

# Vissen met een nieuwe hengel: een onderzoek naar betaalverzoekfraude

*Joke Rooyakkers en Marleen Weulen Kranenborg\**

Computers en mobiele apparaten zijn onlosmakelijk onderdeel geworden van de hedendaagse maatschappij. Hierdoor is er een ontwikkeling gaande waarin steeds meer vormen van criminaliteit een digitale component bevatten (Grabosky 2017). Met deze ontwikkeling ontstaan nieuwe delictsvormen zoals ransomware en DDoS-aanvallen (cybercriminaliteit in enge zin), maar ook de mogelijkheden om traditionele criminaliteit (deels) digitaal te plegen nemen sterk toe (cybercriminaliteit in brede zin) (Reep-van den Bergh & Junger 2018; Rokven e.a. 2017). Betaalverzoekfraude is een recent voorbeeld van een delict waarbij fraudeurs onder andere gebruik maken van een valse identiteit en overtuigingstechnieken (*social engineering*) om via phishing inloggegevens af te vangen en vervolgens te gebruiken om in te loggen op de digitale bankomgeving van het slachtoffer. Sinds de zomer van 2018 is dit een veelvoorkomende vorm van cybercrime. In de onderzochte periode in deze studie (20 juni-20 augustus 2019) betrof betaalverzoekfraude 16% van alle door de informatieorganisatie als cybercrime bestempelde meldingen bij de politie.

Bij deze nieuwe vorm van criminaliteit wordt een verkoper op (in veel gevallen) Marktplaats.nl benaderd door de fraudeur. Deze fraudeur overtuigt de verkoper door middel van social engineering een klein bedrag over te maken via een URL die exact lijkt op een legitieme betaalverzoeklink (zie figuur 1). Deze URL leidt het slachtoffer naar een internetbankieren-phishingsite, waar de inloggegevens ingevuld worden. De fraudeur vangt deze inloggegevens af en gebruikt deze om oneigenlijk toegang te krijgen (computervredebreuk gepleegd met een valse sleutel) tot de gelden op rekeningen van het slachtoffer. Hoewel

\* I.J.M. Rooyakkers MSc. is analist cybercrime bij de Nationale Politie, eenheid Limburg. Dr. M. Weulen Kranenborg is universitair docent Criminologie aan de Vrije Universiteit Amsterdam. Persoonlijke pagina: <https://research.vu.nl/en/persons/marleen-weulen-kranenborg>.

**Figuur 1**      **Voorbeeld WhatsApp-bericht met hierin een illegitieme betaalverzoek-URL, een veelgebruikte benaderingswijze bij betaalverzoekfraude**



phishing via e-mail al bestaat sinds de opkomst van e-mail, blijken fraudeurs met deze nieuwe vorm van phishing mee te gaan in recente digitale ontwikkelingen (zoals ook geïdentificeerd door Grabosky 2017). Zo worden slachtoffers nu gevonden via diverse online platforms en loopt de communicatie met potentiële slachtoffers via andere communicatiekanalen, zoals WhatsApp in plaats van e-mail. Ook maken fraudeurs handig gebruik van de bekendheid van nieuwe betaalmethoden zoals het betaalverzoek. De mate waarin potentiële slachtoffers gebruik maken van deze nieuwe technieken is van invloed op de blootstelling aan dergelijke vormen van phishing en de kenmerken en vaardigheden van het slachtoffer kunnen vervolgens bepalen of het slachtoffer ook daadwerkelijk in de phishingpoging trapt. De reeds bestaande technische preventiemaatregelen voor phishing (zoals e-mailfilters) zijn niet gericht op deze steeds wijzigende manier waarop fraudeurs hun slachtoffers benaderen. Daarnaast blijft de mens de zwakste schakel, ondanks de ontwikkeling van steeds nieuwe technische oplossingen (Canfield e.a. 2016).

Hoewel bovenstaande modus operandi (MO) van betaalverzoekfraude vrij technisch klinkt, is het een delict dat op grote schaal wordt gepleegd en waarvoor weinig technische kennis nodig is. Alle onderdelen van de MO (zoals gehackte Marktplaatsaccounts of het phishing-panel, de achterkant van de valse websites) en bijbehorende kennis kunnen voor een lage prijs worden gekocht of ingehuurd via internet (Van Wegberg e.a. 2018). Hierna is het slechts een kwestie van het op de juiste wijze benaderen van potentiële slachtoffers en op een anonieme manier het verdiende geld wegsluizen (cash-out). In dit artikel

wordt onderzocht hoe deze relatief nieuwe benaderingsvorm van phishing eruit ziet en wat hem zo succesvol maakt. Nu communicatie plaatsvindt via andere kanalen is het bijvoorbeeld ook de vraag in hoeverre daders nieuwe overtuigingstechnieken gebruiken en of slachtoffers wellicht andere kenmerken hebben. In het huidige onderzoek richten we ons daarom op de volgende vragen:

1. Hoe ziet de MO van betaalverzoekfraude eruit?
2. Welke (overtuigings)technieken gebruiken daders?
3. Welke kenmerken hebben slachtoffers van betaalverzoekfraude?

Deze vragen zullen worden beantwoord met behulp van een analyse van 728 betaalverzoekfraudes waarvan bij de politie aangifte of melding is gedaan tussen 20 juni en 20 augustus 2019. Deze betaalverzoekfraudes zijn gefilterd uit de landelijke cybercrime-politieregistraties, waarna ze op diverse variabelen zijn gescoord en geanalyseerd.

### *Relevantie*

Wetenschappelijk onderzoek naar phishing heeft zich vooral gericht op slachtofferkenmerken (o.a. Alseadoon 2014; De Kimpe e.a. 2018; Leukfeldt 2014; Van 't Hoff-de Goede e.a. 2019) en interventies zoals *phishing awareness*-trainingen (o.a. Jansen & Van Schaik 2018; Kumaraguru e.a. 2009; Sheng e.a. 2010). Al dit wetenschappelijk onderzoek richt zich op phishing via e-mail, maar niet op phishing via nieuwe platforms (sms en chatapps zoals WhatsApp). Het huidige onderzoek zal dan ook onderzoeken in hoeverre dezelfde of andere slachtofferkenmerken (zoals geslacht en leeftijd) ook een rol spelen bij deze nieuwe benaderingsvorm. In tegenstelling tot het overheersende slachtoffergerichte perspectief richten we ons in dit onderzoek naast de beschrijving van de slachtofferkenmerken vooral op de werkwijze vanuit daderperspectief. In de literatuur is, op basis van de inhoud van phishing-mails, wel beperkt beschrijvend onderzoek gedaan naar de MO en overtuigingstechnieken van phishers (o.a. Mouton e.a. 2016; Uehara e.a. 2020). In het huidige onderzoek breiden we dit uit naar betaalverzoekfraude, een variant van phishing via WhatsApp en Marktplaats.nl met gebruik van social engineering, waarin ook aandacht is voor de gebruikte overtuigingstechnieken en de mate waarin deze anders zijn dan 'traditionele' overtuigingstechnieken. De nadruk zal liggen op beschrijvende analyses om de karakteristieken van deze

MO te duiden en meer inzicht te krijgen in het fenomeen. De vragen wie, wat, waar, wanneer en hoe zullen worden beantwoord, volgens Thomlison (2001) de primaire taak bij het omschrijven van een relatief nieuw fenomeen.

