Hulp na slachtofferschap van online fraude en ransomware

De ontwikkeling van een interventie om slachtoffers te ondersteunen in hun online zoektocht naar hulp

Sifra Matthijsse, Asier Moneva, Susanne van ’t Hoff-de Goede,

Merel van Leuken & Rutger Leukfeldt

3-11-2026

DE HAAGSE HOGESCHOOL

Inhoudsopgave

Dankwoord 4
Samenvatting 5
Hoofdstuk 1: Inleiding 11
1.1. Achtergrond 11
1.2. Doelstelling 12
1.3. Onderzoeksvragen 12
1.4. Leeswijzer 13
Hoofdstuk 2: Literatuurstudie 15
2.1. Slachtofferbehoeften 15
2.2. Omgaan met slachtofferschap 17
2.3. Hulpzoekgedrag 19
2.4. Het gebruik van online advertenties gericht op online criminaliteit en slachtofferschap 21
Hoofdstuk 3: Methodologie 24
3.1. Deelstudie 1: Vragenlijstonderzoek 24
3.2. Deelstudie 2: Google zoekwoordplanner 28
3.3. Deelstudie 3: Google Advertenties 33
3.4. Ethische toestemming 37
Hoofdstuk 4: Vragenlijstonderzoek onder slachtoffers 38
4.1. Prevalentie van slachtofferschap 38
4.2. Gevolgen van slachtofferschap 40
4.3. Informatie- en hulpbehoeften 48
4.4. Hulpzoekgedrag bij verschillende partijen 49
4.5. Online hulpzoekgedrag 54
4.6. Aanpassingen in gedrag na slachtofferschap 58
Hoofdstuk 5: Advertentiecampagnes 61
5.1. Interactie met advertentiecampagnes 61
5.2. Zoektermen 64
5.3. Prestatie van advertenties 66
Hoofdstuk 6: Discussie 68
6.1. Conclusies 68
6.2. Beperkingen en suggesties voor vervolgonderzoek 72

6.3. Aanbevelingen 74
Referenties 76
Bijlage 1: Vragenlijst slachtoffers online fraude 85
Bijlage 2: Vragenlijst slachtoffers ransomware 99
Bijlage 3: Flowcharts voor selectie zoektermen uit vragenlijsten 114
Bijlage 4: Overzicht van vooraf gedefinieerde zoektermen voor de advertentiecampagnes 118
Bijlage 5: Landingspagina advertentiecampagne online fraude 126
Bijlage 6: Landingspagina advertentiecampagne ransomware 127

Dankwoord

Dit onderzoek is mede mogelijk gemaakt door de inzet van verschillende personen en organisaties. Dit onderzoek is gefinancierd door Stichting Achmea Slachtoffer en Samenleving, het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving, Slachtofferhulp Nederland en de kennisinstellingen van CyberweerbaarNL.

We willen Slachtofferhulp Nederland, in het bijzonder Ronald Effting en Annerieke Velvis, bedanken voor de samenwerking bij het ontwikkelen van landingspagina's voor de advertentiecampagnes. Ook danken we Joeri Loggen en Maaike Vergeer voor het opzetten van een account op het Google Ads-platform. Tot slot willen we alle respondenten bedanken die hun ervaringen met ons wilden delen in de vragenlijsten. We zijn alle betrokkenen dankbaar voor hun bijdrage aan dit onderzoek.

Samenvatting

Achtergrond

Jaarlijks worden ongeveer 1 op de 6 Nederlanders slachtoffer van online criminaliteit (CBS, 2026b). Dit kan uiteenlopende negatieve gevolgen hebben, waaronder fysieke, emotionele, psychologische of financiële gevolgen (Borwell et al., 2025; Button et al., 2021; Leukfeldt et al., 2018). Slachtoffers kunnen na een online misdrijf een beroep doen op diverse hulpbronnen, variërend van formele hulpbronnen zoals de politie, slachtofferhulp of (mentale) gezondheidszorg, private partijen zoals de bank of een verzekeringsmaatschappij, of informele hulpbronnen zoals een partner, familie of vrienden (Pijlman et al., 2025; Smith, 2008; Van Leuken & Van 't Hoff-de Goede, 2025; Voce & Morgan, 2025). Eerder onderzoek laat echter zien dat slachtoffers van online criminaliteit niet altijd hulp zoeken na slachtofferschap (De Kimpe et al., 2020; Pereira et al., 2016; Voce & Morgan, 2025).

Hoewel niet alle slachtoffers bereid zijn om melding te doen bij formele instanties, zoeken zij mogelijk wel anoniem naar hulp via andere bronnen, zoals online. Er is echter nog weinig bekend over hun online hulpzoekgedrag. Dit onderzoek richt zich daarom op het online hulpzoekgedrag van slachtoffers van online fraude en ransomware. Het onderzoek heeft enerzijds als doel om meer inzicht te verkrijgen in de behoeften en het hulpzoekgedrag van slachtoffers en anderzijds als doel om een interventie te ontwikkelen in de vorm van een online advertentiecampagne om slachtoffers van informatie en hulpbronnen te voorzien.

Onderzoeksvragen

In het onderzoek staat de volgende onderzoeksvraag centraal:

> In hoeverre en op welke manier zoeken slachtoffers van online fraude en ransomware online naar hulp en kunnen online advertentiecampagnes worden ingezet om deze slachtoffers te bereiken en hen informatie of hulp te bieden?

De hoofdvraag wordt beantwoord aan de hand van een aantal deelvragen:

1. Welke gevolgen ervaren slachtoffers van online fraude en ransomware? (deelstudie 1)
2. Welke informatie- of hulpbehoeften ervaren slachtoffers van online fraude en ransomware na slachtofferschap? (deelstudie 1)
3. Via welke organisaties of informatiebronnen zoeken slachtoffers van online fraude en ransomware naar hulp? (deelstudie 1)
4. Welke zoektermen gebruiken slachtoffers van online fraude en ransomware wanneer zij via Google naar informatie of hulp zoeken? (deelstudie 1-3)

5. In hoeverre kunnen slachtoffers van online fraude en ransomware bereikt worden via online advertentiecampagnes om hen informatie of hulp te bieden? (deelstudie 3)

Methoden

Om een antwoord te geven op de hoofd- en deelvragen is het onderzoeksproject ingedeeld in drie deelstudies. Als onderdeel van deelstudie 1 zijn twee online vragenlijsten ontwikkeld en tussen 28 januari en 15 februari 2025 uitgezet onder individuele burgers die slachtoffer zijn geworden van online fraude (*n*=535) en ondernemers die slachtoffer zijn geworden van ransomware (*n*=107). In de vragenlijst is gevraagd naar de gevolgen van slachtofferschap, slachtofferbehoeften en (online) hulpzoekgedrag. Slachtoffers die destijds online hadden gezocht naar informatie of ondersteuning werd gevraagd de zoektermen die ze toen daadwerkelijk hebben gebruikt te rapporteren. Daarnaast is in alle respondenten, inclusief de respondenten die niet online gezocht hadden, gevraagd welke zoektermen zij zouden gebruiken als zij nu (opnieuw) slachtoffer zouden worden van online fraude of ransomware.

In deelstudie 2 is gebruikgemaakt van de Google zoekwoordplanner[1] om inzicht te krijgen in de frequentie van het gebruik van de zoektermen die in deelstudie 1 door respondenten zijn genoemd, en om aanvullende gerelateerde zoektermen te identificeren. Na een proces van in- en exclusie is een definitieve lijst met zoektermen opgesteld die als basis diende voor de advertentiecampagnes in deelstudie 3.

In deelstudie 3 zijn twee advertentiecampagnes ontwikkeld via Google Ads voor slachtofferschap van online fraude en ransomware. Advertenties werden weergegeven aan gebruikers die zochten op zoektermen gerelateerd aan online fraude of ransomware, voortkomend uit deelstudie 1 en 2. In totaal zijn zes advertenties ontwikkeld: drie voor online fraude en drie voor ransomware, met 1) een neutrale advertentie (controle); 2) een advertentie gericht op het oplossen van het probleem; en 3) een advertentie gericht op het omgaan met de emotionele gevolgen slachtofferschap. Gebruikers die op een advertentie klikten werden doorgestuurd naar een landingspagina op de website van Slachtofferhulp Nederland. Beide advertentiecampagnes werden gelijktijdig gelanceerd tussen vrijdag 8 augustus en vrijdag 15 augustus 2025 gedurende een periode van zeven dagen.

Conclusies

Gevolgen

De eerste deelvraag van het onderzoek richt zich op de gevolgen die slachtoffers van online fraude en ransomware hebben ervaren na slachtofferschap. Slachtoffers van online fraude rapporteerden over het

[1] De Google zoekwoordplanner maakt het mogelijk om onderzoek te doen naar zoekwoorden, bijvoorbeeld door middel van suggesties voor zoekwoorden en schattingen van maandelijkse zoekopdrachten.

algemeen beperkte financiële gevolgen: 66% gaf aan dat de financiële gevolgen tussen de €1 en €100 lagen en ongeveer 6% van de slachtoffers ervoer geen financiële gevolgen. Onder slachtoffers van ransomware gaf ongeveer 38% aan geen financiële gevolgen te hebben ervaren. Voor de meeste respondenten kostte het ransomware incident tussen 251 en 1.000 euro. Zowel slachtoffers van online fraude als ransomware ervoeren gemiddeld genomen weinig emotionele, psychische of lichamelijke gevolgen. De meest voorkomende emotionele reactie was boosheid, terwijl angstklachten en/of paniekaanvallen en lichamelijke klachten het minst werden ervaren. Ook andere gevolgen werden gemiddeld genomen beperkt ervaren. Respondenten uit beide groepen rapporteerden het vaakst dat ze voorzichtiger zijn geworden op het internet. Een verschil tussen beide groepen is dat slachtoffers van ransomware vaker kosten maakten voor reparatie of herstel. Slachtoffers van online fraude die emotionele, psychische, lichamelijke of andere gevolgen hadden ervaren, beoordeelden deze over het algemeen als ernstig. De financiële gevolgen werden als minder ernstig ervaren. Onder slachtoffers van ransomware werden alleen de financiële gevolgen beoordeeld; slechts een klein deel van de respondenten ervoer deze als ernstig.

Informatie- en hulpbehoeften

De tweede deelvraag van het onderzoek richt zich op de informatie- en hulpbehoeften die slachtoffers van online fraude en ransomware ervaren na slachtofferschap. Uit de vragenlijst (deelstudie 1) blijkt dat slachtoffers van beide delictsvormen vooral behoefte hadden aan informatie bij het oplossen van het probleem. Slachtoffers van online fraude hadden daarnaast relatief vaak behoefte aan informatie over het terugkrijgen van financiële schade en voorkomen van toekomstig slachtofferschap, terwijl slachtoffers van ransomware vaker behoefte hadden aan informatie over hoe het incident heeft kunnen plaatsvinden en het voorkomen van toekomstig slachtofferschap. Wanneer gekeken wordt naar de belangrijkste hulpbehoeften, betreft dit bij beide groepen eveneens hulp bij het oplossen van het probleem, gevolgd door financiële hulp en hulp aangifte bij fraude, en technische ondersteuning en preventie bij ransomware. In beide groepen was de behoefte aan emotionele, psychische of lichamelijke ondersteuning beperkt. De informatie- en hulpbehoeften sluiten hiermee grotendeels aan bij eerder onderzoek naar behoeften van slachtoffers van zowel traditionele als online criminaliteit, met name informatie over het delict, financiële behoeften en beschikbare hulproutes (bijv. Borwell et al., 2024; Cross et al., 2016; Leukfeldt et al., 2019; Ten Boom et al., 2008; Van Leuken et al., 2026). Andere behoeften uit de literatuur komen minder nadrukkelijk naar voren in het huidige onderzoek, zoals emotionele, psychologische of lichamelijke ondersteuning, erkenning als slachtoffer of juridische informatie of hulp.

Hulpzoekgedrag

De derde deelvraag van het onderzoek richt zich op de organisaties of informatiebronnen die slachtoffers van online fraude en ransomware gebruiken om te zoeken naar hulp. Uit de vragenlijst (deelstudie 1) blijkt dat een aanzienlijk deel van de slachtoffers van ransomware (ongeveer 91%) en online fraude (ongeveer 62%) hulp heeft gezocht. Slachtoffers van online fraude wendden zich vooral tot informele netwerken zoals vrienden en familie, gevolgd door de politie en banken of financiële instellingen, terwijl slachtoffers van ransomware vooral hulp zochten bij technische partijen zoals cybersecuritybedrijven en IT-specialisten, naast vrienden, familie, kennissen of collega's en de politie. Deze patronen sluiten grotendeels aan bij eerder onderzoek (Matthijsse et al., 2025; Van Leuken & Van 't Hoff-de Goede, 2025; Voce & Morgan, 2022).

Daarnaast blijkt dat het online zoeken naar hulp relatief vaak voorkomt bij slachtoffers van online fraude (57%) en minder bij ransomware (38%), waarbij Google de voornaamste zoekmachine is. Een deel van de slachtoffers die online heeft gezocht gaf aan niet de gewenste informatie of hulp te hebben gevonden online (ongeveer 20% tot 37% bij fraude en 20% tot 27% bij ransomware).

Zoektermen

De vierde deelvraag richt zich op de zoektermen die slachtoffers van online fraude en ransomware gebruiken wanneer zij via Google zoeken naar informatie of hulp. De resultaten van deelstudie 1 (vragenlijst) laten zien dat slachtoffers uiteenlopende zoektermen gebruikten. Slachtoffers van online fraude zochten bijvoorbeeld op termen gerelateerd aan de verkopende partij, specifieke fraudetypen of hulpvragen (zoals het zoeken naar hulp of melden van fraude), terwijl slachtoffers van ransomware vaker brede termen gebruikten zoals 'hack' of 'cybercrime'. Dit zou er mogelijk op kunnen wijzen dat sommige slachtoffers nog niet goed weten waar ze slachtoffer van zijn geworden en vooral omschrijven wat er is gebeurd, terwijl anderen al gericht naar hulp zoeken.

De in deelstudie 1 verzamelde zoektermen vormden de basis voor deelstudie 2. In deze deelstudie zijn de door slachtoffers gerapporteerde zoektermen aangevuld met gerelateerde zoektermen die door de Google zoekwoordplanner werden voorgesteld. Na een proces van in- en exclusie heeft dit geleid tot een definitieve lijst met zoektermen die de basis vormde voor de advertentiecampagnes in deelstudie 3.

De advertentiecampagnes (deelstudie 3) hebben inzicht gegeven in de zoektermen die gebruikers zelf hebben ingevuld. Ook daarin is er variatie zichtbaar in de zoektermen. Bij online fraude varieerde dit van een beschrijving van het type fraude tot het terugkrijgen van geld of het willen doen van een melding of aangifte. Bij ransomware ging het vooral om brede omschrijvingen van een hack, of de vraag wat te doen. De zoektermen sluiten aan bij de uiteenlopende hulpvragen en behoeften zoals omschreven onder deelvraag 1.

Interactie met advertentiecampagnes

Tot slot richt de vijfde deelvraag van het onderzoek zich op in hoeverre online advertentiecampagnes slachtoffers van online fraude en ransomware kunnen bereiken om hen informatie of hulp te bieden. De advertentiecampagne voor online fraude genereerde in totaal 110.440 impressies en 831 kliks, met een doorklikratio (het percentage van de gebruikers die de advertentie te zien kreeg en hier vervolgens op geklikt heeft) van 0,6, terwijl de advertentiecampagne voor ransomware in totaal 15.296 impressies en 373 kliks genereerde, met een doorklikratio van 2,4%. Hoewel de advertentiecampagne gericht op online fraude vaker te zien was voor gebruikers, leidde deze relatief minder vaak tot het klikken op de advertenties. De hogere doorklikratio voor de ransomware-campagne suggereert dat deze mogelijk beter aansloot bij de behoeften van gebruikers, ondanks de meer generieke zoektermen. De doorklikratio van beide campagnes is vergelijkbaar met eerdere campagnes gericht op geldezels (Bekkers et al., 2022), maar lager dan in andere studies gericht op het plegen van DDoS-aanvallen of slachtofferschap van Image-Based Sexual Harassment (IBSH) en Image-Based Sexual Abuse (IBSA) (Moneva et al., 2022; Pijlman & Burgmeijer, 2024). Dit verschil kan mogelijk worden verklaard door een minder specifieke demografische doelgroep en een grotere variatie in zoektermen, waardoor de campagnes minder gericht waren en daardoor minder efficiënt. Een gebrek aan precisie in de targeting kan echter enkele nadelen hebben, namelijk dat campagnes voor opdringeriger zijn, duurder en bovendien moeilijker te analyseren.

Aanbevelingen

In het kort

- Online advertenties maken het mogelijk om slachtoffers te bereiken op het moment dat zij online zoeken naar informatie of hulp
- Advertenties werken vooral als aanvulling op bestaande hulpkanalen
- Succes hangt af van specifieke targeting en relevante zoektermen
- Hoge kosten en inspanning versus relatief lage interactie (doorklikratio) moeten meegenomen worden in de kosten/baten afweging voor de inzet van advertenties
- Potentiële meerwaarde vooral bij goed afgebakende doelgroepen

De resultaten van dit onderzoek suggereren dat online advertentiecampagnes een waardevol instrument kunnen zijn om slachtoffers van online fraude en ransomware te bereiken op het moment dat zij actief online zoeken naar informatie of hulp. Hoewel veel praktijkpartners zoals Slachtofferhulp Nederland, de Fraudehelpdesk en politie al websites hebben met informatie en contactmogelijkheden, kunnen advertentiecampagnes hierbij een aanvullende rol vervullen door slachtoffers op een relevant moment te verwijzen naar betrouwbare informatie, praktische handelingsperspectieven en beschikbare hulp

gerelateerd aan hun Google zoektermen. Daarnaast kunnen advertentiecampagnes worden toegespitst op verschillende subgroepen van slachtoffers.

Tegelijkertijd laten de resultaten zien dat de toegevoegde waarde van dergelijke campagnes afhankelijk is van verschillende voorwaarden. Zo is het belangrijk dat campagnes zo specifiek mogelijk worden afgestemd op de doelgroep en behoeften van slachtoffers, die blijkens het huidige onderzoek uiteen kunnen lopen. Campagnes die aansluiten bij deze specifieke behoeften zouden mogelijk beter aansluiten bij de hulpvraag van slachtoffers en de kans vergroten om relevante doelgroepen te bereiken. Verdere specificering in de doelgroepen is mogelijk wenselijk, zoals alleen slachtoffers van een specifiek type fraude, of slachtoffers in een specifieke leeftijdscategorie. In het huidige onderzoek bleek bijvoorbeeld dat de doorklikratio afnam naarmate de leeftijd toenam, wat suggereert dat de advertenties het meest relevant waren voor jongere leeftijdscategorieën.

Praktijkpartners dienen in de keuze voor online advertentiecampagnes bovendien een zorgvuldige afweging te maken tussen de potentiële opbrengsten en de benodigde investering. Het identificeren, selecteren en optimaliseren van relevante zoekwoorden bleek een tijdsintensief proces en de kosten van advertentiecampagnes kunnen oplopen, afhankelijk van de gekozen zoektermen en de mate van concurrentie met andere adverteerders op deze termen. Daarnaast leidde slechts een beperkt deel van de grote hoeveelheid impressies tot interactie (kliks) met de advertenties. In combinatie met de benodigde tijd, expertise en financiële middelen roept dit de vraag op in hoeverre de opbrengsten opwegen tegen het aantal slachtoffers dat daadwerkelijk wordt bereikt. Bovendien bieden advertentieplatformen zoals Google slechts gedeeltelijk inzicht in de factoren die bepalen wanneer en aan wie advertenties worden getoond, wat het campagnedesign en bepalen van de effectiviteit van campagnes bemoeilijkt. Online advertentiecampagnes kunnen daarom het beste worden ingezet als aanvulling op bestaande informatie- en hulpkanalen, en niet als enige strategie om slachtoffers te bereiken.

Hoofdstuk 1: Inleiding

1.1. Achtergrond

Slachtofferschap van criminaliteit is een veelvoorkomend maatschappelijk probleem. Jaarlijks worden meer dan 2,5 miljoen Nederlanders slachtoffer van een of meerdere vormen van criminaliteit. Dit omvat traditionele vormen van criminaliteit, zoals vermogens- of geweldsdelicten, maar ook online criminaliteit (CBS, 2026b). In 2025 werd ongeveer 1 op de 6 Nederlanders slachtoffer van een vorm van online criminaliteit, waaronder online fraude (10%), hacken (6%) en online bedreiging en intimidatie (3%) (CBS, 2026b). Slachtofferschap van online criminaliteit kan voor slachtoffers tal van negatieve gevolgen hebben, waaronder fysieke, emotionele, psychologische of financiële gevolgen. Het kan hierbij bijvoorbeeld gaan om gevoelens van angst, stress of schaamte, schade aan het zelfbeeld, verlies van digitale bezittingen, reputatieschade of financiële verliezen (Borwell et al., 2025; Button et al., 2021; Leukfeldt et al., 2018). Voor sommige vormen van cybercriminaliteit kan de impact zelfs groter zijn dan die van traditionele criminaliteit (Borwell et al., 2025).

Slachtoffers kunnen na een online misdrijf een beroep doen op verschillende hulpbronnen. Dit kunnen formele hulpbronnen zijn, zoals de politie, slachtofferhulp of (mentale) gezondheidszorg, private partijen zoals de bank of een verzekeringsmaatschappij, of informele hulpbronnen, zoals een partner, familie of vrienden (Pijlman et al., 2025; Smith, 2008; Van Leuken & Van ’t Hoff-de Goede, 2025; Voce & Morgan, 2025). Uit eerder onderzoek blijkt echter dat slachtoffers van online criminaliteit niet altijd hulp zoeken nadat ze slachtoffer zijn geworden (De Kimpe et al., 2020; Pereira et al., 2016; Voce & Morgan, 2025). Belemmeringen voor het zoeken van hulp omvatten onder andere gevoelens van schaamte, de overtuiging dat organisaties niets zullen of willen doen, angst voor negatieve reacties, een gebrek aan kennis over de opties voor hulp, de overtuiging dat het te veel tijd of moeite kost of omdat slachtoffers het incident niet als ernstig (genoeg) beschouwen (Colburn et al., 2023; Havers et al., 2024; Pijlman et al., 2025; Smith, 2008; Van De Weijer et al., 2020; Voce & Morgan, 2025).

Hoewel niet alle slachtoffers bereid zijn om bij formele instanties melding te maken van wat hun is overkomen, zoeken zij mogelijk wel anoniem naar hulp via andere bronnen. Zoekmachines kunnen een veilig alternatief bieden voor slachtoffers om online anoniem naar hulp te zoeken. Aangezien 96% van de Nederlandse bevolking dagelijks online is (CBS, 2026a), kan worden verwacht dat een deel van de slachtoffers ook gebruikmaakt van internet om informatie of middelen te vinden om met slachtofferschap om te gaan. Zo blijkt uit eerder onderzoek dat 22,4% van de Nederlandse burgers die geconfronteerd werd met ransomware als eerste naar hulp of advies zocht op internet (Matthijsse et al., 2025a). Er is momenteel echter weinig bekend over de mate waarin slachtoffers van cybercriminaliteit online hulp zoeken en waarnaar zij zoeken. Het huidige onderzoek heeft dan ook als doel om meer inzicht te verkrijgen in het

online hulpzoekgedrag van slachtoffers van online fraude en ransomware en een interventie te ontwikkelen om slachtoffers te ondersteunen in hun online zoektocht naar hulp met behulp van Google-advertenties. Google-advertenties zijn in het verleden gebruikt om potentiële daders te ontmoedigen om DDoS-aanvallen uit te voeren (Moneva et al., 2022; Moneva & Leukfeldt, 2024b). Op vergelijkbare wijze hebben onderzoekers Instagram-advertenties gebruikt om potentiële geldezels af te schrikken (Bekkers et al., 2022) en Snapchat-advertenties gebruikt om slachtoffers van technologie-gefaciliteerd seksueel geweld te helpen (Pijlman, 2025). Voor zover bekend is er echter nog geen onderzoek gedaan waarbij Google-advertenties zijn gebruikt om slachtoffers van online criminaliteit te bereiken die online hulp zoeken.

1.2. Doelstelling

Dit onderzoeksproject richt zich op slachtoffers van online fraude en ransomware. Het doel is daarbij tweeledig. Ten eerste is het doel om meer inzicht te verkrijgen in de behoeften en het online hulpzoekgedrag van slachtoffers van online fraude en ransomware. Dit wordt enerzijds gedaan aan de hand van vragenlijsten onder slachtoffers en anderzijds aan de hand van een analyse van Google-zoekopdrachten van slachtoffers met betrekking tot hun slachtofferschap. Ten tweede is het doel om een interventie te ontwikkelen in de vorm van online advertentiecampagnes om slachtoffers van informatie en hulpbronnen te voorzien, en het bereik van deze advertenties te analyseren. Door het zoekgedrag van de slachtoffers van deze twee typen cybercriminaliteit te vergelijken, kunnen we onderzoeken of de interventie voor alle slachtoffers even behulpzaam is of juist voor een specifiek type slachtoffer. Met deze strategie willen we profiteren van de mogelijkheden van big data om slachtoffers van cybercriminaliteit op een niet-indringende manier hulp te bieden en te empoweren.

1.3. Onderzoeksvragen

In het onderzoek staat de volgende onderzoeksvraag centraal:

> In hoeverre en op welke manier zoeken slachtoffers van online fraude en ransomware online naar hulp en kunnen online advertentiecampagnes worden ingezet om deze slachtoffers te bereiken en hen informatie of hulp te bieden?

De hoofdvraag zal beantwoord worden aan de hand van een aantal deelvragen:

1. Welke gevolgen ervaren slachtoffers van online fraude en ransomware? (deelstudie 1)
2. Welke informatie- of hulpbehoeften ervaren slachtoffers van online fraude en ransomware na slachtofferschap? (deelstudie 1)

3. Via welke organisaties of informatiebronnen zoeken slachtoffers van online fraude en ransomware naar hulp? (deelstudie 1)
4. Welke zoektermen gebruiken slachtoffers van online fraude en ransomware wanneer zij via Google naar informatie of hulp zoeken? (deelstudie 1-3)
5. In hoeverre kunnen slachtoffers van online fraude en ransomware bereikt worden via online advertentiecampagnes om hen informatie of hulp te bieden? (deelstudie 3)

Een overzicht van de verschillende onderzoeksvragen en deelstudies is weergegeven in Tabel 1.1.

Tabel 1.1 Overzicht van onderzoeksvragen en deelstudies.

Onderzoeksvraag	**Deelstudie 1** (Vragenlijst onder slachtoffers)	**Deelstudie 2** (Google zoekwoordplanner)	**Deelstudie 3** (Google advertentiecampagne)
1. Welke gevolgen ervaren slachtoffers van online fraude en ransomware?			
2. Welke informatie- of hulpbehoeften ervaren slachtoffers van online fraude en ransomware na slachtofferschap?			
3. Via welke organisaties of informatiebronnen zoeken slachtoffers van online fraude en ransomware naar hulp?			
4. Welke zoektermen gebruiken slachtoffers van online fraude en ransomware wanneer zij via Google naar informatie of hulp zoeken?			
5. In hoeverre kunnen slachtoffers van online fraude en ransomware bereikt worden via online advertentiecampagnes om hen informatie of hulp te bieden?			

1.4. Leeswijzer

Hoofdstuk 2 van deze rapportage omvat een overzicht van de literatuur met betrekking tot behoeften, coping en hulpzoekgedrag na slachtofferschap, zowel in algemene zin als toegespitst op online fraude en ransomware. In hoofdstuk 3 worden de gebruikte onderzoeksmethoden uiteengezet. De resultaten van het

onderzoek zijn opgedeeld in twee delen. Hoofdstuk 4 zich richt op de uitkomsten van het vragenlijstonderzoek onder slachtoffers, waarbij onder andere stil wordt gestaan bij de gevolgen van slachtofferschap, de behoeften- en het online hulpzoekgedrag van slachtoffers. Hoofdstuk 5 richt zich op uitkomsten van de advertentiecampagne. In hoofdstuk 6 volgen de conclusie en discussie van het onderzoek.

Hoofdstuk 2: Literatuurstudie

Dit onderzoek richt zich op het hulpzoekgedrag van slachtoffers van online fraude en ransomware en het gebruik van een online advertentiecampagne om ze hierin te ondersteunen. In sectie 2.1 zal uiteengezet worden welke informatie- of hulpbehoeften slachtoffers ervaren. In sectie 2.2. wordt beschreven hoe slachtoffers omgaan met criminaliteit aan de hand van de copingtheorie van Lazarus en Folkman (1984). Deze theorie vormt tevens de basis voor de achterliggende gedachten van de ontwikkelde advertenties (zie ook sectie 3.3 voor meer informatie over de opzet van de advertentiecampagne). In sectie 2.3 wordt ingegaan op het hulpzoekgedrag van slachtoffers. In deze secties wordt eerst de literatuur over traditionele criminaliteit beschreven, gevolgd door de toepassing op online criminaliteit. Tot slot beschrijft sectie 2.4 eerder onderzoek naar het gebruik van online advertenties bij slachtofferschap of daderschap van online criminaliteit.

2.1. Slachtofferbehoeften

Slachtoffers van criminaliteit kunnen verscheidene behoeften hebben. Op basis van een systematische literatuurstudie naar zelf-gerapporteerde behoeften van slachtoffers van traditionele criminaliteit zijn zes verschillende domeinen van behoeften geïdentificeerd (Ten Boom et al., 2008):

1. **Emotioneel:** O.a. de behoefte aan (eerste) opvang, zorg en steun, erkenning als slachtoffer en van wat er gebeurd is, verwerking en afsluiting, maar ook dat de hulp snel beschikbaar en laagdrempelig is;
2. **Strafproces in ruime zin**: Zowel gericht op de uitkomst van het proces – zoals de behoefte aan arrestatie en bestraffing – als op het proces zelf, zoals de behoefte aan instemming en beslismacht;
3. **Informatie**: Bijvoorbeeld over de dader, het delict en preventie, maar ook het tijdig ontvangen van deze informatie;
4. **Praktisch**: O.a. behoefte aan hulp bij herstelwerkzaamheden, formaliteiten, medische hulp, huishoudelijk werk, vertaaldiensten;
5. **Financieel**: De behoefte aan compensatie en teruggave, maar ook hulp bij het regelen van financiële zaken;
6. **Primair:** O.a. de behoefte aan onmiddellijke veiligheid, bescherming van zichzelf en anderen, huisvesting en noodbehoeften zoals voedsel en kleding.

Behoeften van slachtoffers van criminaliteit zijn in de wetenschappelijke literatuur ook op andere wijzen geclassificeerd. Pemberton (2009) maakt bijvoorbeeld onderscheid tussen procedurele behoeften en uitkomstbehoeften. Hierbij zijn de procedurele behoeften onder te verdelen in respectvolle en eerlijke

behandeling, informatie over het strafproces en de uitkomst hiervan, en mogelijkheden voor participatie. In de uitkomstbehoeften kan onderscheid gemaakt worden tussen behoefte aan erkenning, (materiële) compensatie, bescherming van veiligheid en privacy, het voorkomen van verdere schade, omgaan met stress en verlies, en tot slot, vergelding en omgaan met gevoelens van woede en onrechtvaardigheid (Pemberton, 2009a, 2009b). Reinders Folmer et al. (2019) maken hiernaast onderscheid tussen materiële behoeften zoals financiële compensatie en non-materiële behoeften, zoals het nemen van verantwoordelijkheid of bekennen van wangedrag, erkenning van wat het slachtoffer overkomen is of het ontvangen van excuses.

Het classificeren van behoeften wordt bemoeilijkt door het feit dat verschillende behoeften aan elkaar gerelateerd kunnen zijn of kunnen overlappen (Maguire, 1991; Pemberton, 2009a). Daarnaast verschilt de aard en omvang van behoeften tussen slachtoffers. Hierop is bijvoorbeeld het type criminaliteit waarvan diegene slachtoffer is geworden van invloed, evenals de waargenomen gevolgen van het delict, individuele kenmerken, (de kwaliteit van) de reactie van de omgeving en de context en tijdsperiode van het incident (Borwell et al., 2024; Dunn, 2007; Kool, 2014; Laxminarayan, 2012; Lens et al., 2013; Leukfeldt et al., 2019; Pemberton, 2009b; Pemberton et al., 2008; Ten Boom et al., 2008). Slachtoffers van vergelijkbare delicten kunnen zodoende uiteenlopende slachtofferervaringen hebben en als gevolg daarvan ook verschillende behoeften ervaren (Dunn, 2007).

Slachtoffers van online criminaliteit rapporteren veelal behoeften die overeenkomen met die van slachtoffers van traditionele criminaliteit. Allereerst hebben zij emotionele behoeften, zoals de behoefte aan emotionele ondersteuning en erkenning van het slachtofferschap (Button & Cross, 2017; Cross et al., 2016; Leukfeldt et al., 2019; Parti & Tahir, 2023; Van Leuken et al., 2026). In de tweede plaats rapporteren zij behoeften ten aanzien van het strafproces, zoals de behoefte aan vergelding en de wens dat daders worden veroordeeld en gestraft (Cross et al., 2016; Leukfeldt et al., 2019; Van Leuken et al., 2026). In dit kader geven slachtoffers van online fraude tevens aan behoefte te hebben aan snelle en adequate doorverwijzing naar de juiste instanties voor het doen van aangifte of een melding (Cross et al., 2016; Van Leuken et al., 2026). Ten derde beschikken slachtoffers van online criminaliteit over uiteenlopende informatiebehoeften. Zij wensen bijvoorbeeld informatie te ontvangen over het delict en de wijze waarop dit heeft plaatsgevonden, over de dader en diens motieven, en over het (straf)proces en de voortgang daarvan (Leukfeldt et al., 2019). Slachtoffers van online fraude uiten bovendien de behoefte aan informatie over beschikbare hulproutes en gerelateerde kosten (Cross et al., 2016). Naast zaak-specifieke informatie ontvangen zij met het oog op bewustwording en preventie bovendien graag algemene informatie over fraude (Button et al., 2009; Button & Cross, 2017). Ten vierde hebben slachtoffers van online criminaliteit op praktisch vlak behoefte aan hulp bij herstel van de schade, zoals ondersteuning bij het offline halen van beelden, het ontsleutelen van bestanden of het blokkeren van identiteitsdocumenten, alsmede hulp bij het regelen van formaliteiten, waaronder het doen van aangifte. Daarnaast spelen ten vijfde financiële behoeften

een prominente rol. Compensatie vormt een van de belangrijkste behoeften van slachtoffers van online criminaliteit (Homburg & Van den Tillaart, 2015; Leukfeldt et al., 2019; Van Leuken et al., 2026). Onderzoek naar de behoeften van fraudeslachtoffers laat zien dat het terugkrijgen van de geleden financiële schade als zeer belangrijk wordt beschouwd, hoewel de behoefte aan het schuldig laten verklaren van de dader als meest belangrijkst werd aangemerkt (Button et al., 2009). Ten slotte rapporteren slachtoffers van online criminaliteit op primair vlak de behoefte aan het voorkomen van herhaald slachtofferschap bij henzelf en aan het voorkomen van slachtofferschap bij anderen (Cross et al., 2016; Leukfeldt et al., 2019; Parti & Tahir, 2023; Van Leuken et al., 2026)

Hoewel veel van de behoeften van slachtoffers van online criminaliteit overeenkomen met die van traditionele criminaliteit, zijn er ook verschillen tussen beide groepen (Borwell et al., 2024). In het onderzoek van Borwell et al. (2024) werden de behoeften van beide groepen vergeleken. Uit dit onderzoek bleek dat slachtoffers van online vermogenscriminaliteit in vergelijking met slachtoffers van traditionele vermogenscriminaliteit een sterkere emotionele behoefte rapporteren, namelijk aan erkenning van het delict. Ook uiten zij sterkere informatiebehoeften, namelijk de behoefte aan informatie over het delict, beschikbare hulproutes, en preventieadvies, evenals een sterkere behoefte aan financiële compensatie. Ook de behoefte aan het voorkomen van slachtofferschap bij anderen blijkt sterker onder slachtoffers van online vermogenscriminaliteit dan onder slachtoffers van traditionele vermogenscriminaliteit. De genoemde behoeften hangen samen met de mate van gevolgen die slachtoffers ervaren tijdens het delict of bij de ontdekking daarvan (ook wel peritraumatische stress genoemd). Verder blijkt dat de behoefte aan erkenning van het delict, informatie over beschikbare hulproutes en preventieadvies positief samenhangt met leeftijd. Wat betreft geslacht rapporteren vrouwen sterkere behoeften aan erkenning van het delict, bekende hulproutes, praktische hulp en preventie ten behoeve van anderen. Tot slot speelt de omvang van de financiële schade een rol: de behoeften aan erkenning van het delict, bekende hulproutes, informatie over het delict en preventiemogelijkheden, financiële compensatie én praktische hulp worden sterker naarmate de financiële schade oploopt (Borwell et al., 2024).

2.2. Omgaan met slachtofferschap

Individuen kunnen op verschillende manieren omgaan met slachtofferschap. Een model dat vaak wordt gebruikt om verschillende copingmechanismen te onderscheiden, is het transactionale copingmodel van Lazarus en Folkman (1984). Dit model, dat zijn oorsprong vindt in de psychologie, helpt verschillende reacties op stressvolle situaties te verklaren. Het is toegepast op diverse maatschappelijke problemen, waaronder slachtofferschap van misdrijven (bijv. Caputo & Brodsky, 2004; Green et al., 2010; Green & Pomeroy, 2007; Jansen & Leukfeldt, 2018; Yee et al., 1998). In het huidige onderzoek vormen deze inzichten de basis voor de achterliggende gedachten van de verschillende advertenties.

