WODC

2 | 20

Justitiële verkenningen

Nieuwe vormen van oplichting en fraude

verschijnt 6 maal per jaar • jaargang 46 • juli

JV

Boom juridisch | Ook digitaal via tijdschriften.boomjuridisch.nl

2 | 20

Justitiële verkenningen

Nieuwe vormen van oplichting en fraude

Verschijnt 6 maal per jaar • jaargang 46 • juli

Boomjuridisch

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie en Veiligheid

Justitiële verkenningen is een gezamenlijke uitgave van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie en Veiligheid en Boom juridisch.

Redactiesecretariaat
tel. 088 371 74 12
e-mail infojv@wodc.nl

Redactieadres
Ministerie van Justitie en Veiligheid, WODC
Redactie Justitiële verkenningen
Postbus 20301
2500 EH Den Haag

WODC-documentatie
Voor inlichtingen: Infodesk WODC, e-mail: wodc-informatiedesk@wodc.nl, internet: www.wodc.nl

Abonnementen
Justitiële verkenningen verschijnt zes keer per jaar. In digitale vorm is het tijdschrift beschikbaar op de website van het WODC, zie www.wodc.nl/publicaties/justitiele-verkenningen/index.aspx.
De abonnementsprijs bedraagt in 2020 € 164,00 (excl. btw) voor een online abonnement en € 219,00 (excl. btw, incl. verzendkosten) voor papier & online. Met een online abonnement heeft u toegang tot het volledige online archief en ontvangt u een e-mailattendering. Met papier & online ontvangt u tevens de gedrukte exemplaren.

Abonnementen kunnen op elk gewenst tijdstip ingaan en worden stilzwijgend verlengd, tenzij het abonnement schriftelijk wordt opgezegd. Na afloop van het eerste abonnementsjaar dient u rekening te houden met een opzegtermijn van één maand. Kijk op www.tijdschriften.boomjuridisch.nl voor meer informatie.

Wilt u een abonnement afsluiten of heeft u vragen? Neem dan contact op via klantenservice@boomdenhaag.nl of via telefoonnummer 070-330 70 33.

Uitgever
Boom juridisch
Postbus 85576
2508 CG Den Haag
tel. 070-330 70 33
e-mail info@boomjuridisch.nl
website www.boomjuridisch.nl

Ontwerp
Tappan, Den Haag

Coverfoto
© Hollandse Hoogte

ISSN: 0167-5850

Inhoud

Inleiding

Oplichting en fraude zijn niet nieuw, maar daders gaan wel met hun tijd mee. Veel vormen van oplichting en fraude hebben zich bijvoorbeeld verplaatst naar het internet, waarbij daders hun methoden moesten aanpassen aan het digitale domein. Inmiddels is dit type criminaliteit wijdverspreid. Uit het door het CBS uitgevoerde onderzoek Digitale Veiligheid en Criminaliteit (2019) blijkt dat in 2018 in totaal 1,2 miljoen mensen slachtoffer werden van digitale criminaliteit. Ook andere maatschappelijke ontwikkelingen zorgen voor een nog sterkere toename of veranderingen in dergelijke criminaliteitsvormen. De huidige coronacrisis zorgt bijvoorbeeld voor een nog sterkere toename van oplichting via het internet, zoals gesignaleerd door Theo van der Plas (programmadirecteur Digitalisering en Cybercrime van de Nationale Politie) en Wil van Gemert (Europol).[1] In dit themanummer van *Justitiële verkenningen* belichten we nieuwe vormen van oplichting en fraude die zich vooral (maar niet uitsluitend) manifesteren in communicatie via internet, e-mail en digitale applicaties zoals betaalapps. We richten het vizier op de daders en hun slachtoffers. Welke methoden hanteren daders, en hoe kunnen zij succesvol zijn via nieuwe kanalen? Welke schade wordt aangericht en hoe gaan slachtoffers met die schade om? Hoe kunnen burgers weerbaarder worden gemaakt tegen deze nieuwe criminaliteitsvormen? De langere artikelen worden in dit themanummer afgewisseld met korte kaderteksten waarin een specifieke nieuwe vorm van oplichting of een aspect van de aanpak daarvan centraal staat.