Naast de wetenschappelijke relevantie biedt dit onderzoek ook inzichten die belangrijk zijn voor de opsporingspraktijk en het voorkomen van slachtofferschap. Het aantal cybercrimeaangiftes neemt de laatste jaren namelijk toe<sup>1</sup> en de verwachting is dat online criminaliteit in de toekomst alleen maar verder zal toenemen (Aiken e.a. 2015). Hoewel er wel enige kennis over dit nieuwe fenomeen binnen de politieorganisatie is, zijn bredere bekendheid en kennis over de aard, omvang en schade van belang voor opsporing en preventie. Een recente inventarisatie onder drie regionale cyberteams laat ook zien dat er een sterke vraag is naar meer informatie over nieuwe fenomenen op dit gebied binnen de politie (Boekhoorn 2020). De informatie die in dit onderzoek wordt verkregen over betaalverzoekfraude zal mogelijk breder toepasbaar zijn op andere vormen van cybercrime en inzicht bieden in de manier waarop fraudeurs hun MO aanpassen aan nieuwe mogelijkheden in een gedigitaliseerde maatschappij.

### *Opbouw*

Ten eerste zal kort worden stilgestaan bij eerder onderzoek naar (spear)phishing, overtuigingstechnieken en slachtofferkenmerken. Vervolgens wordt in de methodeparagraaf uitgewerkt hoe de meldingen van betaalverzoekfraude zijn verzameld, gescoord en geanalyseerd. In de resultaten wordt vervolgens stilgestaan bij de MO, waarin ook de acties van dader en slachtoffer en gebruikte overtuigingstechnieken naar voren komen. Daarnaast worden de geobserveerde slachtofferkenmerken en schade besproken. In de conclusie wordt antwoord gegeven op de drie onderzoeksvragen die hierboven zijn genoemd, waarna in de discussie beperkingen en aanbevelingen aan bod komen.

1 Bijlage beantwoording vragen begroting ministerie van Justitie en Veiligheid 2020, zie [www.rijksoverheid.nl/documenten/rapporten/2019/11/14/tk-bijlage-beantwoording-schriftelijke-vragen-begroting-jenv-2020](http://www.rijksoverheid.nl/documenten/rapporten/2019/11/14/tk-bijlage-beantwoording-schriftelijke-vragen-begroting-jenv-2020).

## (Spear)phishing

Bij phishing wordt door criminelen in e-mails of op valse websites gebruik gemaakt van een valse identiteit en overtuigingstechnieken (social engineering) om zo een slachtoffer te bewegen inloggegevens af te geven. Phishing gebeurt over het algemeen ongericht, waarbij hetzelfde phishingbericht in één keer naar een grote groep slachtoffers wordt gestuurd. Bij spearphishing, daarentegen, worden de overtuigingstechnieken specifiek aan de persoon aangepast. Over het algemeen richt spearphishing zich daarbij op specifieke personen binnen bedrijven en niet op individuele internetgebruikers (Gupta e.a. 2018). Hoewel Gupta en collega's in hun beschrijving van de MO van phishers specifiek aangeven dat phishers gebruik maken van e-mails of websites, laat de opkomst van betaalverzoekfraude zien dat er ook andere (communicatie)kanalen zijn om een variant van spearphishing uit te voeren. Bij de variant van spearphishing-betalverzoekfraude wordt immers gebruik gemaakt van een valse identiteit (meestal een gehackt Marktplaatsaccount<sup>2</sup>) om door middel van social engineering die specifiek op de persoon gericht is (ingaan op een Marktplaats-advertentie van het potentiële slachtoffer) het slachtoffer te bewegen inloggegevens van de bank in te voeren op een valse website. Opvallend is dat hierbij de pijlen juist worden gericht op individuen en niet op bedrijven. Daarnaast doet de fraudeur zich niet, zoals bij de meeste andere vormen van phishing, voor als bijvoorbeeld de bank, maar als een willekeurige andere internetgebruiker. Het feit dat Gupta en collega's (2018) deze nieuwe vorm van benadering van het slachtoffer nog niet onder phishing scharen, laat zien dat fraudeurs altijd een stapje voor lopen op onderzoek en opsporing. Cybercrime is een vorm van criminaliteit die zich in vele vormen kan uiten en adaptief is. Doordat er steeds nieuwe methoden ontstaan, zijn veel potentiële slachtoffers niet altijd in staat tijdig preventieve maatregelen te nemen. Hierdoor blijft cybercrime lucratief, ondanks continue (technische) ontwikkelingen op het vlak van preventie. Juist wanneer er een nieuwe vorm van cybercrime opkomt, zijn technische interventies niet direct paraat. Internetbrowsers, banken en andere betrokken partijen helpen met preventie en het herkennen van phishing, maar het komt grotendeels aan op het potentiële slachtoffer

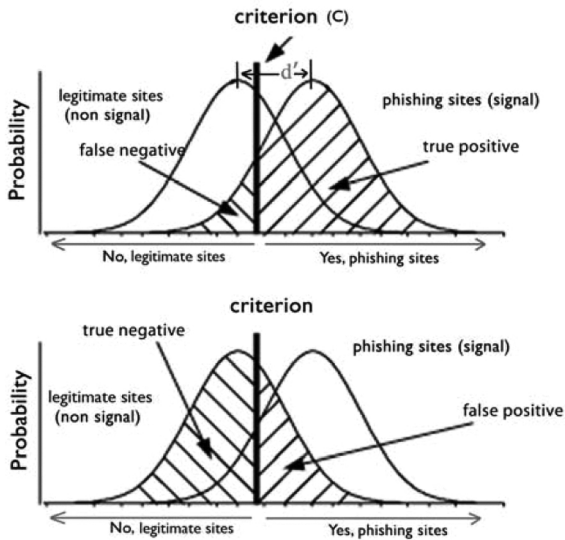
2 Met de inloggegevens van een ander inloggen op een Marktplaatsaccount zorgt ervoor dat je gebruik maakt van iemand anders identiteit.

om een phishingbericht als zodanig te herkennen en juist te handelen. In de literatuur over phishing via e-mail wordt dit besproken aan de hand van de *signal detection theory* (o.a. Green & Swets 1966; Jansen e.a. 2019; Jensen e.a. 2017; Sheng e.a. 2007; Lawson e.a. 2020). Uitgangspunt hierbij is dat een persoon veel e-mails krijgt. De meeste zijn legitiem (ruis), maar er zitten ook phishing-mails tussen (signaal). De manier waarop een persoon hiermee omgaat, hangt af van de mate waarin het voor hem of haar moeilijk of makkelijk is om een phishing-mail van een legitieme e-mail te onderscheiden (*sensitivity*) en hoe voorzichtig iemand hiermee omgaat (*criterion*). Onvoorzichtig handelen kan hierbij zorgen voor veel valsnegatieven (het slachtoffer ziet een phishing-mail onterecht aan voor een legitieme e-mail), waardoor slachtofferschap kan ontstaan. Aan de andere kant zorgt zorgvuldig handelen juist voor veel valspositieven, waardoor ook veel legitieme e-mails als phishing worden behandeld (o.a. Green & Swets 1966; Jensen e.a. 2017; Sheng e.a. 2007).

Het bovenstaande wordt gevisualiseerd in figuur 2 uit het onderzoek van Sheng en collega's (2007). In dit onderzoek wordt gesproken over phishing-sites in plaats van e-mails, maar dit is op gelijke wijze van toepassing op phishing-mails. Daarnaast linken phishing-mails vaak door naar dergelijke sites. Het gebied onder de curve links van het midden geeft het aantal legitieme e-mails weer (ruis), het gebied onder de curve rechts van het midden het aantal phishing-mails (signaal). Het potentiële slachtoffer ontvangt beide typen e-mails en moet bepalen wanneer deze als legitiem of als phishing moeten worden aangemerkt. In de figuur wordt met de afstand tussen de twee toppen (aangegeven met  $d'$ ) de *sensitivity* aangegeven. De mate waarin een individu in staat is om te bepalen of een e-mail wel of niet phishing is, bepaalt hoe sterk de twee grafieken overlappen en daarmee hoeveel potentiële valsnegatieven of valspositieven er zijn. Vervolgens bepaalt de plek van de *criterion*-lijn (dus de voorzichtigheid en risicobereidheid van het potentiële slachtoffer) of het potentiële slachtoffer meer valspositieve of meer valsnegatieve keuzes maakt.