In het model wordt coping omschreven als "voortdurend veranderende cognitieve en gedragsmatige inspanningen om specifieke externe en/of interne eisen te beheersen die worden beoordeeld als belastend of de middelen van de persoon te boven gaan" (Lazarus & Folkman, 1984, p. 141). Met andere woorden verwijst coping naar manieren om om te gaan met interne of externe factoren die als belastend ervaren worden. Dit copingproces komt op gang na cognitieve beoordelingen, i.e. het evalueren van gebeurtenissen en hun facetten in relatie tot het welzijn van de persoon. Hierbij wordt een onderscheid gemaakt tussen een primaire en secundaire beoordeling. Tijdens de primaire beoordeling wordt een gebeurtenis beoordeeld als irrelevant, positief of stressvol (dreiging, schadelijke consequenties en uitdagingen). Wanneer een gebeurtenis als stressvol wordt beoordeeld, volgt een secundaire beoordeling waarbij wordt overwogen welke mogelijkheden er zijn om met de situatie om te gaan, verwijzend naar het copingproces.

Binnen de categorie copingstrategieën wordt onderscheid gemaakt tussen emotiegerichte en probleemgerichte coping (Lazarus & Folkman, 1984). Emotiegerichte coping is gericht op het reguleren van de emotionele reactie op een stressvolle situatie. Hieronder vallen bijvoorbeeld cognitieve processen die gericht zijn op het verminderen van emotionele stress, zoals distantiëring, vermijding of minimalisering. Een andere groep copingstrategieën is gericht op het vergroten van emotionele stress, zoals zelfverwijt of zelfbestraffing. Dergelijke strategieën kunnen tot actie aanzetten. Daarnaast kunnen emotiegerichte copingstrategieën leiden tot een herwaardering van de situatie waardoor deze als minder ernstig wordt ervaren zonder dat de situatie objectief is veranderd. Voorbeelden hiervan zijn het inzicht dat het ook erger had kunnen zijn of dat een situatie bij nader inzien minder ernstig blijkt dan aanvankelijk gedacht (Lazarus & Folkman, 1984). Probleemgerichte coping is gericht op het beheersen of veranderen van de situatie die de stress veroorzaakt. Voorbeelden hiervan zijn het definiëren van een probleem, het bedenken en afwegen van mogelijke oplossingen, het maken van een keuze en ondernemen van actie. Emotiegerichte en probleemgerichte kunnen elkaar faciliteren, dan wel in de weg zitten in het proces van coping.

De wijze waarop individuen omgaan met stressvolle situaties hangt ook samen met de middelen die zij ter beschikking hebben, of de mate waarin zij in staan zijn om deze te vinden of ontwikkelen. (Lazarus & Folkman, 1984). Hierbij kan gedacht worden aan gezondheid en energie, positieve overtuigingen, probleemoplossende vaardigheden, sociale vaardigheden, sociale steun en materiële middelen (Lazarus & Folkman, 1984). Veel stressvolle situaties overstijgen echter de middelen van een individu, of een individu is niet in staat om de beschikbare middelen tot hun volledige potentie te benutten. Samengevat hangt de keuze voor een copingstrategie samen met welke opties beschikbaar zijn, de waarschijnlijkheid dat een copingstrategie de juiste uitkomst biedt, en de waarschijnlijkheid dat een individu in staat is om een dergelijke strategie effectief toe te passen (Lazarus & Folkman, 1984).

Het transactionele copingmodel is ook toegepast op slachtofferschap van online criminaliteit. Empirisch onderzoek hiernaar toont aan dat slachtoffers van online criminaliteit een breed scala aan

copingstrategieën toepassen. Kwalitatief onderzoek naar slachtoffers van phishing en malware illustreert bijvoorbeeld het gebruik van zowel probleemgerichte coping (bijv. melding maken bij de bank en politie, het zoeken van sociale steun en het aanpassen van online gedrag), als emotiegerichte coping, waaronder cognitieve processen (zoals het herinterpreteren van de gebeurtenis) (Jansen & Leukfeldt, 2018). Een onderzoek naar sextortion identificeerde zowel probleemgerichte coping (zoals het zoeken van hulp, het melden van het delict of toegeven aan de afpersing) als emotiegerichte coping (zoals het reguleren van angst, schaamte en stress, of het internaliseren van gevoelens of self-blame) (Wang, 2025). Een groep studies heeft zich daarnaast gericht op online pesten, en identificeerde copingstrategieën zoals het zoeken van hulp, vrienden in vertrouwen nemen, het vermijden van de dader of ander ontwijkend gedrag, het confronteren van de dader, terug pesten of wraak nemen, middelengebruik en self-blame (zie bijvoorbeeld Machmutow et al., 2012; Poh Chua et al., 2022; Schenk & Fremouw, 2012). Naast onderzoek dat expliciet het transactionele copingmodel van Lazarus en Folkman (1984) toepast, bestaat er ook empirisch onderzoek naar slachtofferschap van online criminaliteit dat coping beschrijft in een bredere context. Dergelijke copingstrategieën omvatten onder andere iemand in vertrouwen nemen over wat er gebeurd is, het beperken van activiteiten zoals het gebruik van sociale media, het confronteren van de dader of het zoeken van hulp bij een hulpverlener (O'Malley, 2023; Worsley et al., 2017). De volgende paragraaf zal ingaan op een van deze gebieden, namelijk het hulpzoekgedrag van slachtoffers.

2.3. Hulpzoekgedrag

Net als slachtoffers van traditionele criminaliteit kunnen slachtoffers van online criminaliteit terecht bij een breed scala aan personen of organisaties voor hulp en/of informatie. Informele partijen omvatten onder andere familieleden, vrienden, kennissen of collega's (De Kimpe et al., 2020; Fissel, 2021; Pereira et al., 2016). Daarnaast zijn er diverse formele organisaties waarbij slachtoffers terecht kunnen, zoals de politie, slachtofferorganisaties, de (geestelijke) gezondheidszorg, crisishulplijnen, financiële instituten, verzekeraars, IT-experts, consumentenorganisatie, sociale mediaplatforms, juridisch adviseurs en gerechtsdeurwaarders (bijv. Fissel, 2021; Pereira et al., 2016; Pijlman et al., 2025; Smith, 2008; Van Leuken & Van 't Hoff-de Goede, 2025; Voce & Morgan, 2025). Dat slachtoffers bij meerdere organisaties terecht kunnen, kan ook een negatief effect hebben. Zo zou het grote aantal beschikbare organisaties het vermogen van slachtoffers om aangifte te doen belemmeren, omdat organisaties regelmatig geen verantwoordelijkheid nemen en slachtoffers vervolgens van het kastje naar de muur worden gestuurd (ook wel het 'draaimolen-effect' genoemd) (Button et al., 2009). Dit kan de gevolgen die slachtoffers al ervaren, verergeren en hen opnieuw traumatiseren (Button & Cross, 2017).

Uit eerder onderzoek is gebleken dat slachtoffers van online fraude in Nederland (*n*=1.778) het vaakst contact en/of informatie zochten met/bij de politie (25%), de ontvanger van het geld[2] (23%) en de bank waar zij bankierden (19%). Het minst vaak zochten zij contact en/of informatie bij hun verzekeraar (anders dan rechtsbijstand) (0.4%), Slachtofferhulp Nederland (1%) en een civiele rechtsvertegenwoordiger (1%). Ook zocht een kwart van de slachtoffers bij geen enkele partij contact of informatie. Potentiële slachtoffers (*n*=6.366) – internetgebruikers die (nog) geen slachtoffer van online fraude zijn geworden – zouden in het geval van slachtofferschap naar eigen zeggen het vaakst contact opnemen met of informatie zoeken bij de politie (79%), hun bank (74%) en de Fraudehelpdesk (56%). Het minst vaak zouden zij contact en/of informatie zoeken bij een civiele rechtsvertegenwoordiger (3%), Slachtofferhulp Nederland (4%) of hun verzekeraar (9%) (Van Leuken & Van 't Hoff-de Goede, 2025).

Naast de dertien voorgelegde partijen werden aanvullende organisaties genoemd waar slachtoffers zich naar aanleiding van de fraude hebben gemeld of waar potentiële slachtoffers in geval van slachtofferschap zich zouden melden, waaronder justitie, juridische partijen zoals het Juridisch Loket, toezichthoudende instanties zoals de Autoriteit Consument & Markt (ACM), de Autoriteit Financiële Markten (AFM) en de Autoriteit Persoonsgegevens, telecomproviders, cybersecuritybedrijven zoals Fox-IT, computerwinkels, de Kamer van Koophandel en partijen betrokken bij een aankoop, zoals de webshop, leverancier, fabrikant of het betrokken postorderbedrijf. Ook hebben slachtoffers zich gemeld bij de organisatie die volgens hen verantwoordelijk zou zijn voor het uitlekken van hun gegevens. Verder werden aanvullende partijen genoemd die zich inzetten om de belangen van slachtoffers of internetgebruikers te beschermen, waaronder NietBezorgd en Veiliginternetten.nl (Van Leuken & Van 't Hoff-de Goede, 2025a).

Uit ander Nederlands onderzoek is gebleken dat ondernemers die slachtoffer werden van ransomware (*n*=189) het vaakst hulp zochten bij een cybersecuritybedrijf of IT-leverancier (61%), de politie (18%) en de Fraudehelpdesk (13%). Niet-slachtoffers (*n*=2.496) zouden in het geval van slachtofferschap naar eigen zeggen het vaakst contact opnemen met de politie (92%), een financiële instelling (47%) of de Fraudehelpdesk (42,4%). Andere partijen waar slachtoffers hulp hebben gezocht betroffen een verzekeringsmaatschappij, de autoriteit persoonsgegevens, No More Ransom, Slachtofferhulp en overige partijen (Matthijsse et al., 2025b). In Australisch onderzoek onder slachtoffers van ransomware (*n*=308) zijn aanvullende hulpbronnen naar voren gekomen, waaronder informele hulp van vrienden of familieleden een internet serviceprovider, telecomprovider, een consumentenorganisatie, de advocatuur, dokters, hulpverleners in de mentale gezondheidszorg of maatschappelijk werkers, en mediaorganisaties. Deze groep slachtoffers zocht het vaakste hulp of advies bij een vriend of familielid

[2] Ook wel de begunstigde rekeninghouder genoemd. Onderzoek laat zien dat dit zowel de daadwerkelijke fraudeurs als geldezels kunnen zijn (van Leuken & Van 't Hoff-de Goede, 2024; Van Leuken & Van 't Hoff-de Goede, 2024b).

(29%), gevolgd door een internet service provider (14%), een financiële instelling (14%), en het Australian Cyber Security Centre (12%) (Voce & Morgan, 2022).

2.4. Het gebruik van online advertenties gericht op online criminaliteit en slachtofferschap

Binnen de wetenschap is er veel aandacht uitgegaan naar de vraag in hoeverre berichtgeving het gedrag van individuen kan beïnvloeden, bijvoorbeeld op het gebied van gezondheid of veiligheid (zie bijvoorbeeld Hancock et al., 2020; Mollen et al., 2017; Rosenblatt et al., 2018). Ook op het gebied van online criminaliteit kan online berichtgeving worden ingezet als preventiemiddel tegen dader- of slachtofferschap (Wortley & Prichard, 2023). Eerder onderzoek heeft bijvoorbeeld gekeken naar waarschuwingen van phishingwebsites, waarschuwingen dat het delen van persoonlijke informatie nadelige gevolgen kan hebben voor de privacy van de individu, of waarschuwingen die bedoeld zijn om slachtofferschap van online fraude te voorkomen (zie bijvoorbeeld Carpenter et al., 2014; Silic & Back, 2017; Wang et al., 2022). Met betrekking tot daderschap van online criminaliteit is onderzoek verricht naar het gebruik van surveillance banners of warning banners, bijvoorbeeld om te signaleren dat een website of systeem wordt gemonitord of om daders te waarschuwen dat bepaald gedrag strafbaar is of negatieve gevolgen kan hebben (zie bijvoorbeeld Maimon et al., 2014; Prichard et al., 2022; Stockman, 2014; Testa et al., 2017; Vetterl, 2020; Wilson et al., 2015).

Binnen dit bredere onderzoeksveld is in enkele studies onderzocht in hoeverre online advertenties specifiek kunnen worden ingezet om daders of slachtoffers van online criminaliteit te bereiken, net als in het huidige onderzoek (zie bijvoorbeeld Bekkers et al., 2022; Moneva et al., 2022; Moneva & Leukfeldt, 2024; Pijlman & Burgmeijer, 2024). Met betrekking tot daderschap onderzochten Bekkers et al. (2022) bijvoorbeeld of advertenties op Instagram gebruikt konden worden om het bewustzijn van jongeren over de risico's van geldezelen te verhogen. De onderzoekers ontwikkelden drie advertenties, gericht op een luxe levensstijl, normalisering of neutralisatie. Jongeren die op de contact-knop klikten werden vervolgens doorgeleid naar een van twee voorlichtingspagina's: een pagina waarin gewaarschuwd werden voor de strafbaarheid en gevolgen van het optreden als geldezel (afschrikking) en een pagina waarin jongeren gestimuleerd worden om op een legale manier geld te verdienen. Tijdens de advertentiecampagnes hebben bijna 100.000 Instagramgebruikers de advertenties gezien. Hiervan klikte 0,25% in de eerste campagne op de advertentie en 2,04% in de tweede campagne. De meeste interactie werd gegenereerd door de advertentie gericht op een luxe levensstijl (doorklikratio van respectievelijk 0,30% en 2,36%), en door de landingspagina die jongeren motiveerde om op een legale manier geld te verdienen (Bekkers et al., 2022).

Een aantal andere onderzoeken richtten zich op het gebruik van Google Ads om potentiële daders te ontmoedigen een DDoS-aanval uit te voeren (Collier et al., 2019; Moneva et al., 2022; Moneva & Leukfeldt, 2023). Wanneer gebruikers in Google zochten op zoekwoorden die verband hielden met DDoS-aanvallen, kregen zij verschillende waarschuwingsberichten te zien via Google-advertenties. Na het aanklikken van deze advertenties werden zij doorverwezen naar specifieke landingspagina's. Collier et al. (2019) constateerden dat de stijging van het aantal DDoS-aanvallen in het Verenigd Koninkrijk tijdens de campagne afvlakte. Dit effect werd echter niet gevonden in andere Europese landen of in de Verenigde Staten (Collier et al., 2019). Ook in vervolgonderzoek naar het gebruik van Google Ads om DDoS-aanvallen te voorkomen werd geen eenduidig bewijs gevonden voor een afschrikwekkend effect (Moneva et al., 2022; Moneva & Leukfeldt, 2023). In een advertentiecampagne werd gevarieerd met en afschrikkende advertentieboodschap, sociale boodschap, informatieve boodschap en heroriënterende boodschap. Daarnaast werd gevarieerd tussen een formele landingspagina ondersteund door de Nationale politie en een informele landingspagina ondersteund door ESL Play, een e-sports bedrijf. De gemiddelde doorklikratio van deze advertentiecampagne was 6,2%. De interactie met de verschillende advertenties varieerde, waarbij de sociale advertentie ("DDoS verpest het voor iedereen") bijvoorbeeld tot significant meer interactie (9,3%) leidde dan de afschrikkende advertentie (7,6%) ("Een DDoS aanval is strafbaar"). Er werden geen verschillen gevonden tussen beide landingspagina's (Moneva et al., 2022). In een andere studie is vervolgens vergeleken of verschillende advertentiecampagnes gericht op DDoS-aanvallen, remote-access tools en hacken hebben geleid tot een afname in het aantal aanvallen in twaalf Europese landen (Moneva & Leukfeldt, 2023). De effecten op de korte en lange termijn liepen uiteen. Zo leidde de tweede advertentiecampagne in Nederland tot een toename van DDoS-aanvallen van 29,6% op de korte termijn, terwijl in Portugal de derde advertentiecampagne resulteerde in een significante afname van 36,1%. In overige campagnes en landen was sprake van niet-significante resultaten (Moneva & Leukfeldt, 2023).

Voor zover bekend heeft slechts één onderzoek online advertenties gebruikt om slachtoffers van online criminaliteit te bereiken. In dit onderzoek werden twee advertentiecampagnes ingezet op Snapchat om hulpzoekgedrag te stimuleren onder respectievelijk slachtoffers van Image-Based Sexual Harassment (IBSH) en Image-Based Sexual Abuse (IBSA) (Pijlman & Burgmeijer, 2024). In de advertenties werd gevarieerd in drie factoren: het wel of niet benoemen van gevoelens van schaamte, het wel of niet benoemen van de hulporganisatie en het wel of niet gebruikmaken van taalgebruik gericht op jongeren. Dit resulteerde in acht verschillende advertenties. In dit onderzoek kwam naar voren dat 2,93% van de Snapchatgebruikers interactie had met de advertenties voor IBSH en 3,79% met de advertenties voor IBSA. De onderzoekers rapporteerden een significante toename in de interactie met advertenties waarin gevoelens van schaamte expliciet benoemd werden (Pijlman & Burgmeijer, 2024).

Samengenomen laten deze onderzoeken dat online advertenties een potentieel bruikbaar middel kunnen zijn om doelgroepen die betrokken zijn bij online criminaliteit te bereiken. Hoewel de advertenties veel interactie genereren en in sommige gevallen bewustwording of hulpzoekgedrag lijken te stimuleren, is het bewijs voor daadwerkelijk gedragsverandering vooralsnog beperkt en niet eenduidig. Er is bovendien nog weinig onderzoek gedaan naar het bereiken van slachtoffers van online criminaliteit. Dit onderstreept het belang van vervolgonderzoek naar de omstandigheden waarin online advertenties zouden kunnen bijdragen aan het helpen van slachtoffers van van online criminaliteit.

Hoofdstuk 3: Methodologie

Om een antwoord te geven op de hoofd- en deelvragen (zie paragraaf 1.3) is het onderzoeksproject ingedeeld in drie deelstudies. In het huidige hoofdstuk zullen de onderzoeksmethoden van elke deelstudie uiteengezet worden

3.1. Deelstudie 1: Vragenlijstonderzoek

Als onderdeel van deelstudie 1 zijn twee online vragenlijsten ontwikkeld en uitgezet onder slachtoffers van online fraude en ransomware.

3.1.1. Steekproef

3.1.1.1. Online fraude

Het doel van deelstudie 1 was om Nederlandse burgers te bereiken die slachtoffer zijn geworden van online fraude. Hiervoor is gebruikgemaakt van het Research Panel van onderzoeksbureau Ipsos I&O. Het I&O Research Panel bestaat uit meer dan 37.000 panelleden. Panelleden worden geworven via steekproeven uit bijvoorbeeld (gemeentelijke) bevolkingsregisters en adresbestanden. Panelleden ontvangen voor elk ingevuld onderzoek spaarpunten die ze kunnen inwisselen voor een Bol-tegoedbon of een donatie aan een goed doel.

Tussen 28 januari en 10 februari 2025 zijn 6.700 burgers in het Research Panel uitgenodigd om deel te nemen aan het onderzoek, met een goede verdeling naar leeftijd, geslacht, opleiding en regio. Gedurende de dataverzamelingsperiode zijn naast de initiële uitnodiging, twee rappels uitgestuurd. Om de juiste doelgroep te bereiken bestond de vragenlijst uit twee screeningsvragen. Ten eerste werden respondenten aan het begin van de vragenlijst gevraagd om voor negen vormen van online fraude aan te geven of ze dit in de afgelopen twee jaar hadden meegemaakt. Respondenten hadden daarnaast nog de mogelijkheid om een tiende optie aan te vinken, namelijk dat ze slachtoffer zijn geworden van een andere vorm van oplichting. De respondenten die ‘ja’ hadden aangevinkt op de fraudevormen in opties 1 t/m 9 werden doorgestuurd naar de tweede screeningsvraag. In de tweede screeningsvraag werd aan respondenten voor elke fraudevorm die ze hadden aangevinkt gevraagd welke situatie op hen van toepassing was, waarbij ze konden kiezen uit “Ik ben hierdoor geld of goederen verloren. Ik heb dit geld of deze goederen niet teruggekregen”, “Ik ben hierdoor geld of goederen verloren. Ik heb dit geld of deze goederen inmiddels (voor een deel) teruggekregen” of “Ik ben hierdoor geen geld of goederen verloren, het is gebleven bij een poging tot oplichting”. Respondenten die de eerste twee opties hadden aangevinkt, werden doorgestuurd naar de vragenlijst, om zo poging tot online fraude eruit te filteren.

In totaal zijn 2.937 panelleden begonnen aan de screeningsvragen (response rate: 43,8%). Na het eruit filteren van de respondenten die volgens de screeningsvragen geen slachtoffer waren van online fraude (*n*=2.393), respondenten die langer dan twee jaar geleden slachtoffer waren geworden blijkens de opmerkingen (*n*=1) en speeders[3] (*n*=9), bestaat de uiteindelijke steekproef uit 535 respondenten. De achtergrondkenmerken van de respondenten zijn opgenomen in Tabel 3.1.

Tabel 3.1 Achtergrondkenmerken van burgers (*n*=535)

	n	**%**
Geslacht	**535**	
Man	274	51,2%
Vrouw	261	48,8%
Leeftijd	**535**	
18 t/m 34	110	20,6%
35 t/m 49	125	23,4%
50 t/m 64	131	24,5%
65+	169	31,6%
Opleiding	**535**	
Laag	139	26,0%
Middelbaar	194	36,3%
Hoog	202	37,8%
Werksituatie	**535**	
Werkzaam in loondienst	283	52,9%
Niet werkzaam (bijv. arbeidsongeschikt, gepensioneerd)	217	40,6%
Studerend/schoolgaand	24	4,5%
Anders	11	2,1%
Huishoudsamenstelling	**535**	
Alleenstaand	144	26,9%
Alleenstaand (zonder partner) met kinderen	28	5,2%
Gehuwd/samenwonend zonder thuiswonende kinderen	222	41,5%
Gehuwd/samenwonend met thuiswonende kinderen	106	19,8%
Wonend bij ouder(s)/verzorger(s)	29	5,4%
Anders	4	0,7%
Weet niet/wil niet zeggen	2	0,4%
Jaarinkomen (bruto) huishouden	**530**	
Minimum (minder dan €14.100)	28	5,3%
Beneden modaal (€14.100 tot €29.500)	72	13,6%

[3] Respondenten die 1/3 van de mediaan of minder lang hebben gedaan over het invullen van de vragenlijst. In het huidige onderzoek is dit gebaseerd op de respondenten die de screeningsvragen succesvol hebben doorlopen (*n*=544). Op basis van de verdeling van de responstijd in minuten (*M* = 112,71; *SD* = 653,64; *Mdn* = 10), definieerden we als speeders de respondenten met een responstijd van 3 minuten of minder. Er is geen bovengrens toegepast, omdat de verdeling suggereert dat sommige respondenten de vragenlijst gepauzeerd hebben en op een later tijdstip invulden.

	n	%
Bijna modaal (€29.500 tot €36.500)	65	12,3%
Modaal (€36.500 tot €43.500)	92	17,4%
Tussen 1 en 2 keer modaal (€43.500 tot €73.000)	119	22,5%
Twee keer modaal (€73.000 tot €87.100)	46	8,7%
Meer dan 2 keer modaal (€87.100 of meer)	52	9,8%
Weet niet/wil niet zeggen	56	10,6%

3.1.1.2. Ransomware

Het doel was daarnaast om Nederlandse ondernemers te bereiken die ooit slachtoffer zijn geworden van ransomware. Om dit te doen is gebruikgemaakt van het Research Panel en het Ondernemerspanel van onderzoeksbureau Ipsos I&O. Het I&O Research Panel bestaat uit ongeveer 2.700 ondernemers. Het ondernemerspanel bestaat uit ongeveer 4.200 ondernemers, die grotendeels geworven worden via steekproefonderzoek (Ipsos I&O, z.d.).

Tussen 28 januari en 10 februari 2025 zijn alle ondernemers in het Research Panel (*n*=2.640) en de ondernemers in het Ondernemerspanel die in een eerder onderzoek hadden aangegeven slachtoffer te zijn geweest van ransomware (Matthijsse et al., 2025a) en nog actief panellid waren (*n*=187) uitgenodigd om deel te nemen aan het onderzoek. Gedurende de dataverzamelingsperiode zijn naast de initiële uitnodiging, twee rappels (herinneringen) uitgestuurd. Op peildatum 3 februari 2025 bleek de respons echter achter te blijven (*n*=69). In verband met deze tegenvallende respons zijn tussen 3 januari en 10 februari 2025 alsnog de andere ondernemers in het Ondernemerspanel benaderd (*n*=5.055). Dit leverde 23 extra respondenten op. Om de respons nog verder te verhogen is op 13 februari 2025 een extra rappel verstuurd aan de ondernemers en een extra incentive toegevoegd in de vorm van het verloten van VVV-cadeaukaarten. De dataverzameling is beëindigd op 15 februari 2025. Uiteindelijk zijn in totaal 7.882 panelleden uitgenodigd om deel te nemen aan het onderzoek.

Om de juiste doelgroep te bereiken bestond de vragenlijst uit twee screeningsvragen. Ten eerste werd respondenten aan het begin van de vragenlijst gevraagd om voor acht vormen van cybercriminaliteit (waaronder phishing, CEO-fraude en ransomware) aan te geven of ze dit ooit (of een poging hiertoe[4]) in hun bedrijf hebben meegemaakt. Ransomware werd hierbij gedefinieerd als “de bestanden, gegevens of appara(a)t(en) van uw bedrijf werden geblokkeerd of versleuteld en er werd om losgeld gevraagd om hier weer toegang tot te krijgen”. De respondenten die hebben aangegeven ransomware te hebben meegemaakt is vervolgens een tweede screeningsvraag gesteld waarbij verschillende vormen van ransomware werden voorgelegd en aan de respondenten werd gevraagd welke variant ze hadden meegemaakt. De respondenten

[4] Een poging is hierbij expliciet vermeld om geen respondenten uit te sluiten die wel slachtoffer zijn geworden, maar bijvoorbeeld geen geld hebben betaald of van wie geen geld is gestolen.

die de optie “niet van toepassing, dit is mij niet overkomen” aanvinkten werden vervolgens doorgestuurd naar het einde van de vragenlijst. In tegenstelling tot de vragenlijst voor online fraude, is slachtofferschap van ransomware niet beperkt tot de afgelopen 2 jaar, omdat de verwachting was dat de groep ransomware slachtoffers kleiner zou zijn en het doel was om zoveel mogelijk slachtoffers te bereiken.

In totaal zijn 2.129 panelleden begonnen aan de screeningsvragen (response rate: 27%). Na het eruit filteren van de respondenten die volgens de screeningsvragen geen slachtoffer waren van ransomware (*n*=2.018) en speeders[5] (*n*=4), bestaat de uiteindelijke steekproef uit 107 respondenten. De bedrijfskenmerken van de respondenten zijn opgenomen in Tabel 3.2.

Tabel 3.2 Bedrijfskenmerken van ondernemers (*n*=107).

	n	**%**
Grootte	**107**	
Zzp’er (1 werkzame persoon)	42	39,3%
Micro (2-9 werkzame personen)	42	39,3%
Klein (10-49 werkzame personen)	17	15,9%
Midden (50-250 werkzame personen)	6	5,6%
Groot (>250 werkzame personen)	0	0,0%
Sector	**107**	
Landbouw/visserij	3	2,8%
Industrie, bouw en nutsbedrijven	14	13,1%
Handel en logistiek, horeca	17	15,9%
Financiële en zakelijke dienstverlening	43	40,2%
Overheid, onderwijs, zorg en overig	30	28,0%
Jaaromzet	**107**	
Minder dan €100.000	34	31,8%
€100.000 tot €500.000	33	30,8%
€500.000 tot €1.000.000	8	7,5%
€1.000.000 tot €2.500.000	11	10,3%
€2.500.000 tot €5.000.000	5	4,7%
Meer dan €5.000.000	6	5,6%
Zeg ik liever niet/weet ik niet	10	9,3%

[5] Respondenten die 1/3 van de mediaan of minder lang hebben gedaan over het invullen van de vragenlijst. In het huidige onderzoek is dit gebaseerd op de respondenten die de screeningsvragen succesvol hebben doorlopen (n=111). Op basis van de verdeling van de responstijd in minuten (*M* = 567,98; *SD* = 2195,53; *Mdn* = 13), definieerden we als speeders de respondenten met een responstijd van 4 minuten of minder. Er is geen bovengrens toegepast, omdat de verdeling suggereert dat sommige respondenten de vragenlijst gepauzeerd hebben en op een later tijdstip invulden.

3.1.2. Meetinstrument

Voor deelstudie 1 zijn twee vergelijkbare vragenlijsten opgesteld voor slachtoffers van online fraude (bijlage 1) en slachtoffers van ransomware (bijlage 2). De vragen en antwoordopties zijn gedeeltelijk overgenomen uit eerder vragenlijstonderzoek naar slachtofferschap (o.a. Akkermans et al., 2024; Borwell, 2025; Matthijsse et al., 2025a; Van Leuken & Van 't Hoff-de Goede, 2025). In de vragenlijsten is gevraagd naar de gevolgen van slachtofferschap, slachtofferbehoeften en (online) hulpzoekgedrag. Voor het verzamelen van de door de respondenten gebruikte zoektermen zijn in de vragenlijsten twee vragen opgenomen. De eerste vraag werd alleen aan slachtoffers gesteld die hadden aangegeven online gezocht te hebben naar informatie of ondersteuning. Hen werd gevraagd om terug te denken aan het moment dat de oplichting of versleuteling van data plaatsvond en op te schrijven welke zoektermen ze hadden ingevoerd in de zoekmachine. Voor elke losse zoekopdracht (bestaande uit losse woorden, combinaties van woorden of zinnen) was een apart invulveld beschikbaar. Om te stimuleren dat respondenten alle zoektermen die ze zich konden herinneren invulden, kregen respondenten die wilden doorklikken naar de volgende vraag de volgende mededeling te zien: "Vaak gebruiken mensen verschillende zoektermen, of combinaties van zoektermen. Zijn er nog andere zoektermen die u gebruikt heeft om te zoeken naar informatie of hulp?". Zij konden vervolgens aanvullende antwoorden invullen of doorgaan naar de volgende vraag. De tweede enquêtevraag werd gesteld aan alle respondenten, inclusief respondenten die niet online hebben gezocht toen ze slachtoffer werden. Respondenten werd gevraagd om zich voor te stellen dat ze nu nogmaals geconfronteerd zouden worden met online fraude of ransomware en welke zoektermen ze dan zouden invoeren in een zoekmachine. Net als bij de eerdere enquêtevraag kregen respondenten losse antwoordvelden te zien en volgde een vergelijkbare mededeling als bij de eerste enquêtevraag.

3.1.3. Analyse

De data zijn opgeschoond en geanalyseerd in IBM SPSS Statistics 28.0.1.0 (IBM, 2021). Voor de analyse is gebruikgemaakt van beschrijvende statistieken. De resultaten zijn beschreven in hoofdstuk 4.

3.2. Deelstudie 2: Google zoekwoordplanner

3.2.1. Zoekopdrachten selecteren

Het doel in deelstudie 2 was om a) meer inzicht te krijgen in hoe vaak de zoektermen die slachtoffers in deelstudie 1 hebben ingevuld gebruikt worden via Google, en b) of er gerelateerde zoektermen geïdentificeerd kunnen worden die in Google gebruikt zijn. Deze informatie kon vervolgens gebruikt worden voor het uitzetten van de Google-advertenties (deelstudie 3).

De verschillende zoekopdrachten die de slachtoffers in deelstudie 1 hebben ingevuld in de open antwoorden zijn samengevoegd in een Excel-bestand. Hierbij zijn 4 lijsten ontwikkeld:

1. Zoekopdrachten die daadwerkelijk gebruikt zijn door slachtoffers van *online fraude*.
2. Zoekopdrachten die slachtoffers van *online fraude* zouden gebruiken als ze opnieuw slachtoffer zouden worden.
3. Zoekopdrachten die daadwerkelijk gebruikt zijn door slachtoffers van *ransomware*.
4. Zoekopdrachten die slachtoffers van *ransomware* zouden gebruiken als ze opnieuw slachtoffer zouden worden.

Vervolgens zijn enkele stappen genomen om de data op te schonen:

1. Het verbeteren van typfouten.
2. Het verwijderen van speciale tekens.
   Speciale tekens zoals een vraagteken, uitroepteken of ampersand zijn uit de zoekopdrachten verwijderd omdat de Google zoekwoordplanner deze niet accepteert.

Om tot een bruikbare selectie aan zoekopdrachten te komen voor de zoekwoordplanner, zijn vervolgens alle zoektermen nagelopen op een aantal exclusiecriteria[6]. De volgende aspecten zijn eruit gefilterd:

1. Respondenten die in de open antwoordvelden hebben aangegeven dat ze niet (meer) weten wat ze hebben ingevuld of zouden invullen.
2. Respondenten die in de open antwoordvelden geen zoektermen hebben ingevuld.
   Het gaat hier bijvoorbeeld om respondenten die hebben aangegeven dat ze niet zouden zoeken, iets anders zouden (zoals een expert om hulp vragen) of overige opmerkingen (zoals “er viel niet meer zoveel in te typen, het scherm was rood met de boodschap: 'you are encrypted'”).
3. Duplicaten.
   Deze kunnen aanwezig zijn in de data omdat verschillende respondenten dezelfde zoekopdracht hebben ingevoerd. Het gaat hierbij om zoekopdrachten die precies hetzelfde geschreven zijn. Gevallen waarbij er een verschil was in het gebruik van een hoofdletter zijn ook als een duplicaat samengenomen. Zoektermen die op elkaar lijken maar bijvoorbeeld verschillen door het gebruik van tussenvoegsels zijn niet beschouwd als duplicaten.
4. Zoekopdrachten bestaande uit één woord.

[6] Noot dat voor fraude ook zoektermen meegenomen zijn die niet zozeer spreken van online fraude of oplichting, maar alleen van fraude of oplichting.

Dit is gedaan vanuit de overweging dat één woord te kort en abstract is om tot relevante resultaten te komen.

5. Zoekopdrachten die op basis van de expertise van de onderzoekers naar verwachting geen relevante resultaten opleveren voor potentiële slachtoffers.
   Hierbij kunnen een aantal redenen onderscheiden worden:
   A. De zoektermen hebben geen betrekking op ransomware (voor ondernemers) of online fraude (voor burgers).
      Dit betekent ook dat zoektermen gerelateerd aan online fraude die door slachtoffers van ransomware ingevuld zijn, geëxcludeerd zijn.
   B. De zoektermen kunnen potentieel te maken hebben met ransomware of online fraude, maar zijn te algemeen.
      Voorbeelden hiervan zijn “Bestanden naar pdf zetten” of “Backups terug zetten”. Uitzondering hierop zijn concrete cybercrime-gerelateerde termen als “mijn computer is gehackt”, of “ik ben gehackt” omdat dit beschrijvingen van symptomen kunnen zijn die slachtoffers alsnog kunnen leiden naar de juiste hulp voor ransomware of online fraude. De mogelijkheid bestaat immers dat slachtoffers niet precies weten te beschrijven wat hen is overkomen of welke hulp ze zoeken, maar dit wel in meer algemene terminologie hebben beschreven.
   C. De zoektermen hebben betrekking op een link, code, naam van een bedrijf, telefoonnummer of dergelijke, maar respondenten hebben hierbij geen naam vermeld.
      Voorbeelden hiervan zijn “emailadres van de afzender”, “het telefoonnummer” of “De link waarop ik moest klikken”.
   D. De zoektermen hebben betrekking op ransomware (voor ondernemers) of online fraude (voor burgers), maar zijn te generiek en hebben niet per definitie betrekking op slachtofferschap.
      Hierbij kan gedacht worden aan “ransomware aanval”, “gevaar ransomware” of “oplichting internet”. Concrete vormen van oplichting vormen hier de uitzondering op, zoals “vliegticket fraude”.
   E. De zoektermen hebben betrekking op ransomware (voor ondernemers) of online fraude (voor burgers), maar zijn zo specifiek dat deze zelfs met enige aanpassingen niet relevant zijn voor de zoektermplanner, bijvoorbeeld omdat een naam van een specifiek merk wordt genoemd. Zoektermen die betrekking hebben op landen, platformen (e.g. Vinted, Marktplaats, WhatsApp, Vrbo) of een type product (e.g. festivaltickets) zijn wel meegenomen in de selectie.

Dit proces van opschoning en selectie heeft voor online fraude geleid tot in totaal 283 zoektermen, waaronder 73 zoektermen die daadwerkelijk door slachtoffers zijn gebruikt (zie ook Figuur 1 in bijlage 3)

en 210 zoektermen die slachtoffers zouden gebruiken in het hypothetische geval dat ze opnieuw slachtoffer zouden worden (zie ook Figuur 2 in bijlage 3). Bij 7 zoektermen gerelateerd aan online fraude is de formulering aangepast omdat de zoektermen wel potentieel relevant, maar te specifiek waren. Zo is "Naam webshop product niet ontvangen" aangepast naar "webshop product niet ontvangen". Voor ransomware heeft dit selectieproces geleid tot in totaal 86 unieke zoektermen, waaronder 9 zoektermen die daadwerkelijk door slachtoffers zijn gebruikt (zie ook Figuur 3 in bijlage 3) en 77 zoektermen die slachtoffers in het hypothetische geval dat ze opnieuw slachtoffer zouden worden zouden gebruiken (zie ook Figuur 4 in bijlage 3).

Omdat er tussen de daadwekelijke en hypothetische zoektermen tevens overlap kan zitten, zijn over het totaal nogmaals duplicaten geïdentificeerd en verwijderd. Hiermee is het totaal aantal zoektermen dat gebruikt is voor de zoektermplanner voor online fraude geëindigd op 261 en voor ransomware op 84.