We beginnen met een artikel dat inhaakt op de actualiteit van de coronacrisis, geschreven door ***Clarissa Meerts en Wim Huisman***. Met concrete voorbeelden van 'coronacriminaliteit' laten zij zien hoe de huidige crisis leidt tot nieuwe gelegenheden voor het plegen van misdrijven. De auteurs grijpen daarbij terug op een analysekader dat eerder werd ingezet om nieuwe vormen van criminaliteit tijdens de bankencrisis te duiden.

Joke Rooyakkers en Marleen Weulen Kranenbarg doen verslag van hun onderzoek naar de steeds vaker voorkomende betaalverzoek-

1 Zie het tv-programma *EenVandaag*: https://eenvandaag.avrotros.nl/item/opvallende-stijging-aangiftes-van-online-fraude-tijdens-coronacrisis-vooral-kwetsbaren-en-ouderen/ en https://eenvandaag.avrotros.nl/item/criminele-economie-profiteert-van-coronacrisis-flinke-toename-van-cybercrime/.

doi: 10.5553/JV/016758502020046002001

fraude. Zij schetsen een beeld van deze nieuwe vorm van phishing en proberen het succes ervan te verklaren door onder andere te kijken naar de overtuigingstechnieken van daders en naar de kenmerken van slachtoffers.

Robby Roks en Nahom Monshouwer verrichtten een zogeheten netnografisch onderzoek naar fraude en oplichting op het platform Telegram Messenger. In dit artikel presenteren zij daarvan de resultaten. Net als cryptomarkten en online forums lijkt Telegram te functioneren als een criminele markt. Er worden specifieke goederen en diensten aangeboden ten behoeve van het plegen van phishing. Bovendien bevat de informatie op Telegram specifieke manieren van werken met uitgebreide en stapsgewijze handleidingen om bepaalde financiële cybercriminaliteit met succes af te ronden.

Vervolgens schetst ***Jildau Borwell*** in een kort artikel een beeld van helpdeskfraude in Nederland en actuele ontwikkelingen daarbinnen.

Raoul Notté gaat in op een heel andere en relatief nieuwe vorm van oplichting, namelijk datingfraude, en de enorme impact daarvan op slachtoffers. De schade is niet alleen financieel van aard, maar omvat ook vaak psychische problemen en verstoorde relaties met familieleden en vrienden.

De bijdrage van ***Johan van Wilsem, Take Sipma en Esther Meijer-van Leijsen*** heeft als centrale vraag welk type slachtoffer van identiteitsfraude actie onderneemt om het gestolen bedrag vergoed te krijgen en of slachtoffers daarin slagen. Criminologische theorieën leveren hiervoor aanvullende inzichten.

In de daaropvolgende kadertekst constateert ***Dieke Miltenburg*** dat het verre van eenvoudig is om na te gaan of trainingen in het herkennen van phishingmails effectief zijn. De respondenten zijn zich er namelijk van bewust dat ze aan een test meewerken, waardoor zij wellicht ander gedrag vertonen dan in werkelijkheid. Zij doet vervolgens verslag van een onderzoek waarbij de respondenten niet weten dat ze deelnemen aan een phishingtest, maar denken dat het een ander type test betreft.