Toegepast op betaalverzoekfraude werkt dit als volgt. Wanneer iemand een advertentie plaatst op Marktplaats.nl, kunnen hier reacties op komen. Hiervan zal de overgrote meerderheid legitiem zijn (ruis), maar er zitten ook phishingberichten tussen. Deze (spear)phishingberichten (signaal) zullen erg lijken op deze legitieme berichten,

**Figuur 2** Visualisatie signal detection theory (Sheng e.a. 2007)



omdat ze specifiek op de advertentie en verkoper zijn toegespitst. Hierdoor zijn de niet-legitieme berichten lastig van de legitieme reacties op advertenties te onderscheiden, de grafieken overlappen sterk (*sensitivity*). Sterker nog, het eerste bericht bevat over het algemeen geen verdachte informatie. Pas wanneer de verkoper in gesprek gaat met de fraudeur wordt in de loop van het gesprek het phishingbetaalverzoek verstuurd. Deze vorm van phishing lijkt dus veel interactiever te zijn dan phishing via e-mail. Hoewel het daarnaast zo kan zijn dat een verkoper relatief weinig berichten ontvangt en er dus weinig ruis is, zal een verkoper juist dan wellicht minder voorzichtig zijn, omdat slechts een beperkt aantal potentiële kopers zich aanbiedt en hij blij is het product voor een goede prijs te verkopen. De *criterion*-lijn ligt dus wellicht relatief ver naar rechts, waardoor er relatief veel valsnegatieven zijn en de verkoper een bericht ten onrechte niet als phishing aanmerkt.

## Overtuigingstechnieken

Door in te spelen op beide elementen van de signal detection theory wordt dus niet ingespeeld op een technische kwetsbaarheid, maar op de kwetsbaarheid van de gebruiker: de mens. Via misleiding en overtuiging wordt geprobeerd om via de menselijke kant toegang te krijgen tot systemen (Bullée e.a. 2018). Deze techniek wordt social engineering genoemd, het gebruik van sociale invloeden om mensen (ongemerkt) te overtuigen bepaalde stappen te ondernemen. Cialdini (2009) onderscheidt zes traditionele overtuigingsprincipes die in de marketing veelvuldig worden gebruikt om mensen te bewegen zich op een bepaalde manier te gedragen. Deze technieken blijken ook zeer waardevol in het ontrafelen van het succes van social engineering (o.a. Albladi & Weir 2016; Uebelacker & Quiel 2014; Uehara e.a. 2020; Wright e.a. 2014; Lawson e.a. 2020). Het eerste principe is autoriteit: mensen zijn geneigd om zich te conformeren aan autoritaire/leidende personen. Ten tweede sympathie: mensen zijn bereid om anderen die vriendelijk en behulpzaam zijn te helpen. Ten derde conformiteit: mensen zijn groepsdieren en vertonen graag het gedrag dat anderen al vertonen. Ten vierde schaarste: mensen zijn sneller geneigd mee te gaan als een product of dienst beperkt beschikbaar is. Ten vijfde consistentie: als mensen eenmaal iets toezeggen, zijn ze sneller geneigd om ook de vervolgstap te nemen. Als laatste wederkerigheid: mensen zijn geneigd om een tegengebaar te maken als iemand iets heeft gegeven. In het geval waarin bovenstaande mechanismen gecombineerd voorkomen (bijvoorbeeld bij het benaderen van een potentieel phishingslachtoffer), is de kans op succes groter (Cialdini 2009).

## Slachtofferkenmerken

Hoewel daders dus bepaalde verspreidingsstrategieën gebruiken en bepaalde overtuigingstechnieken inzetten, zal niet iedereen in een phishingpoging trappen. Kenmerken van het slachtoffer kunnen bepalen of het slachtoffer voldoende kennis en vaardigheden heeft om een phishing-e-mail te detecteren (*sensitivity*) en of het slachtoffer geneigd is hier voorzichtig of onvoorzichtig mee om te gaan (*criterion*). Daarnaast bepalen activiteiten van het slachtoffer hoeveel e-mails of

berichten een slachtoffer op een dag te verwerken krijgt (ruis) en kunnen bepaalde activiteiten waarin slachtoffers hun e-mailadres achterlaten (zoals socialmediagebruik of ontvangst van veel nieuwsbrieven) ook het risico op het ontvangen van phishingberichten verhogen (signaal), omdat hierdoor contactgegevens van het slachtoffer beschikbaar zouden kunnen zijn voor fraudeurs. De kenmerken en het gedrag van het potentiële slachtoffer kunnen dus bepalen hoe groot het risico op slachtofferschap is. Eerder onderzoek heeft zich dan ook gericht op risicofactoren voor slachtofferschap van phishing.

Een aantal achtergrondkenmerken lijkt vooral indirect samen te hangen met slachtofferschap van phishing. Zo lopen jonge mensen en andere personen die veel online zijn een hoger risico (Alseadoon 2014; Sheng e.a. 2010). De hoeveelheid aan online activiteiten kan hierbij het aantal e-mails (ruis) en blootstelling aan phishing-mails (signaal) verhogen. Voor wat betreft geslacht zijn resultaten wat minder eenduidig. Onderzoek naar vatbaarheid voor phishing laat bijvoorbeeld zien dat vrouwen in een trainingssetting minder goed in staat zijn om phishing-mails te herkennen dan mannen (Alseadoon 2014; Sheng e.a. 2010), terwijl cijfers over daadwerkelijk slachtofferschap geen verband laten zien tussen geslacht en slachtofferschap (Leukfeldt 2014). Dit zou erop kunnen wijzen dat het totaal aantal ontvangen e-mails en/of de blootstelling aan phishing niet gelijk verdeeld zijn tussen mannen en vrouwen.

Naast kenmerken en activiteiten die met blootstelling te maken hebben, blijken mensen met meer IT-kennis en -ervaring of mensen die een phishingtraining hebben gevolgd een lager risico op slachtofferschap te hebben (o.a. Pattinson e.a. 2012; Sheng e.a. 2010; Wright & Marett 2010). Deze personen zijn vermoedelijk beter in staat om phishing-mails te herkennen (*sensitivity*). Verder zijn er nog kenmerken die van invloed zouden kunnen zijn op de voorzichtigheid (*criterion*) van potentiële slachtoffers, waarbij impulsiviteit, een lagere zelfcontrole en gelijksoortige persoonskenmerken het risico verhogen (Wright e.a. 2009; Pattinson e.a. 2012).

In het huidige onderzoek kan niet worden onderzocht of bovenstaande risicofactoren ook aanwezig zijn bij slachtoffers van betaalverzoekfraude. De gegevens gaan immers alleen over personen die slachtoffer zijn geworden en dat ook hebben gemeld bij de politie. Desalniettemin is het wel van belang om te kijken op welke manier de daders mogelijk inspelen op deze risicofactoren in hun MO.

## Methodie

### *Sampleselectie*

In de analyse zijn alle cybercrimeregistraties (meldingen en aangiftes) in het politiesysteem bekeken met als kennisnamedatum 20 juni tot en met 20 augustus 2019. In de periode voorafgaand aan deze periode werd in de praktijk steeds duidelijker dat dit fenomeen in opkomst was. Een eerdere beperkte analyse bood hierdoor niet meer voldoende inzicht. Daarnaast was er in deze periode meer capaciteit beschikbaar om het fenomeen grondig te analyseren, waardoor de analyse zich dus op deze periode heeft gericht. Deze cybercrimeregistraties zijn gefilterd uit het landelijke meldingensysteem van de politie: Basisvoorziening Handhaving (BVH). In BVH staan alle aangiftes en meldingen van overtredingen en misdrijven. Op de meldingen en aangiftes in de periode 20 juni tot en met 20 augustus 2019 is vervolgens een filtering toegepast door de breed gebruikte Cyber Query, een brede zoekvraag met een groot aantal zoektermen die kunnen duiden op een cybercrimeregistratie (wordt regelmatig bijgesteld naar aanleiding van nieuwe ontwikkelingen of inzichten).