3.2.2. Gebruik van de zoekwoordplanner

Om meer inzicht te krijgen in de mate waarin de zoekopdrachten uit deelstudie 1 zijn gebruikt in Google en gerelateerde zoektermen te identificeren om zo tot een complete selectie te komen, is de selectie aan zoekopdrachten uit deelstudie 1 (ransomware = 84, online fraude = 261) vervolgens ingevoerd in de Google zoekwoordplanner tussen 14 mei en 15 mei 2025. De Google zoekwoordplanner maakt het mogelijk om onderzoek te doen naar zoekwoorden, bijvoorbeeld door middel van suggesties voor zoekwoorden en schattingen van maandelijkse zoekopdrachten. In de Google zoekwoordplanner werden enkele criteria aangehouden, namelijk:

- Locatie: Nederland
- Periode: Laatste 12 maanden (Mei 2024 – April 2025)
- Focus op Google, niet op Google en partners.
- Includeren van zowel merken als niet-merken[7]
- Taal: Nederlands.

De zoekwoordplanner geeft voor elke ingevulde zoekopdracht een aantal gegevens weer:

- Het **gemiddelde aantal maandelijkse zoekopdrachten**, i.e. de populariteit van een zoekopdracht. Het gaat hierbij om een ruime schatting, zo wordt onderscheid gemaakt tussen 0-10, 10-100 en 100-1000.

[7] Hierbij worden zowel merkgerelateerde termen (zoals bijv. een merk- of productnaam) als niet-merkgerelateerde termen (alleen de productcategorie) meegenomen.

- De **driemaandelijkse verandering in zoektrends** in een percentage, waarbij de gegevens van de laatste maand vergeleken worden met de gegevens van de twee maanden daarvoor. De **jaar-op-jaar verandering** vergelijkt het maandelijkse zoekvolume van de afgelopen maand met dezelfde maand van het voorgaande jaar (in dit geval 2024).
- De kosten voor het gebruik van een zoekopdracht in een Google-advertentie, waarbij onderscheid gemaakt wordt tussen:
    - **"Bovenste paginabod (laag bereik)",** wat het laagste bereik toont van wat adverteerders in het verleden hebben betaald voor het bovenste paginabod van een trefwoord, gebaseerd op de locatie en zoeknetwerkinstellingen.
    - **"Bovenste paginabod (hoog bereik)",** wat het hoogste bereik toont van wat adverteerders in het verleden hebben betaald voor het bovenste paginabod van een trefwoord, gebaseerd op de locatie en zoeknetwerkinstellingen.
- **Concurrentieniveau**, wat gaat om hoe concurrerend advertentieplaatsing is voor een zoekwoord, specifiek voor de locatie en de zoeknetwerkinstellingen. Het concurrentieniveau kan variëren tussen laag, gemiddeld of hoog en wordt bepaald door het aantal adverteerders dat biedt op elk trefwoord in verhouding tot alle trefwoorden in Google.
- Indien beschikbaar worden **suggesties voor vergelijkbare trefwoorden** gegeven. Deze trefwoorden zijn tevens voorzien van alle hiervoor genoemde informatie.

Al deze informatie is opgeslagen in Microsoft Excel. Voor online fraude zijn alle 261 zoektermen uit de vragenlijst ingevoerd in de Google zoekwoordplanner. Zes zoektermen bleken niet toegestaan volgens het beleid van Google en zijn alsnog geëxcludeerd.[8] Op basis van de zoektermen werden er 1714 gerelateerde zoektermen weergegeven door Google. Ook in de voorgestelde zoektermen heeft een verdere selectie plaatsgevonden, vergelijkbaar met de selectie die heeft plaatsgevonden onder paragraaf 3.2.1. Om de lijst op te schonen zijn eerst alle duplicaten verwijderd binnen de voorgestelde zoektermen (n=912), evenals de zoektermen die al in de oorspronkelijke lijst met zoektermen uit de vragenlijst stonden (n=42). Dat deze duplicaten verschenen is het gevolg van het feit dat in de Google zoekwoordplanner slechts 10 zoektermen tegelijk ingevuld kunnen worden. Dit leverde een selectie van 760 zoektermen op. Deze zoektermen zijn vervolgens nagelopen op overige exclusiecriteria. Dit heeft tot een uiteindelijke selectie geleid van 652 voorgestelde zoektermen voor online fraude, bovenop de 255 zoektermen uit de vragenlijst (totale n=907).

[8] Dit betreffen "bitcoin fraude", "bitcoin hoax", "bitcoin oplichting", "onbetrouwbare sites checken", "oplichting festival ticket" en "oplichting via bitcoin".

Voor ransomware zijn 84 zoektermen uit de vragenlijst ingevoerd in de Google zoekwoordplanner, maar twee zoektermen bleken niet toegestaan volgens het beleid van Google en zijn alsnog geëxcludeerd.[9] Op basis van de zoektermen werden er 41 voorgestelde zoektermen weergegeven door Google. In de suggesties voor vergelijkbare trefwoorden heeft een verdere selectie plaatsgevonden, vergelijkbaar met de selectie die heeft plaatsgevonden onder paragraaf 3.2.1. Om de lijst op te schonen zijn eerst alle duplicaten verwijderd binnen de voorgestelde zoektermen (n=2), evenals de zoektermen die al in de oorspronkelijke lijst met zoektermen uit de vragenlijst stonden (n=3). Dit leverde een selectie van 36 zoektermen op. Deze zoektermen zijn vervolgens nagelopen op overige exclusiecriteria. Dit heeft tot een uiteindelijke selectie geleid van 33 voorgestelde zoektermen voor ransomware, bovenop de 82 zoektermen uit de vragenlijst (totale n=115).

3.2.3. Analyse

De data zijn opgeschoond en geanalyseerd in Microsoft Excel. De resultaten zijn gebruikt als input voor de advertentiecampagne in deelstudie 3.

3.3. Deelstudie 3: Google Advertenties

In deelstudie 3 zijn twee advertentiecampagnes ontwikkeld voor slachtofferschap van online fraude en ransomware. Beide advertentiecampagnes waren gericht op gebruikers die reeds slachtoffers zijn geworden van online fraude of ransomware, om hen te informeren over wat ze kunnen doen en hulp te bieden.

3.3.1. Ontwerp van advertenties

Om de advertentiecampagne op te zetten is gebruikgemaakt van Google Ads, het online advertentieprogramma van Google. Wanneer gebruikers bepaalde zoektermen gebruikten in de zoekmachine gerelateerd aan online fraude of ransomware, werden korte advertenties weergegeven in de zoekresultaten. De betreffende zoektermen zijn vastgesteld in deelstudie 1 en 2.

In totaal zijn zes advertenties ontwikkeld. Gebruikers die zochten op zoekwoorden gerelateerd aan online fraude konden een van drie mogelijke advertenties zien (Tabel 3.3). Gebruikers die zochten op zoekwoorden gerelateerd aan ransomware konden evenals een van drie mogelijke advertenties zien (Tabel 3.4). Voor de achterliggende gedachte van de advertenties is gebruikgemaakt van het transactionele copingmodel (Lazarus & Folkman, 1984, zie ook hoofdstuk 2), waarbij onderscheid wordt gemaakt tussen probleemgerichte en emotiegerichte coping in stressvolle situaties. De eerste advertentie bevatte een neutrale beschrijving en diende als controlegroep. De tweede advertentie was gericht op het oplossen van

[9] Dit betreffen “losgeld bitcoin” en “ransomware wat nu”.

het probleem. De derde advertentie was gericht op het omgaan met de emotionele gevolgen van slachtofferschap.

Tabel 3.3 Advertenties gericht op slachtofferschap van online fraude

Type	Advertentie
Neutraal	Online opgelicht, wat nu? | Slachtofferhulp Nederland | Hulp na online oplichting Ad www.slachtofferhulp.nl Oplichters maken gebruik van bedrog met als doel geld te verdienen. Lees hier meer.
Probleemgerichte coping	Wat te doen bij oplichting? | Slachtofferhulp Nederland | Hulp na online oplichting Ad www.slachtofferhulp.nl Ben je online opgelicht en hierdoor geld verloren? Lees wat je kunt doen.
Emotiegerichte coping	Emotionele steun na oplichting | Slachtofferhulp Nederland | Hulp na online oplichting Ad www.slachtofferhulp.nl Online oplichting kan leiden tot negatieve emoties en stress. Wij helpen je daarbij.

Tabel 3.4 Advertenties gericht op slachtofferschap van ransomware

Type	Advertentie
Neutraal	Ransomware, wat nu? | Slachtofferhulp Nederland | Hulp na ransomware Ad www.slachtofferhulp.nl Ransomware blokkeert toegang tot bestanden in ruil voor losgeld. Lees hier meer.
Probleemgerichte coping	Wat te doen bij ransomware? | Slachtofferhulp Nederland | Hulp na ransomware Ad www.slachtofferhulp.nl Zijn je bestanden versleuteld en wordt er losgeld gevraagd? Lees wat je kunt doen.
Emotiegerichte coping	Emotionele steun na ransomware | Slachtofferhulp Nederland | Hulp na ransomware Ad www.slachtofferhulp.nl Ransomware kan leiden tot negatieve emoties en stress. Wij helpen je daarbij.

Elke keer dat gebruikers zochten naar een van de zoektermen die de advertenties triggerden, en de advertentie werd weergegeven, werd dit geteld als een *impressie*. Elke keer dat gebruikers op de advertenties klikten, werd dit geteld als een *klik*. De *doorklikratio* betreft het percentage van de gebruikers die de advertentie te zien kreeg (impressie) en hier vervolgens op geklikt heeft.

3.3.2. Landingspagina

Elke keer dat gebruikers op de advertenties klikten, werden ze doorgestuurd naar een zogeheten landingspagina. Voor de landingspagina is samengewerkt met Slachtofferhulp Nederland. Deze organisatie is gekozen omdat zij slachtoffers van verschillende vormen van criminaliteit, waaronder online

criminaliteit, informatie, emotionele steun en ondersteuning in het strafrechtelijke proces en/of krijgen van schadevergoeding bieden, wat ze een relevante partner maakt voor het huidige onderzoek. Alle advertenties gericht op online fraude leidden naar https://www.slachtofferhulp.nl/hulp-na-online-oplichting/ (zie ook bijlage 4). Alle advertenties gericht op ransomware leidden naar https://www.slachtofferhulp.nl/hulp-na-ransomware/ (zie ook bijlage 5). De inhoud van beide landingspagina's was gebaseerd op de inhoud van de oorspronkelijke website van Slachtofferhulp Nederland, met enkele aanpassingen en aanvullingen op basis van de kennis van de onderzoekers en de resultaten uit deelstudie 1. De periode van dataverzameling is afgestemd met Slachtofferhulp Nederland zodat deze niet zou overlappen met lopende of geplande campagnes van deze organisatie. Bovendien heeft Slachtofferhulp Nederland ervoor gezorgd dat zij gedurende de dataverzamelingsperiode niet zelf adverteerden op de zoektermen die in het huidige onderzoek zijn gebruikt.

3.3.3. Doelgroep

De advertentiecampagnes zijn geconfigureerd om zich te richten op gebruikers van 18 jaar en ouder (de minimumleeftijd die Google Ads hanteert) in Nederland.

3.3.4. Zoektermen

Voor de advertentiecampagnes was het doel om voor zowel online fraude als ransomware de gecombineerde zoektermen uit de vragenlijsten (deelstudie 1) als de Google zoekwoordplanner (deelstudie 2) te gebruiken. Voor de advertentiecampagne voor ransomware is dit daadwerkelijk gebeurd (n=115). Bij het configureren van de advertentiecampagne van online fraude zijn echter per abuis alleen de zoektermen uit de vragenlijst (n=255) opgenomen in de campagne en niet de zoektermen uit de zoekwoordplanner. Als gevolg hiervan zou het kunnen dat een aantal personen die bereikt hadden kunnen worden de advertentiecampagne mogelijk niet te zien hebben gekregen. We denken echter dat dit beperkt invloed heeft op de uitkomsten van het onderzoek, gezien het grote aantal zoektermen dat uit de vragenlijst over online fraude naar voren gekomen is, een groot aantal vergelijkbare (maar niet identieke) zoektermen in de vragenlijst en de zoektermplanner en het gebruik van *broad matching* in de campagnes. Bij broad matching worden de advertenties ook weergegeven voor zoekopdrachten die gerelateerd zijn aan de vooraf gedefinieerde zoektermen. Een overzicht van de zoektermen die gebruikt zijn in de advertentiecampagnes is opgenomen in bijlage 4.

3.3.5. Campagne

De online advertentiecampagnes werden tegelijkertijd gelanceerd tussen vrijdag 8 augustus en vrijdag 15 augustus 2025 voor een duur van 7 dagen (Tabel 3.5). Gedurende deze periode genereerde de advertentiecampagne voor online fraude in totaal 110.440 impressies en 831 kliks, met een doorklikratio van 0,75%. De advertentiecampagne voor ransomware genereerde in totaal 15.296 impressies en 373 kliks, met een doorklikratio van 2,44%.

Tabel 3.5 Informatie over de advertentiecampagne

Campagne	Startdatum	Einddatum	Duur (in aantal dagen)	Impressies	Kliks	Kosten (in €)	Gemiddelde kosten per klik (in €)	CTR
Online fraude	08-08-2025	15-08-2025	7	110.440	831	1.341,61	1,61	0,75%
Ransomware	08-08-2025	15-08-2025	7	15.296	373	1.196,36	3,21	2,44%

3.3.6. Analyse

De data zijn gedownload van het Google Ads platform in .csv bestandsformaat. De data zijn opgeschoond en geanalyseerd in Microsoft Excel. Voor de analyse is gebruikgemaakt van beschrijvende statistieken. De resultaten zijn beschreven in hoofdstuk 5.

3.4. Ethische toestemming

Voor dit onderzoeksproject is een positief ethisch advies verkregen van de Facultaire Commissie Ethiek Rechtswetenschappelijk & Criminologisch Onderzoek (CERCO) van de Vrije Universiteit Amsterdam.

Hoofdstuk 4: Vragenlijstonderzoek onder slachtoffers

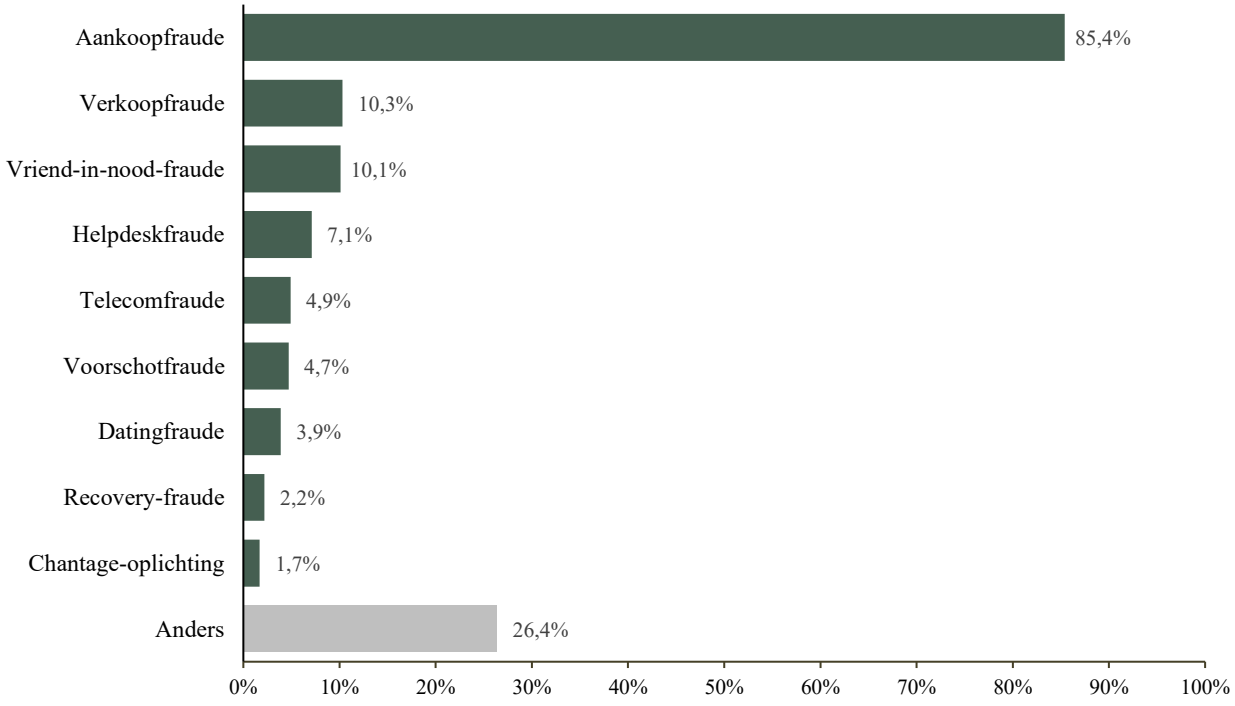
In dit hoofdstuk worden de resultaten uiteengezet van het vragenlijstonderzoek dat heeft plaatsgevonden onder slachtoffers van online fraude en ransomware.

4.1. Prevalentie van slachtofferschap

4.1.1. Prevalentie en incidentie van online fraude onder burgers

De respondenten die tot de doelgroep behoorden (slachtoffer van online fraude in de afgelopen 2 jaar en geld of goederen verloren) zijn allereerst gevraagd van welke vormen van fraude zij in de afgelopen 2 jaar slachtoffer zijn geworden. Respondenten konden meerdere antwoorden kiezen. Zoals in Figuur 4.1 te zien is, zijn de meeste respondenten slachtoffer geworden van aankoopfraude (85,4%), gevolgd door andere vormen van oplichting (26,4%), vriend-in-nood-fraude (10,1%) en verkoopfraude (10,3%).

Figuur 4.1 Prevalentie van slachtofferschap online fraude in afgelopen 2 jaar onder burgers (*meerdere antwoorden mogelijk)* (*n*=535)



Wanneer naar de verschillende fraudevormen (exclusief de optie ‘anders’) gekeken wordt die in de vragenlijst zijn uitgevraagd, zijn respondenten van minimaal 1 fraudevorm en van maximaal 9 verschillende fraudevormen slachtoffer geworden in de afgelopen 2 jaar. Gemiddeld genomen zijn respondenten van 1,3

fraudevormen slachtoffer geworden (Tabel 4.1). Respondenten die van van meerdere vormen van online fraude slachtoffer zijn geworden (12,1%), hebben de vervolgvragen in de vragenlijst ingevuld over de meest recente keer dat ze slachtoffer zijn geworden. De meeste respondenten zijn in 2023 voor het laatst slachtoffer geworden van online fraude (52,1%) (Tabel 4.2).

Tabel 4.1 Beschrijvende statistieken van slachtofferschap van verschillende fraudevormen in de afgelopen 2 jaar onder burgers (*n*=535)

	Min	Max	*M*	*SD*
Aantal verschillende fraudevormen	1	9	1,30	,790

Tabel 4.2 Frequentie van jaartal meest recente slachtofferschap online fraude onder burgers (*n*=535)

	n	**%**
Laatste keer slachtoffer	**535**	
2023	279	52,1%
2024	234	43,7%
2025[10]	22	4,1%

4.1.2. Incidentie van ransomware onder ondernemers

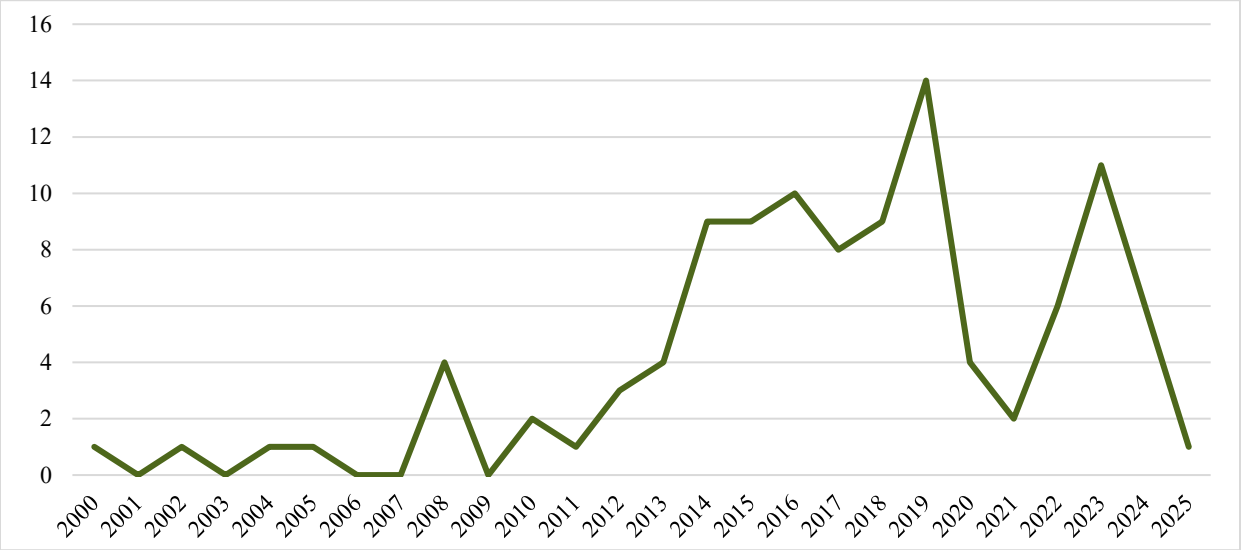
De meerderheid van de slachtoffers van ransomware (*n*=107) is een keer slachtoffer geworden (80,4%) (Tabel 4.3). Het grootste aandeel van de slachtoffers is relatief recent slachtoffer geworden, met de hoogste prevalentie in 2019 (Figuur 4.2).

Tabel 4.3 Frequentie van jaartal meest recente slachtofferschap ransomware onder ondernemers (*n*=107)

	n	**%**
Incidentie	**107**	
1 keer	86	80,4%
2 keer	15	14,0%
3 keer	6	5,6%

[10] De dataverzameling heeft plaatsgevonden in augustus van 2025, wat mogelijk de cijfers heeft beïnvloed.

Figuur 4.2 Frequentie van jaartal meeste recente slachtofferschap van ransomware onder ondernemers (*n*=107)



4.2. Gevolgen van slachtofferschap

De respondenten zijn gevraagd naar de gevolgen van het laatste incident (Tabel 4.4). Als het gaat om de financiële gevolgen (bijv. geld kwijt of kosten voor hulp), gaf 6,2% van de slachtoffers van online fraude aan geen financiële gevolgen te hebben ervaren, en 0,9% het niet te weten. Voor de meerderheid van de respondenten waren de financiële gevolgen tussen de 1 en 100 euro (66%). Een aantal respondenten hadden echter ook hogere kosten, oplopend tot 100.000 euro.

Een groter aandeel van de ransomware slachtoffers gaf aan geen financiële kosten te hebben gemaakt (38,3%). In vergelijking met de slachtoffers van online fraude waren de schadebedragen voor ransomware slachtoffers meer gevarieerd. Voor de meeste respondenten kostte het ransomware incident tussen 251 en 500 euro (13,1%) of tussen 501 euro en 1.000 euro (11,2%).

Tabel 4.4 Frequentie van financiële gevolgen onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude		**Ransomware**	
	n	**%**	***n***	**%**
Financiële gevolgen	**535**		**107**	
Geen financiële kosten[11]	33	6,2%	41	38,3%
€1 t/m €100	353	66,0%	5	4,7%
€101 t/m €250	70	13,1%	10	9,3%
€251 t/m €500	24	4,5%	14	13,1%
€501 t/m €1.000	19	3,6%	12	11,2%
€1.001 t/m €2.500	12	2,2%	7	6,5%
€2.501 t/m €5.000	7	1,3%	10	9,3%
€5.001 t/m €10.000	6	1,1%	2	1,9%
€10.001 t/m €25.000	4	0,7%	4	3,7%
€25.001 t/m €50.000	1	0,2%	1	0,9%
€50.001 t/m €100.000	1	0,2%	0	0,0%
€100.001 of meer	0	0,0%	0	0,0%
Weet ik niet	5	0,9%	1	0,9%

Respondenten zijn ook gevraagd of ze (tijdelijke) emotionele, psychische of lichamelijke gevolgen hebben ervaren naar aanleiding van het incident (Tabel 4.5). Respondenten werd voor verschillende gevolgen gevraagd of ze dit hebben ervaren, waarbij ze konden antwoorden op een schaal van 1 (helemaal mee oneens) tot en met 5 (helemaal mee eens). Wanneer alle items worden samengenomen (*Cronbach's alpha* = ,925) blijkt dat slachtoffers van online fraude gemiddeld genomen geen (tijdelijke) emotionele, psychische of lichamelijke gevolgen hebben ervaren (*M* = 2,21, *SD* = ,773) (Tabel 4.4). Wanneer gekeken wordt naar de verschillende gevolgen, blijkt dat er variaties zijn in de mate waarin respondenten deze hebben ervaren. Uit Tabel 4.4 blijkt dat slachtoffers van online fraude gemiddeld genomen het minst angstklachten en/of paniekaanvallen hebben ervaren (*M* = 1,43, *SD* = ,743) en zich het meest boos voelden over het incident (*M* = 3,64, *SD* = 1,136).

Ook slachtoffers van ransomware blijken gemiddeld genomen geen (tijdelijke) emotionele, psychische of lichamelijke gevolgen te hebben ervaren (*M* = 2,12, *SD* = ,773) wanneer alle items worden samengenomen (*Cronbach's alpha* = ,931). Maar ook bij deze groep bestaat er variatie tussen items. Uit tabel 4.4 blijkt dat slachtoffers van ransomware gemiddeld genomen het minst angstklachten en/of paniekaanvallen (*M* = 1,41, *SD* = ,672) en lichamelijke klachten (*M* = 1,41, *SD* = ,713) hebben ervaren. Deze groep voelde zich gemiddeld genomen het meest boos over het incident (*M* = 3,48, *SD* = 1,369).

[11] De screeningsvragen waren bedoeld om alleen slachtoffers van online fraude te includeren die financiële schade hadden geleden, ongeacht of deze kosten vergoed is. Een kleine groep slachtoffers rapporteerde desondanks geen financiële gevolgen. Deze respondenten zijn geïncludeerd in de analyses, omdat onduidelijk is waarom zij geen financiële kosten rapporteren. Mogelijk hebben zij de vraag anders geïnterpreteerd, bijvoorbeeld omdat ze geen aanvullende kosten gemaakt hebben of de kosten volledig vergoed hebben gekregen. Voor slachtoffers van ransomware was financiële schade geen voorwaarde voor inclusie in de studie.

Tabel 4.5 Beschrijvende statistieken van emotionele, psychische of fysieke gevolgen onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude				**Ransomware**			
	Min	**Max**	***M***	***SD***	**Min**	**Max**	***M***	***SD***
Emotionele, psychische of lichamelijke gevolgen (schaal)	1	4,67	2,21	,773	1	3,73	2,12	,797
Emotionele, psychische of lichamelijke gevolgen (items)								
Het voorval telkens opnieuw beleven	1	5	1,81	1,015	1	5	1,86	1,094
Ontkennen van wat er gebeurd is of het moeilijk kunnen geloven	1	5	1,95	1,122	1	4	1,87	1,056
Minder vertrouwen in mensen	1	5	2,96	1,216	1	5	2,64	1,284
Minder vertrouwen in mijn eigen online vaardigheden	1	5	2,32	1,149	1	5	2,35	1,275
Slaapproblemen	1	5	1,60	,934	1	4	1,53	,816
Angstklachten en/of paniekaanvallen	1	5	1,43	,743	1	4	1,41	,672
Depressieve klachten	1	5	1,50	,854	1	4	1,42	,673
Lichamelijke klachten zoals hartkloppingen, duizeligheid, trillen of buikpijn	1	5	1,46	,815	1	4	1,41	,713
Een minder veilig gevoel	1	5	2,11	1,189	1	5	2,56	1,409
Schaamte over wat er gebeurd is	1	5	2,58	1,295	1	5	2,14	1,217
Een schuldgevoel over wat er is gebeurd	1	5	2,29	1,298	1	4	1,99	1,137
Machteloos voelen over wat er is gebeurd	1	5	3,04	1,338	1	5	2,91	1,384
Verdrietig voelen over wat er is gebeurd	1	5	2,64	1,301	1	5	2,43	1,333
Boos voelen over wat er is gebeurd	1	5	3,64	1,136	1	5	3,48	1,369
Andere emotionele of psychische gevolgen	1	5	1,75	,940	1	4	1,76	,899

Respondenten zijn daarnaast gevraagd of ze nog andere gevolgen hebben ervaren naar aanleiding van het incident (Tabel 4.6). Respondenten werd voor verschillende gevolgen gevraagd of ze dit hebben ervaren, waarbij ze konden antwoorden op een schaal van 1 (helemaal mee oneens) tot en met 5 (helemaal mee eens). Wanneer alle items worden samengenomen (*Cronbach's alpha* = ,766) blijkt dat slachtoffers van online fraude gemiddeld genomen geen (tijdelijke) andere gevolgen hebben ervaren (*M* = 2,12, *SD* = ,610) (Tabel 4.5). Wanneer gekeken wordt naar de verschillende gevolgen, blijkt echter wel dat er variaties zijn in de mate waarin respondenten deze hebben ervaren. Uit tabel 4.5 blijkt dat slachtoffers van online fraude gemiddeld genomen het minst hebben ervaren dat ze geld moesten lenen omdat ze niet (meer) rond konden komen (*M* = 1,36, *SD* = ,716) en het meest hebben ervaren dat ze voorzichter zijn geworden op het internet (*M* = 3,74, *SD* = 1,089).

Ook slachtoffers van ransomware blijken gemiddeld genomen geen andere gevolgen te hebben ervaren (*M* = 2,18, *SD* = ,578) wanneer alle items worden samengenomen (*Cronbach's alpha* = ,839). Maar ook bij deze groep bestaat er variatie tussen items. Uit tabel 4.6 blijkt dat ook slachtoffers van ransomware gemiddeld genomen het minst hebben ervaren dat ze geld moesten lenen omdat ze niet (meer) rond konden komen (*M* = 1,28, *SD* = ,491) en het meest hebben ervaren dat ze voorzichter zijn geworden op het internet (*M* = 4,06, *SD* = 1,026). Hoewel de slachtoffers van ransomware en online fraude over het algemeen vergelijkbaar antwoorden, is een opvallend verschil dat bij slachtoffers van ransomware meer sprake lijkt te zijn van het maken van kosten vanwege reparatie of herstel (*M* = 3,41, *SD* = 1,373) in vergelijking met slachtoffers van online fraude (*M* = 1,74, *SD* = ,985). Dit ligt echter in lijn met de aard van het delict.

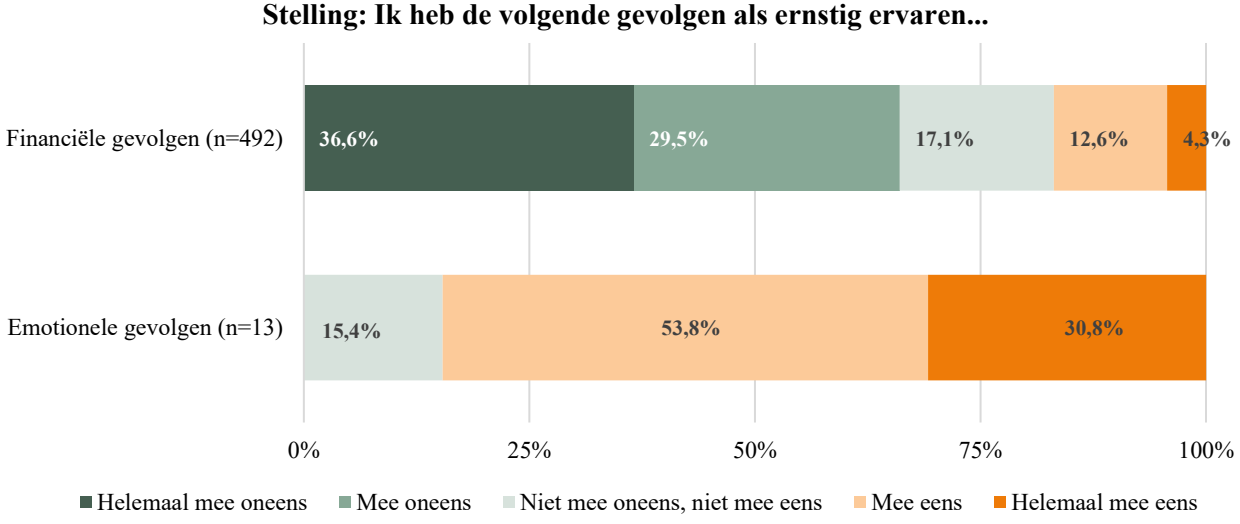
Tabel 4.6 Beschrijvende statistieken van andere gevolgen onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude				**Ransomware**			
	Min	**Max**	***M***	***SD***	**Min**	**Max**	***M***	***SD***
Andere gevolgen (schaal)	1	4,63	2,21	,610	1	3,60	2,18	,578
Andere gevolgen (items)								
Tijd besteed aan het oplossen van het incident	1	5	3,42	1,233	1	5	3,72	1,204
Kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	1	5	1,74	,985	1	5	3,41	1,373
Geld moeten lenen omdat ik niet (meer) rond kon komen	1	5	1,36	,716	1	3	1,28	,491
Moeten afzien van een geplande activiteit of uitgave (zoals een vakantie)	1	5	1,53	,909	1	5	1,72	1,114
Een negatieve reactie ervaren van mijn partner, kinderen of andere familieleden	1	5	1,76	1,026	1	5	1,67	,979
Een negatieve reactie ervaren van andere mensen om mij heen, zoals vrienden, kennissen, buren of collega's	1	5	1,59	,875	1	4	1,59	,846
Ik ben voorzichtiger geworden op het internet	1	5	3,74	1,089	1	5	4,06	1,026
Verhinderd in het uitvoeren van dagelijkse werkzaamheden	-	-	-	-	1	5	2,71	1,408
Verlies aan inkomsten, waarde van aandelen of inkomen	-	-	-	-	1	5	2,18	1,265
Bestanden of gegevens verloren	-	-	-	-	1	5	2,55	1,455
Boetes van regelgevers of wetgevers, of verwante juridische kosten	-	-	-	-	1	4	1,40	,0642
Reputatieschade	-	-	-	-	1	4	1,53	,731

	Online fraude				Ransomware			
	Min	**Max**	***M***	***SD***	**Min**	**Max**	***M***	***SD***
Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders	-	-	-	-	1	4	1,49	,793
Mijn bedrijf heeft een schadevergoeding, compensatie of korting verleend aan klanten	-	-	-	-	1	4	1,36	,605
Andere gevolgen	1	5	1,85	1,009	1	5	1,96	1,054

Aan respondenten die gevolgen hebben ervaren is tevens gevraagd in hoeverre ze de financiële, emotionele, psychische of lichamelijke en andere gevolgen als ernstig hebben ervaren op een schaal van 1 (helemaal mee oneens) tot en met 5 (helemaal mee eens). Zoals in Figuur 4.3 te zien is, waren de meeste slachtoffers van online fraude het (helemaal) oneens met deze stelling in relatie tot de financiële gevolgen, maar (helemaal) eens met de stelling in relatie tot de emotionele, psychische of lichamelijke gevolgen. Ook de vier respondenten die andere gevolgen hebben ervaren (niet opgenomen in het figuur) waren het voornamelijk (helemaal) eens met de stelling.[12] Met andere woorden, in de meerderheid van de gevallen werden de emotionele, psychische en lichamelijke en andere gevolgen onder slachtoffers van online fraude als ernstig ervaren. De financiële gevolgen werden als minder ernstig ervaren.

Figuur 4.3 Inschatting van de ernst van gevolgen van online fraude onder burgers

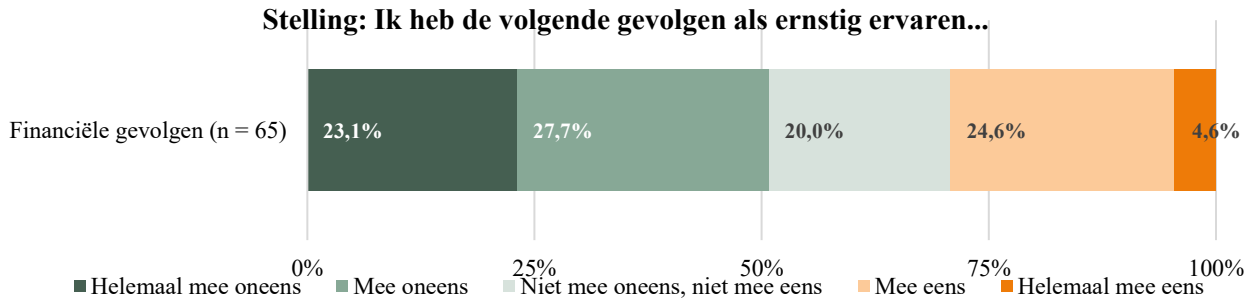


Onder slachtoffers van ransomware was geen enkele respondent het (helemaal) eens dat ze emotionele, psychische, lichamelijke of andere gevolgen hebben ervaren. Deze respondenten zijn zodoende niet meegenomen in de stelling in hoeverre ze die gevolgen als ernstig hebben ervaren. Met betrekking tot de

[12] Niet opgenomen in figuur 4.3. in verband met de lage respons op deze stelling.