Jan-Willem Bullée en Marianne Junger richten zich in hun artikel op het fenomeen *social engineering*, een verzamelterm voor misleiding, bedrog en andere overtuigingstechnieken als een online aanvalstactiek om slachtoffers gevoelige informatie te laten delen of kwaadwillige acties uit te laten voeren met als uiteindelijk doel het slachtoffer geld afhandig te maken. De auteurs doen verslag van hun systema-

doi: 10.5553/JV/016758502020046002001

tisch vergelijkend onderzoek naar de effectiviteit van interventies die de kwetsbaarheid voor social engineering beogen te verminderen. Zij concluderen dat effectieve interventies relatief intensief zijn en eerder een specifieke focus dan een brede focus hebben. De auteurs besluiten met het ontwerp van de best mogelijke interventie gegeven de resultaten van het onderzoek.
De centrale vraag in de korte bijdrage van ***Anouk van de Beek*** luidt: aan welke criteria moeten bewustwordingscampagnes over online gedrag voldoen om effectief te zijn?
We besluiten met een artikel van ***Rick van der Kleij, Susanne van 't Hoff-de Goede, Steve van de Weijer en Rutger Leukfeldt.*** Het is gebaseerd op een recent onderzoek dat in kaart brengt hoe veilig Nederlanders zich online zeggen te gedragen, hoe (on)veilig ze zich daadwerkelijk gedragen en welke verklaringen hiervoor zijn. De auteurs bespreken de implicaties van de uitkomsten voor effectief beïnvloedingsbeleid door de overheid.

Marleen Weulen Kranenbarg
Marit Scheepmaker*

* Gastredacteur dr. M. Weulen Kranenbarg is als universitair docent Criminologie verbonden aan de Vrije Universiteit Amsterdam. Mr. drs. M.P.C. Scheepmaker is hoofdredacteur van *Justitiële verkenningen*.

doi: 10.5553/JV/016758502020046002001

Coronacrisis en fraude: vier mogelijke relaties

Clarissa Meerts en Wim Huisman*

> 'Fraudsters have been very quick to adapt well-known fraud schemes to capitalise on the anxieties and fears of victims throughout the crisis. These include various types of adapted versions of telephone fraud schemes, supply scams and decontamination scams. A large number of new or adapted fraud schemes can be expected to emerge over the coming weeks [as] fraudsters will attempt to capitalise further on the anxieties of people across Europe.'

Bovenstaand citaat komt uit een persbericht op de website van Europol,[1] waarin wordt ingegaan op de te verwachten gevolgen van de wereldwijde uitbraak van het coronavirus voor ernstige criminaliteit, waaronder fraude. In deze bijdrage zullen wij ons specifiek richten op de mogelijke relaties tussen de coronacrisis en fraude en andere financieel-economische criminaliteit.

In Huismans bijdrage aan het themanummer van *Justitiële verkenningen* over de kredietcrisis, ruim tien jaar geleden, legde hij de lezers een aantal scenario's voor (Huisman 2009). Met deze scenario's verkende hij de mogelijke causale relaties tussen de kredietcrisis en de drie onderzoeksobjecten van de criminologie: criminaliteit, criminalisering en criminaliteitsbestrijding (Van Dijk e.a. 2018). Deze relaties sluiten elkaar niet uit, omdat crisis als gevolg van criminaliteit bijvoorbeeld kan leiden tot nieuwe criminalisering, zoals in het geval van de kredietcrisis (Levi 2008). Omdat de kredietcrisis zich binnen de financiële sector voltrok, richtte Huisman zijn scenario's op organisatiecriminaliteit (criminaliteit door en binnen wettige organisaties).

* Dr. C. Meerts is als universitair docent Criminologie verbonden aan de Vrije Universiteit Amsterdam. Dr. W. Huisman is hoogleraar Criminologie aan de Vrije Universiteit Amsterdam.

1 Europol, *How criminals profit from the COVID-19 pandemic press release*, 27 maart 2020, zie www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic. De aanleiding voor het persbericht was de verschijning van het Europol-rapport *Pandemic profeteering. How criminals exploit the Covid-19 crisis* (maart 2020).