Middels handmatige selectie zijn bovenstaande cybercrimeregistraties bekeken, waarbij de registraties die trefwoorden bevatten in relatie tot betaalverzoekfraude ('marktplaats', 'tikkie', '1 cent', 'betaalverzoek' en 'cent') zijn geselecteerd. Dit betrof uiteindelijk 16% van het totaal aantal cybercrimeregistraties in de geselecteerde periode. Hierbij zijn alle aangiftes die zijn opgenomen op een bureau meegeteld, maar niet de aangiftes gedaan via [www.politie.nl](http://www.politie.nl). Dit omdat online alleen aangifte gedaan kan worden van de 'tech support scam' en 'aan- of verkoopfraude'.<sup>3</sup> In het resterende sample van 777 meldingen en aangiftes bleek één sterk afwijkende MO aanwezig te zijn, die duidelijk door één dadergroep werd uitgevoerd. Alleen bij deze MO werd gebruik gemaakt van een QR-code.<sup>4</sup> Deze dadergroep was verantwoordelijk voor 49 (6%) van de meldingen en aangiftes. Om te voorkomen dat de resultaten te veel gekleurd zouden worden door de MO van slechts één dadergroep, is besloten om deze meldingen/aangiftes uit het sample te verwijderen. Het uiteindelijke sample betrof 728 meldin-

3 Zie [www.politie.nl/aangifte-of-melding-doen/aangifte-van-helpdeskfraude.html](http://www.politie.nl/aangifte-of-melding-doen/aangifte-van-helpdeskfraude.html).

4 Een QR-code is een vierkant dat bestaat uit vierkante blokjes en werkt als een streepjescode, na scannen wordt men naar een bepaalde internetpagina gestuurd.

gen of aangiftes van betaalverzoekfraude, waarvan het in 8% van de gevallen ging om een poging. De kennisnamedatum van 20 juni tot en met 20 augustus 2019 betekent niet dat het moment van (poging tot) slachtofferschap ook in deze periode valt. Mensen kunnen ook maanden na het moment van slachtofferschap erachter komen dat ze slachtoffer zijn geworden van betaalverzoekfraude en dan pas aangifte doen. Het later doen van aangifte (buiten de onderzochte periode) was in 1,3% van de onderzochte betaalverzoekfraudes het geval.

### *Scoring*

Van de 728 betaalverzoekfraudes zijn de volgende kenmerken uit het systeem gehaald: regionale eenheid waartoe de woonplaats van het slachtoffer behoort, datum kennisname, geslacht en geboortedatum van het slachtoffer. Daarnaast zijn de volgende variabelen gescoord die samenhangen met de drie onderzoeksgebieden (MO, overtuigings-technieken en slachtofferkenmerken), namelijk: of het een poging betreft (ja of nee), de benaderingswijze van de fraudeur (social engineering, drie mogelijkheden), gebruik van WhatsApp of Marktplaats-chat in de communicatie, het bedrag dat zogenaamd overgemaakt wordt op de phishing-site, de wijze waarop het slachtoffer achter de betaalverzoekfraude is gekomen (drie mogelijkheden), en of het slachtoffer contact heeft gehad met de bank (ja of nee). Om de interbeoordelaarsbetrouwbaarheid te controleren is uit deze 728 betaalverzoekfraudes een willekeurige steekproef getrokken van twintig aangiftes. Deze twintig aangiftes zijn door de beide onderzoekers onafhankelijk van elkaar gescoord op bovenstaande kenmerken en vervolgens vergeleken. Hierna is de scoringsmethodiek bijgesteld en uiteindelijk toegepast op alle 728 betaalverzoekfraudes.<sup>5</sup> Tijdens het scoren zijn ook opvallende overeenkomsten in de MO en voorbeelden genoteerd, om zo het proces goed te kunnen beschrijven.

De informatie die per melding of aangifte beschikbaar is, verschilt. Hierdoor was het niet voor elke betaalverzoekfraude mogelijk om alle scoringskenmerken in te vullen. De getoonde cijfers in de resultatenparagraaf zijn hiermee dus enkel gebaseerd op de cases waarin informatie over het betreffende scoringskenmerk aanwezig was. Kenmerken met relatief veel missings (meer dan 10%) waren: benade-

5 Waarvoor ook dank aan collega Paul Bastings.

ringswijze/gebruikt overtuigingsverhaal (29% missing) en hoogte van het bedrag dat zogenaamd overgemaakt wordt op de phishingwebsite (17% missing). Bij de interpretatie van de resultaten moet dus rekening worden gehouden met de mogelijkheid dat registraties van betaalverzoekfraudes waarin deze informatie ontbreekt, op deze punten afwijken van de registraties waarin deze informatie wel is opgenomen.

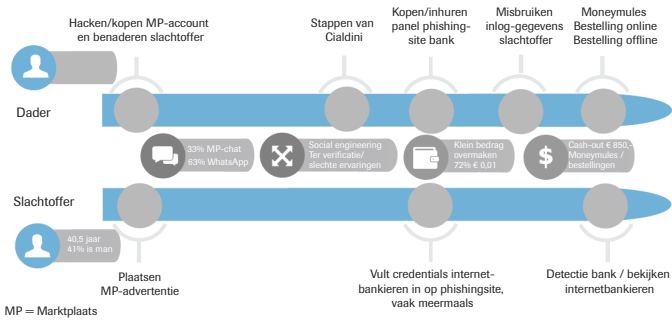
### *Analyse*

Een groot deel van de resultaten is beschrijvend van aard en is gebaseerd op prevalentie van de scoringskenmerken die hierboven zijn genoemd, aangevuld met de kwalitatieve informatie over de MO en voorbeelden uit de gebruikte aangiftes en meldingen. Waar mogelijk zijn gevonden verbanden tussen scoringskenmerken getoetst op statistische significantie, zoals verbanden tussen MO-kenmerken en het schadebedrag of slachtofferkenmerken en manieren van detectie. Afhankelijk van het type data zijn hier verschillende toetsen voor gebruikt, zoals t-toetsen en chikwadraattoetsen.

## **Resultaten**

### *Modus operandi*

De MO met daarin de acties van zowel de dader/dadergroep als het slachtoffer is visueel weergegeven in figuur 3. Bij de onderzochte betaalverzoekfraudes is iedere verkoper die een advertentie plaatst op Marktplaats.nl een potentieel slachtoffer. Vervolgens worden verkopers door een zogenaamd geïnteresseerde koper (hierna: fraudeur) met behulp van een gehackt Marktplaatsaccount benaderd via de Marktplaats-chat en/of via WhatsApp. Hierbij lijken advertenties voor producten die per post verstuurd kunnen worden (kleine pakketpost) en de minder populaire producten (bijvoorbeeld antiek, huishoudelijke producten en servies) vaak te worden benaderd. Fraudeurs lijken voor WhatsApp te kiezen wanneer het 06-nummer in de advertentie genoemd is, of als daarnaar gevraagd is via de chat. Uit de analyse blijkt dat 33% van de slachtoffers in de Marktplaats-chat is gebleven en 63% van hen (ook) contact heeft gehad via WhatsApp. Het is voor

**Figuur 3** Visuele weergave van MO betaalverzoekfraude

de fraudeur aantrekkelijk om te kiezen voor communicatie via WhatsApp, omdat detectie- en waarschuwsystemen van Marktplaats.nl daar niet werken. Uit de analyse blijkt een MO waarin WhatsApp gebruikt is effectiever; wanneer er schade is, is deze significant hoger dan wanneer er uitsluitend via de Marktplaats-chat is gecommuniceerd (gemiddelde schade € 636 versus € 868;  $t(621)=-1,97, p<,5$ ).