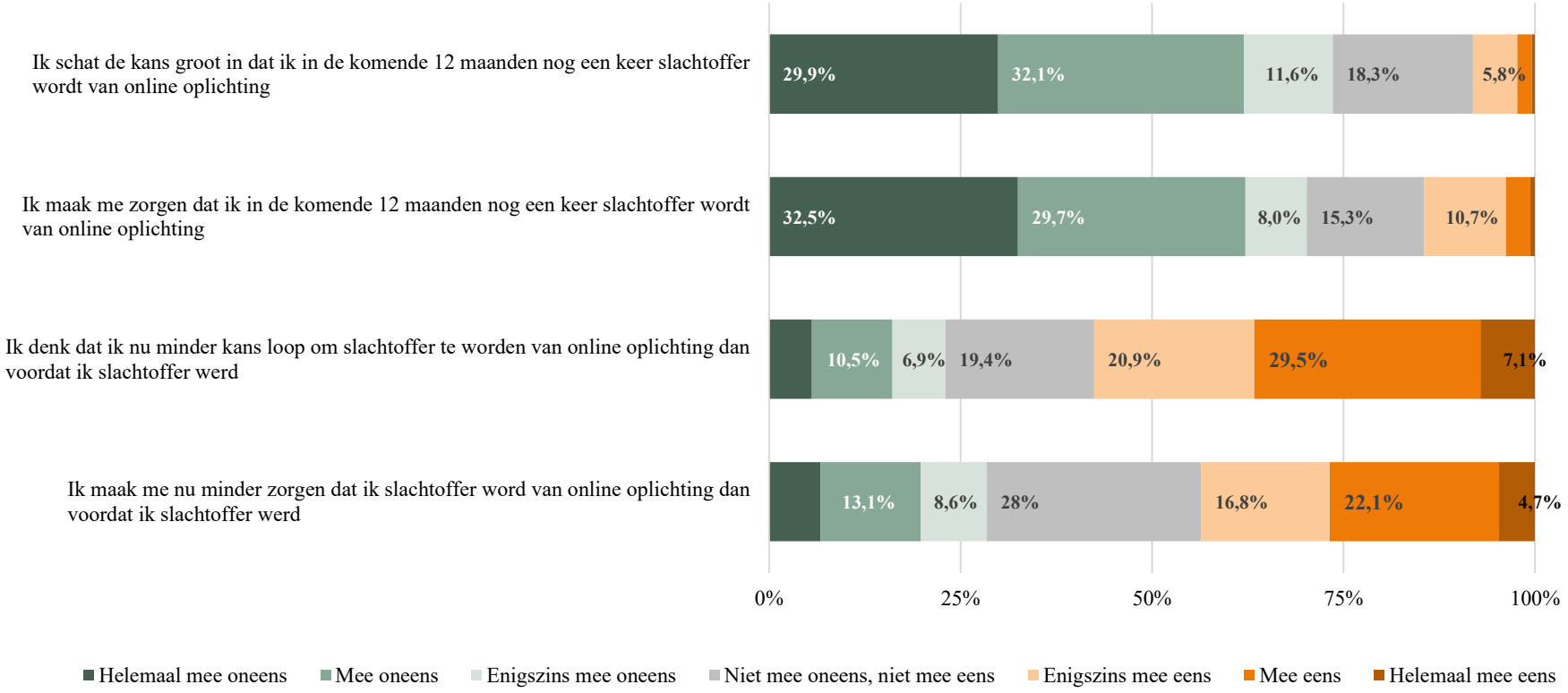
financiële gevolgen blijkt uit Figuur 4.4. dat slecht een klein van de respondenten het (helemaal) eens is met de stelling dat ze de financiële gevolgen als ernstig hebben ervaren, hoewel dit aandeel wel groter was in vergelijking met slachtoffers van online fraude.

Figuur 4.4 Inschatting van de ernst van gevolgen van ransomware onder ondernemers

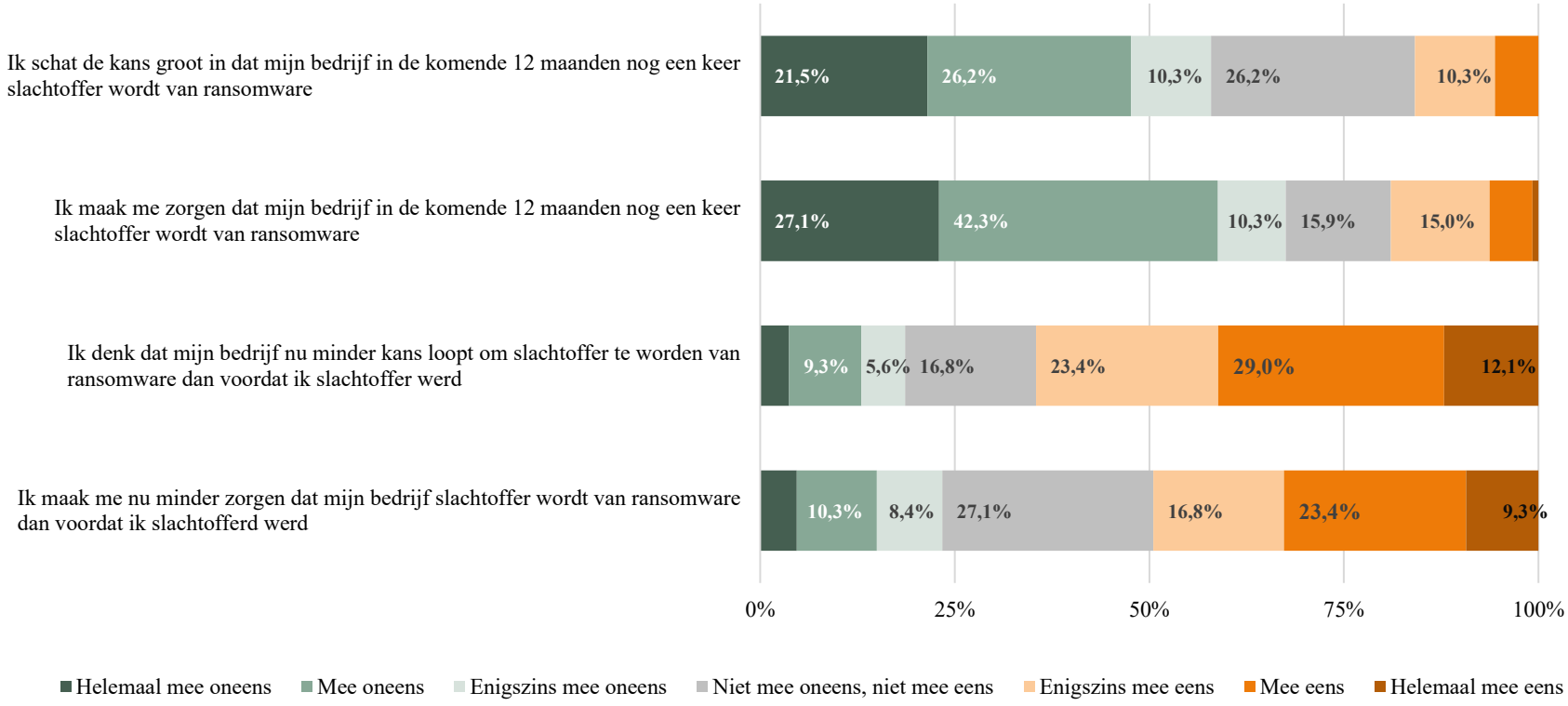


Aan respondenten is gevraagd hoe ze de kans inschatten om in de komende 12 maanden opnieuw slachtoffer te worden en in hoeverre ze zich hier zorgen om maken op een schaal van 1 (helemaal mee oneens) tot en met 7 (helemaal mee eens). Uit Figuur 4.5 en Figuur 4.6. blijkt dat meer dan de helft van de slachtoffers van online fraude en ransomware denkt dat ze nu minder kans lopen om slachtoffer te worden, en zich hier weinig zorgen om maken.

Figuur 4.5 Angst voor revictimisatie van online fraude onder burgers (*n*=535)



Figuur 4.6 Angst voor revictimisatie van ransomware onder ondernemers (*n*=107)



4.3. Informatie- en hulpbehoeften

Respondenten is gevraagd welke informatie- of hulpbehoeften ze hebben ervaren naar aanleiding van het incident. Zoals blijkt uit Tabel 4.7, hadden de meeste slachtoffers van online fraude behoefte aan informatie over het oplossen van het probleem (47,7%), gevolgd door informatie over het vergoed krijgen van de financiële schade (34,6%) en het voorkomen van slachtofferschap in de toekomst (29,3%). Een klein aandeel van de respondenten rapporteerde geen enkele van de genoemde informatiebehoeften (3,9%).

De meeste slachtoffers van ransomware hadden tevens behoefte aan informatie over het oplossen van het probleem (73,8%), gevolgd door informatie over het voorkomen van slachtofferschap in de toekomst (61,7%) en informatie over hoe het heeft kunnen gebeuren (43,9%). In vergelijking met de slachtoffers van online fraude, had echter een aanzienlijk groter aandeel van de respondenten deze informatiebehoeften. In tegenstelling tot bij de slachtoffers van online fraude, hadden weinig slachtoffers van ransomware behoefte aan informatie over het vergoed krijgen van de financiële schade (3,7%). Dit heeft er mogelijk mee te maken dat een groter aandeel van de ransomware slachtoffers geen financiële schade heeft geleden in vergelijking met de fraude slachtoffers. Slechts één respondent rapporteerde geen enkele van de genoemde informatiebehoeften.

Tabel 4.7 Frequentie van informatie- en hulpbehoeften onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude		**Ransomware**	
	n	**%**	***n***	**%**
Informatiebehoeften	**535**		**107**	
Wat me precies overkomen is	104	19,4%	40	37,4%
Hoe het heeft kunnen gebeuren	139	26,0%	47	43,9%
Het oplossen van het probleem	255	47,7%	79	73,8%
Hoe ik kan voorkomen dat ik in de toekomst opnieuw slachtoffer word	157	29,3%	66	61,7%
De organisaties waarbij ik terecht kan voor hulp	95	17,8%	21	19,6%
De status van mijn aangifte (indien van toepassing)	63	11,8%	3	2,8%
Het vergoed krijgen van de financiële schade	185	34,6%	4	3,7%
Emotionele, psychische of lichamelijke gevolgen of klachten	5	0,9%	0	0,0%
Het doen van een melding of aangifte bij de politie	140	26,2%	24	22,4%
Juridische zaken	31	5,8%	9	8,4%
Anders	55	10,3%	11	10,3%

Als het gaat om de hulpbehoeften, hadden de meeste slachtoffers van online fraude behoefte aan hulp bij het oplossen van het probleem (37%), gevolgd door hulp bij het vergoed krijgen van de financiële schade (32,7%) en andere behoeften dan in de vragenlijst bevraagd werden (17%). Een klein aandeel van de respondenten rapporteerde geen enkele van de genoemde hulpbehoeften (7,9%) (Tabel 4.8). Zoals te zien

is in Tabel 4.8, hadden de meeste slachtoffers van ransomware ook behoefte aan hulp bij het oplossen van het probleem (81,3%), gevolgd door hulp bij het voorkomen van slachtofferschap in de toekomst (52,3%) en hulp bij het doen van een melding of aangifte bij de politie (10,3%). Ook hier had een groter aandeel van de slachtoffers van ransomware deze hulpbehoeften in vergelijking met de slachtoffers van online fraude. Drie respondenten rapporteerden geen enkele van de genoemde hulpbehoeften te hebben ervaren (2,8%).

Tabel 4.8 Frequentie van hulpbehoeften onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

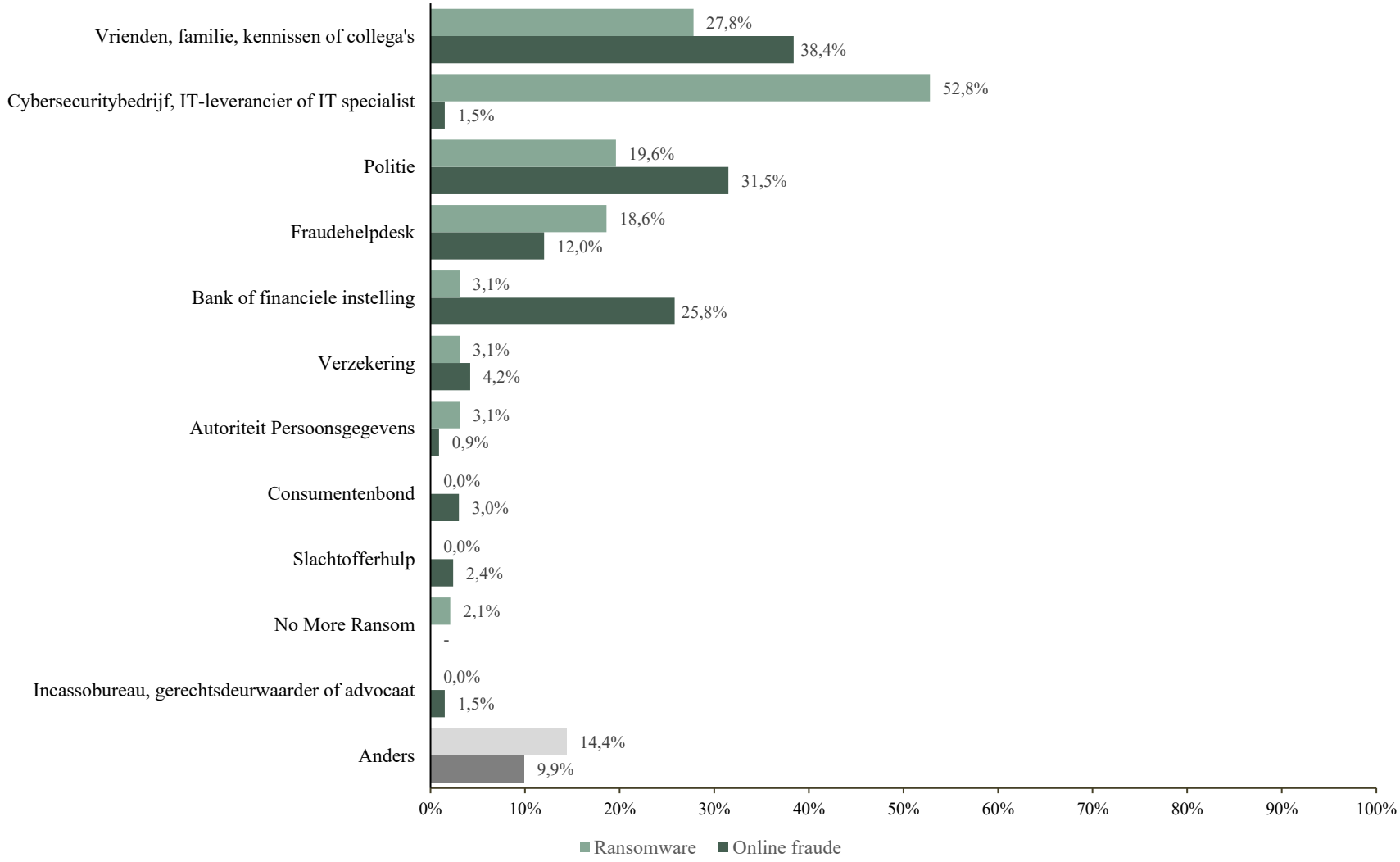
	Online fraude		**Ransomware**	
	n	**%**	***n***	**%**
Hulpbehoeften	**535**		**107**	
Hulp bij het oplossen van het probleem	198	37,0%	87	81,3%
Hulp om te voorkomen dat ik in de toekomst opnieuw slachtoffer word	85	15,9%	56	52,3%
Hulp bij het vergoed krijgen van de financiële schade	175	32,7%	7	6,5%
Hulp voor emotionele, psychische of lichamelijke gevolgen of klachten	14	2,6%	1	1,0%
Hulp bij het doen van een melding of aangifte bij de politie	72	13,5%	11	10,3%
Hulp bij juridische vragen of problemen	38	7,1%	9	8,4%
Erkenning als slachtoffer	39	7,3%	2	1,9%
Erkenning van wat me overkomen is	75	14,0%	6	5,6%
Anders, namelijk… [open antwoord]	91	17,0%	10	9,3%

4.4. Hulpzoekgedrag bij verschillende partijen

Tevens is onderzocht in hoeverre respondenten hulp hebben gezocht nadat ze slachtoffer zijn geworden en bij welke partij (Figuur 4.7). Bijna twee op de drie slachtoffers van online fraude heeft hulp gezocht (62,2%). Zij deden dit voornamelijk bij vrienden, familie, kennissen of collega's (23,9%), gevolgd door bij de politie (19,6%) en een bank- of financiële instelling (16,1%). Een minderheid van de slachtoffers van online fraude heeft geen hulp gezocht (37,8%).

Negen op de tien slachtoffers van ransomware hebben hulp gezocht (90,7%). Zij deden dit voornamelijk bij een cybersecuritybedrijf, IT-specialist of IT-leverancier (52,8%), gevolgd door vrienden, familie, kennissen of collega's (27,8%) en de politie (19,6%). Geen enkel slachtoffer van ransomware heeft contact opgenomen met Slachtofferhulp, de Consumentenbond of een incassobureau, gerechtsdeurwaarder of advocaat. Ook een minderheid van de slachtoffers van ransomware heeft geen hulp gezocht (9,3%).

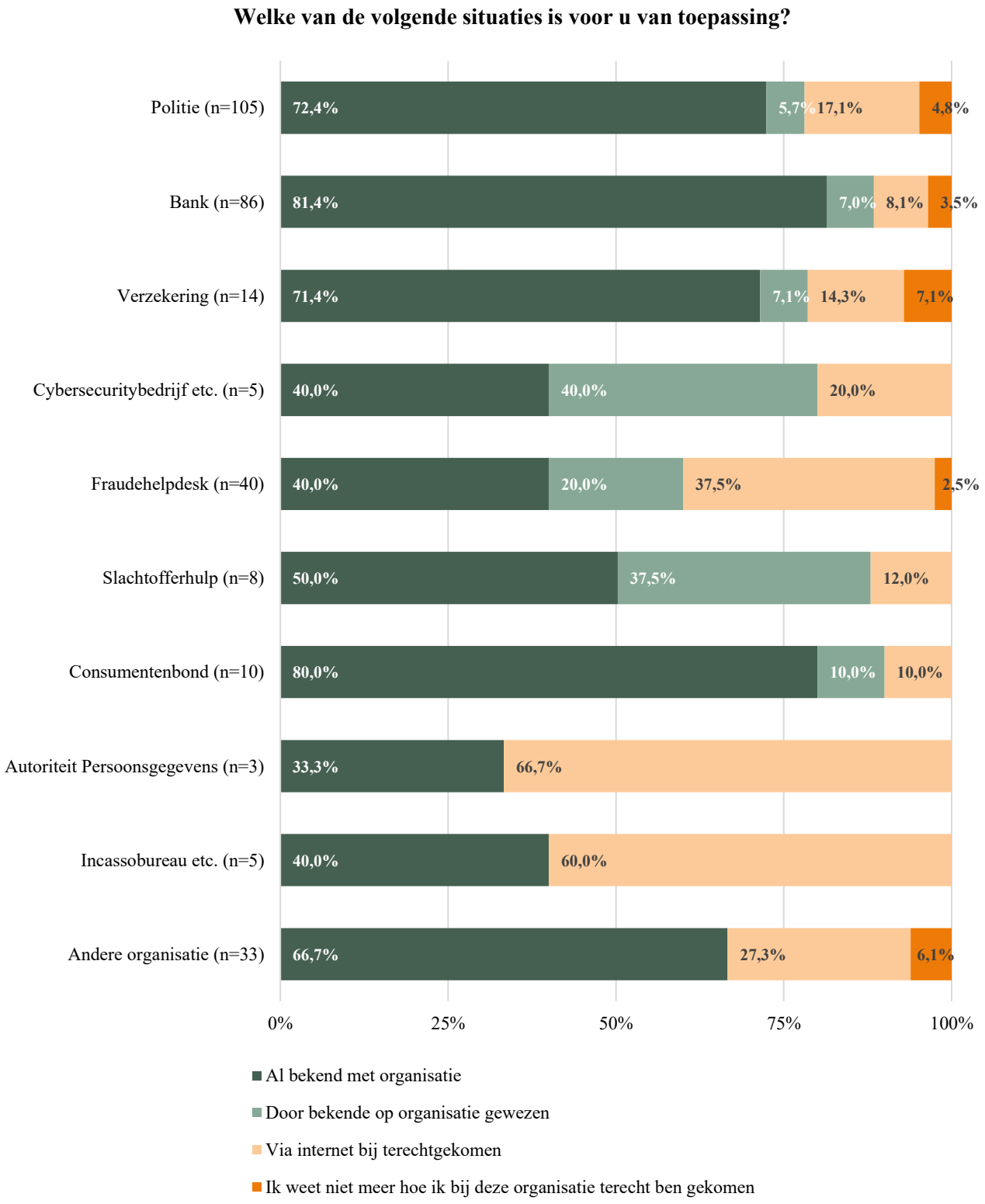
Figuur 4.7 Partijen waarbij naar hulp gezocht is naar aanleiding van het incident onder slachtoffers van online fraude (*n*=333) en ransomware (*n*=97) (*meerdere antwoorden mogelijk)*



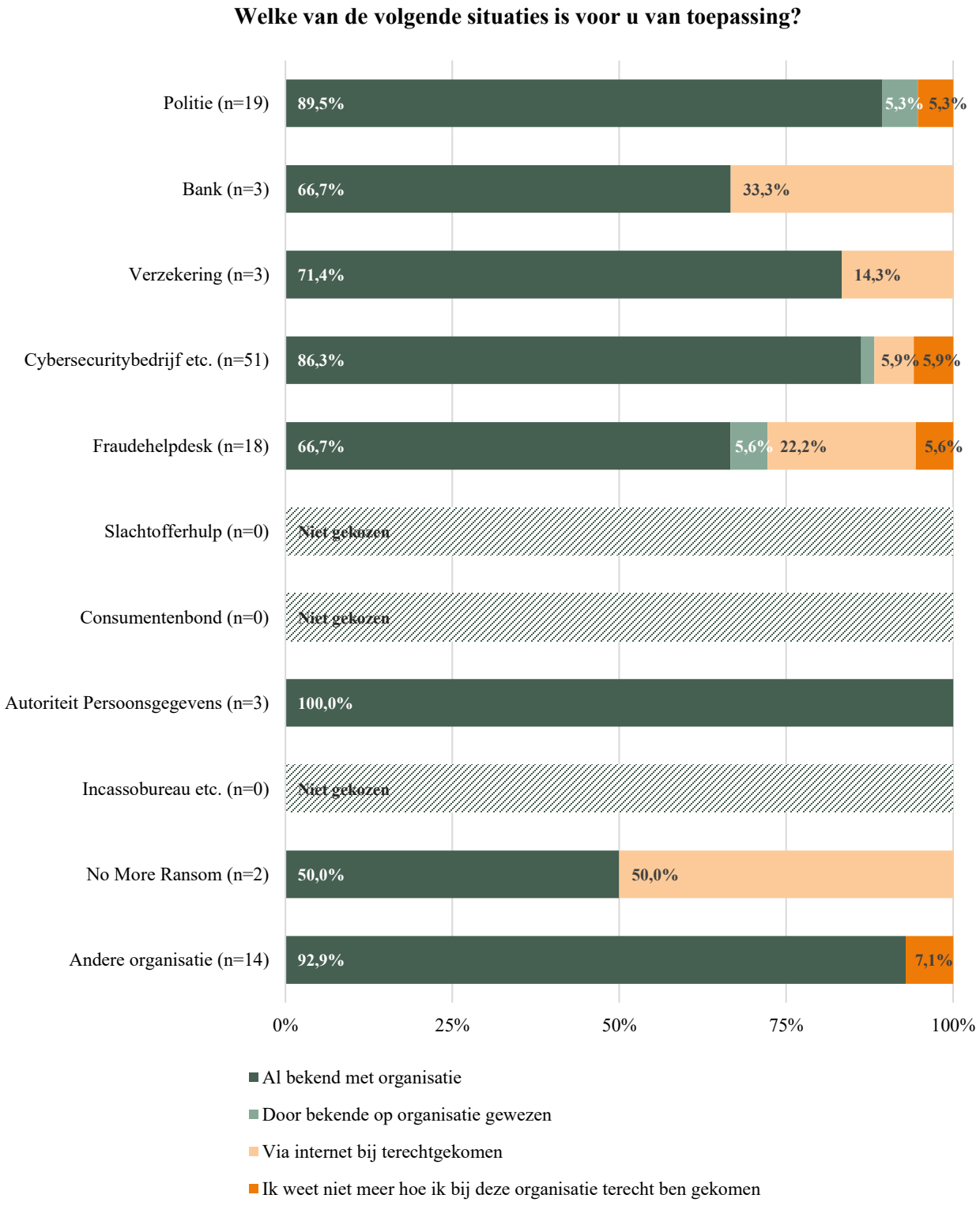
Voor elke organisatie die de respondenten hebben aangeduid is bovendien gevraagd of ze al bekend waren met deze organisatie, door een bekende op de organisatie zijn gewezen, de organisatie via internet gevonden hebben of niet meer weten hoe ze bij de organisatie terecht zijn gekomen. Uit Figuur 4.8 blijkt dat de meerderheid van de respondenten al bekend was met de partij waarmee zij contact opnamen: de politie (72,4%), bank of financiële instelling (81,4%), verzekeringsmaatschappij (71%), Consumentenbond (80%) en andere organisaties die door respondenten zijn benaderd (66,7%). De meerderheid van de respondenten die contact opnamen met de Autoriteit Persoonsgegevens, een incassobureau, gerechtsdeurwaarder of advocaat is daarentegen via internet terecht gekomen bij deze partijen (respectievelijk 66,7% en 60%). Voor de Fraudehelpdesk, Slachtofferhulp Nederland en een cybersecuritybedrijf was een deel van de respondenten al met deze partijen bekend, een ander deel is erop gewezen door bekenden of heeft deze partijen via het internet gevonden.

Bij de slachtoffers van ransomware blijkt uit Figuur 4.9 dat de meerderheid van de respondenten al bekend was met de partij waarmee zij contact opnamen: de politie (89,5%), bank (66,7%), verzekeringsmaatschappij (71,4%), cybersecuritybedrijf, IT-specialist of IT-leverancier (86,3%), de Fraudehelpdesk (66,7%), Autoriteit Persoonsgegevens (100%) en andere organisaties (92,9%). Daarnaast is een kleiner deel van de respondenten uitgekomen via internet bij de bank (33,3%), verzekeringsmaatschappij (13,4%), Fraudehelpdesk (22,2%) en No More Ransom (50%).

Figuur 4.8 Bekendheid met gecontacteerde instanties onder slachtoffers van online fraude (*n*=333)



Figuur 4.9 Bekendheid met gecontacteerde instanties onder slachtoffers van ransomware (*n*=97)

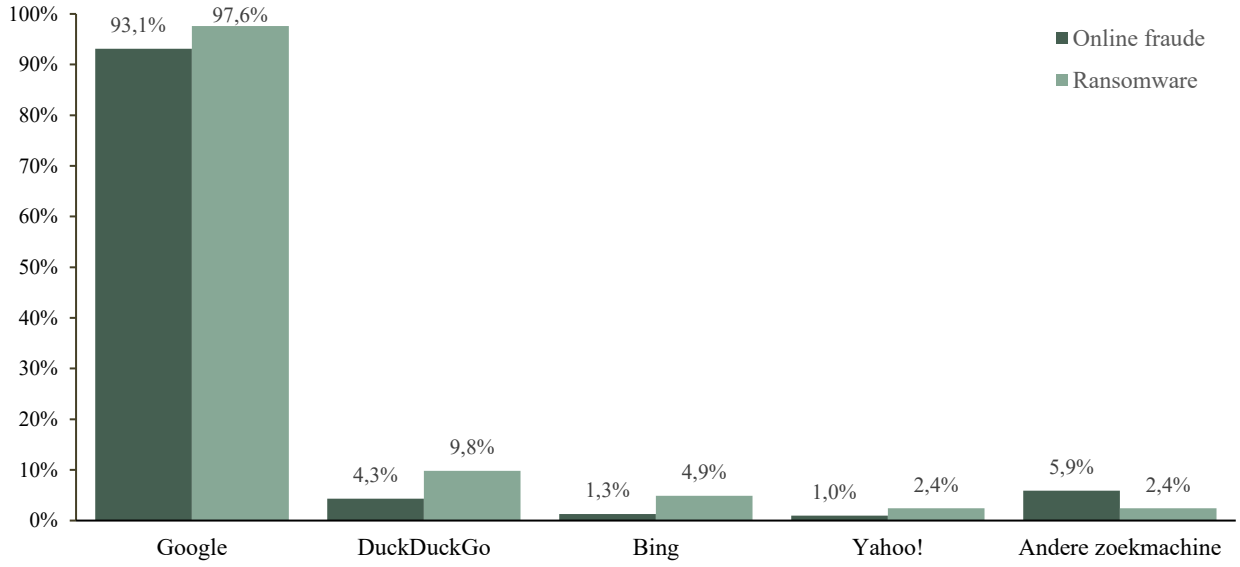


4.5. Online hulpzoekgedrag

Uit de vragenlijst blijkt dat een kleine meerderheid van de slachtoffers van online fraude op internet gezocht heeft tijdens of na het incident (57%), waarbij de meerderheid gebruikgemaakt heeft van Google (93,1%) (Figuur 4.10). Een kleiner deel heeft niet op internet gezocht (43%) tijdens of na het incident.

De meerderheid van de slachtoffers van ransomware heeft niet gezocht op internet (61,7%). Van de slachtoffers van ransomware die dat wel gedaan hebben (38,3%), gebruikte de overgrote meerderheid Google (97,6%) (Figuur 4.10).

Figuur 4.10 Gebruik van online zoekmachines tijdens of na slachtofferschap onder slachtoffers van online fraude (*n*=305) en ransomware (*n*=41) (***meerdere antwoorden mogelijk)***

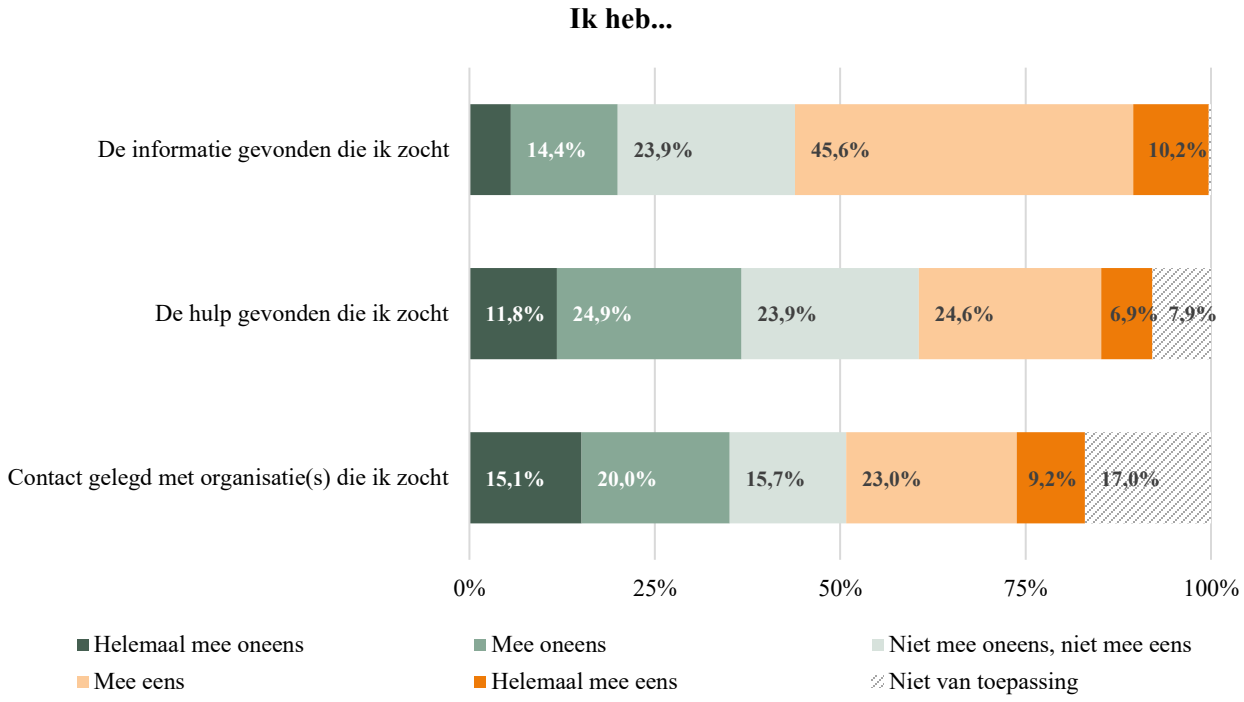


Aan respondenten is gevraagd op een schaal van 1 (helemaal mee oneens) tot en met 5 (helemaal mee eens) of zij het eens zijn met de stellingen dat ze de informatie en hulp hebben gevonden die ze zochten, en contact hebben kunnen leggen met de organisatie(s) die ze zochten. Van de slachtoffers van online fraude die op internet gezocht hebben, geeft iets meer dan de helft aan dat ze de informatie gevonden hebben die ze zochten (Figuur 4.11). Een iets kleiner aandeel, ongeveer een derde van de respondenten, heeft de hulp gevonden die ze zochten, of door internet contact hebben kunnen leggen met de organisatie(s) die ze zochten (Figuur 4.11). Uit Figuur 4.11 kan ook geconcludeerd worden dat ongeveer 20% tot 37% van de slachtoffers niet (helemaal) de informatie of hulp heeft gevonden die ze zochten, of dat het zoeken op internet niet bijgedragen heeft aan contact met de organisatie(s) die ze zochten.

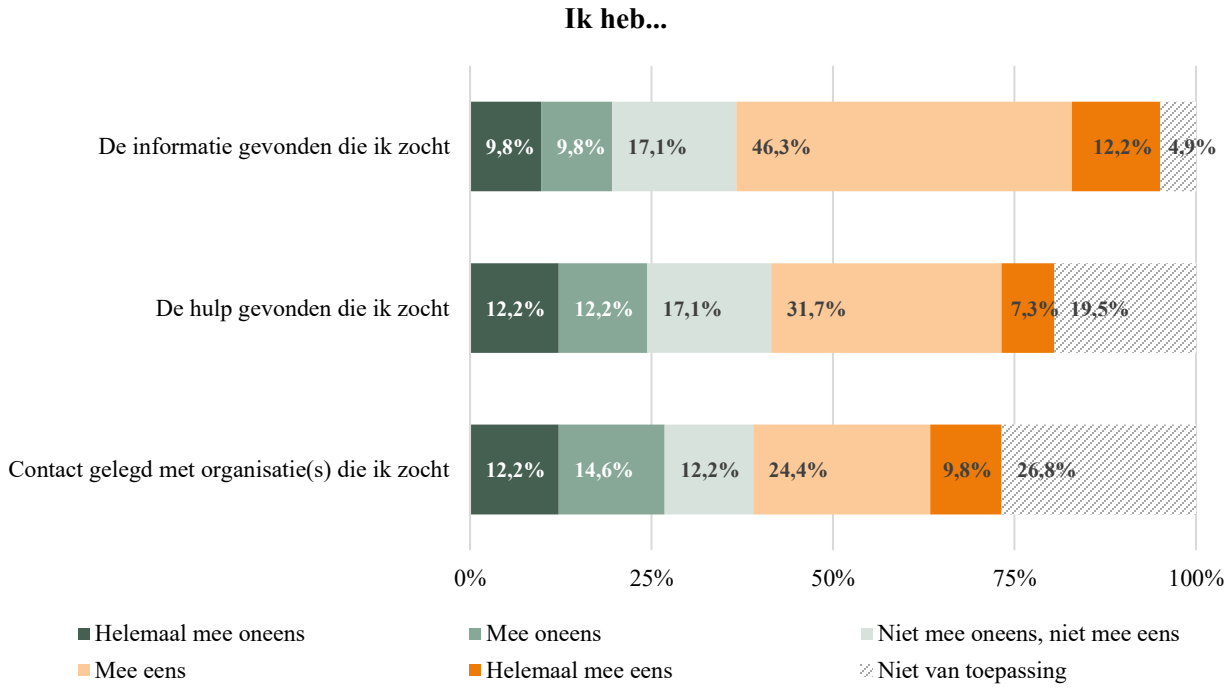
Van de slachtoffers van ransomware die op internet gezocht hebben heeft iets meer dan de helft de informatie gevonden hebben die ze zochten (Figuur 4.12). Een kleiner aandeel, ongeveer een derde van de

respondenten, heeft de hulp gevonden die ze zochten, of heeft door internet contact kunnen leggen met de organisatie(s) die ze zochten (Figuur 4.12). Ongeveer 20% tot 27% heeft niet de informatie, hulp of organisaties gevonden die ze zochten.