doi: 10.5553/JV/016758502020046002002

Nu, in een tijd waarin het sociale leven op ongekende wijze op zijn kop is gezet, en de coronacrisis ook wordt geassocieerd met fraude en andere financieel-economische criminaliteit, lijkt het ons waardevol om naar deze scenario's terug te keren. De scenario's kunnen helpen de diverse in de media gerapporteerde en met de coronacrisis geassocieerde gevallen van financieel-economische criminaliteit te ordenen en te duiden met oog op nader onderzoek en op aanpak.[2] Door te leren van vorige crisis kunnen we een negatieve bijdrage van fraude aan de onvermijdelijke economische recessie als gevolg van de pandemie proberen te beperken. Hoewel de omstandigheden uiteraard verschillen (de kredietcrisis was immers deels veroorzaakt door fraude), is het interessant om de coronacrisis te bekijken met een 'fraudebril' op. De vier scenario's waar Huisman (2009, p. 27) het over heeft zijn:

1. De crisis is (mede) veroorzaakt door gevallen van organisatiecriminaliteit.
2. De crisis leidt tot gevallen van organisatiecriminaliteit.
3. De crisis leidt tot de criminalisering van meer ondernemingsgedrag.
4. Door de crisis zal meer organisatiecriminaliteit aan het licht komen.

In het navolgende zullen wij ingaan op deze vier scenario's. Wij passen bovenstaande scenario's enigszins aan, door ons te richten op financieel-economische criminaliteit in plaats van (alleen) op organisatiecriminaliteit.

Scenario 1: de crisis is (mede) veroorzaakt door gevallen van financieel-economische criminaliteit

Terwijl de kredietcrisis werd veroorzaakt door fraude met *sub-prime* hypotheken in de VS en daarvan afgeleide financiële producten (Nguyen e.a. 2010), ligt een direct causaal verband tussen financieel-economische criminaliteit en de coronacrisis niet voor de hand.

2 Daarbij dient te worden opgemerkt dat er op dit moment nog geen wetenschappelijk onderzoek is gepubliceerd over tijdens coronacrisis gepleegde financieel-economische criminaliteit. Onderzoekers beschikken daarmee over niet veel meer dan de in de media beschreven gevallen. Bovendien gaat het hier op zijn best om verdenkingen en is er nog niemand voor aan corona gerelateerde financieel-economische criminaliteit veroordeeld. De eerste aanhangig gemaakte zaak betreft grootschalige mondkapjesfraude, waarin het Openbaar Ministerie celstraffen van vier en drie jaar eiste tegen de twee verdachten, zie bijvoorbeeld https://nos.nl/artikel/2337566-celstraffen-geeist-tegen-twee-mannen-voor-mondkapjesfraude.html).

doi: 10.5553/JV/016758502020046002002

Ondanks complottheorieën over de productie van het virus in een Chinees laboratorium, is het bestaan van COVID-19 niet veroorzaakt door een vorm van fraude. Het is wel mogelijk dat de gezondheidscrisis die op de wereldwijde uitbraak is gevolgd mede het gevolg is van frauduleus handelen door organisaties en mensen met een machtspositie. De vraag is echter of we het hier hebben over criminaliteit, onhandig gedrag, of onethisch maar rechtmatig gedrag (*lawful but awful*, zie Passas 2005). Het laat ingrijpen van regeringen en organisaties zal in veel gevallen eerder vallen onder de tweede (en derde) categorie dan onder de eerste.
Terwijl ondernemingen of andere organisaties de coronacrisis niet hebben veroorzaakt, kunnen hun handelingen de crisis wel verergeren. Omdat overheden hun eigen gedrag niet snel zullen criminaliseren, kiezen criminologen bij de definitie van *state crime* vaak niet voor op de wet gebaseerde definities van criminaliteit. Het gaat dan eerder om *socially injurious action* (Friedrichs 2009).
Activiteiten of bewuste nalatigheid van overheden, overheidsfunctionarissen en regeringsleiders die een bestrijding van de pandemie in de weg staan, kunnen hieronder vallen. De toekomst zal leren of de verwijten dat China het ontstaan van de pandemie heeft proberen te verhullen, dat president Trump te lang heeft volgehouden dat zijn regering de uitbraak onder controle had en dat president Bolsenaro de ernst van het virus ontkende, worden gedefinieerd als voorbeelden van staatscriminaliteit. En ook ondernemingen kunnen verwijten treffen dat zij – *lawful but awful* – bedrijfsbelang boven volksgezondheid hebben geplaatst, zoals de aanvankelijke weigering van Roche om het recept van de vloeistof voor het ontwikkelen van coronatests te delen.[3] Hierover meer onder scenario 3.