In het gesprek tussen fraudeur en slachtoffer in de Marktplaats-chat en/of WhatsApp vraagt de fraudeur vaak eerst of het goed nog te koop is. Indien het slachtoffer hierop positief reageert, vindt er een korte onderhandeling plaats, waarna er overeenstemming wordt bereikt over de verkoop (hierbij wordt vaak direct de vraagprijs geboden door de fraudeur). Nu er een deal is, stapt de fraudeur over op het overtuigen van het slachtoffer om op een niet-legitiem betaalverzoeklinkje te klikken (figuur 1). Uit de analyse blijkt dat de meest voorkomende methode (56%) van social engineering is om het slachtoffer te vragen een klein bedrag over te maken ter verificatie van het beheer van de desbetreffende rekening (zoals ook gebruikelijk bij diverse andere online betalingen). Een tweede methode ligt in het verlengde, hierbij wordt specifiek gevraagd om een verificatie voor extra zekerheid na het benoemen van eerdere slechte ervaringen met bijvoorbeeld oplichting (36%). Een voorbeeld hiervan: 'Kan ik je een verificatie sturen? Sorry voor mijn wantrouwen; heb een paar keer incidenten ervaren op Marktplaats waar ik niet zo blij van word?' Daarnaast komen ook het overmaken van de verzendkosten (4%) en een soort garantie voor het daadwerkelijk kopen van het product voor (1%). In veel gevallen worden de overtuigingstechnieken ook door elkaar gebruikt

**Figuur 4** Voorbeelden van gateway-URL's van illegitieme en legitieme betaalverzoeken

❏ <a href="https://betaalverzoek.rabobank.nl/betaalverzoek?id=❏">https://betaalverzoek.rabobank.nl/betaalverzoek?id=❏</a>	<a href="https://rabobank.overboeking.online">https://rabobank.overboeking.online</a> ❏
❏ <a href="https://tikkie.me/pay/">https://tikkie.me/pay/</a> ❏	<a href="https://betaalverzoek-tikkie.nl/">https://betaalverzoek-tikkie.nl/</a> ❏
❏ Legitiem❏	Illegitiem❏

om de kans groter te maken dat het slachtoffer op het niet-legitieme betaalverzoekje klikt.

De fraudeur vraagt het slachtoffer omwille van bovenstaande genoemde redenen een bedrag over te maken en stuurt het slachtoffer daartoe een niet-legitieme link met een betaalverzoek (zie voor voorbeelden figuur 4). In 88% van de gevallen gaat het om een bedrag tussen 0 en 10 cent, waarbij 1 cent het vaakst voorkomt (72%). Indien deze link verstuurd wordt binnen de omgeving van de Marktplaatschat gaat dit door middel van een 'gatewaylink', ofwel een forwarder naar een phishing-site (zie voor een voorbeeld figuur 5). Indien het contact is verlopen via WhatsApp wordt er een URL (linkje) gestuurd die lijkt op een legitiem betaalverzoek, inclusief bijbehorende logo's en tekstuele stijl (zie figuur 1).

Door te klikken op de door de fraudeur verstuurd niet-legitieme betaalverzoekenlink om het bedrag over te maken, komt het slachtoffer op een phishingwebsite. Deze phishing-site heeft de 'look and feel' van een legitiem betaalverzoek. Hier kan het slachtoffer zijn of haar bank selecteren, waarmee bijvoorbeeld de betaling van € 0,01 moet worden doorgevoerd. Hierna wordt het slachtoffer verder geleid naar de phishing-site met de 'betaalomgeving van de gekozen bank'. Ook dit is echter weer een phishing-site in de 'look and feel'-opmaak van betreffende bank en staat wederom onder controle van de fraudeur. De valse websites doen zich bijna uitsluitend voor als de grootste banken van Nederland (ING, ABN AMRO en Rabobank), wat logisch is gezien het marktaandeel van deze banken.

Op deze internetbankieren-phishing-site worden vervolgens gegevens gevraagd zoals gebruikersnaam, wachtwoord en betaalpasgegevens, om zogenaamd in te kunnen loggen op de internetbankierenomgeving ter afronding van de betaling. Op deze wijze en in de daaropvolgende handelingen worden door de fraudeur eveneens authenticatie- en verificatiecodes afgevangen in zijn 'panel'. De fraudeur ziet alle

## Figuur 5 Voorbeeld van een Marktplaats-gateway-URL + bijbehorende waarschuwing

`marktplaats.nl/gateway.html?url=http%3A%2F%2Fwww.tikkie.nl-pay`

### Je gaat de Marktplaats-omgeving verlaten

Sta je op het punt om een betaling uit te voeren? Weet dat Betaalverzoeken met iDEAL via Marktplaats NOOIT via externe links verlopen. Marktplaats stuurt je automatisch door naar internetbankieren. Weet je zeker dat je de Marktplaats-omgeving wilt verlaten? De link verwijst naar de volgende externe website: <http://www.tikkie.nl-pay>

informatie die het slachtoffer invoert op de phishing-site daar binnenkomen. De phishing-site geeft door de fraudeur gestuurde foutmeldingen weer, zodat slachtoffers meermaals inloggegevens invoeren en inlogcodes genereren. Met deze afgevangen gegevens wordt door de fraudeur ingelogd op het internetbankierenaccount van het slachtoffer en worden bijvoorbeeld telefoons of tablets die in het bezit zijn van de fraudeur gekoppeld aan de bankrekening van het slachtoffer. Zonder medeweten van het slachtoffer heeft de fraudeur nu toegang tot de bankrekening en kunnen transacties worden doorgevoerd.

De laatste stap is vervolgens het wegsluizen van het geld dat op de rekeningen staat waartoe de fraudeur nu toegang heeft (de cash-out). Op basis van het verhaal van het slachtoffer in de aangifte is niet altijd te achterhalen hoe dit wegsluizen precies gebeurt, maar in 77% van de gevallen wel. Cash-out gebeurt vaak middels overboekingen naar *moneymules*,<sup>6</sup> het plaatsen van online bestellingen (tegoedkaarten, cryptocurrency of bestellingen bij webshops) of betalingen in fysieke winkels (vanaf de telefoon, via de Apple Pay-betaalmethode).

Vervolgens zal de fraudeur (indien er via WhatsApp contact is geweest) vaak de berichten wissen, zodat het slachtoffer bijvoorbeeld het telefoonnummer of de verstuurd phishing-URL niet meer kan opzoeken. Wanneer het delict voltooid is, komen de slachtoffers er in de meeste gevallen achter doordat ze zelf een 'niet-pluisgevoel' krijgen en zelf hun eigen internetbankieren raadplegen (67%). Er zijn echter ook slachtoffers bij wie de bank de fraude detecteert en contact met hen opneemt (31%). Enkele slachtoffers merken dat er geld is weggesluisd van hun rekening omdat ze niet meer kunnen pinnen (2%). Vrijwel alle slachtoffers geven bij het doen van aangifte aan al contact te hebben gehad met hun bank (89%). Zij werden vaak doorverwezen naar de

6 Het gaat hier om zogenaamde katvangers, die hun bankrekening (laten) gebruiken ten behoeve van het laten storten en opnemen van via misdaad verkregen geld.

politie om ook aangifte of melding te doen, om in aanmerking te komen voor een schadevergoeding. Uiteindelijk zal mede om de schadevergoeding vrijwel ieder slachtoffer van betaalverzoekfraude contact hebben met de bank.