Figuur 4.11 Uitkomst van gebruik van internet tijdens of na slachtofferschap van online fraude onder burgers (*n*=305)



Figuur 4.12 Uitkomst van gebruik van online zoekmachine na slachtofferschap van ransomware onder ondernemers (*n*=41)

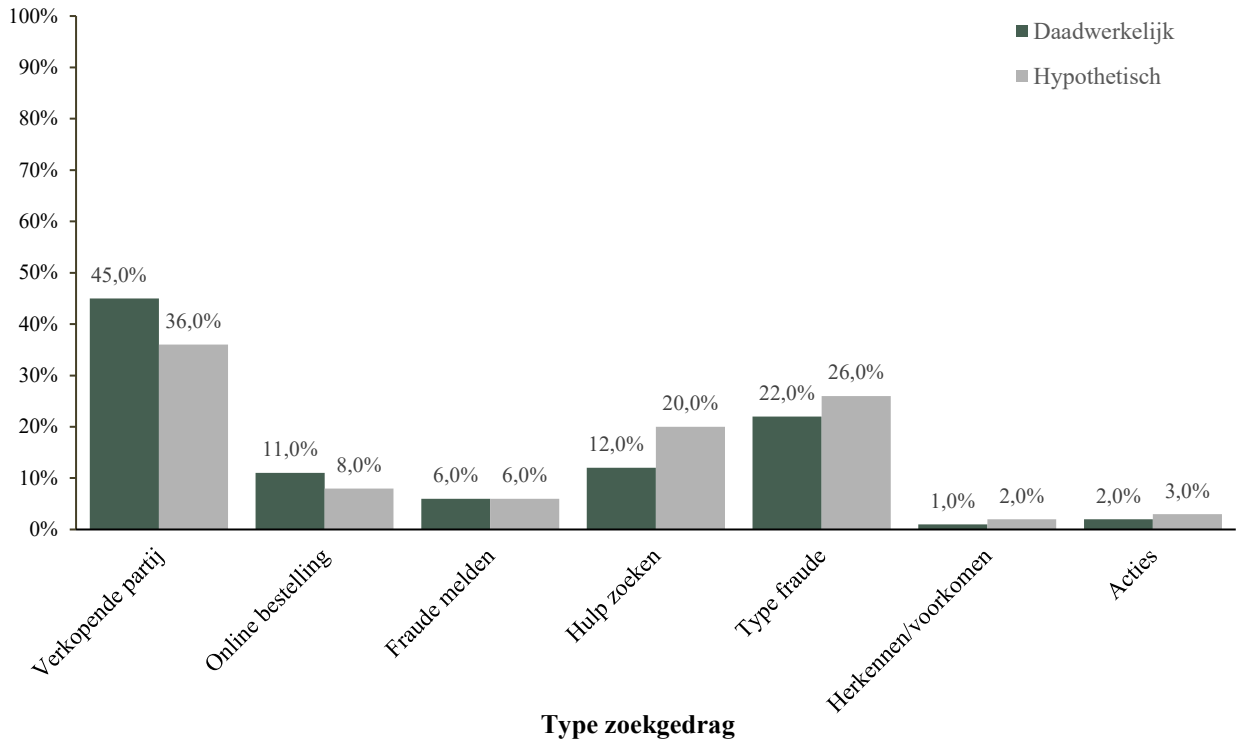


De slachtoffers die online gezocht hebben is gevraagd wat ze tijdens het incident ingetypt hebben in de zoekmachine. Zowel de slachtoffers die online gezocht hebben als de slachtoffers die niet online gezocht hebben is bovendien gevraagd wat ze zouden intypen in een zoekmachine als ze nu opnieuw slachtoffer zouden worden. Onder de slachtoffers die online gezocht hebben, heeft 41% (n=125) van de slachtoffers van online fraude en 51% (n=25) van de slachtoffers van ransomware aangegeven het niet (meer) te weten. Onder de groep respondenten die zoektermen heeft ingevuld, heeft dit voor online fraude geleid tot 400 daadwerkelijke zoektermen en 1049 hypothetische zoektermen. Voor ransomware heeft dit geleid tot 40 daadwerkelijke zoektermen en 232 hypothetische zoektermen.

In Figuur 4.13 zijn de zoektermen van slachtoffers van online fraude weergegeven, uitgesplitst naar verschillende thema's. Zo blijkt uit Figuur 4.13 dat het grootste aandeel van de respondenten heeft gezocht of zou zoeken op zoektermen gerelateerd aan de verkopende partij. Deze categorie is naar alle waarschijnlijkheid gerelateerd aan slachtofferschap van aankoopfraude. Deze zoektermen hebben bijvoorbeeld betrekking op het opzoeken van de verkoper, het zoeken naar recensies, en het achterhalen van bankgegevens of contactgegevens van de verkoper. De op een na meest voorkomende categorie betreft zoektermen gerelateerd aan een specifiek type fraude. Zo is gezocht op zoektermen zoals WhatsApp fraude, datingfraude, identiteitsfraude en Marktplaats oplichting. De op twee na meest voorkomende categorie

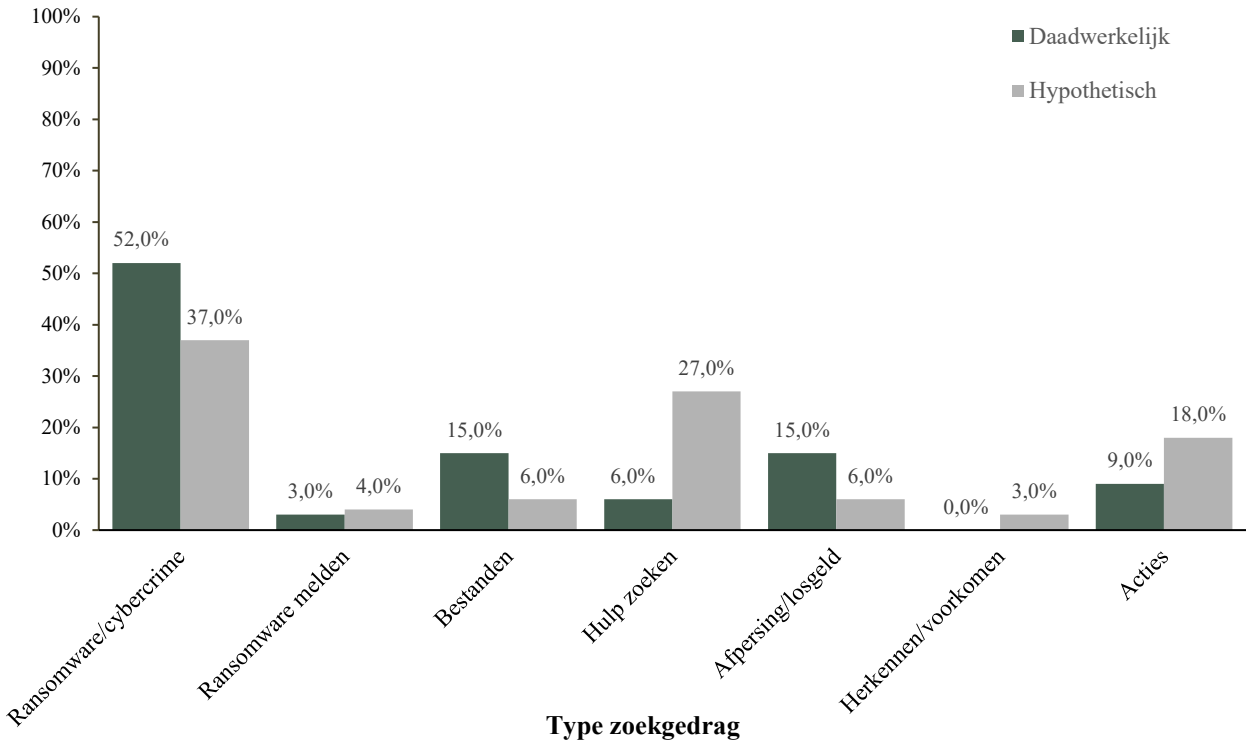
betreft het zoeken van hulp. Zoektermen in deze categorie richten zich bijvoorbeeld op aspecten als hulp bij internet oplichting of het opzoeken van de politie, de contactgegevens van de eigen bank, of de Fraudehelpdesk.

Figuur 4.13 Verschillende typen zoekgedrag na slachtofferschap van fraude onder burgers



In Figuur 4.14 zijn de zoektermen van slachtoffers van ransomware weergegeven, tevens uitgesplitst naar verschillende thema's. Uit Figuur 4.14 blijkt dat het grootste aandeel van de respondenten heeft gezocht of zou zoeken op zoektermen gerelateerd aan ransomware of cybercrime. Dit heeft bijvoorbeeld betrekking op zoektermen gerelateerd aan een hack of gijzeling van een computer, malware of een cyber aanval. De op een na meeste voorkomende categorie betreft voor de hypothetische zoektermen het zoeken naar hulp. Voor de daadwerkelijke zoektermen betreft dit zoektermen gerelateerd aan versleutelde bestanden of afpersing en losgeld (bijv. moet ik losgeld betalen).

Figuur 4.14 Verschillende typen zoekgedrag na slachtofferschap van ransomware onder ondernemers



4.6. Aanpassingen in gedrag na slachtofferschap

Tot slot is aan respondenten gevraagd of ze hun gedrag hebben aangepast nadat ze slachtoffer zijn geworden. Eerst is aan respondenten gevraagd of ze, met uitzondering van eventuele maatregelen die ze al namen, een aantal beveiligingsmaatregelen genomen hebben nadat ze slachtoffer zijn geworden (Tabel 4.9). Respondenten konden meerdere antwoorden kiezen. De meerderheid van de slachtoffers van online fraude heeft geen van de genoemde beveiligingsmaatregelen genomen na het slachtofferschap (70,8%). Onder de slachtoffers van fraude die wel (aanvullende) beveiligingsmaatregelen hebben genomen, waren de meest voorkomende maatregelen het gebruik van sterke, unieke wachtwoorden (16,6%), gevolgd door het gebruik van tweestapsverificatie (11,6%) en gebruik van een up-to-date antivirus product (9%).

In tegenstelling tot de slachtoffers van online fraude, heeft juist de meerderheid van de ransomware slachtoffers een of meer van de genoemde beveiligingsmaatregelen genomen (95,3%). De meest voorkomende maatregelen waren regelmatige back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server (58,9%), gevolgd door gebruik van een antivirus product (49,5%) en gebruik van tweestapsverificatie (43,9%).

Tabel 4.9 Frequentie van getroffen beveiligingsmaatregelen na slachtofferschap onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude		**Ransomware**	
	n	**%**	***n***	**%**
Getroffen beveiligingsmaatregelen na slachtofferschap *(meerdere antwoorden mogelijk)*	**535**		**107**	
Een ander besturingssysteem genomen	9	1,7%	8	7,5%
Regelmatige back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	36	6,7%	63	58,9%
Gebruik van sterke, unieke wachtwoorden	89	16,6%	45	42,1%
Gebruik van een up-to-date antivirus product	48	9,0%	53	49,5%
Gebruik van een firewall	28	5,2%	35	32,7%
Beveiligingssoftware netwerken en apparaten laten scannen op virussen of andere kwaadaardige software	29	5,4%	33	30,8%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	37	6,9%	27	25,2%
Een ander standaardbrowser genomen	7	1,3%	4	3,7%
Gebruik van een VPN-verbinding	25	4,7%	15	14,0%
Installatie van browser extensies die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren	11	2,1%	7	6,5%
Gevoelige bestanden en gegevens worden versleuteld	13	2,4%	9	8,4%
Tweestapsverificatie	62	11,6%	47	43,9%
Monitoren van gebruikers- of netwerkactiviteiten	-	-	6	5,6%
Iemand (intern of extern) in dienst die verantwoordelijk is voor de cybersecurity	-	-	9	8,4%
Een bedrijfscontinuïteitsplan dat betrekking heeft op de cybersecurity	-	-	6	5,6%
Geen van bovenstaande opties	379	70,8%	5	4,7%

Ten tweede is aan respondenten gevraagd of ze bepaalde online activiteiten beperkt of verminderd hebben nadat ze slachtoffer zijn geworden (Tabel 4.10). Respondenten konden meerdere antwoorden kiezen. Bijna de helft van de slachtoffers van online fraude beperkte of verminderde bepaalde online activiteiten (43.6%). Bijna een derde van de slachtoffers van online fraude beperkte of verminderde het online bestellen, reserveren of betalen voor producten of diensten (31%). Dit wordt gevolgd door het beperken of verminderen van gebruik van accounts of pagina's op sociale media (13,1%) en informatie zoeken of surfen op internet (4,1%). Iets meer dan de helft van de slachtoffers van online fraude heeft geen van de genoemde activiteiten beperkt of verminderd (56,4%).

De meerderheid van de slachtoffers van ransomware heeft geen van de genoemde activiteiten beperkt of verminderd (72,9%). Ongeveer 12% van de slachtoffers van ransomware beperkte of verminderde het gebruik van accounts of pagina's op sociale media (11,2%), gevolgd door het beperken of

verminderen van surfen op internet (9,3%) en het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs (8,4%).

Tabel 4.10 Frequentie van beperkingen in online activiteiten na slachtofferschap onder slachtoffers van online fraude (*n*=535) en ransomware (*n*=107)

	Online fraude		**Ransomware**	
	n	**%**	***n***	**%**
Beperkingen in online activiteiten *(meerdere antwoorden mogelijk)*	**535**		**107**	
Gebruik van accounts of pagina's op sociale media	70	13,1%	12	11,2%
E-mailen	13	2,4%	3	2,8%
Informatie zoeken of surfen op internet	22	4,1%	10	9,3%
Tekstberichten sturen, bijv. via WhatsApp	11	2,1%	7	6,5%
Bellen of beeldbellen, bijv. via WhatsApp, Zoom of FaceTime	5	0,9%	5	4,7%
Online bestellen, reserveren, betalen voor producten of diensten	166	31%	-	-
De mogelijkheid voor klanten om online te bestellen, reserveren, betalen voor producten of diensten, of een schenking te doen.	-	-	1	0,9%
Gebruik van internetbankieren of mobiel bankeren	16	3%	4	3,7%
Streamen van muziek, films, software en/of games	5	0,9%	-	-
Gamen of spelletjes spelen	3	0,6%	-	-
Bezoek van datingsites of apps	12	2,2%	-	-
Bezoek van goksites	5	0,9%		
De mogelijkheid voor klanten om online toegang te krijgen tot (enkele van) mijn diensten	-	-	3	2,8%
Gebruik van online systemen of software, zoals een industrieel controlesysteem of ERP systeem	-	-	3	2,8%
Elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs	-	-	9	8,4%
Geen van de bovenstaande opties	302	56,4%	78	72,9%

Hoofdstuk 5: Advertentiecampagnes

In dit hoofdstuk worden de resultaten uiteengezet van de advertentiecampagnes gericht op slachtofferschap van online fraude en ransomware.

5.1. Interactie met advertentiecampagnes

Gedurende de duur van de advertentiecampagnes genereerde de campagne voor online fraude in totaal 110.440 impressies en 831 kliks, met een doorklikratio van 0,6%. De advertentiecampagne voor ransomware genereerde in totaal 15.296 impressies en 373 kliks, met een doorklikratio van 2,4%.

Uit Tabel 6.1 blijkt dat de meeste internetgebruikers de advertenties in beide campagnes te zien kregen op hun mobiele telefoon. Voor online fraude was het aantal impressies en kliks het hoogst onder de leeftijdscategorie 65+. Voor ransomware was het aantal impressies tevens het hoogst onder de leeftijdscategorie 65+, maar is het vaakst geklikt op de advertenties door internetgebruikers in de leeftijdscategorie 25-34 jaar. Daarnaast blijkt uit de tabel dat de doorklikratio voor beide campagnes afnam naarmate de leeftijd toenam, wat zou kunnen suggereren dat de advertenties relevanter zijn voor jongere leeftijdsgroepen dan oudere leeftijdsgroepen. Het aandeel impressies en kliks was het hoogste onder vrouwen voor online fraude, en het hoogst onder mannen voor ransomware. Een belangrijke kanttekening bij deze resultaten is dat voor een grote groep respondenten geen demografische kenmerken bekend zijn, zoals aangeduid in de tabel.

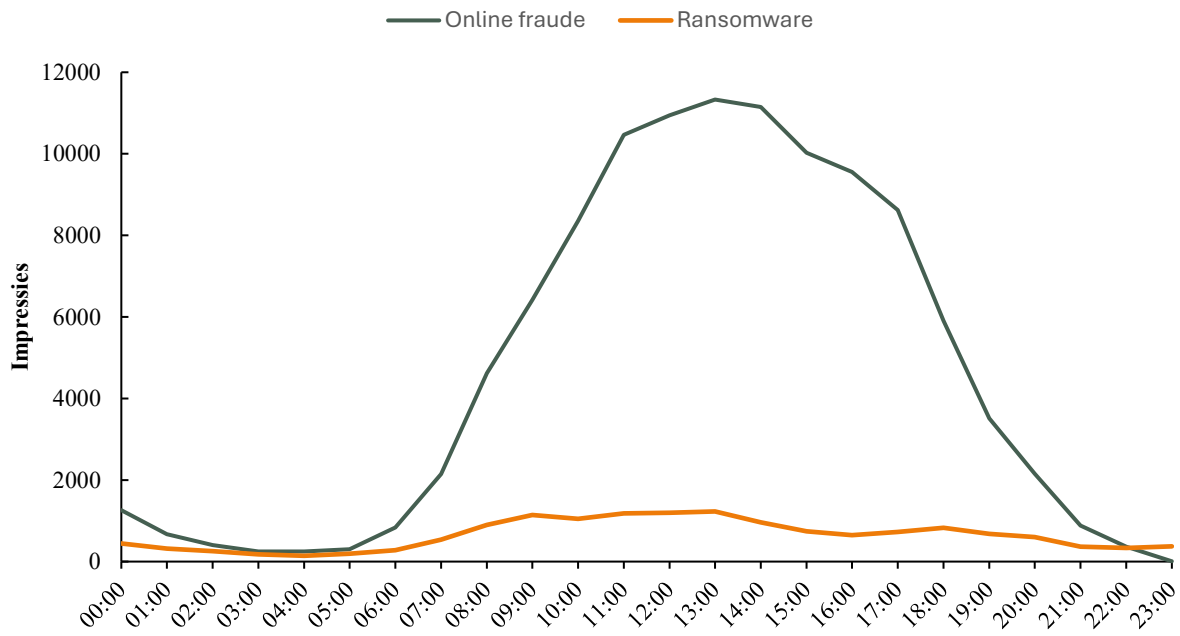
Tabel 6.1 Interactie met advertentiecampagnes gericht op online fraude en ransomware, uitgesplitst naar leeftijd, geslacht, provincie en gebruikte apparaten

	Online fraude					**Ransomware**				
	Impressies (*n*=110.440)		**Kliks (*n*=831)**		**CTR (%)**	**Impressies (*n*=15.296)**		**Kliks (*n*=373)**		**CTR (%)**
	n	**%**	***n***	**%**		***n***	**%**	***n***	**%**	
Leeftijd										
18-24	668	0,6%	41	4,9%	6,1%	498	3,3%	27	7,2%	5,4%
25-34	2.724	2,5%	105	12,6%	3,9%	1.777	7,7%	58	15,5%	4,9%
35-44	3.552	3,2%	91	11,0%	2,6%	840	5,5%	29	7,8%	3,5%
45-54	6.566	5,9%	83	10,0%	1,3%	903	5,9%	24	6,4%	2,7%
55-64	16.946	15,3%	93	11,2%	0,6%	1.298	8,5%	24	6,4%	1,9%
65+	53.821	48,7%	117	14,1%	0,2%	2.750	18,0%	35	9,4%	1,3%
Onbekend	26.163	23,7%	301	36,2%	1,2%	7.830	51,2%	176	47,2%	2,3%
Geslacht										
Vrouw	51.790	46,9%	266	32,0%	0,5%	3.589	23,5%	71	19,0%	2,0%
Man	31.529	28,5%	259	31,2%	0,8%	3.898	25,5%	128	34,3%	3,3%
Onbekend	27.121	24,6%	306	36,8%	1,1%	7.809	51,1%	174	46,6%	2,2%
Provincie										
Drenthe	3.015	2,7%	17	2,0%	0,6%	424	2,8%	7	1,9%	1,7%

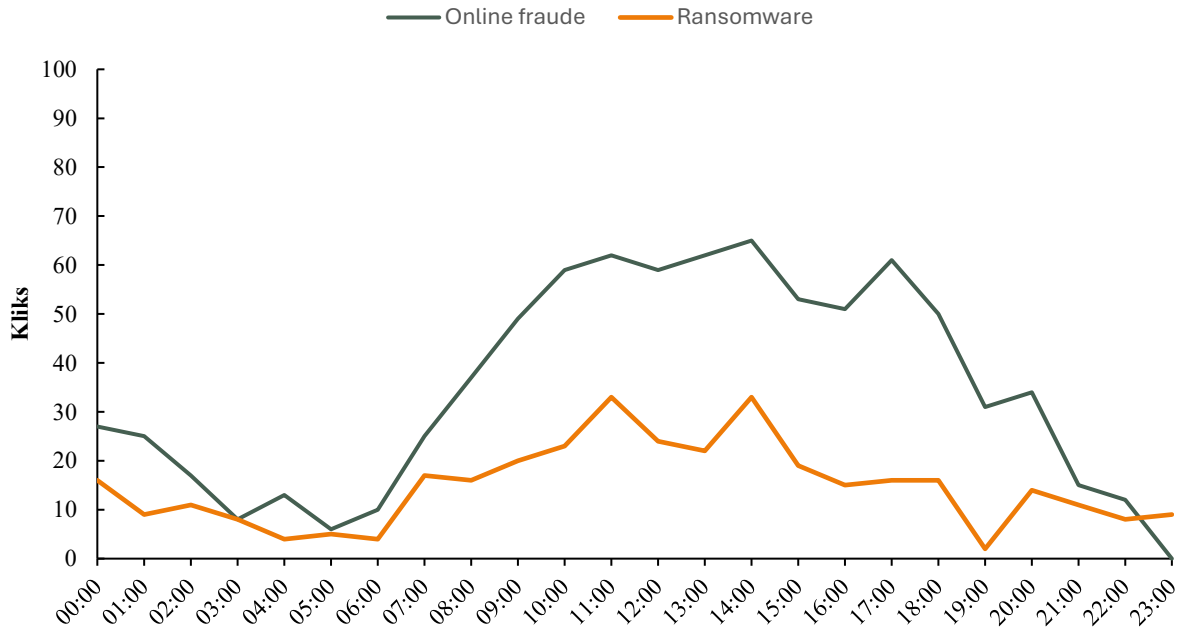
	Online fraude					Ransomware				
	Impressies (*n*=110.440)		**Kliks (*n*=831)**		**CTR (%)**	**Impressies (*n*=15.296)**		**Kliks (*n*=373)**		**CTR (%)**
	n	**%**	***n***	**%**		***n***	**%**	***n***	**%**	
Flevoland	1.978	1,8%	15	1,8%	0,8%	285	1,9%	3	0,8%	1,0%
Friesland	3.158	2,9%	19	2,3%	0,6%	451	2,9%	6	1,6%	1,3%
Gelderland	12.603	11,4%	91	11,0%	0,7%	1.693	11,1%	35	9,4%	2,1%
Groningen	3.307	3,0%	25	3,0%	0,8%	376	2,5%	12	3,2%	3,2%
Limburg	8.713	7,9%	53	6,4%	0,6%	893	5,8%	20	5,4%	2,2%
Noord-Brabant	19.871	18,0%	118	14,2%	0,6%	1.958	12,8%	45	12,1%	2,3%
Noord-Holland	15.384	13,9%	161	19,4%	1,1%	3.312	21,7%	105	28,2%	3,2%
Overijssel	5.977	5,4%	46	5,5%	0,8%	741	4,8%	14	3,8%	2,0%
Zuid-Holland	25.272	22,9%	206	24,8%	0,8%	3.746	24,5%	84	22,5%	2,2%
Utrecht	5.422	4,9%	48	5,8%	0,9%	800	5,2%	20	5,4%	2,5%
Zeeland	5.430	4,9%	23	2,8%	0,4%	310	2,0%	9	2,1%	2,6%
Onbekend	310	0,3%	9	1,1%		307	2,0%	14	3,8%	
Gebruikte apparaat										
Computer	2.845	2,6%	107	12,9%	3,8%	2.668	17,4%	82	22,0%	3,1%
Mobiele telefoon	103.026	93,3%	705	84,8%	0,7%	11.933	78,0%	265	71,0%	2,2%
Tablet	4.569	4,1%	19	2,3%	0,4%	695	4,5%	26	7,0%	3,7%
Tv-scherm	0	0,0%	0	0,0%	0,0%	0	0,0%	0	0,0%	0,0%
Onbekend	0	0,0%	0	0,0%	0,0%	0	0,0%	0	0,0%	0,0%

Wanneer gekeken wordt naar de interactie met de advertentiecampagne naar uren van de dag, is te zien dat de grootste piek in het aandeel impressies (Figuur 6.1) en kliks (Figuur 6.2) voor beide campagnes het hoogst was tussen 11:00 en 14:00 uur. Voor online fraude was er daarnaast een piek in het aandeel kliks rond 17:00 uur.

Figuur 6.1 Impressies van de campagnes uitgesplitst naar uren per dag



Figuur 6.2 Kliks van de campagnes uitgesplitst naar uren per dag



5.2. Zoektermen

De data geven ook inzicht in welke vooraf gedefinieerde zoektermen het vaakst een van de advertenties hebben getriggerd, evenals de door internetgebruikers daadwerkelijk ingevulde zoektermen. Met betrekking tot de vooraf gedefinieerde zoektermen (zie ook hoofdstuk 4) valt op dat er voor de advertentiecampagne gericht op online fraude variatie zit in de zoektermen, variërend van een omschrijving van wat internetgebruikers is overkomen, te ondernemen acties of het melden of doen van aangifte (Tabel 6.3). Tevens valt op dat de meest gebruikte zoektermen variëren tussen impressies, kliks en de doorklikratio. Ook wanneer gekeken wordt naar de zoektermen die door gebruikers zijn ingevuld (Tabel 6.4) is er variatie zichtbaar in de zoektermen, variërend van een beschrijving van het type fraude, het terugkrijgen van geld of het willen doen van een melding of aangifte.

Tabel 6.3 Top 10 vooraf gedefinieerde zoektermen voor de advertentiecampagne voor online fraude

Rang	O.b.v. impressies	O.b.v. kliks	O.b.v. CTR (met >49 impressies)[13]
1.	Oplichting melden	Oplichting melden	Juridische hulp oplichting
2.	Wat te doen bij oplichting	Opgelicht via internet	Account gehackt
3.	Wat te doen bij fraude	Online fraude melden	Gekocht product niet geleverd
4.	Opgelicht via internet	Aangifte doen van oplichting	Is deze website betrouwbaar
5.	Online fraude melden	Account gehackt	Aangifte politie online oplichting
6.	Hoe weet je of je bent opgelicht	Wat te doen bij oplichting	Ik ben opgelicht wat nu
7.	Wat te doen bij oplichting	Is deze website betrouwbaar	Aangifte oplichting
8.	Online opgelicht wat nu	Aangifte politie online oplichting	Marktplaats oplichting
9.	Wat doen bij oplichting	Hulp bij oplichting	Bestelling niet ontvangen
10.	Aangifte doen van oplichting	Opgelicht tros	Geld terugkrijgen na fraude

[13] Sommige zoekopdrachten leveren een hoge doorklikratio op ondanks dat ze slechts een enkele keer zijn ingevoerd (bijvoorbeeld een zoekopdracht die één impressie en één klik oplevert resulteert in een doorklikratio van 100%). Daarom is voor de derde kolom gefilterd op zoekopdrachten met ten minste 50 impressies, in navolging van (Moneva & Leukfeldt, 2024a).

Tabel 6.4 Top 10 gebruikte zoektermen door gebruikers voor de advertentiecampagne voor online fraude

Rang	O.b.v. impressies	O.b.v. kliks	O.b.v. CTR (met >49 impressies)
1.	Oplichting	Oplichting	My instagram account hacked
2.	Telefonische fraude	Opgelicht	Aangifte doen van oplichting
3.	Opgelicht	Aangifte doen politie	Aangifte doen politie
4.	Fraude	Fraude melden	Ik ben opgelicht hoe krijg ik mijn geld terug
5.	Phishing	Aangifte doen van oplichting	Internet oplichting melden
6.	Aangifte doen politie	Identiteitsfraude	Fraudehelpdesk
7.	Internetoplichters lijst	My Instagram account hacked	Fraude melden
8.	Identiteitsfraude	Oplichtingspraktijken melden	Oplichtingspraktijken melden
9.	Aangifte doen	Ik ben opgelicht hoe krijg ik mijn geld terug	Identiteitsfraude
10.	Fraude melden	Opgelicht door webshop	Instagram gehackt

Bij de advertentiecampagne voor ransomware valt op dat zowel de vooraf gedefinieerde zoektermen (Tabel 6.5) als de zoektermen van gebruikers de zoektermen (Tabel 6.6) meer generiek zijn dan bij de advertentiecampagne voor fraude. Zo hebben veel zoektermen geen betrekking op ransomware of versleuteling, maar op een ruimere beschrijving van een hack. De zoektermen richten zich op een omschrijving van wat internetgebruikers overkomen is en wat men moet doen. In vergelijking met de advertentiecampagne voor online fraude is het willen doen van een melding of aangifte minder aanwezig in de zoektermen.

Tabel 6.5 Top 10 vooraf gedefinieerde zoektermen voor de advertentiecampagne voor ransomware

Rang	O.b.v. impressies	O.b.v. kliks	O.b.v. CTR (met >49 impressies)
1.	Ben ik gehackt	Ben ik gehackt	Online chantage
2.	Ik krijg een mail dat ik gehackt ben	Ik word gehackt	Ben ik gehackt website
3.	Ik word gehackt	Ben ik gehackt website	Bestanden versleuteld
4.	Computer gehackt	Computer gehackt	Ben ik gehackt check
5.	Cybercrime hulp	Ik krijg een mail dat ik gehackt ben	Ransomware voorkomen
6.	Ik ben gehackt	Online chantage	Controleren of ik gehackt ben
7.	Ik denk dat ik gehackt ben	Ik ben gehackt wat moet ik doen	Ik word gehackt
8.	Ransomware wat te doen	Ben ik gehackt check	Check of ik gehackt ben
9.	Ben ik gehackt op mijn telefoon	Ik ben gehackt	Ransomware solution
10.	Ik ben gehackt wat moet ik doen	Computer gehackt	Ik ben gehackt wat moet ik doen

Tabel 6.6 Top 10 gebruikte zoektermen door gebruikers voor de advertentiecampagne voor ransomware

Rang	O.b.v. impressies	O.b.v. kliks	O.b.v. CTR (met >49 impressies)
1.	Phishing	Dark web	Dark web
2.	Cyberaanval	Comment on I need a hacker to recover my stolen btc	Ben ik gehackt check
3.	Ben ik gehackt	Ben ik gehackt	Ben ik gehackt
4.	Ransomware	Ben ik gehackt check	Telefoon gehackt wat nu
5.	Dark web	Telefoon gehackt wat nu	Hoe weet ik of mijn telefoon gehackt is
6.	Telefoon gehackt wat nu	Ransomware	Ransomware
7.	Computercriminaliteit	Ransomware betekenis	Is this link safe
8.	Ransomware betekenis	Ik ben gehackt wat nu	Wat is ransomware
9.	Zijn mijn gegevens gehackt	My instagram account hacked	Iphone gehackt
10.	Ben ik gehackt check	Phishing	Ransomware betekenis

5.3. Prestatie van advertenties

Zoals in paragraaf 3.3.1. is beschreven, is er binnen de advertentiecampagne gevarieerd in de achterliggende gedachte van de advertenties, waarbij onderscheid is gemaakt tussen een neutrale advertentie, probleemgerichte coping en emotiegerichte coping. Uit Tabel 6.7 blijkt dat bij de advertentiecampagne voor online fraude de neutrale advertentie het beste presteert met een doorklikratio van 2,1%. Daarentegen presteert de advertentie gericht op emotiegerichte coping het beste bij de advertentiecampagne voor ransomware met een doorklikratio van 5% (Tabel 6.8).

Tabel 6.7 Interactie met advertenties gericht op online fraude

Advertentie	Impressies		Kliks		CTR
	n	**%**	***n***	**%**	**%**
Online opgelicht, wat nu? | Slachtofferhulp Nederland | Hulp na online oplichting Oplichters maken gebruik van bedrog met als doel geld te verdienen. Lees hier meer.	21.709	19,6%	459	55,2%	2,1%
Wat te doen bij oplichting? | Slachtofferhulp Nederland | Hulp na online oplichting Ben je online opgelicht en hierdoor geld verloren? Lees wat je kunt doen.	62.776	56,8%	338	40,7%	0,5%
Emotionele steun na oplichting| Slachtofferhulp Nederland | Hulp na online oplichting Online oplichting kan leiden tot negatieve emoties en stress. Wij helpen je daarbij.	25.955	23,5%	34	4,1%	0,1%

Tabel 6.8 Interactie met advertenties gericht op ransomware

Advertentie	**Impressies**		**Kliks**		**CTR**
	n	**%**	***n***	**%**	**%**
Ransomware, wat nu? | Slachtofferhulp Nederland | Hulp na ransomware Ransomware blokkeert toegang tot bestanden in ruil voor losgeld. Lees hier meer	4.172		87		2,1%
Wat te doen bij ransomware? | Slachtofferhulp Nederland | Hulp na ransomware Zijn je bestanden versleuteld en wordt er losgeld gevraagd? Lees wat je kunt doen.	10.113		235		2,3%
Emotionele steun bij ransomware | Slachtofferhulp Nederland | Hulp na ransomware Ransomware kan leiden tot negatieve emoties en stress. Wij helpen je daarbij.	1.011		51		5,0%

Hoofdstuk 6: Discussie

Jaarlijks worden ongeveer 1 op de 6 Nederlanders slachtoffer van online criminaliteit (CBS, 2026b). Een deel van de slachtoffers zoekt hulp bij formele instanties of informele hulpbronnen (De Kimpe et al., 2020; Pereira et al., 2016; Voce & Morgan, 2025). Tegelijkertijd zoekt een deel van de slachtoffers mogelijk ook online naar informatie of middelen om met slachtofferschap om te gaan. Tot op heden is er echter nauwelijks onderzoek gedaan naar het online hulpzoekgedrag van slachtoffers van online criminaliteit. Het huidige onderzoek had enerzijds als doel om meer inzicht te verkrijgen in de behoeften en het online hulpzoekgedrag van slachtoffers van online fraude en ransomware en anderzijds als doel om een interventie te ontwikkelen in de vorm van een online advertentiecampagne om slachtoffers van informatie en hulpbronnen te voorzien. Dit is onderzocht aan de hand van een vragenlijst onder slachtoffers van online fraude en ransomware, een analyse van zoektermen in de Google zoekwoordplanner en advertentiecampagnes in Google Ads.

In de volgende paragrafen zal eerst een antwoord gegeven worden op de deelvragen. Vervolgens wordt ingegaan op de beperkingen van het onderzoek, suggesties voor vervolgonderzoek en aanbevelingen voor de praktijk.

6.1. Conclusies

6.1.1. Gevolgen van slachtofferschap

De eerste deelvraag van het onderzoek richtte zich op de gevolgen die slachtoffers van online fraude en ransomware ervaren na slachtofferschap. Slachtoffers van online fraude rapporteerden over het algemeen beperkte financiële gevolgen: 66% gaf aan dat de financiële gevolgen tussen de €1 en €100 lagen. Daarnaast gaf ongeveer 6% van de slachtoffers van online fraude aan geen financiële gevolgen te hebben ervaren. Onder slachtoffers van ransomware gaf een groter aandeel (ongeveer 38%) aan geen financiële gevolgen te hebben ervaren. De schadebedragen waren onder slachtoffers van ransomware over het algemeen meer gevarieerd en hoger. Voor de meeste respondenten kostte het ransomware incident tussen 251 en 1.000 euro.

Een groot deel van slachtoffers van online fraude en ransomware ervaarde geen emotionele, psychische of lichamelijke gevolgen. De gerapporteerde gevolgen kwamen grotendeels overeen voor beide groepen. Respondenten rapporteerden het meest dat ze zich boos voelden over het incidenten, en rapporteerden het minst dat ze angstklachten en/of paniekaanvallen en lichamelijke klachten hadden.

Ook andere gevolgen werden gemiddeld genomen beperkt ervaren, maar respondenten uit beide groepen gaven relatief vaak aan voorzichtiger te zijn geworden op het internet. Een verschil tussen beide groepen was dat slachtoffers van ransomware vaker kosten maakten voor reparatie of herstel. Slachtoffers van online fraude die gevolgen hadden ervaren, beoordeelden deze over het algemeen als ernstig, met

uitzondering van de financiële gevolgen. Onder slachtoffers van ransomware werden alleen de financiële gevolgen beoordeeld omdat geen respondenten aangaven emotionele, psychische, lichamelijke of andere gevolgen te hebben ervaren. Slechts een klein deel van de respondenten ervoer de financiële gevolgen als ernstig, hoewel dit aandeel groter was in vergelijking met slachtoffers van online fraude.

6.1.2. De informatie- en hulpbehoeften van slachtoffers

De tweede deelvraag van het onderzoek richtte zich op de informatie- en hulpbehoeften die slachtoffers van online fraude en ransomware ervaren na slachtofferschap. Uit de resultaten van de vragenlijst (deelstudie 1) blijkt dat de informatiebehoeften van beide groepen slachtoffers zowel overeenkomsten als verschillen vertonen. Hoewel de meeste slachtoffers van zowel online fraude als ransomware behoefte hadden aan informatie over het oplossen van het probleem, liepen andere behoeften meer uiteen. Veel slachtoffers van online fraude hadden ook behoefte aan informatie over het vergoed krijgen van de financiële schade en het voorkomen van slachtofferschap in de toekomst. Daarentegen hadden ransomware slachtoffers behoefte aan informatie over het voorkomen van toekomstig slachtofferschap en informatie over hoe het heeft kunnen gebeuren. Beide groepen slachtoffers hadden weinig behoefte aan informatie over emotionele, psychische of lichamelijke gevolgen.