Scenario 2: de crisis leidt tot gevallen van financieel-economische criminaliteit

Dit scenario is waarschijnlijker. Criminologische theorieën zoals de gelegenheidstheorie (Wilcox & Cullen 2018), benadrukken dat een toename van gelegenheden kan leiden tot een toename van criminaliteit. Een crisis als die rondom corona, waarin een tekort is aan specifieke

3 Algemeen Dagblad, 27 maart 2020, te vinden op: https://www.ad.nl/binnenland/gebouw-coronatestmaker-roche-in-almere-beklad-met-tekst-hoeveel-doden~afe34f3a/.

doi: 10.5553/JV/016758502020046002002

producten, zoals mondkapjes en desinfecterende handgel, biedt mogelijkheden tot misbruik. Voorbeelden uit de media zijn woekerprijzen voor mondkapjes[4] en het leveren van ondeugdelijke of namaakmondkapjes. Op 22 februari, nog voor de uitbraak van corona in Nederland, bericht nos.nl dat een Nederlands bedrijf van oplichting wordt beticht rondom de verkoop van mondkapjes aan China.[5] Op 24 maart 2020 meldt de Nationale Politie daarnaast dat zij heeft kunnen voorkomen dat Nederlandse ziekenhuizen bij de aankoop van mondkapjes voor tientallen miljoenen euro's zouden worden opgelicht.[6] CNN deed bericht van websites waarop geneesmiddelen tegen corona worden aangeboden.[7] Het zijn slechts enkele voorbeelden.

Het is treffend dat Sutherland, die het begrip 'witteboordencriminaliteit' heeft geïntroduceerd in zijn boek over de misdaden van grote ondernemingen al een heel deel besteedde aan het profiteren van de sterk toegenomen vraag en het ontbreken van tijd voor deugdelijke aanbestedingsprocedures tijdens de Eerste en Tweede Wereldoorlog. Gevolg was dat diverse bedrijven ondeugdelijke producten en grondstoffen gingen leveren die nodig waren voor de oorlogsindustrie en woekerprijzen gingen vragen (Sutherland 1949). De huidige economie ten tijde van corona is door economen al vergeleken met een oorlogseconomie.[8]

We vinden in de media echter ook voorbeelden van andere vormen van financieel-economische criminaliteit in de tijd van corona, zoals handel met voorkennis. Hoewel dit vanuit een gelegenheidsperspectief kan worden bekeken, kunnen we hier ook de 'straint'heorieën op los laten: een gevoelde of verwachte spanning (bijvoorbeeld geanticipeerd verlies van welvaart) kan leiden tot crimineel gedrag om deze *strain* te vermijden (Agnew & Brezina 2010). Een voorbeeld hiervan is het misbruik van voorwetenschap door Amerikaanse senatoren die op basis van geheime kennis over het coronagevaar aandelen verkochten

4 Nieuwsuur, 24 maart 2020, zie https://nos.nl/nieuwsuur/artikel/2328187-ziekenhuizen-bijna-voor-tientallen-miljoenen-opgelicht-bij-aankoop-mondkapjes.html.
5 Zie https://nos.nl/artikel/2324114-nederlands-bedrijf-beticht-van-oplichting-bij-verkoop-mondkapjes-voor-china.html.
6 Zie https://nos.nl/nieuwsuur/artikel/2328187-ziekenhuizen-bijna-voor-tientallen-miljoenen-opgelicht-bij-aankoop-mondkapjes.html.
7 Zie https://edition.cnn.com/2020/03/28/europe/spain-coronavirus-black-market-gougers-intl/index.html.
8 Zie www.rtlz.nl/algemeen/buitenland/artikel/5065681/italiaanse-economie-stilgelegd-corona-covid19-noodmaatregel.