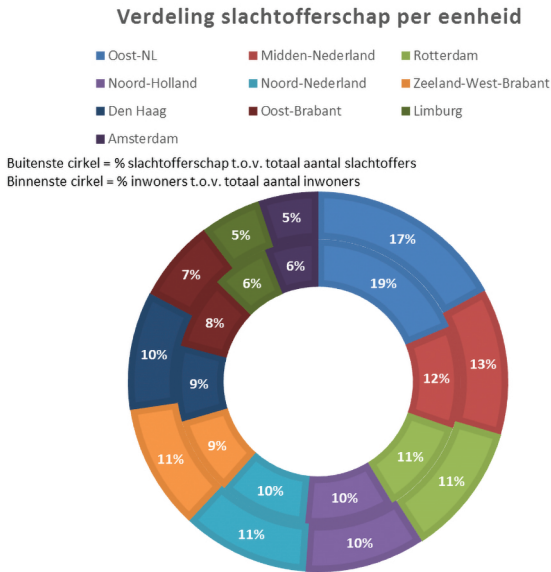
### *Slachtofferkenmerken*

Zoals gezegd kan dit onderzoek voornamelijk inzicht bieden in het verloop van betaalverzoekfraudes en de rol van het slachtoffer, de dader en diens overtuigingstechnieken in deze MO. Desalniettemin is het wel relevant om te weten welke kenmerken van slachtoffers uit de onderzochte aangiftes en meldingen naar voren komen. Allereerst valt op te merken dat het slachtofferschap geografisch gezien gelijk verdeeld is over de politie-eenheden, hoe meer inwoners per eenheid, hoe meer slachtoffers (zie figuur 6). Verder is 41% van de slachtoffers man en de leeftijd varieert sterk van 14 tot 81 jaar, met een gemiddelde van 40,5 jaar (SD=15,73). Leeftijd en geslacht van het slachtoffer blijken niet significant samen te hangen met de bovengenoemde verschillende MO-kenmerken. Een belangrijke bevinding is wel dat slachtoffers die er zelf achter komen dat ze slachtoffer zijn doordat ze zelf hun bankrekening controleren, gemiddeld iets jonger zijn dan slachtoffers bij wie de bank contact met hen opneemt (gemiddelde leeftijd 39,56 jaar versus 43,13 jaar;  $t(677)=-2,76, p<.01$ ).

Als laatste is onderzocht wat het schadebedrag is van de onderzochte betaalverzoekfraudes. Het schadebedrag varieerde van 1 cent tot € 50.000,<sup>7</sup> met een gemiddelde van € 850 per geslaagde betaalverzoekfraude. Hierbij moet worden opgemerkt dat enkele zeer hoge schadebedragen dit beeld vertekenen, de mediaan bij de geslaagde betaalverzoekfraudes bedraagt € 223. Zie figuur 7 voor een overzicht van schadecategorieën. Buiten de materiële schade wordt ook veelvuldig gerefereerd aan immateriële schade, zoals dat het vertrouwen in online bankieren of handelen is beschadigd en dat mensen emotionele impact ondervinden. Dit werd bijvoorbeeld als volgt verwoord door slachtoffers: 'Ik heb mij een hele week rot gevoeld, ik was er naar van en totaal ontdaan', of 'Dat iemand volledig mijn internetbankieren kan overnemen, maakt mij erg boos, verdrietig en onzeker.'

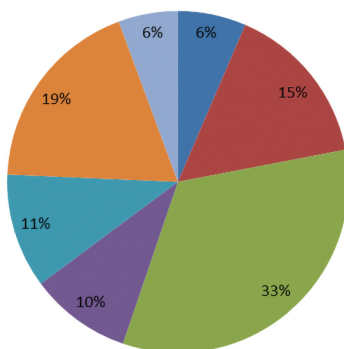
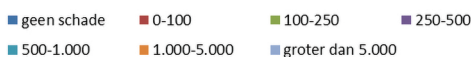
7 De schade van € 50.000 was een uitzondering, analyses met schadebedragen zijn daarom zonder deze outlier uitgevoerd. Het hoogste schadebedrag is dan € 13.110.

**Figuur 6 (Relatieve) verdeling van slachtofferschap per regionale politie-eenheid**



## Conclusie

In dit onderzoek is met behulp van een analyse van 728 meldingen en aangiftes getracht om (1) de MO, (2) overtuigingstechnieken en (3) slachtofferkenmerken van betaalverzoekfraude in kaart te brengen. Deze vorm van spearfishing betreft een aanzienlijk deel van alle bij de politie gemelde gevallen van cybercrime (in de onderzochte periode 16%). De MO laat duidelijk zien dat daders vissen met een nieuwe hengel. In de MO van betaalverzoekfraude is er overgestapt van traditionele e-mails naar nieuwe digitale platforms en communicatiemiddelen om criminele activiteiten te ontplooiën (Grabosky 2017). Daders proberen het slachtoffer te bewegen tot klikken op een phishinglink, waarbij wordt geprobeerd de technische preventiemaatregelen van bijvoorbeeld Marktplaats.nl te omzeilen door over te stappen naar het minder gecontroleerde WhatsApp.

**Figuur 7** Schadecategorieën (in €)

Deze nieuwe MO (deelvraag 1) is goed te begrijpen in het licht van de signal detection theory (o.a. Sheng e.a. 2007). De nieuwe omgeving waar het delict plaatsvindt, zorgt er mogelijk voor dat slachtoffers minder op hun hoede zijn (*criterion*) en wellicht ook minder goed in staat zijn om phishing te herkennen dan wanneer zij e-mails ontvangen (*sensitivity*). Het gaat bij betaalverzoekfraude duidelijk om spearphishing (Gupta e.a. 2018), waarbij de communicatie is aangepast aan de specifieke advertentie van het beoogde slachtoffer. De spearphishing richt zich op de *sensitivity* door berichten erg te laten lijken op legitieme reacties op de advertentie. Zo worden er gesprekken gevoerd over bijvoorbeeld de vraag of het product nog steeds beschikbaar is en wordt er onderhandeld. Daarnaast proberen daders het *criterion* te beïnvloeden door vooral te reageren op relatief onpopulaire producten, waar ze vaak de vraagprijs voor bieden. Hiermee hopen ze dat het slachtoffer eerder bereid is om een risico te nemen. Ook spelen ze op deze manier in op risicofactoren voor slachtofferschap die in eerder onderzoek zijn gevonden, zoals impulsiviteit of lage zelfcontrole van het slachtoffer (o.a. Wright e.a. 2009). Al met al zorgt dit ervoor dat er waarschijnlijk relatief veel valsnegatieven zijn, potentiële slachtoffers zullen relatief makkelijk in deze vorm van phishing trappen.

In de MO komen veelal twee overtuigingstechnieken naar voren (deelvraag 2). Ten eerste proberen daders het slachtoffer er voornamelijk van te overtuigen een klein bedrag over te maken. Bij veel legitieme diensten is dit gebruikelijk en wordt op deze manier geverifieerd of de betreffende persoon ook daadwerkelijk toegang heeft tot het opgegeven bankaccount. Ten tweede geven daders in dit verhaal aan dat zij eerder slechte ervaringen hebben gehad en daarom meer zekerheid vragen. Deze verhalen in combinatie met andere onderdelen van de MO sluiten aan bij vijf van de zes overtuigingsprincipes van Cialdini (2009); enkel autoriteit is minder duidelijk terug te vinden in deze MO (fraudeurs doen zich juist niet voor als de bank, maar als een andere Marktplaatsgebruiker). Ten eerste sympathie, de dader spreekt op een vriendelijke toon met het slachtoffer en door de suggestie te wekken dat hij zelf eerder opgelicht is, zal het slachtoffer sneller behulpzaam willen zijn. Hier hangt de conformiteit mee samen. Mensen zijn van nature geneigd om anderen te helpen en zijn in dit geval ook nog uit vergelijkbare situaties gewend aan het overmaken van bijvoorbeeld 1 cent ter verificatie. Vervolgens spelen de daders met het bieden van de vraagprijs (of in ieder geval een goede prijs) op onpopulaire producten in op het principe van schaarste. Slachtoffers zijn dan sneller geneigd om erin mee te gaan als er geen andere goede kopers beschikbaar zijn. Ook consistentie zorgt ervoor dat slachtoffers in de phishing worden meegezogen. Zodra ze ingaan op het verhaal en op de phishinglink klikken, is de eerste stap genomen en zijn ze sneller geneigd om ook de vervolgstappen te nemen en bijvoorbeeld zelfs meerdere keren hun inloggegevens in te voeren wanneer de phishing-site niet goed lijkt te werken. Als laatste speelt wederkerigheid een belangrijke rol. De dader is bereid het product te kopen en vraagt hier slechts een heel kleine tegenprestatie voor (meestal het overmaken van slechts 1 cent).