Ook als het gaat om de hulpbehoeften zijn er overeenkomsten en verschillen tussen beide groepen slachtoffers, zo blijkt uit de resultaten van de vragenlijst (deelstudie 1). Het grootste aandeel van zowel de slachtoffers van online fraude als slachtoffers van ransomware had behoefte aan hulp bij het oplossen van het probleem, hoewel dit aandeel hoger was onder slachtoffers van ransomware. Voor online fraude werd dit gevolgd door hulp bij het vergoed krijgen van de financiële schade en andere behoeften dan in de vragenlijst bevraagd werden, terwijl dit voor ransomware gevolg werd door hulp bij het voorkomen van slachtofferschap in de toekomst en hulp bij het doen van een melding of aangifte bij de politie. Ook bij de hulpbehoeften hadden beide groepen slachtoffers de minste behoefte aan hulp bij emotionele, psychische of lichamelijke gevolgen. De hulpbehoeften van beide groepen sluiten hiermee grotendeels aan bij de behoeften zoals geïdentificeerd uit eerder onderzoek naar traditionele criminaliteit (bijv. Ten Boom et al., 2008) en online criminaliteit (bijv. Borwell et al., 2024; Cross et al., 2016; Leukfeldt et al., 2019; Van Leuken et al., 2026), waaronder informatie over het delict en hoe het heeft kunnen gebeuren, financiële behoeften en beschikbare hulproutes. Andere behoeften uit de literatuur komen minder nadrukkelijk naar voren in het huidige onderzoek, zoals hulp bij emotionele, psychologische of lichamelijke klachten, erkenning als slachtoffer of informatie of hulp over juridische zaken.

6.1.3. Het (online) hulpzoekgedrag van slachtoffers

De derde deelvraag van het onderzoek richtte zich op de organisaties of informatiebronnen die slachtoffers van online fraude en ransomware gebruiken om te zoeken naar hulp.

Uit de vragenlijst (deelstudie 1) blijkt dat een aanzienlijke groep slachtoffers van online fraude en ransomware hulp heeft gezocht, hoewel dit aandeel onder slachtoffers van online fraude lager lag (ongeveer 62%) dan bij slachtoffers van ransomware (ongeveer 91%). De slachtoffers van online fraude zochten vooral hulp bij vrienden, familie, kennissen of collega's, gevolgd door bij de politie, en een bank- of financiële instelling. Die laatste twee partijen kwam in eerder onderzoek ook naar voren als belangrijke informatie- of hulpbronnen (Van Leuken & Van 't Hoff-de Goede, 2025). Slachtoffers van ransomware zochten vooral hulp bij een cybersecuritybedrijf, IT-specialist of IT-leverancier, gevolgd door vrienden, familie, kennissen of collega's en de politie. Ook dit is voor een groot deel in overeenstemming met eerder onderzoek (Matthijsse et al., 2025a; Voce & Morgan, 2022). Hoewel er wat variatie is tussen hulpbronnen, zijn er ook overeenkomsten in de hulpbronnen die beide groepen slachtoffers benutten. Uit de resultaten blijkt bovendien dat een groot deel van respondenten al bekend was met de formele organisaties waarbij ze hulp hebben gezocht.

In de vragenlijst is ook bevraagd of slachtoffers op internet gezocht hebben, bijvoorbeeld naar informatie of ondersteuning. Onder slachtoffers van online fraude was dit het geval bij iets meer dan de helft van de respondenten (57%), terwijl dit bij slachtoffers van ransomware bij de minderheid van de respondenten het geval was (ongeveer 38%). Beide groepen slachtoffers die online gezocht hebben maakten grotendeels gebruik van Google. Ongeveer 20% tot 37% van de slachtoffers van online fraude heeft niet de informatie, hulp of organisaties gevonden die ze zochten. Bij slachtoffers van ransomware was dit bij ongeveer 20% tot 27% het geval.

6.1.4. De zoektermen die slachtoffers online gebruiken

De vierde deelvraag richtte zich op de zoektermen die slachtoffers van online fraude en ransomware gebruiken wanneer zij via Google zoeken naar informatie of hulp.

In de vragenlijst (deelstudie 1) is aan respondenten die online hebben gezocht gevraagd wat ze tijdens het incident hebben ingetypt in de zoekmachine. Zowel de slachtoffers die online gezocht hebben als de slachtoffers die niet online gezocht hebben is bovendien gevraagd wat ze zouden intypen in een zoekmachine als ze nu opnieuw slachtoffer zouden worden. Het grootste aandeel van de slachtoffers van online fraude heeft gezocht of zou zoeken op zoektermen gerelateerd aan de verkopende partij (mogelijk duidend op slachtofferschap van aankoopfraude), gevolgd door zoektermen gerelateerd aan een specifieke type fraude en zoektermen gerelateerd aan het zoeken naar hulp. Het grootste aandeel van de slachtoffers van ransomware heeft gezocht of zou zoeken op zoektermen gerelateerd aan ransomware of cybercrime,

gevolgd door zoektermen gerelateerd aan het zoeken naar hulp of zoektermen gerelateerd aan versleutelde bestanden of afpersing en losgeld. Deze resultaten duiden aan dat slachtoffers uiteenlopende zoektermen gebruiken, die ook een ander doel lijken te dienen. Waar sommige respondenten geen concrete hulpvraag lijken te formuleren en vooral zoeken op termen gerelateerd aan het delict, zijn andere respondenten specifiek naar hulpverlening of praktische oplossingen op zoek.

De in deelstudie 1 verzamelde zoektermen vormden de basis voor deelstudie 2. In deze deelstudie zijn de door slachtoffers gerapporteerde zoektermen aangevuld met gerelateerde zoektermen die voorgesteld zijn door de Google zoekwoordplanner. Na een proces van in- en exclusie heeft dit geleid tot een definitieve lijst met zoektermen die de basis vormde voor de advertentiecampagnes in deelstudie 3.

In de advertentiecampagnes (deelstudie 3) is nader inzicht verkregen in de zoektermen uit de vragenlijsten (deelstudie 1) en zoekwoordplanner (deelstudie 2) die het vaakst een van de advertenties hebben getriggerd. Bij online fraude varieerden zoektermen van een omschrijving van de fraude tot te nemen acties of het doen van een melding of aangifte. Bij ransomware ging het om een vergelijkbare variatie in thema's, behalve dat het willen doen van een melding of aangifte minder duidelijk terugkwam in de zoektermen ten opzichte van online fraude. Daarnaast blijkt uit de resultaten dat de zoektermen van ransomware meer generiek zijn, zoals een ruime beschrijving van een hack, terwijl de zoektermen voor online fraude meer gericht zijn op fraude in het algemeen of specifieke fraudevormen. Dit zou er mogelijk op kunnen duiden dat internetgebruikers bij de advertentiecampagne van ransomware nog niet goed weten waar ze slachtoffer van zijn geworden.

De advertentiecampagnes (deelstudie 3) hebben ook inzicht gegeven in de zoektermen die gebruikers zelf hebben ingevuld. Ook daarin is er variatie zichtbaar in de zoektermen. Bij online fraude varieert dit van een beschrijving van het type fraude, het terugkrijgen van geld of het willen doen van een melding of aangifte. Bij ransomware gaat het vooral om brede omschrijving van een hack, of de vraag wat te doen. Uit de resultaten kan geconcludeerd worden dat slachtoffers uiteenlopende zoektermen gebruiken, die corresponderen met uiteenlopende hulpvragen of behoeften.

6.1.5. Interactie met advertentiecampagnes

Tot slot was de vijfde deelvraag van het onderzoek in hoeverre online advertentiecampagnes slachtoffers van online fraude en ransomware kunnen bereiken om hen informatie of hulp te bieden.

Uit deelstudie 3 blijkt dat de advertentiecampagne in zeven dagen tijd voor online fraude in totaal 110.440 impressies en 831 kliks genereerde, met een doorklikratio (het percentage van de gebruikers die de advertentie te zien kreeg (impressie) en hier vervolgens op geklikt heeft) van 0,6%. De advertentiecampagne voor ransomware genereerde in totaal 15.296 impressies en 373 kliks, met een doorklikratio van 2,4%. Hieruit kan worden opgemaakt dat er veel meer gezocht wordt op terminologie

gerelateerd aan online fraude, maar dat deze zoekopdrachten bij slechts een klein deel van de internetgebruikers leiden tot kliks op de advertentie. Bij de advertentiecampagne voor de ransomware is de discrepantie tussen impressie en kliks kleiner, wat suggereert dat deze advertentiecampagne beter in staat is om de juiste doelgroep van slachtoffers van ransomware te bereiken, hoewel de vooraf-gedefinieerde zoektermen juist meer generiek waren dan bij online fraude.

Uit de resultaten blijkt bovendien dat de doorklikratio voor beide campagnes vergelijkbaar is met de advertentiecampagne gericht op geldezels (Bekkers et al., 2022), maar relatief laag is in vergelijking met eerdere advertentiecampagnes gericht op het plegen van DDoS-aanvallen of slachtofferschap van Image-Based Sexual Harassment (IBSH) en Image-Based Sexual Abuse (IBSA) (Moneva et al., 2022; Pijlman & Burgmeijer, 2024). Dit is nog meer het geval voor de advertentiecampagne gericht op online fraude. Dit zou ermee te maken kunnen hebben dat sommige van deze onderzoeken zich op specifieke onderwerpen richten zoals DDoS en booters die gekenmerkt worden door een meer afgebakende demografische groep en specifiek taalgebruik of slang. Dat maakt het mogelijk om meer specifieke zoekwoorden voor de advertentiecampagne te ontwikkelen. Een gebrek aan precisie in de targeting heeft enkele nadelen, namelijk dat campagnes voor opdringeriger zijn, duurder en bovendien moeilijker te analyseren.

6.2. Beperkingen en suggesties voor vervolgonderzoek

Bij de interpretatie van de resultaten dient er rekening te worden gehouden met enkele beperkingen. Voor deelstudie 1 is een vragenlijstonderzoek uitgevoerd onder slachtoffers van online fraude en ransomware middels een panelbureau. Door gebruik te maken van het panelbureau was het mogelijk om onder een grote, representatieve groep respondenten slachtoffers te werven. Hoewel de groep respondenten niet representatief is voor de populatie burgers en ondernemers in Nederland, was het doel van het onderzoek niet om een representatieve steekproef van deze populatie te verkrijgen, maar om slachtoffers van online fraude en ransomware te bevragen. Het gebrek aan representativiteit is daarmee een logisch gevolg van het feit dat alleen slachtoffers zijn geselecteerd. Wel moet opgemerkt worden dat de steekproef voor online fraude een aanzienlijke groep slachtoffers van aankoopfraude omvat. Hoewel dit de hoge prevalentie van aankoopfraude in de Nederlandse maatschappij weerspiegelt (CBS, 2026b), kan dit mogelijk de resultaten wat vertekend hebben. In toekomstig onderzoek zou het raadzaam zijn om meer slachtoffers van andere fraudevormen te includeren, zodat een grotere variatie aan delicten wordt vertegenwoordigd.

Een andere beperking van deze deelstudie is dat de gegevens zijn verzameld door middel van zelfrapportage, wat *biases* met zich mee kan brengen. Zo bestaat de mogelijkheid dat respondenten sociaal wenselijke antwoorden geven of hun ervaringen anders rapporteren dan zij deze daadwerkelijk hebben beleefd. Daarnaast werd respondenten gevraagd terug te denken aan een incident dat voor sommigen al

langere tijd geleden had plaatsgevonden. Dit retrospectieve karakter kan hebben geleid tot herinneringsbias, waardoor antwoorden minder nauwkeurig zijn. Dit geldt met name voor de gerapporteerde zoektermen, omdat respondenten zich mogelijk niet alle zoekopdrachten of de exacte formuleringen daarvan konden herinneren. De gerapporteerde daadwerkelijke zoektermen moeten daarom met enige voorzichtigheid worden geïnterpreteerd. Deze beperking is echter gedeeltelijk ondervangen door in deelstudie 2 de gerapporteerde zoektermen in te voeren in de Google zoekwoordplanner, waardoor het mogelijk was om het daadwerkelijke zoekvolume en gerelateerde zoektermen op te halen. Bovendien maakte het gebruik van *broad matching* in deelstudie 3 het mogelijk om de advertenties ook weer te geven aan internetgebruikers die zoektermen invoerden die afweken van de in de vragenlijst gerapporteerde zoektermen.

Ook bij deelstudie 3 moet rekening gehouden worden met enkele beperkingen. Ten eerste hadden de advertentiecampagnes een relatief korte looptijd van zeven dagen. Hoewel deze periode voldoende was om eerste inzichten te verkrijgen in het bereik, de gebruikte zoektermen en de interactie met de advertenties, is onduidelijk in hoeverre de resultaten representatief zijn voor langere campagnes. Zoekgedrag van internetgebruikers kan variëren over tijd, waardoor een langere meetperiode mogelijk een completer beeld geeft van de effectiviteit van online advertentiecampagnes. Vervolgonderzoek zou daarom kunnen onderzoeken hoe campagneprestaties zich ontwikkelen gedurende een langere doorlooptijd.

Een tweede beperking betreft de roulatie van de verschillende advertenties binnen de campagnes. Hoewel de advertenties waren ingesteld om gelijkmatig te rouleren, bleek in de praktijk dat sommige advertentiegroepen aanzienlijk vaker werden weergegeven dan andere, zichtbaar in het aantal impressies. Hierdoor is het minder goed mogelijk om verschillen tussen advertentiegroepen toe te schrijven aan de achterliggende gedachte van de verschillende advertenties. Deze bevinding onderstreept tevens de beperkte transparantie van advertentieplatformen, waarbij niet altijd inzichtelijk is welke factoren bepalend zijn voor de vertoning van advertenties (zie ook Moneva et al., 2022).

Een derde beperking is dat niet kan worden vastgesteld in hoeverre de internetgebruikers die de advertenties te zien kregen of erop klikten daadwerkelijk slachtoffer waren van online fraude of ransomware. Hoewel de campagnes waren gebaseerd op zoektermen die uit de vragenlijsten naar voren kwamen en aannemelijk samenhangen met slachtofferschap, kunnen ook andere internetgebruikers deze zoektermen gebruiken. Hierdoor blijft onduidelijk in welke mate de campagnes daadwerkelijk slachtoffers hebben bereikt.

Tot slot is meer onderzoek nodig naar de invloed van specifieke campagne-instellingen op het bereik en de effectiviteit van online advertentiecampagnes. Daarbij kan onder meer worden gekeken naar de effecten van verschillende vormen van zoekterm matching, doelgroepen en advertenties. Daarnaast zouden in vervolgonderzoek interviews gehouden kunnen worden met gebruikers die de advertenties hebben gezien of erop geklikt hebben, om beter te begrijpen wie deze gebruikers zijn en hoe zij de advertenties hebben

ervaren. Dergelijk onderzoek kan bijdragen aan een beter begrip van de factoren die bepalen of online advertentiecampagnes slachtoffers van online criminaliteit daadwerkelijk weten te bereiken en activeren. Daarnaast is het mogelijk dat internetgebruikers in toenemende mate gebruikmaken van andere manieren om informatie te zoeken, zoals artificiële intelligentie, waardoor campagnes die zich uitsluitend richten op zoekmachines mogelijk niet alle potentiële slachtoffers bereiken. Vervolgonderzoek zou zich kunnen richten op de mate waarin slachtoffers van online criminaliteit gebruikmaken van artificiële intelligentie bij het zoeken naar informatie en hulp, en in hoeverre deze kanalen kunnen bijdragen aan het bereiken en ondersteunen van slachtoffers.

6.3. Aanbevelingen

De resultaten van dit onderzoek suggereren dat online advertentiecampagnes een waardevol instrument kunnen zijn om slachtoffers van online fraude en ransomware te bereiken op het moment dat zij actief zoeken naar informatie of hulp. Een aanzienlijk deel van de slachtoffers zoekt online naar informatie na slachtofferschap, waarbij Google de meest gebruikte zoekmachine is. Hoewel veel praktijkpartners zoals Slachtofferhulp Nederland, de Fraudehelpdesk en politie al websites hebben met informatie en contactmogelijkheden, kunnen advertentiecampagnes praktijkpartners een aanvullende mogelijkheid bieden om slachtoffers op een relevant moment te verwijzen naar betrouwbare informatie, praktische handelingsperspectieven en beschikbare hulp. Hiermee kunnen vraag en aanbod van hulp aan slachtoffers beter met elkaar worden verbonden. Advertentiecampagnes kunnen bovendien toegespitst worden op subgroepen van slachtoffers.

Tegelijkertijd laten de resultaten zien dat de toegevoegde waarde van dergelijke campagnes afhankelijk is van verschillende voorwaarden. Ten eerste lijkt het belangrijk om campagnes zo specifiek mogelijk af te stemmen op de doelgroep en de informatie- of hulpbehoeften van slachtoffers. Uit het huidige onderzoek blijkt bijvoorbeeld dat slachtoffers uiteenlopende zoektermen gebruiken die samenhangen met verschillende behoeften, zoals het oplossen van het probleem, het doen van een melding of aangifte, het terugkrijgen van financiële schade of het voorkomen van toekomstig slachtofferschap. Campagnes die aansluiten bij deze specifieke behoeften kunnen mogelijk beter inspelen op de hulpvraag van slachtoffers en hebben daarmee een grotere kans om relevante slachtoffers te bereiken. Campagnes zouden zich bovendien kunnen richten op meer specifieke doelgroepen dan in het huidige onderzoek het geval was, zoals alleen slachtoffers van een specifieke type fraude, of slachtoffers in een specifieke leeftijdscategorie. In het huidige onderzoek bleek bijvoorbeeld dat de doorklikratio afnam naarmate de leeftijd toenam, wat suggereert dat de advertenties het meest relevant waren voor jongere leeftijdscategorieën.

Praktijkpartners dienen in de keuze voor online advertentiecampagnes wel een zorgvuldige afweging te maken tussen de potentiële opbrengsten en de benodigde investering. Het identificeren, selecteren en optimaliseren van relevante zoekwoorden was in het huidige onderzoek een tijdsintensief proces. Daarnaast kunnen de kosten van advertentiecampagnes aanzienlijk oplopen, afhankelijk van de gekozen zoektermen en de mate van concurrentie met andere adverteerders op deze termen. Hoewel de campagnes in dit onderzoek erin slaagden internetgebruikers te bereiken, leidde slechts een beperkt deel van de impressies tot interactie (kliks) met de advertenties. Dit roept de vraag op in hoeverre de benodigde tijd, expertise en financiële middelen opwegen tegen het aantal slachtoffers dat daadwerkelijk wordt bereikt. Een bijkomstigheid daarbij is dat advertentieplatformen zoals Google slechts gedeeltelijk inzicht bieden in de factoren die bepalen wanneer en aan wie advertenties worden getoond, wat het campagnedesign en bepalen van de effectiviteit van campagnes bemoeilijkt. Online advertentiecampagnes kunnen daarom het beste worden ingezet als aanvulling op bestaande informatie- en hulpkanalen, en niet als enige strategie om slachtoffers te bereiken.

Referenties

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). *Veiligheidsmonitor 2023*. CBS. https://download.cbs.nl/maatwerk/Veiligheidsmonitor-2023.pdf

Bekkers, L. M. J., Moneva, A., & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*, *20*(2), 375-394. https://doi.org/10.1007/s11292-022-09537-7

Borwell, J. (2025). *Unravelling the impact of cybercrime: Understanding victim experiences and implications for police practice* [Dissertation, Open Universiteit]. https://doi.org/10.71583/20251017JB

Borwell, J., Jansen, J., & Stol, W. (2024). Recht doen aan de behoeften van cybercrimeslachtoffers: Reflecties op de rol van de politie. *Tijdschrift voor Veiligheid*, *23*, 47-78. https://doi.org/10.5553/TvV/.000076

Borwell, J., Jansen, J., & Stol, W. (2025). Exploring the impact of cyber and traditional crime victimization: Impact comparisons and explanatory factors. *International Review of Victimology*, *31*(1), 156-181. https://doi.org/10.1177/02697580241282782

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 1-11. https://doi.org/10.1016/j.tele.2021.101675

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and their Victims* (1ste dr.). Routledge. https://doi.org/10.4324/9781315679877

Button, M., Lewis, C., & Tapley, J. (2009). *A better deal for fraud victims: Research into victims' needs and experiences* (pp. 1-96). National Fraud Authority.

Caputo, A. A., & Brodsky, S. L. (2004). Citizen coping with community notification of released sex offenders. *Behavioral Sciences & the Law*, *22*(2), 239-252. https://doi.org/10.1002/bsl.566

Carpenter, S., Zhu, F., & Kolimi, S. (2014). Reducing online identity disclosure using warnings. *Applied Ergonomics*, *45*(5), 1337-1342. https://doi.org/10.1016/j.apergo.2013.10.005

CBS. (2026a). *Digitalisering en kenniseconomie 2025*. CBS. https://www.cbs.nl/nl-nl/longread/rapportages/2026/digitalisering-en-kenniseconomie-2025/4-ict-gebruik-personen

CBS. (2026b). *Veiligheidsmonitor 2025* (pp. 1-127). CBS. https://www.cbs.nl/nl-nl/longread/rapportages/2026/veiligheidsmonitor-2025

Colburn, D. A., Finkelhor, D., & Turner, H. A. (2023). Help-Seeking From Websites and Police in the Aftermath of Technology-Facilitated Victimization. *Journal of Interpersonal Violence*, *38*(21-22), 11642-11665. https://doi.org/10.1177/08862605231186156

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks. *Proceedings of the Internet Measurement Conference*, 50-64. https://doi.org/10.1145/3355369.3355592

Cross, C., Richards, K., & Smith, R. (2016). *The reporting experiences and support needs of victims of online fraud*. Australian Institute of Criminology. https://doi.org/10.52922/ti148355

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, *108*, 106310. https://doi.org/10.1016/j.chb.2020.106310

Dunn, P. (2007). Matching service delivery to need. In S. Walklate (Red.), *Handbook of victims and victimology* (1ste dr., pp. 255-281). Willan Publishing.

Fissel, E. R. (2021). The Reporting and Help-Seeking Behaviors of Cyberstalking Victims. *Journal of Interpersonal Violence*, *36*(11-12), 5075-5100. https://doi.org/10.1177/0886260518801942

Green, D. L., Choi, J. J., & Kane, M. N. (2010). Coping Strategies for Victims of Crime: Effects of the Use of Emotion-Focused, Problem-Focused, and Avoidance-Oriented Coping. *Journal of Human Behavior in the Social Environment*, *20*(6), 732-743. https://doi.org/10.1080/10911351003749128

Green, D. L., & Pomeroy, E. C. (2007). Crime Victims: What Is the Role of Social Support? *Journal of Aggression, Maltreatment & Trauma*, *15*(2), 97-113. https://doi.org/10.1300/J146v15n02_06

Hancock, P. A., Kaplan, A. D., MacArthur, K. R., & Szalma, J. L. (2020). How effective are warnings? A meta-analysis. *Safety Science*, *130*, 104876. https://doi.org/10.1016/j.ssci.2020.104876

Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. (2024). A qualitative study exploring factors preventing older adults from reporting cybercrime and seeking help. *CrimRxiv*. https://doi.org/10.21428/cb6ab371.8c4e3181

Homburg, G., & Van den Tillaart, J. (2015). *Fraudemeldpunten: Synergie en samenwerking*. Regioplan.

IBM. (2021). *IBM SPSS Statistics for Windows* (Versie 28) [Software]. IBM.

Ipsos I&O. (z.d.). *I&O Research Panel*. I&O Research Panel. Geraadpleegd 15 december 2022, van https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/

Jansen, J., & Leukfeldt, R. (2018). Coping with Cybercrime Victimization: An Exploratory Study into the Impact and Change. *Journal of Qualitative Criminal Justice & Criminology*, *6*(2). https://doi.org/10.21428/88de04a1.976bcaf6

Kool, R. (2014). Alles naar wens? Observaties naar aanleiding van het conceptwetsvoorstel ter aanvulling van het spreekrecht voor slachtoffers en nabestaanden in het strafproces. *Tijdschrift voor Herstelrecht*, *14*(3). https://doi.org/10.5553/TvH/1568654X2014014003003

Laxminarayan, M. S. (2012). *The heterogeneity of crime victims: Variations in procedural and outcome preferences* [Dissertation]. Universiteit Tilburg.

Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping*. Springer Publishing Company.

Lens, K. M. E., Pemberton, A., & Bogaerts, S. (2013). Heterogeneity in victim participation: A new perspective on delivering a Victim Impact Statement. *European Journal of Criminology*, *10*(4), 479-495. https://doi.org/10.1177/1477370812469859

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2019). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders*, *15*(1), 60-77. https://doi.org/10.1080/15564886.2019.1672229

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en*

gedigitaliseerde criminaliteit. NSCR. https://repository.wodc.nl/bitstream/handle/20.500.12832/2355/2839_Volledige_Tekst_tcm28-368216.pdf?sequence=1&isAllowed=y

Machmutow, K., Perren, S., Sticca, F., & Alsaker, F. D. (2012). Peer victimisation and depressive symptoms: Can specific coping strategies buffer the negative impact of cybervictimisation? *Emotional and Behavioural Difficulties*, *17*(3-4), 403-420. https://doi.org/10.1080/13632752.2012.704310

Maguire, M. (1991). The Needs and Rights of Victims of Crime. *Crime and Justice*, *14*, 363-433. https://doi.org/10.1086/449190

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System. *Criminology*, *52*(1), 33-59. https://doi.org/10.1111/1745-9125.12028

Matthijsse, S. R., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2025a). *Onderhandelen, betalen en melden na slachtofferschap van ransomware: Een mixed methods onderzoek naar de factoren die bijdragen aan beslissingsgedrag van burgers en ondernemers* (No. 127; PK, pp. 1-280). SDU Uitgevers.

Matthijsse, S. R., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2025b). To report or not to report: Exploring the motivations and factors associated with reporting of ransomware victimisation among entrepreneurs. *Journal of Criminal Justice*, *97*. https://doi.org/https://doi.org/10.1016/j.jcrimjus.2025.102378

Mollen, S., Engelen, S., Kessels, L. T. E., & Van Den Putte, B. (2017). Short and Sweet: The Persuasive Effects of Message Framing and Temporal Context in Antismoking Warning Labels. *Journal of Health Communication*, *22*(1), 20-28. https://doi.org/10.1080/10810730.2016.1247484

Moneva, A., & Leukfeldt, E. R. (2023). The effect of online ad campaigns on DDoS-attacks: A cross-national difference-in-differences quasi-experiment. *Crimnology & Public Policy*, *22*(4), 869-894. https://doi.org/https://doi.org/10.1111/1745-9133.12649

Moneva, A., & Leukfeldt, E. R. (2024a). *Interest in booter services and DDoS attacks: Insight from Google search data*. https://doi.org/10.31219/osf.io/x857s

Moneva, A., & Leukfeldt, E. R. (2024b). Interest in booter services and distributed denial of service attacks: Insight from Google search data. *European Journal of Criminology*, *22*(4), 508-533. https://doi.org/10.1177/14773708241275424

Moneva, A., Leukfeldt, E. R., & Klijnsoon, W. (2022). Alerting consciences to reduce cybercrime: A quasi-experimental design using warning banners. *Journal of Experimental Criminology*, *19*(3), 835-862. https://doi.org/10.1007/s11292-022-09504-2

O'Malley, R. L. (2023). Short-Term and Long-Term Impacts of Financial Sextortion on Victim's Mental Well-Being. *Journal of Interpersonal Violence*, *38*(13-14), 8563-8592. https://doi.org/10.1177/08862605231156416

Parti, K., & Tahir, F. (2023). "If We Don't Listen to Them, We Make Them Lose More than Money:" Exploring Reasons for Underreporting and the Needs of Older Scam Victims. *Social Sciences*, *12*(5), 264. https://doi.org/10.3390/socsci12050264

Pemberton, A. (2009a). Needs of Victims of Terrorism. In R. Letschert, A. Pemberton, & I. Staiger (Red.), *Assisting Victims of Terrorism* (pp. 73-141). Springer Netherlands. https://doi.org/10.1007/978-90-481-3025-2_3

Pemberton, A. (2009b). Victim Movements: From diversified needs to varying criminal justice agenda's. *Acta Criminologica*, *22*(3), 1-23.

Pemberton, A., Winkel, F.-W., & Groenhuijsen, M. S. (2008). Evaluating Victims Experiences in Restorative Justice. *British Journal of Community Justice*, *6*(2), 98-119.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, *62*, 136-146. https://doi.org/10.1016/j.chb.2016.03.039

Pijlman, V., & Burgmeijer, A. (2024). Using A/B testing to study engagement with Snapchat advertisements promoting help-seeking after image-based sexual harassment and abuse

victimization. *Computers in Human Behavior*, *158*, 108312. https://doi.org/10.1016/j.chb.2024.108312

Pijlman, V. E. (2025). *Caught in the Web: A Study of Help-Seeking for Sexual Victimization* [Dissertation, Vrije Universiteit Amsterdam]. https://doi.org/10.5463/thesis.1088

Pijlman, V., Waardt, M. D., Schoonmade, L., Eichelsheim, V., & Pemberton, A. (2025). The Help-Seeking Behavior of Victims of Image-Based Sexual Harassment and Abuse: A Scoping Review. *Trauma, Violence, & Abuse*, *26*(4), 734-754. https://doi.org/10.1177/15248380241289435

Poh Chua, S., Xiang Yi, T., Chin Choo, G. Y., Chee Seng, T., Tjin Ai, J. T., Sew Kim, L., & Lokithasan, K. A. P. (2022). Cyber-victimization among adolescents: Its relationships with primary appraisal and coping strategies. *Vulnerable Children and Youth Studies*, *17*(4), 334-343. https://doi.org/10.1080/17450128.2021.2008077

Prichard, J., Scanlan, J., Krone, T., Spiranovic, C., Watters, P., & Wortley, R. (2022). Warning messages to prevent illegal sharing of sexual images: Results of a randomised controlled experiment. *Trends & Issues in Crime and Criminal Justice*, (647). https://doi.org/https://doi.org/10.52922/ti78559

Reinders Folmer, C. P., Desmet, P. T. M., & Van Boom, W. H. (2019). Beyond compensation? Examining the role of apologies in the restoration of victims' needs in simulated tort cases. *Law and Human Behavior*, *43*(4), 329-341. https://doi.org/10.1037/lhb0000335

Rosenblatt, D. H., Bode, S., Dixon, H., Murawski, C., Summerell, P., Ng, A., & Wakefield, M. (2018). Health warnings promote healthier dietary decision making: Effects of positive versus negative message framing and graphic versus text-based warnings. *Appetite*, *127*, 280-288. https://doi.org/10.1016/j.appet.2018.05.006

Schenk, A. M., & Fremouw, W. J. (2012). Prevalence, Psychological Impact, and Coping of Cyberbully Victims Among College Students. *Journal of School Violence*, *11*(1), 21-37. https://doi.org/10.1080/15388220.2011.630310

Silic, M., & Back, A. (2017). Deterrent Effects of Warnings on Users Behavior in Preventing Malicious Software Use. *Proceedings of the 50th Hawaii International Conference on System Sciences*. https://doi.org/10.24251/HICSS.2017.600

Smith, R. G. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change*, *49*(5), 379-396. https://doi.org/10.1007/s10611-008-9112-x

Stockman, M. (2014). Insider hacking: Applying situational crime prevention to a new white-collar crime. *Proceedings of the 3rd Annual Conference on Research in Information Technology*, 53-56. https://doi.org/10.1145/2656434.2656436

Ten Boom, A., Kuijpers, K. F., & Meone, M. H. (2008). *Behoeften van slachtoffers van delicten: Een systematische literatuurstudie naar behoeften zoals door slachtoffers zelf geuit*. Boom Juridische Uitgevers.

Testa, A., Maimon, D., Sobesto, B., & Cukier, M. (2017). Illegal Roaming and File Manipulation on Target Computers: Assessing the Effect of Sanction Threats on System Trespassers' Online Behaviors. *Criminology & Public Policy*, *16*(3), 689-726. https://doi.org/10.1111/1745-9133.12312

Van De Weijer, S. G. A., Leukfeldt, E. R., & Van Der Zee, S. (2020). Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal*, *43*(1), 17-34. https://doi.org/10.1108/PIJPSM-07-2019-0122

Van Leuken, M. A. G., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2026). Taking matters into their own hands: Examining online fraud victims' needs and motivations for pursuing civil litigation. *International Review of Victimology*, 02697580261419851. https://doi.org/10.1177/02697580261419851

Van Leuken, M., & Van 't Hoff-de Goede, M. S. (2024a). *Praktische uitvoering en juridische grondslag van de civielrechtelijke afdoening van online fraude*. De Haagse Hogeschool.

Van Leuken, M., & Van 't Hoff-de Goede, S. (2024b). *Ervaringen van slachtoffers met de civielrechtelijke afdoening*. De Haagse Hogeschool.

Van Leuken, M., & Van 't Hoff-de Goede, S. (2025). *De kennis en behoeften van (potentiële) slachtoffers van online fraude* (pp. 1-90). The Hague University of Applied Sciences. https://www.dehaagsehogeschool.nl/media/deelrapport-2-naar-een-toekomstbestendige-civielrechtelijke-afdoening-van-online-fraude

Vetterl, A. (2020). *Honeypots in the age of universal attacks and the Internet of Things* (Technical Report No. 944; pp. 1-115). University of Cambridge. https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-944.pdf

Voce, I., & Morgan, A. (2022). Help-seeking among Australian ransomware victims. *Statistical Bulletin*, (38), 1-13. https://doi.org/https://doi.org/10.52922/sb78504

Voce, I., & Morgan, A. (2025). *Cybercrime in Australia 2024* (Statistical Report No. 52). Australian Institute of Criminology. https://doi.org/10.52922/sr77918

Wang, F. (2025). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. *International Review of Victimology*, *31*(1), 91-116. https://doi.org/10.1177/02697580241234331

Wang, J., Shi, J., Wen, X., Xu, L., Zhao, K., Tao, F., Zhao, W., & Qian, X. (2022). The effect of signal icon and persuasion strategy on warning design in online fraud. *Computers & Security*, *121*, 102839. https://doi.org/10.1016/j.cose.2022.102839

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The Effect of a Surveillance Banner in an Attacked Computer System: Additional Evidence for the Relevance of Restrictive Deterrence in Cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829-855. https://doi.org/10.1177/0022427815587761

Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. *Sage Open*, *7*(2), 1-13. https://doi.org/10.1177/2158244017710292

Wortley, R., & Prichard, J. (2023). Online Messaging as a Cybercrime Prevention Tool in the Post-pandemic Age. In R. G. Smith, R. Sarre, L. Y.-C. Chang, & L. Y.-C. Lau (Red.), *Cybercrime in*

the Pandemic Digital Age and Beyond (pp. 209-232). Springer International Publishing. https://doi.org/10.1007/978-3-031-29107-4_11

Yee, J. L., Greenberg, M. S., & Beach, S. R. (1998). Attitudes toward various modes of coping with criminal victimization: The effects of gender and type of crime. *journal of Social and Clinical Psychology*, *17*(3), 273-294.

Bijlage 1: Vragenlijst slachtoffers online fraude

Inleiding en toestemmingsverklaring
Bedankt dat u wilt deelnemen aan dit onderzoek van de Haagse Hogeschool. Dit onderzoek gaat over online criminaliteit. Wij willen aan u vragen of u zelf online criminaliteit heeft meegemaakt, en zo ja, of u online naar informatie of hulp heeft gezocht en welke behoefte aan informatie of hulp u had.

Waarom uw ervaringen van waarde zijn
Meer inzicht in de behoeften en het online zoekgedrag van slachtoffers van online criminaliteit is nodig om toekomstige slachtoffers van de juiste informatie en hulpbronnen te voorzien.

Privacy en anonimiteit
Dit vragenlijstonderzoek is gemaakt door onderzoekers van de Haagse Hogeschool en wordt uitgevoerd door Ipsos I&O. Uw antwoorden worden verwerkt volgens de privacyverklaring van Ipsos I&O en worden uitsluitend gebruikt voor het doel van dit onderzoek, tenzij u akkoord gaat met verder gebruik van uw antwoorden voor vervolgonderzoek. Indien dat het geval is, kunt u dat onderaan dit formulier aangeven. Er zijn maatregelen genomen om ervoor te zorgen dat uw antwoorden niet naar u te herleiden zijn. Dat betekent bijvoorbeeld dat Ipsos I&O uw antwoorden verstuurt aan de Haagse Hogeschool op een manier dat deze niet naar u te zijn herleiden. In een publicatie zullen anonieme gegevens worden gebruikt.
Ik verklaar dat:

- Ik weet dat het onderzoek wordt uitgevoerd zoals beschreven in bovenstaande toelichting. Ik heb dit gelezen en begrijp de informatie.
- Ik genoeg tijd heb gehad om te beslissen of ik wil deelnemen.
- Ik weet dat meedoen vrijwillig is en dat ik op ieder moment kan beslissen om toch niet mee te doen of te stoppen met het onderzoek. Daarvoor hoef ik geen reden te geven. Ik begrijp dat het intrekken van mijn toestemming geen gevolgen heeft voor de verwerking van mijn persoonsgegevens in de periode voorafgaand aan het intrekken van de toestemming.
- Ik toestemming geef voor het verzamelen, bewaren en gebruiken van mijn ingevulde gegevens.
- Ik weet dat de gegevens die de onderzoekers bewaren geanonimiseerd zijn en niet rechtstreeks te herleiden zijn naar mijn persoon.
- Ik weet dat onderzoeksgegevens na het onderzoek nog 10 jaar worden bewaard en daarna worden vernietigd.

Door ‘ja’ aan te klikken stemt u in met deelname aan het onderzoek en gaat u ermee akkoord dat Ipsos I&O en de Haagse Hogeschool uw gegevens verwerken.

Stemt u ermee in? [Verplichte vraag]
☐ Ja, ik geef toestemming voor het gebruik van mijn gegevens voor dit onderzoeksproject, maar niet voor vervolgonderzoek [door naar Q1]
☐ Ja, ik geef toestemming voor het gebruik mijn gegevens voor dit onderzoeksproject en vervolgonderzoek [door naar Q1]
☐ Nee, ik geef geen toestemming [Einde vragenlijst]

Q1. Screeningsvraag 1

Welke van de volgende vormen van **online oplichting** heeft u **in de afgelopen 2 jaar** meegemaakt?

