgt de respondent score 0. Hier is geen sprake van het, op frauduleuze wijze, vragen naar persoonlijke gegevens.	Phishing Geen crime
20000431	Phishing	2	Phishing: Mail van bank zogenaamd waarin iets stonmd over een storing en ik daarom moest inloggen via die mail	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
40000431	Phishing	2	Phishing: Krege mailtje met vraag om in te loggen met mn bankgegevens.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
70000431	Phishing	2	Phishing: Ja eigenlijk wat ik eerder noemde dat ze mijn creditcard gegevens hebben gevraagd voor pokeraccount en toen gebruikt voor andere zaken zonder ik dat wist.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
110000431	Phishing	2	Phishing: Mailtje van de bank waarin dan staat dat jke moet inloggen via een link in die mail.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
120000431	Phishing	2	Phishing: Mail die van de bank leek te zijn met de vraag om in te loggen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
160000431	Phishing	2	Phishing: Mail waarin stond dat ik een prijs had gewonnen en alleen maar mijn gegevens zou hoeven in te vullen en deze dan op mijn rekning gestort zou worden	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails,	

				die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	
190000431	Phishing	2	Phishing: Mail dat ik mij had aangemeld voor een site en daarom mijn gegevens moest invullen terwijl ik heel die site niet kende.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	5 Phishing
200017430	Phishing	1	Phishing: Voor mijn vakantie is mij gevraagd om mijn accountgegevens bij ene collega neer te leggen zodoende ze in mijn vakantie bij een noodgeval belangrijke bestanden kunnen komen. Dit heb ik geweigerd	Er was in dit geval geen sprake van een crime, maar de respondent heeft wel correct gerapporteerd. Er is namelijk gevraagd naar de inloggegevens van zijn/haar account. Echter niet op frauduleuze wijze/criminele ideeën, zoals wel de bedoeling is (genoemd in de inleidende tekst vóór de phishing vragen) Vandaar een score 1	Geen crime
210017430	Phishing	2	Phishing: Mail van nep ING dat ik moest inloggen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
220017430	Phishing	2	Phishing: Mailtje van de bank, leek net echt. Dochter zei dat het nep was.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
310738430	Phishing	2	Phishing: Mail van zogenaamd de bank waarin ze vroegen naar mijn inloggegevens omdat er een storing was.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
410682430	Phishing	2	Phishing: Een mail dat ik veel geld kon verdienen bij een nieuw bedrijf dat mij zogenaamd via internet had gevonden en graag als medewerker wilde hebben. Ik moest daarvoor al mijn gegevens invullen. De mail was in zeer slecht Nederlands	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
560000431	Phishing	2	Phishing: Mail waarin wordt gevraagd naar inloggevens van internetbankieren	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties (bank), en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
660000431	Phishing	2	Phishing: Ik kreeg een mail waarin ze vroegen naar mijn gegevens voor een platina account voor online pokeren. Ik kende de site niet dus heb niet gereageerd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	Phishing
680000431	Phishing	2	Phishing: Een pop-up waar naar mijn creditcard gegevens	Deze respondent krijgt score 2. De respondent lijkt correct	Phishing

			werd gevraagd omdat ik zogenaamd extra punten zou hebben gewonnen	gerapporteerd te hebben. De beschrijving van de phishing klopt geheel met de definitie. Er is immers sprake van frauduleuze e-mails, die afkomstig lijken van betrouwbare organisaties, en die vragen om persoonlijke informatie van het slachtoffer.	
340659110	Online oplichting	2	Online oplichting met financiële schade: Videogame gekocht via marktplaats maar niet ontvangen. De desbetreffende persoon bleek een oplichter te zijn en had heel veel anderen ook opgelicht. Het gekke is dat ik gewoon (via ING - RV) geld over kon maken, terwijl ik niet zijn echte naam ingevuld had (die had de oplichter namelijk niet gegeven - RV). Ik heb via internet aangifte gedaan, maar marktplaats, de bank en de politie doet er niks aan	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
410000311	Online oplichting	2	Online oplichting met financiële schade: Spelletje via Marktplaats niet geleverd	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
440006420	Online oplichting	2	Online oplichting met financiële schade: Via markplaats.nl een tas gekocht van een particuliere verkoper, waarde 3999 euro. Tas nooit ontvangen, geprobeerd contact te zoeken met verkoper maar niet meer gelukt. Klacht ingediend bij Marktplaats	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
70000431	Online oplichting	2	Online oplichting met financiële schade: Er was ineens betaald mijn kaart zonder dat ik dat wist. Heb geld terug gekregen	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
80000431	Online oplichting	2	Online oplichting met financiële schade: Nooit geld gehad voor een product dat ik heb verkocht via marktplaats maar wel via verzekering.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
430008430	Online oplichting	2	Zoals ik eerder al aangaf is er gebruik gemaakt van mijn creditcard zonder dat ik dit wist.	Deze respondent krijgt score 2. De respondent lijkt correct gerapporteerd te hebben. Er is immers duidelijk sprake van een oplichting via internet	Online oplichting
50000431	Geld kwijt via internet	2	Geld kwijt via het internet: Had via marktplaats tickets gekocht en nooit gekregen	Deze respondent krijgt score 2. De respondent is immers geld kwijtgeraakt via internet. Echter via online oplichting en de respondent is zijn of haar geld dus niet ‘simpelweg’ kwijtgeraakt	Online oplichting
390682430	Geld kwijt via internet	2	Geld kwijt via het internet: Iets gekocht via marktplaats maar nooit gehad thuis	Deze respondent krijgt score 2. De respondent is immers geld kwijtgeraakt via internet.	Geld kwijt via internet
240005521	Geld kwijt via internet	2	Geld kwijt via het internet: Product besteld, was niet goed, terug gestuurd, nooit geld retour ontvangen. Bij bellen aangegeven retourzending ontvangen te hebben.	Deze respondent krijgt score 2. De respondent is immers geld kwijtgeraakt via internet.	Geld kwijt via internet
500000311	Geld kwijt via internet	2	Geld kwijt via het internet: Gewoon iets gekocht uit China, nooit aangekomen	Het is niet te bepalen of het hier gaat om een crime, een door de douane onderschept artikel, of een fout bij de postbezorging. Wel heeft de respondent correct gerapporteerd. Hij of zij is daadwerkelijk geld kwijtgeraakt	Geld kwijt via internet

460000311	Geld kwijt via internet	2	Geld kwijt via het internet: Sleutels voor de fiets besteld bij fabrikant en niet aangekomen.	Het is niet te bepalen of het hier gaat om een crime, een door de douane onderschept artikel, of een fout bij de postbezorging. Wel heeft de respondent correct gerapporteerd. Hij of zij is daadwerkelijk geld kwijtgeraakt	Geld kwijt via internet