Hoewel de nieuwe MO en de gebruikte overtuigingstechnieken er wellicht voor hebben gezorgd dat dit delict in korte tijd zo sterk is toegenomen, zal niet iedere Nederlandse burger in dezelfde mate risico lopen op slachtofferschap van betaalverzoekfraude (deelvraag 3). De mate waarin slachtoffers vatbaar zijn voor de overtuigingstechnieken van de dader is een belangrijk onderdeel van het succes van deze MO. De mens is dus ook hier de zwakste schakel (Canfield e.a. 2016). Zoals gezegd kunnen op basis van de aangiftes echter geen sterke uitspraken worden gedaan over risicofactoren, aangezien deze geen beeld geven

van de totale populatie. Op basis van de relatief gelijke verdeling over politieregio's lijkt dit delict in ieder geval door heel Nederland voor te komen (als je maar op Marktplaats.nl actief bent). Of vrouwen daadwerkelijk vaker slachtoffer zijn van dit delict is onbekend. Desalniettemin ligt het, zoals hierboven aangegeven en ook in lijn met eerder onderzoek naar phishing (o.a. Alseadoon 2014; Sheng e.a. 2010), in ieder geval voor de hand dat veelvuldig gebruik van online platforms waar betaalverzoeken onderdeel zijn van de normale communicatie kan zorgen voor een hogere blootstelling aan dergelijke phishing-pogingen. Daar komt bij dat het vermelden van bijvoorbeeld een telefoonnummer in de advertentie of het hiernaar vragen in de Marktplaats-chat een doelwit aantrekkelijk kan maken, omdat de communicatie dan via WhatsApp kan verlopen. Hierdoor is er minder toezicht (zoals dit wel is op de Marktplaats-chat) en blijkt de schade ook significant hoger te zijn. Naast eerdergenoemde impulsiviteit is verder uit eerder onderzoek gebleken dat personen met meer kennis door bijvoorbeeld ervaring of training een lager risico hebben op phishing-slachtofferschap (o.a. Pattinson e.a. 2012). Hoewel het huidige onderzoek geen informatie heeft over dergelijke kennis bij slachtoffers, blijkt dat de iets jongere slachtoffers (die wellicht meer kennis hebben op dit gebied) eerder onraad ruiken en zelf ontdekken dat ze slachtoffer zijn geworden. Hoewel deze iets jongere generatie dus wellicht vaker gebruik maakt van nieuwe online platforms, zijn zij wellicht ook beter in staat om de schade te beperken door eerdere detectie.

## **Discussie**

Het volgen en inzetten van hedendaagse technologische ontwikkelingen voor het ontplooiën van criminele activiteiten zorgt ervoor dat daders, bewijsmateriaal en opbrengsten ongrijpbaarder zijn dan bij traditionele criminaliteit. De onderzochte 728 aangiftes van betaalverzoekfraudes en bijbehorende resultaten zijn uiteraard niet gevrijwaard van methodologische beperkingen. Enerzijds kennen politieregistraties beperkingen op het gebied van validiteit en betrouwbaarheid, waardoor ze niet altijd een goed beeld vormen van de werkelijkheid. Denk hierbij aan de invloed van de aangiftebereidheid (in dit geval wellicht lager omdat de onderzoeksperiode in de

vakantieperiode viel), waardoor er selectiviteit is (alleen slachtoffers met een hoog schadebedrag die schade vergoed willen van de bank doen mogelijk aangifte). Ook de kwaliteit van de opname van de aangifte, beïnvloed door zowel politiemensen bij Intake en Service als de kennis van het slachtoffer, kan zorgen voor een vertekening van de werkelijkheid (Hesseling & Versteegh 2016). Anderzijds kent het gebruik van politieregistraties voordelen, ze kunnen inzicht geven in zowel de gehanteerde MO door de dader als slachtofferkenmerken van een nieuw fenomeen, vaak een noodzakelijke eerste stap. Het kan enige tijd duren voordat een nieuwe benaderingswijze meegenomen wordt in bijvoorbeeld slachtofferenquêtes. Bovendien bevatten politieregistraties hele rijke data en door de grote hoeveelheid aan registraties is de diversiteit aan stappen in de MO goed in kaart te brengen. Dit onderzoek laat dan ook zien dat er naast de verschijningsvormen van phishing die in de wetenschappelijke literatuur naar voren komen, ook nieuwe vormen zijn. De literatuur loopt daarmee enigszins achter op de snelheid van de digitale ontwikkelingen. Vervolgonderzoek kan zich enerzijds richten op het in kaart brengen van andere nieuwe vormen of benaderingswijzen binnen cybercrime. Door ook in de wetenschappelijke literatuur aan te sluiten bij nieuwe fenomenen en werkwijzen kan beschrijvende kennis hierover vervolgens gebruikt worden in meer verklarend en toetsend onderzoek. Anderzijds is het voor betaalverzoekfraude ook noodzakelijk om nog verder diepgaand onderzoek te doen naar slachtofferkenmerken en de manieren waarop slachtoffers weerbaar gemaakt kunnen worden tegen deze fraudeurs. Juist nu het slachtofferschap ontstaat door benadering op nieuwe platforms, is het erg belangrijk om bijvoorbeeld via slachtofferenquêtes of diepte-interviews meer inzicht te krijgen in de mechanismen die het risico op slachtofferschap verhogen. Hieruit zal dan ook blijken in hoeverre de bestaande literatuur over slachtofferkenmerken van phishing voldoende inzicht biedt in nieuwe vormen van slachtofferschap.

Buiten de mogelijkheden die er zijn bij de opsporing en verdergaande inzichten vergaren in dit fenomeen, waarbij vooral aandacht besteed dient te worden aan landelijke clustering en gestructureerde opname van aangiftes (bijvoorbeeld digitaal), is er vooral veel winst te behalen in de preventie en verstoring van deze vorm van cybercrime. Wanneer men de MO van betaalverzoekfraude uitgewerkt ziet in figuur 3, doen wij een aantal praktische aanbevelingen. Ten eerste zou de monitoring

van geregistreerde domeinnamen gelijkend op bestaande betaalverzoekdomeinen en het plegen van interventies hierop een vroegtijdige barrière kunnen zijn. Ten tweede zouden banken, Marktplaats.nl, internetbrowsers en andere relevante partijen nog meer aandacht kunnen besteden aan het inbouwen van extra controlemechanismen. Denk hierbij aan waarschuwingen, tijdig offline halen van illegitieme websites en het blijven verfijnen van de signaleringen bij afwijkingen in het betalingsverkeer. Ook onderlinge afstemming en informatie-uitwisseling over phishing en betaalverzoekfraude in het bijzonder zijn van groot belang. Ten derde blijft het vergroten van digitale *awareness* in de gedigitaliseerde samenleving een belangrijk aandachtspunt. Hierbij moet niet alleen worden gefocust op bijvoorbeeld ‘traditionele’ vormen van phishing, maar juist ook alertheid worden gecreëerd op phishing op nieuwe wijze en in nieuwe omgevingen.