1. Ik heb iets gekocht of gehuurd via internet, zoals een product, dienst of (vakantie)woning, en een deel of alles betaald. Daarna kreeg ik het niet of het was niet zoals afgesproken.
   ☐ Nee
   ☐ Ja
2. Ik heb via internet een product verkocht of dienst geleverd, maar de ontvanger heeft nooit betaald.
   ☐ Nee
   ☐ Ja
3. Ik ontving (bijvoorbeeld via WhatsApp of sms) berichten van iemand die zich voordeed als een bekende. Toen deze persoon om geld vroeg vanwege een hulpvraag of zogenaamd noodgeval, heb ik geld overgemaakt.
   ☐ Nee
   ☐ Ja
4. Iemand belde mij en deed alsof hij een medewerker van een helpdesk was, zoals van een bank of softwarebedrijf. Ik gaf deze persoon toegang tot mijn computer of bankaccount, en er werd geld gestolen. Of ik gaf mijn pincode, en iemand kwam mijn betaalpas thuis ophalen.
   ☐ Nee
   ☐ Ja
5. Ik heb geld overgemaakt naar iemand die mij via e-mail of internet benaderde met verhalen over snel geld verdienen via een erfenis, investering, loterij of iets soortgelijks.
   ☐ Nee
   ☐ Ja
6. Ik heb geld overgemaakt naar iemand die ik heb ontmoet op een datingsite of sociale media (bijvoorbeeld voor een bezoek of vanwege een noodgeval), maar deze persoon bleek een oplichter te zijn.
   ☐ Nee
   ☐ Ja
7. Ik belde een (buitenlands) telefoonnummer naar aanleiding van een gemiste oproep of een terugbelverzoek per sms, waarna ik de (hoge) kosten van dit gesprek moest betalen.
   ☐ Nee
   ☐ Ja
8. Ik heb geld overgemaakt naar iemand die online dreigde gevoelige informatie of vervelend beeldmateriaal te verspreiden (zoals mijn surfgedrag of webcambeelden). (Let op: het maakt hierbij niet uit of deze informatie juist was of de beelden echt waren.)
   ☐ Nee
   ☐ Ja
9. Ik heb had geld verloren aan fraude. Vervolgens heb ik geld overgemaakt naar iemand die aanbood te helpen om het verloren geld terug te krijgen, maar ik ontving de beloofde hulp niet.
   ☐ Nee

☐ Ja

10. Ik ben via internet slachtoffer geworden van een andere vorm van online oplichting.
    ☐ Nee
    ☐ Ja

[Indien een van antwoordopties 1 t/m 9 bij Q1 = 'ja', ga naar Q2*].*
[Indien antwoordoptie 10 bij Q1 = 'ja' of *'nee',* Einde vragenlijst*]*
[Indien alle antwoordopties bij 1 t/m 9 bij Q1 = 'nee', einde vragenlijst*].*

Q2. Screeningsvraag 2
[Als Q1*=meerdere antwoorden, dan deze screeningsvraag voor elke vorm vragen]*
U heeft aangegeven dat u **in de afgelopen 2 jaar** het volgende u is overkomen: [*antwoord 1 van Q1*].
Welke van de volgende situaties is voor u van toepassing?
☐ Ik ben hierdoor geld of goederen verloren. Ik heb dit geld of deze goederen niet teruggekregen [door naar Q3]
☐ Ik ben hierdoor geld of goederen verloren. Ik heb dit geld of deze goederen inmiddels (voor een deel) teruggekregen [door naar Q3]
☐ Ik ben hierdoor geen geld of goederen verloren, het is gebleven bij een poging tot oplichting [einde vragenlijst]

[herhalen voor antwoord 2 van Q1, antwoord 3 van Q1 etc.]

Q3. Meest recente delict
[Als Q1=meerdere antwoorden]
U heeft aangegeven dat u meerdere keren slachtoffer bent geworden van online oplichting. Wat gebeurde er de **laatste keer** dat u online bent opgelicht en geld of goederen heeft verloren?
[Lijst met antwoorden van Q1 waarbij respondenten geld hebben verloren (optie 1 en 2 van Q2). Respondent moet een optie aanklikken]

De vervolgvragen gaan over de vorm van oplichting die u de laatste keer heeft meegemaakt.

Q4. Wanneer_slachtoffer
Wanneer bent u voor het laatst slachtoffer geworden van online oplichting? *Als u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.*
Dropdownmenu met jaartallen t/m 2025.

Blok 1: Impact
We willen u vragen stellen over wat er gebeurde toen u slachtoffer werd van online oplichting en aan welke hulp u behoefte had. Uw antwoorden blijven anoniem en kunnen niet naar u worden herleid.

We zullen u eerst vragen stellen over de (mogelijke) gevolgen die u heeft ervaren.

Q5. Gevolgen_financieel
Hoeveel denkt u dat dit incident u heeft gekost? Denk hierbij aan geld dat u kwijt bent of kosten voor hulp, bijvoorbeeld voor verwerking. Het maakt niet uit of u inmiddels (een deel van) het geld of de goederen vergoed of terug heeft teruggekregen.

Weet u het niet precies? Kies dan de categorie die het meest klopt.

☐ Geen financiële kosten
☐ €1 t/m €100
☐ €101 t/m €250
☐ €251 t/m €500
☐ €501 t/m €1.000
☐ €1.001 t/m €2.500
☐ €2.501 t/m €5.000
☐ €5.001 t/m €10.000
☐ €10.001 t/m €25.000
☐ €25.001 t/m €50.000
☐ €50.001 t/m €100.000
☐ €100.001 of meer
☐ Weet ik niet

Q6. Gevolgen_emotioneel
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Door het incident had of heb ik de volgende (tijdelijke) emotionele, psychische of lichamelijke gevolgen ervaren…

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**
Het voorval telkens opnieuw beleven	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Ontkennen van wat er gebeurd is of het moeilijk kunnen geloven	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Minder vertrouwen in mensen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Minder vertrouwen in mijn eigen online vaardigheden	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Slaapproblemen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Angstklachten en/of paniekaanvallen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Depressieve klachten	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Lichamelijke klachten zoals hartkloppingen, duizeligheid, trillen of buikpijn	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een minder veilig gevoel	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Schaamte over wat er gebeurd is	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een schuldgevoel over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Machteloos voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Verdrietig voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Boos voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Andere emotionele of psychische gevolgen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q7. Gevolgen_anders
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Door het incident had of heb ik de volgende andere gevolgen ervaren…

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**
Tijd besteed aan het oplossen van het incident	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Geld moeten lenen omdat ik niet (meer) rond kon komen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Moeten afzien van een geplande activiteit of uitgave (zoals een vakantie)	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een negatieve reactie ervaren van mijn partner, kinderen of andere familieleden	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een negatieve reactie ervaren van andere mensen om mij heen, zoals vrienden, kennissen, buren of collega's	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Ik ben voorzichtiger geworden op het internet	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Andere gevolgen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q8. Gevolgen_ ernst
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**	**NIET VAN TOEPASSING**
Ik heb de **financiële gevolgen** van het incident als ernstig ervaren.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8
Ik heb de **emotionele, psychische of lichamelijk gevolgen** van het incident (bijv. slaapproblemen, gevoel van onveiligheid) als ernstig ervaren.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8
Ik heb de **andere gevolgen** van het incident (bijv. tijd besteed aan het oplossen van het incident, moeten afzien van een geplande activiteit) als ernstig ervaren.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8

Q9. Angst_online fraude
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

		HELEMAAL MEE ONEENS	MEE ONEENS	ENIGSZINS MEE ONEENS	NIET MEE ONEENS, NIET MEE EENS	ENIGSZINS MEE EENS	MEE EENS	HELEMAAL MEE EENS
1	Ik schat de kans groot in dat ik in de komende 12 maanden nog een keer slachtoffer wordt van online oplichting.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7
2	Ik maak me zorgen dat ik in de komende 12 maanden nog een keer slachtoffer wordt van online oplichting.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7

Q10. Angst_online fraude_verschil
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

		HELEMAAL MEE ONEENS	MEE ONEENS	ENIGSZINS MEE ONEENS	NIET MEE ONEENS, NIET MEE EENS	ENIGSZINS MEE EENS	MEE EENS	HELEMAAL MEE EENS
1	Ik denk dat ik nu minder kans loop om slachtoffer te worden van online oplichting, wanneer ik dat vergelijk	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7

	met de situatie voordat ik voor de laatste keer slachtoffer werd.						
2	Ik maak me nu minder zorgen dat ik slachtoffer word van online oplichting, wanneer ik dat vergelijk met de situatie voordat ik voor de laatste keer slachtoffer werd.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7

Blok 2: Online zoekgedrag
We zullen u nu vragen stellen over uw online zoekgedrag naar aanleiding van het incident.

Q11. Online gezocht
Heeft u toen de oplichting plaatsvond of toen u ontdekte dat de oplichting had plaatsgevonden gezocht in een van de volgende zoekmachines, bijvoorbeeld naar informatie of ondersteuning?

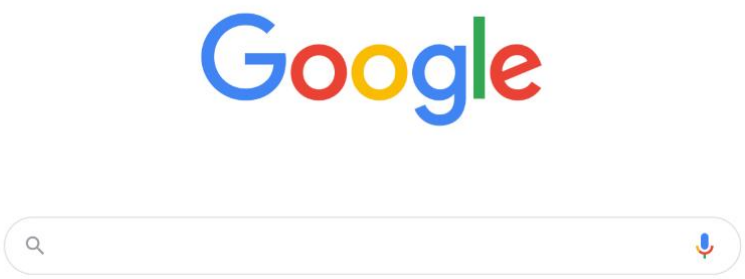
☐ Google
☐ Bing
☐ Yahoo!
☐ DuckDuckGo
☐ Andere zoekmachine, namelijk… [open antwoord]
☐ Ik heb niet gezocht in een zoekmachine

[Routing:
Indien antwoordoptie 1, 2,3, 4, 5 ‘ja’ → door naar Q12]
Indien antwoordoptie 6 → door naar Q14]

Q12. Uitkomst_zoekopdrachten
In hoeverre heeft het zoeken naar informatie of hulp in een online zoekmachine u opgeleverd wat u zocht?

Matrix

	HELEMAAL MEE ONEENS	MEE ONEENS	NIET MEE ONEENS, NIET MEE EENS	MEE EENS	HELEMAAL MEE EENS	NIET VAN TOEPASSING
Ik heb de informatie gevonden die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
Ik heb de hulp gevonden die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
Ik heb contact kunnen leggen met een of meer organisaties die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6



Q13. Zoektermen_daadwerkelijk
U heeft aangegeven dat u tijdens het incident gezocht heeft naar informatie of ondersteuning op internet. Wij willen onderzoeken wat mensen in dit geval intypen in een zoekmachine.

Denkt u terug aan het moment dat de oplichting plaatsvond of toen u ontdekte dat de oplichting had plaatsgevonden. Wat heeft u ingetypt in de zoekmachine? Uw zoektermen kunnen bestaan uit losse woorden, combinaties van woorden of zinnen. Ze kunnen bijvoorbeeld betrekking hebben op vragen, personen of organisaties. **We willen u vragen om elke losse zoekopdracht in een apart antwoordveld in te vullen.**

Als u het niet meer precies weet, vult u dan alstublieft in wat u ongeveer ingetypt heeft in die tijd.

Vult u alstublieft alle zoektermen in die u gebruikt heeft, ook als deze geen passend resultaat opleverden.

☐ Ik weet het niet meer

[ ]

[Open antwoord]

[ ]

[Open antwoord]

[ ]

[Open antwoord]

[ ]

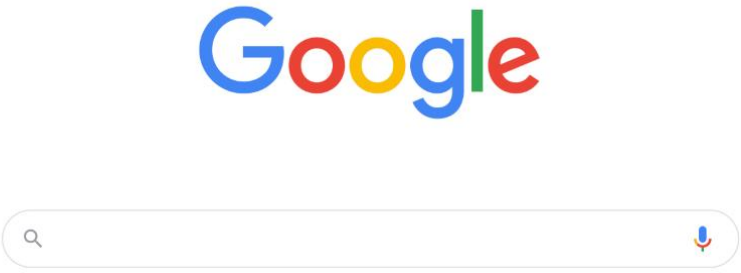
[Open antwoord]

[ ]

[Open antwoord]

[Pop-up als respondent wil doorklikken naar de volgende vraag: Vaak gebruiken mensen verschillende zoektermen, of combinaties van zoektermen. Zijn er nog andere zoektermen die u gebruikt heeft om te zoeken naar informatie of hulp? → Respondent optie geven om nog meer in te vullen, of definitief door te klikken naar de volgende pagina**]**

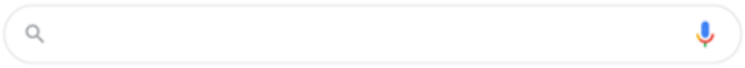
Q14. Zoektermen_hypothetisch



Stelt u zich voor dat u nu nogmaals geconfronteerd wordt met online oplichting. Wat zou u dan intypen in een zoekmachine? Uw zoektermen kunnen bestaan uit losse woorden, combinaties van woorden of

zinnen. Ze kunnen bijvoorbeeld betrekking hebben op vragen, personen of organisaties. **We willen u vragen om elke losse zoekopdracht in een apart antwoordveld in te vullen.**

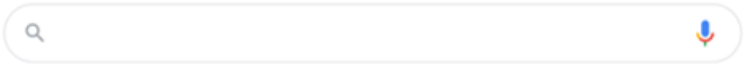
Als u het niet precies weet, vult u dan alstublieft in wat u ongeveer zou intypen.



[Open antwoord]



[Open antwoord]



[Open antwoord]



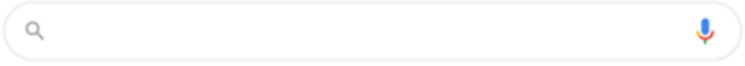
[Open antwoord]



[Open antwoord]



[Open antwoord]



[Open antwoord]

[Pop-up als respondent wil doorklikken naar de volgende vraag: Vaak gebruiken mensen verschillende zoektermen, of combinaties van zoektermen. Zijn er nog andere zoektermen die u zou gebruiken om te zoeken naar informatie of hulp? → Respondent optie geven om nog meer in te vullen, of definitief door te klikken naar de volgende pagina**]**

Blok 3: Behoefte(n)

We gaan u nu vragen stellen over wat u nodig had of waar u naar op zoek was na het incident**.**

Q15. Informatiebehoefte(n)
Nadat ik werd opgelicht wilde ik meer informatie over…. (*Meerdere antwoorden mogelijk)*

☐ Wat me precies overkomen is
☐ Hoe het heeft kunnen gebeuren
☐ Het oplossen van het probleem
☐ Hoe ik kan voorkomen dat ik in de toekomst opnieuw slachtoffer word
☐ De organisaties waarbij ik terecht kan voor hulp
☐ De status van mijn aangifte (indien van toepassing)
☐ Het vergoed krijgen van de financiële schade
☐ Emotionele, psychische of lichamelijke gevolgen of klachten
☐ Het doen van een melding of aangifte bij de politie
☐ Juridische zaken
☐ Anders, namelijk… [open antwoord]

Q16. Hulpbehoefte(n)
Nadat ik werd opgelicht wilde ik… (*Meerdere antwoorden mogelijk)*

☐ Hulp bij het oplossen van het probleem
☐ Hulp om te voorkomen dat ik in de toekomst opnieuw slachtoffer word
☐ Hulp bij het vergoed krijgen van de financiële schade
☐ Hulp voor emotionele, psychische of lichamelijke gevolgen of klachten
☐ Hulp bij het doen van een melding of aangifte bij de politie
☐ Hulp bij juridische vragen of problemen
☐ Anders, namelijk… [open antwoord]
☐ Erkenning als slachtoffer
☐ Erkenning van wat me overkomen is

Q17. Contact_organisaties
Heeft u naar aanleiding van het incident bij een van de volgende partijen (mensen of organisaties) hulp gezocht? *Meerdere antwoorden mogelijk.*

☐ Vrienden, familie, kennissen of collega's
☐ Op internet
☐ De politie
☐ Bank of financiële instelling
☐ Verzekeringsmaatschappij
☐ Cybersecuritybedrijf, IT-leverancier of IT-specialist

☐ Fraudehelpdesk
☐ Slachtofferhulp Nederland
☐ Consumentenbond
☐ Autoriteit Persoonsgegevens
☐ Incassobureau, gerechtsdeurwaarder of advocaat
☐ Anders, namelijk… [open antwoord]
☐ Ik heb geen hulp gezocht

Q18. Contact_organisatie_online
[Als Q17*=meerdere antwoorden, dan deze vraag voor elke vorm vragen (behalve 'vrienden, familie, kennissen of collega's', 'op internet' en 'Ik heb geen hulp gezocht')]*

U heeft aangegeven dat u bij de volgende organisatie hulp heeft gezocht: [*antwoord 1 van Q17*]. Welke van de volgende situaties is voor u van toepassing?

☐ Ik was al bekend met deze organisatie
☐ Een bekende heeft me op deze organisatie gewezen
☐ Ik ben bij deze organisatie terecht gekomen via het internet
☐ Ik weet niet meer hoe ik bij deze organisatie terecht ben gekomen

[herhalen voor antwoord 2 van Q17, antwoord 3 van Q17 etc]

Q19. Beveiligingsmaatregelen
Heeft u, met uitzondering van eventuele maatregelen die u al nam, een van de volgende beveiligingsmaatregelen genomen nadat u slachtoffer bent geworden van online oplichting? *Meerdere antwoorden mogelijk.*

☐ Een ander besturingssysteem genomen
☐ Regelmatige back-ups maken van bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Gebruik van sterke, unieke wachtwoorden
☐ Gebruik van een up-to-date antivirus product
☐ Gebruik van een firewall
☐ Beveiligingssoftware netwerken en apparaten laten scannen op virussen of andere kwaadaardige software
☐ Updates van besturingssystemen, apps en/of software direct uitvoeren zodra deze beschikbaar zijn
☐ Een ander standaardbrowser genomen
☐ Gebruik van een VPN-verbinding
☐ Installatie van browser extensies die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Gevoelige bestanden en gegevens worden versleuteld

☐ Tweestapsverificatie (2 stappen in plaats van 1 stap om in te loggen)
☐ Geen van bovenstaande opties

Pop-up 19i: Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.

Q20. Gedrag
Heeft u een van de volgende activiteiten **beperkt of verminderd** nadat u slachtoffer bent geworden van online oplichting? *Meerdere antwoorden mogelijk.*
☐ Het gebruik van accounts of pagina's op sociale media (zoals Facebook of Instagram)
☐ E-mailen
☐ Informatie zoeken of surfen op internet
☐ Tekstberichten sturen, bijvoorbeeld via WhatsApp
☐ Bellen of beeldbellen, bijv. via Whatsapp, Zoom of FaceTime
☐ Het online bestellen, reserveren of betalen voor producten of diensten
☐ Het gebruik van internetbankieren of mobiel bankieren
☐ Het streamen van muziek, films, software en/of games
☐ Gamen of spelletjes spelen
☐ Bezoek van datingsites of apps
☐ Bezoek van goksites
☐ Geen van bovenstaande opties

[Door naar afsluiting]

Afsluiting slachtoffers
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname aan dit onderzoek.

Wilt u verder praten over of melding maken van wat u is overkomen? Dan kunt u contact opnemen met een van de volgende instanties:
Politie Nederland
Slachtofferhulp Nederland
Fraudehelpdesk

Afsluiting niet-slachtoffers

U behoort niet tot de doelgroep van deze vragenlijst. Bedankt voor uw interesse in het onderzoek.

Bijlage 2: Vragenlijst slachtoffers ransomware

Inleiding en toestemmingsverklaring
Bedankt dat u wilt deelnemen aan dit onderzoek van de Haagse Hogeschool. Dit onderzoek gaat over online criminaliteit. Wij willen aan u vragen of uw bedrijf online criminaliteit heeft meegemaakt, en zo ja, of u online naar informatie of hulp heeft gezocht en welke behoefte aan informatie of hulp u had.

Waarom uw ervaringen van waarde zijn
Meer inzicht in de behoeften en het online zoekgedrag van slachtoffers van online criminaliteit is nodig om toekomstige slachtoffers van de juiste informatie en hulpbronnen te voorzien.

Privacy en anonimiteit
Dit vragenlijstonderzoek is gemaakt door onderzoekers van de Haagse Hogeschool en wordt uitgevoerd door Ipsos I&O. Uw antwoorden worden verwerkt volgens de privacyverklaring van Ipsos I&O en worden uitsluitend gebruikt voor het doel van dit onderzoek, tenzij u akkoord gaat met verder gebruik van uw antwoorden voor vervolgonderzoek. Indien dat het geval is, kunt u dat onderaan dit formulier aangeven. Er zijn maatregelen genomen om ervoor te zorgen dat uw antwoorden niet naar u te herleiden zijn. Dat betekent bijvoorbeeld dat Ipsos I&O uw antwoorden verstuurt aan de Haagse Hogeschool op een manier dat deze niet naar u of uw bedrijf te zijn herleiden. In een publicatie zullen anonieme gegevens worden gebruikt.

Ik verklaar dat:

- Ik weet dat het onderzoek wordt uitgevoerd zoals beschreven in bovenstaande toelichting. Ik heb dit gelezen en begrijp de informatie.
- Ik genoeg tijd heb gehad om te beslissen of ik wil deelnemen.
- Ik weet dat meedoen vrijwillig is en dat ik op ieder moment kan beslissen om toch niet mee te doen of te stoppen met het onderzoek. Daarvoor hoef ik geen reden te geven. Ik begrijp dat het intrekken van mijn toestemming geen gevolgen heeft voor de verwerking van mijn persoonsgegevens in de periode voorafgaand aan het intrekken van de toestemming.
- Ik toestemming geef voor het verzamelen, bewaren en gebruiken van mijn ingevulde gegevens.
- Ik weet dat de gegevens die de onderzoekers bewaren geanonimiseerd zijn en niet rechtstreeks te herleiden zijn naar mijn persoon.
- Ik weet dat onderzoeksgegevens na het onderzoek nog 10 jaar worden bewaard en daarna worden vernietigd.

Door ‘ja’ aan te klikken stemt u in met deelname aan het onderzoek en gaat u ermee akkoord dat Ipsos I&O en de Haagse Hogeschool uw gegevens verwerken.

Stemt u hiermee in? [Verplichte vraag]
☐ Ja, ik geef toestemming voor het gebruik van mijn gegevens voor dit onderzoeksproject, maar niet voor vervolgonderzoek [door naar Q1]
☐ Ja, ik geef toestemming voor het gebruik mijn gegevens voor dit onderzoeksproject en vervolgonderzoek [door naar Q1]

☐ Nee, ik geef geen toestemming [Einde vragenlijst]

Q1. Screeningsvraag 1
Welke van de volgende vormen van online criminaliteit of een poging daartoe heeft uw bedrijf ooit meegemaakt?

1. Een medewerker van mijn bedrijf ontving een opdracht van iemand die zich voordeed als CEO of directeur om een groot bedrag over te boeken, bijvoorbeeld vanwege een factuur.
   ☐ Nee
   ☐ Ja
2. Mijn bedrijf heeft een product of dienst via internet gekocht en (een deel daarvan) betaald, waarna het product of de dienst nooit geleverd is.
   ☐ Nee
   ☐ Ja
3. Mijn bedrijf heeft via internet een product verkocht of dienst geleverd, maar de ontvanger heeft nooit betaald.
   ☐ Nee
   ☐ Ja
4. Mijn bedrijf heeft betaald voor het plaatsen van advertenties die niet of nauwelijks vertoond zijn of waarvoor geen opdracht is verleend.
   ☐ Nee
   ☐ Ja
5. Mijn bedrijf heeft iemand die zich voordeed als een medewerker van een helpdesk toegang gegeven tot een computer, waarna er geld afhandig is gemaakt.
   ☐ Nee
   ☐ Ja
6. Iemand heeft zonder mijn toestemming persoonlijke en/of financiële gegevens van mijn bedrijf gebruikt, deze persoon heeft bijvoorbeeld producten gekocht of kredieten aangevraagd op naam van mijn bedrijf.
   ☐ Nee
   ☐ Ja
7. De bestanden, gegevens of appara(a)t(en) van mijn bedrijf werden geblokkeerd of versleuteld en er werd om losgeld gevraagd om hier weer toegang tot te krijgen.
   ☐ Nee
   ☐ Ja
8. Iemand heeft online negatieve berichten over mijn bedrijf verspreid.
   ☐ Nee
   ☐ Ja

[Indien 7 (ransomware) = ‘ja’, ga naar Q2. Indien 7 (ransomware) = nee, ga naar einde vragenlijst]

Q2. Screeningsvraag 2
U heeft aangegeven dat de bestanden, gegevens of apparaten van uw bedrijf ooit geblokkeerd of versleuteld zijn door kwaadwillenden en dat er om losgeld is gevraagd om hier weer toegang tot te krijgen. Welke van de volgende situaties is voor u van toepassing?
☐ Ik zag een scherm, pop-up of bericht waarin stond dat apparaten waren vergrendeld (*locked*) en ik moest betalen om weer toegang te krijgen [door naar Q3]
☐ Ik zag een scherm, pop-up of bericht waarin stond dat gegevens of bestanden waren versleuteld (*encrypted*) en ik moest betalen om weer toegang te krijgen [door naar Q3]
☐ Ik zag een scherm, pop-up of bericht, zogenaamd van een wetshandhavingsinstantie (bijv. FBI, Ministerie van Justitie), dat me informeerde dat ik betrapt was op het uitvoeren van een illegale of ongewenste activiteit online en ik een boete moest betalen [door naar Q3]
☐ Ik zag een bericht, zogenaamd van een (antivirus)softwarebedrijf of helpdesk (bijv. Microsoft), dat me informeerde dat mijn computer besmet was met een virus en dat ik moest betalen of een nummer moest bellen om het probleem op te lossen [door naar Q3]
☐ Niet van toepassing, dit is mij niet overkomen [einde vragenlijst]

Q3. Slachtofferschap_frequentie
Wat uw bedrijf overkomen is noemen we een ransomware aanval. Hoe vaak is uw bedrijf slachtoffer geworden van ransomware?

Dropdownmenu 1 t/m 10.

De vervolgvragen gaan over de ransomware aanval die uw bedrijf de laatste keer heeft meegemaakt.

Q4. Wanneer_slachtoffer
Wanneer is uw bedrijf voor het laatst slachtoffer geworden van ransomware?

Als u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.

Dropdownmenu met jaartallen t/m 2025.

Blok 1: Impact
We willen u vragen stellen over wat er gebeurde toen uw bedrijf slachtoffer werd van ransomware en aan welke hulp u behoefte had. Uw antwoorden blijven anoniem en kunnen niet naar u worden herleid.

We zullen u eerst vragen stellen over de (mogelijke) gevolgen die u heeft ervaren.

Q5. Gevolgen_financieel
Hoeveel denkt u dat dit incident u heeft gekost? Denk hierbij bijvoorbeeld aan de kosten van het losgeld of kosten voor herstel. Het maakt niet uit of u inmiddels (een deel van) het geld vergoed of terug heeft teruggekregen.

Weet u het niet precies? Kies dan de categorie die het meest klopt.

☐ Geen financiële kosten
☐ €1 t/m €100
☐ €101 t/m €250
☐ €251 t/m €500
☐ €501 t/m €1.000
☐ €1.001 t/m €2.500
☐ €2.501 t/m €5.000
☐ €5.001 t/m €10.000
☐ €10.001 t/m €25.000
☐ €25.001 t/m €50.000
☐ €50.001 t/m €100.000
☐ €100.001 t/m €250.000
☐ €250.001 of meer
☐ Weet ik niet

Q6. Gevolgen_emotioneel
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Door het incident had of heb ik de volgende (tijdelijke) emotionele, psychische of lichamelijke gevolgen ervaren…

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**
Het voorval telkens opnieuw beleven	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Ontkennen van wat er gebeurd is of het moeilijk kunnen geloven	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Minder vertrouwen in mensen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Minder vertrouwen in mijn eigen online vaardigheden	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Slaapproblemen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Angstklachten en/of paniekaanvallen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Depressieve klachten	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Lichamelijke klachten zoals hartkloppingen, duizeligheid, trillen of buikpijn	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een minder veilig gevoel	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Schaamte over wat er gebeurd is	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een schuldgevoel over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Machteloos voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Verdrietig voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Boos voelen over wat er is gebeurd	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Andere emotionele of psychische gevolgen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q7. Gevolgen_anders
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Door het incident had of heb ik de volgende andere gevolgen ervaren…

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**
Verhinderd in het uitvoeren van dagelijkse werkzaamheden	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Verlies aan inkomsten, waarde van aandelen of inkomen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Tijd besteed aan het oplossen van het incident of het inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Geld moeten lenen omdat ik niet (meer) rond kon komen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Moeten afzien van een geplande activiteit of uitgave	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Bestanden of gegevens verloren	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Boetes van regelgevers of wetgevers, of verwante juridische kosten	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Reputatieschade	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een negatieve reactie ervaren van mijn partner, kinderen of andere familieleden	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Een negatieve reactie ervaren van andere mensen om mij heen, zoals vrienden, kennissen, buren of collega's	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Mijn bedrijf heeft een schadevergoeding, compensatie of korting verleend aan klanten	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Ik ben voorzichtiger geworden op het internet	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
Andere gevolgen	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q8. Gevolgen_ernst
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**	**NIET VAN TOEPASSING**
Ik heb de financiële gevolgen van het incident als ernstig ervaren.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8
Ik heb de emotionele, psychische of lichamelijk gevolgen van het incident	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8

(bijv. slaapproblemen, gevoel van onveiligheid) als ernstig ervaren.						
Ik heb de andere gevolgen van het incident (bijv. tijd besteed aan het oplossen van het incident, verlies van data) als ernstig ervaren.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 8

Q9. Angst_ransomware
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

		HELEMAAL MEE ONEENS	MEE ONEENS	ENIGSZINS MEE ONEENS	NIET MEE ONEENS, NIET MEE EENS	ENIGSZINS MEE EENS	MEE EENS	HELEMAAL MEE EENS
1	Ik schat de kans groot in dat mijn bedrijf in de komende 12 maanden nog een keer slachtoffer wordt van ransomware.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7
2	Ik maak me zorgen dat mijn bedrijf in de komende 12 maanden nog een keer slachtoffer wordt van ransomware.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7

Q10. Angst_ransomware_verschil
Kunt u voor de volgende stellingen aangeven in hoeverre u het hiermee eens bent?

Matrix

		HELEMAAL MEE ONEENS	MEE ONEENS	ENIGSZINS MEE ONEENS	NIET MEE ONEENS, NIET MEE EENS	ENIGSZINS MEE EENS	MEE EENS	HELEMAAL MEE EENS
1	Ik denk dat mijn bedrijf nu minder kans loopt om slachtoffer te worden van ransomware, wanneer ik dat vergelijk met de situatie voordat mijn bedrijf voor de laatste keer slachtoffer werd.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7
2	Ik maakt me nu minder zorgen dat mijn bedrijf slachtoffer wordt van ransomware, wanneer ik dat vergelijk met de situatie voordat mijn bedrijf voor de laatste keer slachtoffer werd.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6	☐ 7

Blok 2: Online zoekgedrag

We zullen u nu vragen stellen over uw online zoekgedrag naar aanleiding van het incident.

Q11. Online gezocht

Heeft u toen de ransomware aanval plaatsvond of toen u geconfronteerd werd met het losgeldbericht op internet gezocht in een van de volgende zoekmachines, bijvoorbeeld naar informatie of ondersteuning?

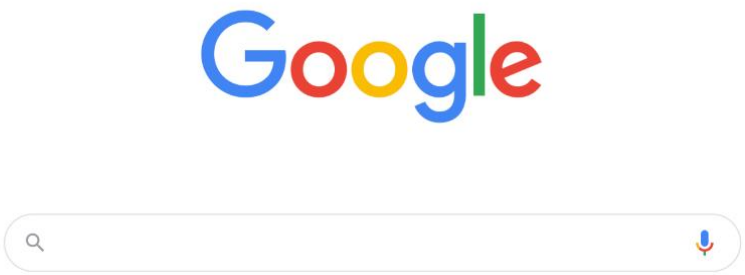
☐ Google
☐ Bing
☐ Yahoo!
☐ DuckDuckGo
☐ Andere zoekmachine, namelijk… [open antwoord]
☐ Ik heb niet gezocht in een zoekmachine

[Routing:
Indien antwoordoptie 1, 2,3, 4, 5 'ja' → door naar Q12]
Indien antwoordoptie 6 → door naar Q14]

Q12. Uitkomst_zoekopdrachten
In hoeverre heeft het zoeken naar informatie of hulp in een online zoekmachine u opgeleverd wat u zocht?

Matrix

	HELEMAAL MEE ONEENS	**MEE ONEENS**	**NIET MEE ONEENS, NIET MEE EENS**	**MEE EENS**	**HELEMAAL MEE EENS**	**NIET VAN TOEPASSING**
Ik heb de informatie gevonden die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
Ik heb de hulp gevonden die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
Ik heb contact kunnen leggen met een of meer organisaties die ik zocht	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6



Q13. Zoektermen_daadwerkelijk
U heeft aangegeven dat u tijdens het incident gezocht heeft naar informatie of ondersteuning op internet. Wij willen onderzoeken wat mensen in dit geval intypen in een zoekmachine.

Denkt u terug aan het moment dat u geconfronteerd werd met het losgeldbericht. Wat heeft u ingetypt in de zoekmachine? Uw zoektermen kunnen bestaan uit losse woorden, combinaties van woorden of zinnen. Ze kunnen bijvoorbeeld betrekking hebben op vragen, personen of organisaties. We willen u vragen om elke losse zoekopdracht in een apart antwoordveld in te vullen.

Als u het niet meer precies weet, vult u dan alstublieft in wat u ongeveer ingetypt heeft in die tijd.

Vult u alstublieft alle zoektermen in die u gebruikt heeft, ook als deze geen passend resultaat opleverden.

☐ Ik weet het niet meer

[Open antwoord]

[Open antwoord]

[Open antwoord]

[Open antwoord]

[Open antwoord]

[Open antwoord]

[**Pop-up als respondent wil doorklikken naar de volgende vraag**: Vaak gebruiken mensen verschillende zoektermen, of combinaties van zoektermen. Zijn er nog andere zoektermen die u zou gebruiken om te zoeken naar informatie of hulp? → Respondent optie geven om nog meer in te vullen, of definitief door te klikken naar de volgende pagina]

Blok 3: Behoefte(n)
We gaan u nu vragen stellen over wat u nodig had of waar u naar op zoek was na het incident.

Q15. Informatiebehoefte(n)
Na de ransomware aanval wilde ik meer informatie over…. (*Meerdere antwoorden mogelijk)*

☐ Wat me precies overkomen is
☐ Hoe het heeft kunnen gebeuren
☐ Het oplossen van het probleem
☐ Hoe ik kan voorkomen dat ik in de toekomst opnieuw slachtoffer word
☐ De organisaties waarbij ik terecht kan voor hulp
☐ De status van mijn aangifte (indien van toepassing)
☐ Het vergoed krijgen van de financiële schade
☐ Emotionele, psychische of lichamelijke gevolgen of klachten
☐ Het doen van een melding of aangifte bij de politie
☐ Juridische zaken
☐ Anders, namelijk… [open antwoord]

Q16. Hulpbehoefte(n)
Na de ransomware aanval wilde ik …. (*Meerdere antwoorden mogelijk)*

☐ Hulp bij het oplossen van het probleem
☐ Hulp om te voorkomen dat ik in de toekomst opnieuw slachtoffer word
☐ Hulp bij het vergoed krijgen van de financiële schade
☐ Hulp voor emotionele, psychische of lichamelijke gevolgen of klachten
☐ Hulp bij het doen van een melding of aangifte bij de politie
☐ Hulp bij juridische vragen of problemen
☐ Erkenning als slachtoffer
☐ Erkenning van wat me overkomen is
☐ Anders, namelijk… [open antwoord]

Q17. Contact_organisaties

Heeft u naar aanleiding van het incident bij een van de volgende partijen (mensen of organisaties) hulp gezocht? *Meerdere antwoorden mogelijk.*

☐ Vrienden, familie, kennissen of collega's
☐ Op internet
☐ De politie
☐ Bank of financiële instelling
☐ Verzekeringsmaatschappij
☐ Cybersecuritybedrijf, IT-leverancier of IT-specialist
☐ Fraudehelpdesk
☐ Slachtofferhulp Nederland
☐ Consumentenbond
☐ Autoriteit Persoonsgegevens
☐ Incassobureau, gerechtsdeurwaarder of advocaat
☐ No More Ransom
☐ Anders, namelijk… [open antwoord]
☐ Ik heb geen hulp gezocht

Q18. Contact_organisatie_online
[Als Q17*=meerdere antwoorden, dan deze vraag voor elke vorm (behalve 'vrienden, familie, kennissen of collega's', 'op internet' en 'ik heb geen hulp gezocht') vragen]*
U heeft aangegeven dat u bij de volgende organisatie hulp heeft gezocht: [*antwoord 1 van Q15*]. Welke van de volgende situaties is voor u van toepassing?
☐ Ik was al bekend met deze organisatie
☐ Een bekende heeft me op deze organisatie gewezen
☐ Ik ben bij deze organisatie terecht gekomen via het internet
☐ Ik weet niet meer hoe ik bij deze organisatie terecht ben gekomen

[herhalen voor antwoord 2 van Q17, antwoord 3 van Q17 etc.]

Q19. Beveiligingsmaatregelen
Heeft u, met uitzondering van eventuele maatregelen die u al nam, een van de volgende beveiligingsmaatregelen genomen nadat u slachtoffer bent geworden van ransomware? *Meerdere antwoorden mogelijk.*
☐ Een ander besturingssysteem genomen
☐ Regelmatige back-ups maken van bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Gebruik van sterke, unieke wachtwoorden
☐ Gebruik van een up-to-date antivirus product
☐ Gebruik van een firewall die zowel volledige IT-netwerken, als individuele apparaten beschermt

☐ Beveiligingssoftware netwerken en apparaten laten scannen op virussen of andere kwaadaardige software
☐ Monitoren van gebruikers- of netwerkactiviteiten
☐ Updates van besturingssystemen, apps en/of software direct uitvoeren zodra deze beschikbaar zijn
☐ Een ander standaardbrowser genomen
☐ Gebruik van een VPN-verbinding
☐ Installatie van browser extensies die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Gevoelige bestanden en gegevens worden versleuteld
☐ Tweestapsverificatie (2 stappen in plaats van 1 stap om in te loggen)
☐ Iemand (intern of extern) in dienst die verantwoordelijk is voor cybersecurity
☐ Een bedrijfscontinuïteitsplan dat betrekking heeft op de cybersecurity
☐ Geen van bovenstaande opties

Pop-up 19j: Een VPN (Virtual Private Network) verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.

Q20. Gedrag
Heeft u een van de volgende online activiteiten beperkt of verminderd binnen uw bedrijf nadat u slachtoffer bent geworden van ransomware? *Meerdere antwoorden mogelijk.*
☐ Het gebruik van accounts of pagina's op sociale media (zoals Facebook of Instagram) voor mijn bedrijf
☐ E-mailen
☐ Informatie zoeken of surfen op internet
☐ Tekstberichten sturen, bijvoorbeeld via WhatsApp
☐ Bellen of beeldbellen, bijv. via Whatsapp, Zoom of FaceTime
☐ De mogelijkheid voor klanten om online te bestellen, te reserveren, te betalen voor producten of diensten, of een schenking te doen
☐ De mogelijkheid voor klanten om online toegang te krijgen tot (enkele van) mijn diensten
☐ Het gebruik van internetbankieren of mobiel bankieren
☐ Het gebruik van online systemen of software, zoals een industrieel controlesysteem of Enterprise Resource Planning (ERP) systeem
☐ Het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs.
☐ Geen van bovenstaande opties

Blok 4: Achtergrondinformatie
We stellen u tot slot nog enkele algemene vragen.

Q21. Grootteklasse

Hoeveel personen zijn er momenteel werkzaam in uw bedrijf of vestiging, inclusief uzelf?
☐ 1 werkzame persoon (zelfstandige/eenmanszaak)
☐ 2 t/m 9 werkzame personen
☐ 10 t/m 49 werkzame personen
☐ 50 t/m 249 werkzame personen
☐ Meer dan 250 werkzame personen

Q22. Sector
In welke sector is uw bedrijf of vestiging momenteel werkzaam?
☐ A. Landbouw, bosbouw en visserij
☐ B. Winning van delfstoffen
☐ C. Industrie
☐ D. Productie, distributie, handel in elektriciteit en aardgas
☐ E. Winning/distributie van water; afval(water)beheer, sanering
☐ F. Bouwnijverheid
☐ G. Groot- en detailhandel; reparatie van auto's
☐ H. Vervoer en opslag
☐ I. Logies-, maaltijd- en drankverstrekking
☐ J. Informatie en communicatie
☐ K. Financiële instellingen
☐ L. Verhuur van en handel in onroerend goed
☐ M. Advisering, onderzoek, speciale zakelijke dienstverlening
☐ N. Verhuur van roerende goederen, overige zakelijke dienstverlening
☐ O. Openbaar bestuur, overheidsdiensten, sociale verzekeringen
☐ P. Onderwijs
☐ Q. Gezondheids- en welzijnszorg
☐ R. Cultuur, sport en recreatie
☐ S. Overige maatschappelijke dienstverlening
☐ U. Extraterritoriale organisaties en lichamen

Q23. Jaaromzet
Wat is momenteel de jaaromzet van uw bedrijf, in euro's?
☐ Minder dan €100.000
☐ €100.000 tot €500.000
☐ €500.000 tot €1.000.000
☐ €1.000.000 tot €2.500.000
☐ €2.500.000 tot €5.000.000
☐ Meer dan €5.000.000
☐ Zeg ik liever niet

☐ Weet ik niet

[Door naar afsluiting]

Afsluiting slachtoffers
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname aan dit onderzoek.

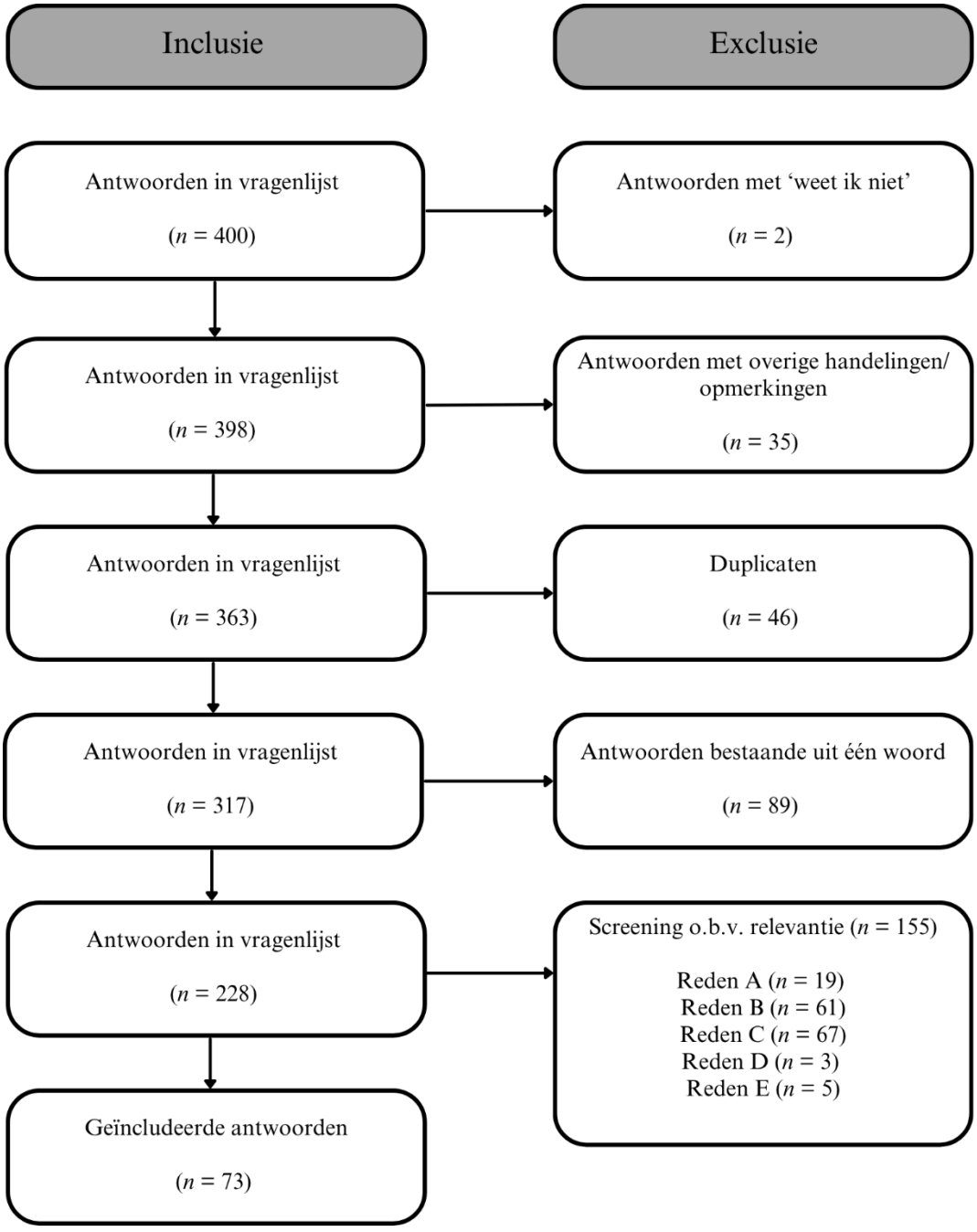
Wilt u verder praten over of melding maken van wat u is overkomen? Dan kunt u contact opnemen met een van de volgende instanties:
Politie Nederland
Slachtofferhulp Nederland

Afsluiting niet slachtoffers.

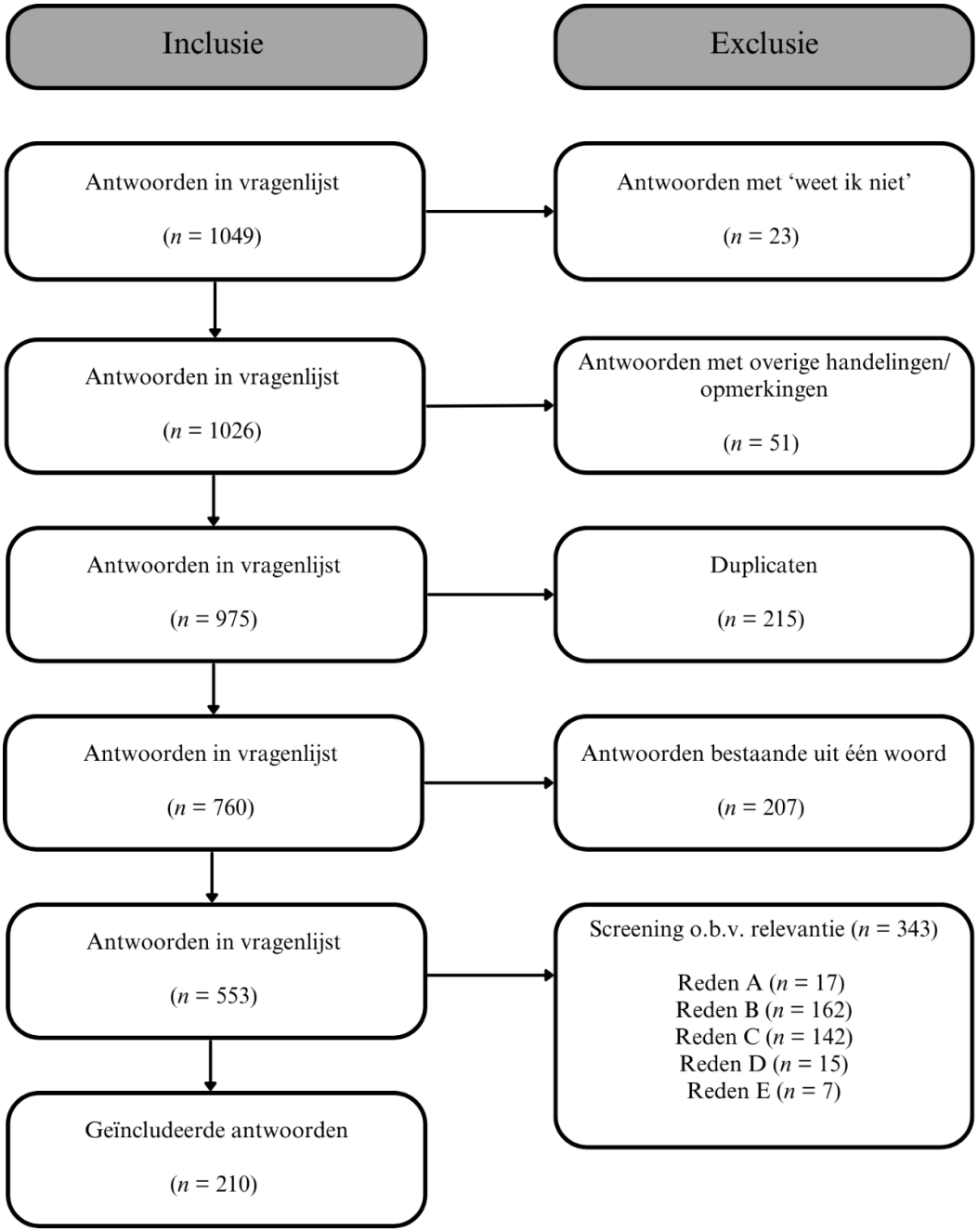
U behoort niet tot de doelgroep van deze vragenlijst. Bedankt voor uw moeite om deel te nemen aan dit onderzoek.

Bijlage 3: Flowcharts voor selectie zoektermen uit vragenlijsten

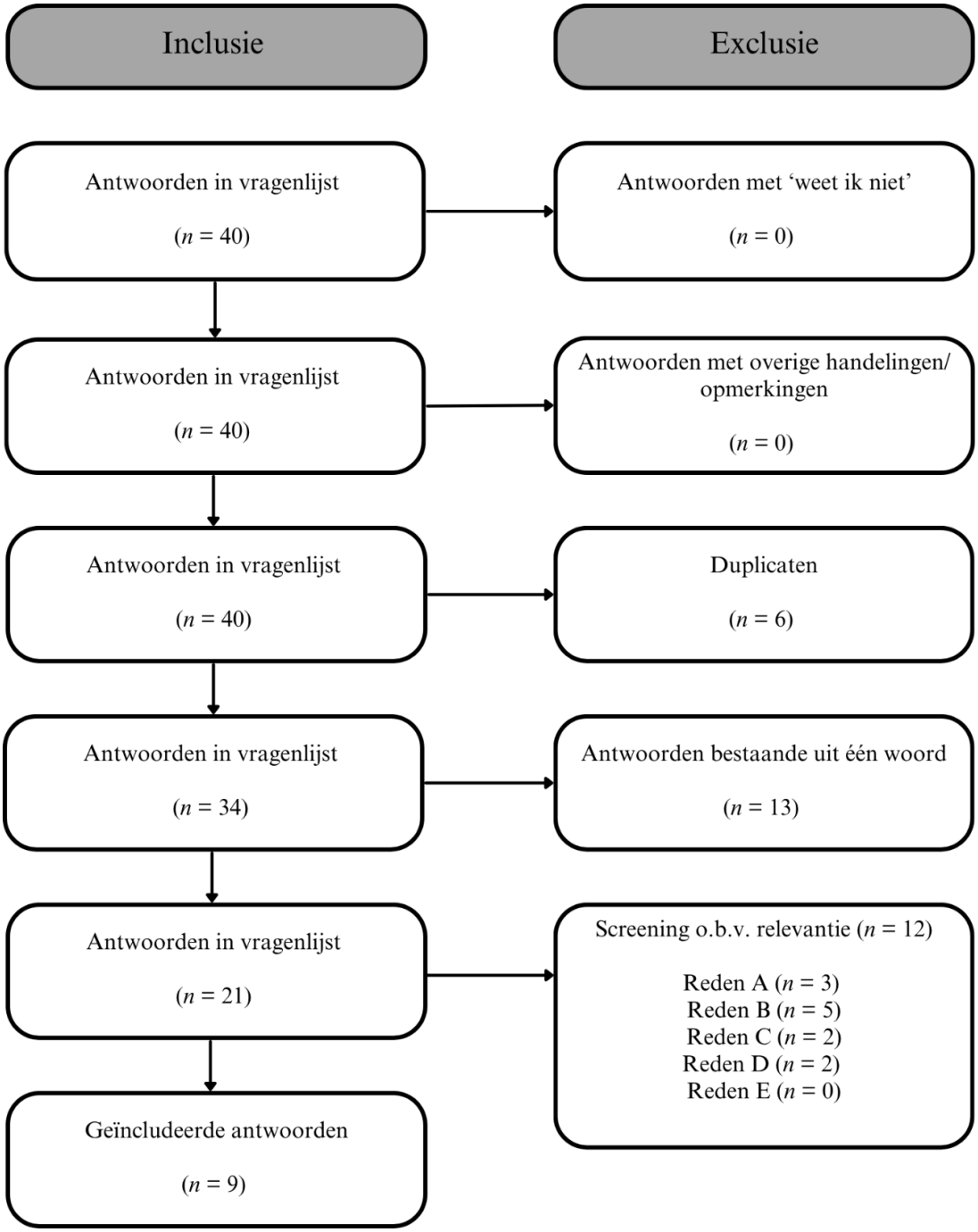
Figuur 1 Flowchart van geïncludeerde daadwerkelijke zoektermen onder slachtoffers van online fraude



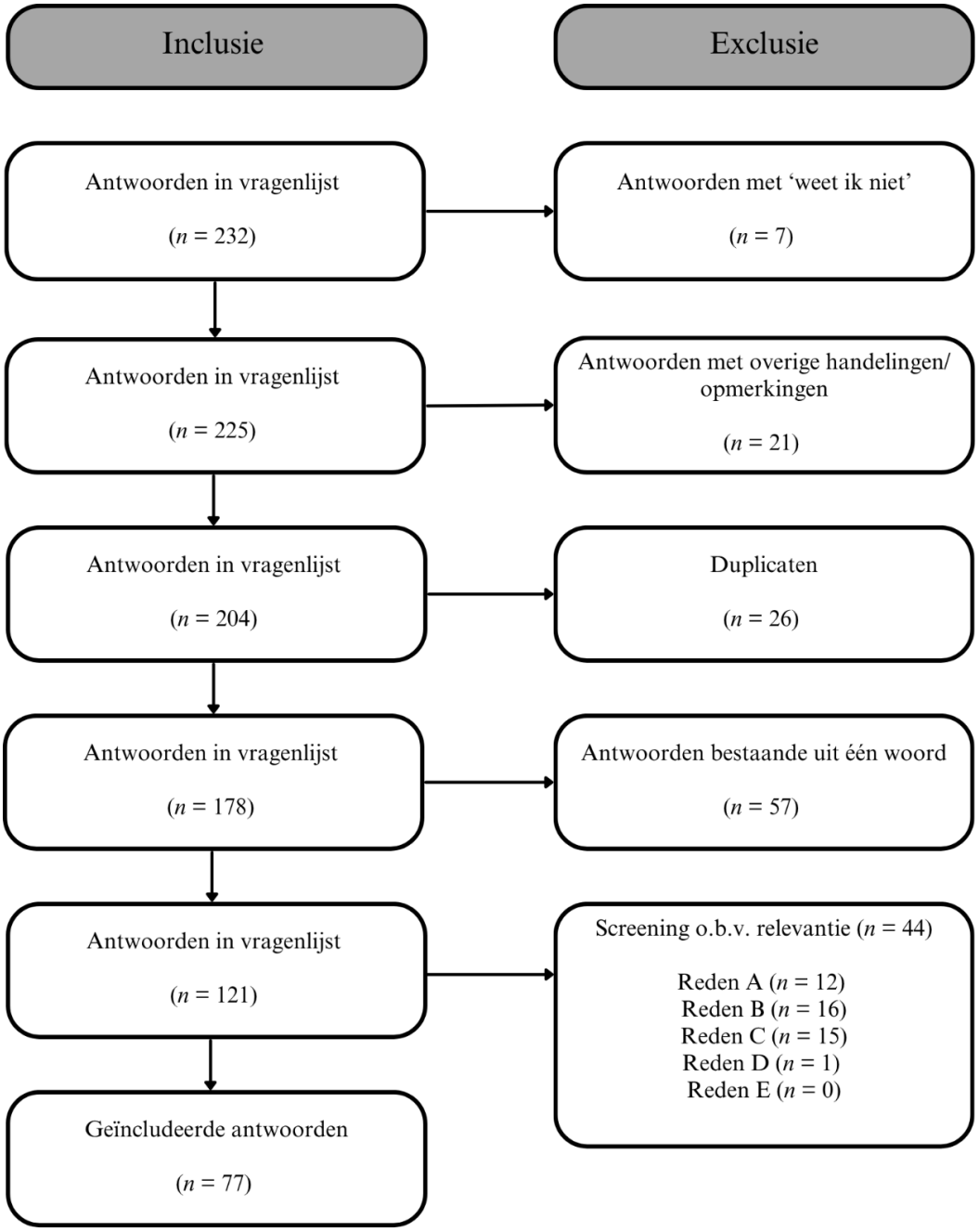
Figuur 2 Flowchart van geïncludeerde hypothetische zoektermen onder slachtoffers van online fraude



Figuur 3 Flowchart van geïncludeerde daadwerkelijke zoektermen onder slachtoffers van ransomware



Figuur 4 Flowchart van geïncludeerde hypothetische zoektermen onder slachtoffers van ransomware



Bijlage 4: Overzicht van vooraf gedefinieerde zoektermen voor de advertentiecampagnes

Tabel 1 Overzicht van vooraf gedefinieerde zoektermen voor online fraude (alfabetisch) (*n*=255)

#	**Zoekterm**
1.	aangifte doen internet oplichting
2.	aangifte doen na online scam
3.	aangifte doen online oplichting
4.	aangifte doen oplichting
5.	aangifte doen politie na fraude
6.	aangifte doen van oplichting
7.	aangifte doen van oplichting wanneer
8.	aangifte internet oplichting
9.	aangifte online oplichting
10.	aangifte oplichting
11.	aangifte oplichting marktplaats
12.	aangifte politie online oplichting
13.	aankoop niet geleverd
14.	account gehackt
15.	aliexpress pakket nooit verstuurd
16.	artikel betaald iets anders ontvangen
17.	artikel webwinkel niet geleverd
18.	assistentie cybercrime
19.	belastingdienst fake mail in omloop
20.	ben ik opgelicht
21.	bestaat deze winkel echt
22.	bestaat dit bedrijf
23.	bestaat verkoper
24.	besteld maar niet gekregen
25.	bestelling niet ontvangen
26.	bestelling via marktplaats betaald maar niet ontvangen
27.	betaald en niets ontvangen
28.	bij koop geen levering
29.	catfish scam
30.	creditcardfraude rabobank
31.	crypto oplichters
32.	deze website is fake
33.	dhl oplichting
34.	diefstal digitale gegevens
35.	doorverkoop fraude
36.	douane oplichting
37.	eerste hulp bij oplichting
38.	facebook oplichting
39.	fraude bij aliexpress
40.	fraude bij betaling
41.	fraude bij kopen muziek
42.	fraude bol com

#	**Zoekterm**
43.	fraude checklist
44.	fraude dienst bank
45.	fraude festivaltickets
46.	fraude helpdesk
47.	fraude helpdesks
48.	fraude herkennen
49.	fraude leverancier x
50.	fraude marktplaats
51.	fraude oplichting melden
52.	fraude temu
53.	fraude via online verkoop
54.	fraude webaankoop
55.	fraudedesk van mijn bank
56.	gebeld door onbekend nummer
57.	geen betaling ontvangen na verkoop
58.	gekocht product niet geleverd
59.	geld terug bij fraude
60.	geld terug bij oplichting
61.	geld terug bij oplichting via internet
62.	geld terug krijgen na oplichting
63.	geld terug na oplichting
64.	geld terug oplichter
65.	geld terug oplichting
66.	geld terug van oplichting
67.	geld terugkrijgen na fraude
68.	geld terugkrijgen product niet ontvangen
69.	geld terugkrijgen van bank na fraude
70.	gevolgen oplichting
71.	goederen verstuurd geen geld ontvangen
72.	help bij fraude
73.	help geld overgemaakt oplichting
74.	helpdesk fraude
75.	hoe herken ik oplichting
76.	hoe herken ik phishing
77.	hoe ingrijpen tegen oplichters
78.	hoe kan ik ik oplichters aangeven
79.	hoe krijg ik geld terug na oplichting
80.	hoe krijg ik hulp met online oplichting
81.	hoe te handelen bij oplichting via internet
82.	hoe voorkom ik fraude
83.	hoe voorkom ik internet fraude
84.	hoe voorkomen dat je opgelicht wordt
85.	hoe weet ik of iets betrouwbaar is
86.	hoe weet je of je bent opgelicht
87.	hoe ziet whatsappfraude eruit
88.	hulp bij internet oplichting
89.	hulp bij online fraude
90.	hulp bij online oplichting

#	**Zoekterm**
91.	hulp bij oplichting
92.	hulp bij oplichting online
93.	hulp bij oplichtingen
94.	hulp digitale fraude
95.	hulp krijgen met oplichting
96.	hulp nadat je opgelicht bent
97.	hulp online oplichting
98.	hulp oplichting
99.	hulp tegen oplichters
100.	ik ben online opgelicht wat nu
101.	ik ben opgelicht
102.	ik ben opgelicht waar hulp
103.	ik ben opgelicht wat kan ik doen
104.	ik ben opgelicht wat nu
105.	ik denk dat ik ben opgelicht
106.	ik heb de bestelling niet ontvangen maar wel betaald
107.	ik heb een product wel betaald maar niet ontvangen
108.	informatie over online oplichting via datingsite
109.	internet aankoop oplichting
110.	internetoplichting melden
111.	is deze website betrouwbaar
112.	juridische hulp oplichting
113.	kan ik geld retour krijgen via marktplaats als ik mijn spullen niet heb gekregen
114.	klachten na oplichting
115.	maatregelen tegen online oplichting
116.	malafide webshops
117.	marktplaats fraude
118.	marktplaats klant betaalt niet
119.	marktplaats opgelicht
120.	marktplaats oplichter melden
121.	marktplaats oplichting
122.	marktplaats scam
123.	martkplaats direct betalen scam
124.	melden fraude internet oplichting
125.	melden identiteitsfraude
126.	melden internet oplichting
127.	melden oplichting
128.	melden van internet fraude
129.	melden van oplichting
130.	melding acm verkoper
131.	meldpunt online oplichting
132.	nep berichten
133.	nep producten herkennen
134.	nep winkel ervaringen
135.	niet bestaande webshop
136.	niet geleverde betaalde artikelen
137.	nieuwe manieren online oplichting
138.	nooit betaald marktplaats

#	**Zoekterm**
139.	onbekende beller buitenland
140.	online fraude melden
141.	online nep winkel
142.	online opgelicht wat kan ik doen
143.	online opgelicht wat nu
144.	online oplichting support
145.	online oplichting vermelden
146.	online oplichting wat te doen reddit
147.	online verkoper niet bereikbaar
148.	opgelicht bij internetaankoop
149.	opgelicht bij wie moet ik zijn
150.	opgelicht hulp
151.	opgelicht internetwinkel dropshipping
152.	opgelicht marktplaats
153.	opgelicht marktplaats oplossing reddit
154.	opgelicht op marktplaats
155.	opgelicht op platform incident melden
156.	opgelicht tros
157.	opgelicht via internet
158.	opgelicht via marktplaats
159.	opgelicht via telefonisch contact
160.	opgelicht wat nu
161.	oplichters melden marktplaats
162.	oplichting aangifte politie
163.	oplichting aankoop
164.	oplichting aankoop bitcoins
165.	oplichting bij ali express
166.	oplichting bij temu
167.	oplichting dhl
168.	oplichting door whatsapp
169.	oplichting doorgeven
170.	oplichting filipijnen
171.	oplichting financieel
172.	oplichting google waarschuwen
173.	oplichting help
174.	oplichting herkennen
175.	oplichting hoe te handelen
176.	oplichting lp marktplaats
177.	oplichting marktplaats
178.	oplichting marktplaats rekeningnummer
179.	oplichting melden
180.	oplichting melden bij de politie
181.	oplichting politie
182.	oplichting via internet
183.	oplichting via marktplaats
184.	oplichting via whatsapp
185.	oplichting vinted
186.	oplichting voorkomen

#	**Zoekterm**
187.	oplichting wat te doen
188.	oplichting webshop
189.	oplichting whatsapp
190.	oplossing oplichting
191.	pas op oplichter
192.	phishing voorkomen
193.	politie aangifte online oplichting
194.	politie aangifte oplichting internetwinkel
195.	politie oplichting
196.	politie site oplichting
197.	product gekocht maar niet ontvangen
198.	product niet ontvangen
199.	product niet ontvangen wat nu
200.	product online aankoop niet geleverd
201.	product voldoet geheel niet aan eisen wat zijn de opties
202.	product voldoet niet aan verwachting
203.	profiel misbruikt
204.	rechten fraude
205.	rechtsbijstand oplichting
206.	schade internetaankoop
207.	site oplichting
208.	slachtofferhulp datingfraude
209.	slachtoffers online oplichting
210.	telefonische oplichting
211.	ticket fraude
212.	tinder doorgeven fakers
213.	tinder oplichting
214.	valse website
215.	vergoeding naar aanleiding van oplichting
216.	verkopers via bol com oplichting
217.	vinted fraude
218.	voorbeelden fraude
219.	vrbo huisje bestaat niet
220.	vrbo opgelicht
221.	vrbo oplichting
222.	waar kan ik melden als product niet overeen komt met omschrijving
223.	waar melden oplichting
224.	waar op letten online oplichting
225.	waarom kan ik de oplichter niet meer vinden
226.	wanneer politie benaderen na oplichting
227.	wat doe ik als ik opgelicht ben
228.	wat doe je bij vermoeden van fraude
229.	wat doen bij oplichting
230.	wat doen tegen oplichting
231.	wat kan ik doen bij online oplichting
232.	wat kan ik doen bij oplichting
233.	wat kan ik doen wanneer ik ben opgelicht
234.	wat moet ik doen als ik ben opgelicht

#	**Zoekterm**
235.	wat te doen aan online oplichting
236.	wat te doen als je opgelicht bent
237.	wat te doen bij fraude
238.	wat te doen bij internet fraude
239.	wat te doen bij internet oplichting
240.	wat te doen bij niet betalen marktplaats
241.	wat te doen bij online oplichting
242.	wat te doen bij oplichting
243.	wat te doen bij oplichting bol com
244.	wat te doen bij vermoeden fraude
245.	wat te doen met oplichterij
246.	wat te doen na oplichting
247.	wat zijn de regels wat betreft online oplichting
248.	webshop opgelicht
249.	webshop oplichting
250.	webshop pakket komt niet aan
251.	webshop product niet ontvangen
252.	website opgelicht
253.	website oplichting
254.	welke instantie helpt bij online oplichting
255.	winkel opgelicht

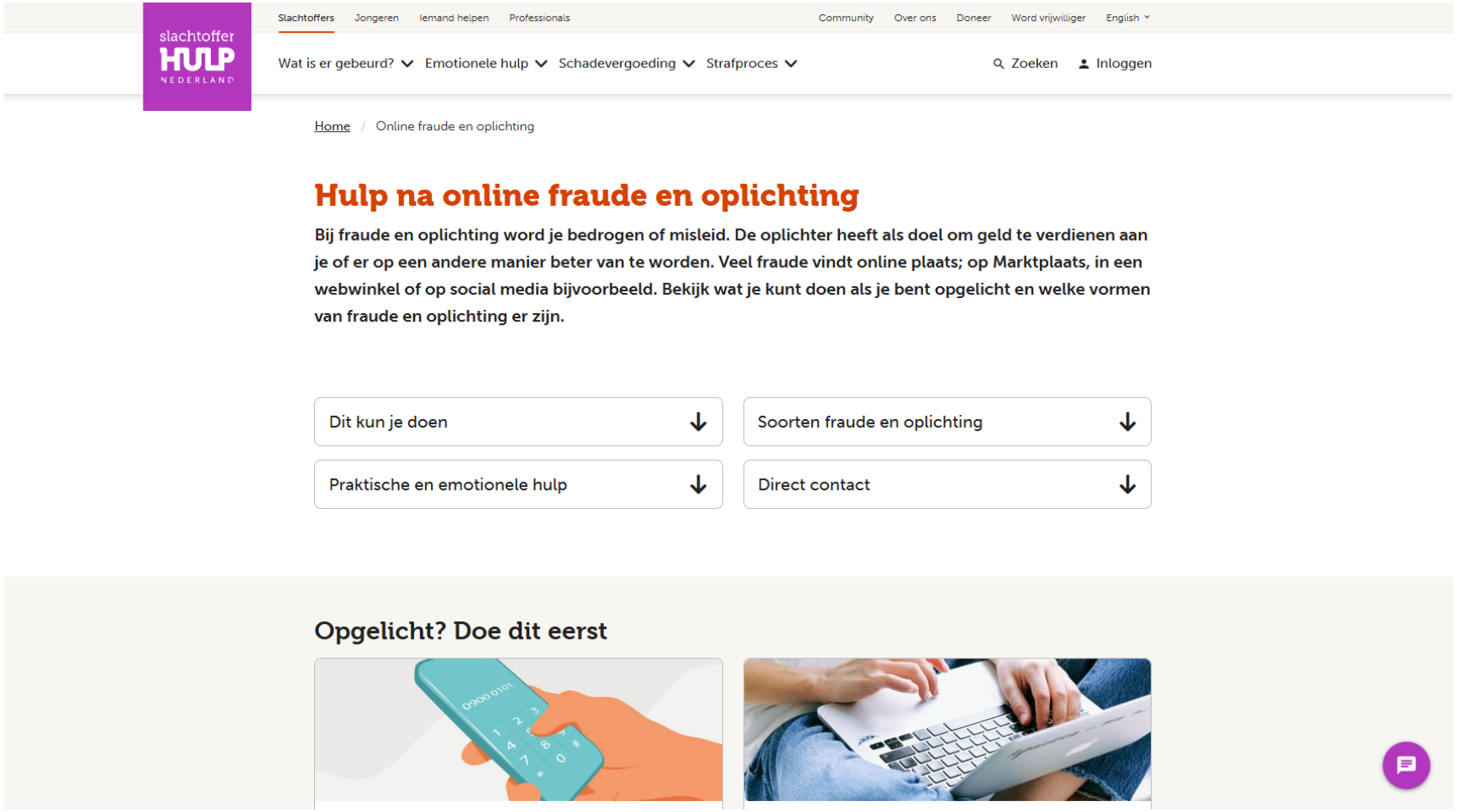
Tabel 2 Overzicht van vooraf gedefinieerde zoektermen voor ransomware (alfabetisch) (*n*=115)

#	**Zoekterm**
1.	aangifte online chantage
2.	aangifte ransom aanval
3.	advies bij ransomware
4.	afpersing software
5.	afpersing via computer
6.	afzetting online
7.	ben ik gehacked check
8.	ben ik gehackt
9.	ben ik gehackt 2021
10.	ben ik gehackt check
11.	ben ik gehackt email
12.	ben ik gehackt op mijn telefoon
13.	ben ik gehackt politie
14.	ben ik gehackt website
15.	bestanden gegijzeld
16.	bestanden ontgrendelen
17.	bestanden versleuteld
18.	blokkering pc
19.	chantage computer
20.	chantage data
21.	check of ik gehackt ben
22.	computer geblokkeerd door ransomware

#	**Zoekterm**
23.	computer geblokkeerd losgeld
24.	computer gehackt
25.	computer vergrendeld losgeld
26.	computer vergrendeling oplossen
27.	computerblokkade en politie
28.	controleren of ik gehackt ben
29.	cryptoware verwijderen
30.	cybercrime helpdesk
31.	cybercrime hulp
32.	deadbolt ransomware verwijderen
33.	deblokkeren bestanden
34.	eerste hulp bij ransomware
35.	gehackt telefoonnummer
36.	gehackte computer
37.	gijzelen computer
38.	gijzelsoftware op computer
39.	gijzelsoftware verwijderen
40.	gijzelsoftware voorkomen
41.	hoe kan ik zien of mijn computer gehackt is
42.	hoe kan ik zien of mijn pc gehackt is
43.	hoe los ik een ransomware aanval op
44.	hoe verwijder ik ransomware
45.	hoe weet ik of mijn computer gehackt is
46.	hoe weet ik of mijn laptop gehackt is
47.	hoe weet ik of mijn pc gehackt is
48.	hulp bij aanval pc
49.	hulp bij cybercrime
50.	hulp bij ransomware
51.	ik ben gehackt
52.	ik ben gehackt wat moet ik doen
53.	ik ben gehackt wat te doen
54.	ik denk dat ik gehackt ben
55.	ik krijg een mail dat ik gehackt ben
56.	ik word gehackt
57.	it bureau gijzelsoftware
58.	it bureau ransomware
59.	kan ik aangifte doen voor computer aanval
60.	kan ik ook aangifte doen tegen ransomware
61.	losgeld internet
62.	losgeld voor bestanden
63.	losgeld voor computerblokkade
64.	losgeld voor gegegevens weer terug krijgen
65.	masterdata unlockcode
66.	melden ransomware
67.	meldingen van ransomware
68.	mijn bestanden zijn gegijzeld
69.	mijn bestanden zijn versleuteld
70.	mijn computer is gehackt

#	**Zoekterm**
71.	moet je losgeld betalen
72.	omgaan met ransomware
73.	online chantage
74.	ontgrendel specialist desktop
75.	ontsluiten pc gijzelsoftware
76.	opheffen ransomware
77.	oplichters versleutelen bestanden
78.	oplossen hack
79.	oplossen ransomprobleem
80.	probleem oplossen ransom aanval
81.	ransom software verwijderen
82.	ransomware aanval voorkomen
83.	ransomware advies
84.	ransomware attack countermeasures
85.	ransomware incident response plan
86.	ransomware losgeld
87.	ransomware mail
88.	ransomware melden
89.	ransomware op pc
90.	ransomware oplossen
91.	ransomware release
92.	ransomware slachtoffer
93.	ransomware social media
94.	ransomware solution
95.	ransomware specialist oplossing
96.	ransomware verwijderen
97.	ransomware voorkomen
98.	ransomware wat te doen
99.	regain access to files
100.	specialist voor ontgrendelen pc
101.	unlock data
102.	versleutelde bestanden
103.	voorkomen ransomware
104.	wat doe ik bij gekaapte website
105.	wat is ransomware en hoe komt het op je computer
106.	wat kun je doen tegen ransomware
107.	wat nooit doen bij ransomware
108.	wat te doen als ik gehackt ben
109.	wat te doen bij computer op slot en eisen van geld
110.	wat te doen bij internetafpersing
111.	wat te doen bij ransomsoftware
112.	wat te doen bij ransomware
113.	wat te doen bij ransomware
114.	website gegijzeld wat kan ik doen
115.	wie kan ik aansprakelijk stellen bij ransomware

Bijlage 5: Landingspagina advertentiecampagne online fraude



Bijlage 6: Landingspagina advertentiecampagne ransomware