## Literatuur

### **Aiken e.a. 2015**

M. Aiken, C. McMahon, C. Haughton, L. O’Neill e.a., ‘A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online’, *Contemporary Social Science* (11) 2015, afl. 4, p. 373-391.

### **Albladi & Weir 2016**

S. Albladi & G.R. Weir, ‘Vulnerability to social engineering in social networks: A proposed user-centric framework’, in: B. Cartwright, G. Weir & L. Yiu-Chung Lau (red.), *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver: IEEE 2016, p. 1-6.

### **Alseadoon 2014**

I.M.A. Alseadoon, *The impact of users’ characteristics on their ability to detect phishing emails*, Brisbane: Queensland University of Technology 2014.

### **Boekhoorn 2020**

P. Boekhoorn, *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging*, Den Haag: Sdu Uitgevers/Politie en Wetenschap/BBSO 2020.

**Bullée e.a. 2018**

J.W.H. Bullée, L. Montoya, W. Pieters, M. Junger e.a., 'On the anatomy of social engineering attacks – A literature-based dissection of successful attacks', *Journal of Investigative Psychology and Offender Profiling* (15) 2018, afl. 1, p. 20-45.

**Canfield e.a. 2016**

C.I. Canfield, B. Fischhoff & A. Davis, 'Quantifying phishing susceptibility for detection and behavior decisions', *Human Factors* (58) 2016, afl. 8, p. 1158-1172.

**Cialdini 2009**

R.B. Cialdini, *Influence: Science and practice*, Harlow: Pearson 2009.

**De Kimpe e.a. 2018**

L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels e.a., 'You've got mail! Explaining individual differences in becoming a phishing target', *Telematics and Informatics* (35) 2018, afl. 5, p. 1277-1287.

**Grabosky 2017**

P.N. Grabosky, 'The evolution of cybercrime, 2006-2016', in: T.J. Holt (red.), *Cybercrime through an interdisciplinary lens*, New York: Routledge 2017, p. 15-36.

**Green & Swets 1966**

D.M. Green & J.A. Swets, *Signal detection theory and psychophysics*, New York: Wiley 1966.

**Gupta e.a. 2018**

B.B. Gupta, N.A.G. Arachchilage & K.E. Psanis, 'Defending against phishing attacks: Taxonomy of methods, current issues and future directions', *Telecommunication Systems* (67) 2018, afl. 2, p. 247-267.

**Hesseling & Versteegh 2016**

R. Hesseling & P. Versteegh, 'Politiecijfers: meten is weten, maar doe vooral ook meer met ongeveer', *Cahiers Politiestudies* (41) 2016, afl. 7, p. 25-43.

**Van 't Hoff-de Goede e.a. 2019**

S. van 't Hoff-de Goede, R. van der Kleij, S. van de Weijer & R. Leukfeldt, *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*, Den Haag: WODC, Ministerie van Justitie en Veiligheid 2019.

**Jansen & Van Schaik 2018**

J. Jansen & P. van Schaik, 'Persuading end users to act cautiously online: A fear appeals study on phishing', *Information & Computer Security* (26) 2018, afl. 3, p. 264-276.

**Jansen e.a. 2019**

J. Jansen, S. Westers, S. Twickler & W. Stol, *Aankoopfraude vanuit het buitenland. Alternatieven voor opsporing*, Den Haag: Sdu Uitgevers/Politie en Wetenschap/NHL Stenden Hogeschool 2019.

**Jensen e.a. 2017**

M.L. Jensen, M. Dinger, R.T. Wright & J.B. Thatcher, 'Training to mitigate phishing attacks using mindfulness techniques', *Journal of Management Information Systems* (34) 2017, afl. 2, p. 597-626.

**Kumaraguru e.a. 2009**

P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor e.a., 'School of phish: A real-world evaluation of anti-phishing training', in: L. Faith Cranor (red.), *Proceedings of the 5th Symposium on Usable Privacy and Security*, New York: Association for Computing Machinery 2009, p. 1-12.

**Lawson e.a. 2020**

P. Lawson, C.J. Pearson, A. Crowson & C.B. Mayhorn, 'Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy', *Applied Ergonomics* (86) 2020, p. 1-10.

**Leukfeldt 2014**

E.R. Leukfeldt, 'Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization', *Cyberpsychology, Behavior, and Social Networking* (17) 2014, afl. 8, p. 551-555.

**Mouton e.a. 2016**

F. Mouton, L. Leenen & H.S. Venter, 'Social engineering attack examples, templates and scenarios', *Computers & Security* (59) 2016, afl. 3, p. 186-209.

**Pattinson e.a. 2012**

M. Pattinson, C. Jerram, K. Parsons, A. McCormac e.a., 'Why do some people manage phishing e-mails better than others?', *Information Security Management & Computer Security* (20) 2012, afl. 1, p. 18-28.

**Reep-van den Bergh & Junger 2018**

C.M.M. Reep-van den Bergh & M. Junger, 'Victims of cybercrime in Europe: A review of victim surveys', *Crime Science* (7) 2018, afl. 5, p. 1-15.

**Rokven e.a. 2017**

J.J. Rokven, G. Weijters & A.M. van der Laan, *Jeugddelinquentie in de virtuele wereld. Een nieuwe type daders of nieuwe mogelijkheden voor traditionele daders?*, Den Haag: WODC 2017.

**Sheng e.a. 2007**

S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti e.a., 'Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish', in: L. Faith Cranor (red.), *Proceedings of the 3rd Symposium on Usable Privacy and Security*, New York: Association for Computing Machinery 2007, p. 88-99.

**Sheng e.a. 2010**

S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor e.a., 'Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions', in: E. Mynatt (red.), *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York: Association for Computing Machinery 2010, p. 373-382.

**Thomlison 2001**

B. Thomlison, 'Descriptive studies', in: B. Thyer (red.), *The handbook of social work research methods*, Thousand Oaks, CA: Sage 2001, p. 131-141.

**Uebelacker & Quiel 2014**

S. Uebelacker & S. Quiel, 'The social engineering personality framework', in: G. Bella & G. Lenzi (red.), *2014 Workshop on socio-technical aspects in security and trust*, IEEE 2014, p. 24-30.

**Uehara e.a. 2020**

K. Uehara, H. Nishikawa, T. Yamamoto, K. Kawachi e.a., 'Analysis of the relationship between psychological manipulation techniques and personality factors in targeted emails', in: L. Barolli, P. Hellinckx & T. Enokido (red.), *Advances on broadband wireless computing, communication and applications*, Cham: Springer 2020, p. 338-351.

**Van Wegberg e.a. 2018**

R. van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi e.a., 'Plug and prey? Measuring the commoditization of cybercrime via online anonymous markets', in: *Proceedings of the 27th USENIX Security Symposium*, Baltimore: USENIX 2018, p. 1009-1026.

**Wright & Marett 2010**

R.T. Wright & K. Marett, 'The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived', *Journal of Management Information Systems* (27) 2010, afl. 1, p. 273-303.

**Wright e.a. 2009**

R.T. Wright, S. Chakraborty, A. Basoglu & K. Marett, 'Where did they go right? Understanding the deception in phishing communications', *Group Decision and Negotiation* (19) 2009, afl. 4, p. 391-416.

**Wright e.a. 2014**

R.T. Wright, M.L. Jensen, J.B. Thatcher, M. Dinger e.a., 'Research note – Influence techniques in phishing attacks: An examination of vulnerability and resistance', *Information Systems Research* (25) 2014, afl. 2, p. 385-400.