doi: 10.5553/JV/016758502020046002002

of aankochten (zoals senator Loeffler, die naast het verkopen van aandelen, ook aandelen aanschafte van thuiswerk-software maker Citrix). Het lijkt er op dat zij hun voorkennis voor eigen gewin hebben ingezet, terwijl zij tegelijkertijd richting het Amerikaanse publiek uitdroegen dat alles onder controle was.[9]

De Autoriteit Financiële Markten (AFM) en de Europese Bankautoriteit (EBA) waarschuwen daarnaast voor nieuwe vormen van witwassen en financieren van terrorisme tijdens de coronacrisis.[10] Het verleden bewijst volgens de EBA dat criminelen in tijden van crisis hun activiteiten op dit gebied regelmatig opvoeren en nieuwe technieken ontwikkelen voor onder meer witwassen. Volgens de EBA zijn er al aanwijzingen van verhoogde niveaus van cyber crime, corona-gerelateerde fraudes en oplichtingspraktijken gericht op kwetsbare personen en bedrijven en valse donatiewervingscampagnes.[11]

Ten slotte kan op basis van de criminologische 'strain'-theorie worden voorspeld dat bedrijven in nood wettelijke regels gaan overtreden om kosten te besparen of alternatieve bronnen van inkomsten te vinden. Dit kan leiden tot fraude en andere criminaliteit (Agnew e.a. 2009). Ondernemers in geldnood lopen extra risico om ingepalmd te worden door criminelen voor gebruik van lege bedrijfsruimtes voor drugslabs, fictieve omzet om wit te wassen en het verkrijgen van zwarte leningen. De nood van ondernemers biedt gelegenheid voor georganiseerde criminaliteit, zo laten voorbeelden uit Italië zien.[12]

Zowel economische hoogconjunctuur als economische laagconjunctuur zijn geassocieerd aan verhoogde niveaus van fraude (Simpson & Rorie 2016). Tijdens momenten van economische recessie zien we bijvoorbeeld dat er sterke druk op bedrijven bestaat om financiële doelen te bereiken en dat er tegelijkertijd een situatie ontstaat waarin het externe toezicht minder strikt wordt, vanwege zorgen over de economie en bezuinigingen bij toezichthouders (Simpson & Rorie 2016). Accountants hebben al gewezen op de fraudegevoeligheid van de Noodmaatregel Overbrugging Werkgelegenheid waarmee de overheid

9 De Volkskrant 20 maart 2020, zie www.volkskrant.nl/nieuws-achtergrond/republikeinse-senatoren-verkochten-grote-aandelenpakketten-met-voorkennis-over-coronavirus~bd290d4b/?referer=https%3A%2F%2Fwww.google.com%2F.

10 Accountancy Vanmorgen, 1 april 2020, zie www.accountancyvanmorgen.nl/2020/04/01/corona-afm-let-juist-nu-op-nieuwe-vormen-van-witwassen/.

11 European Banking Authority, zie https://bit.ly/37vnAwX.

12 NRC 8 april 2020, zie https://www.nrc.nl/nieuws/2020/04/08/maffia-deelt-in-deze-crisis-geld-uit-de-rekening-komt-later-wel-a3996216.

doi: 10.5553/JV/016758502020046002002

ondernemers voor faillissement probeert te behoeden.[13] Sinds het uitbreken van de coronacrisis zijn bij de Inspectie Sociale Zaken en Werkgelegenheid (SZW), de Financial Intelligence Unit (FIU) en de UWV ruim tweehonderd meldingen ontvangen over mogelijke fraude met steunmaatregelen van de overheid.[14]
Behalve een motief kunnen de omstandigheden dus ook gelegenheid geven voor het plegen van financieel-economische criminaliteit, bijvoorbeeld door een afname van toezicht. De Europese autoriteit voor effecten en markten (ESMA) heeft bijvoorbeeld al aangekondigd dat nationale toezichthouders soepeler mogen omgaan met de regels voor ondernemingen die door de coronacrisis niet voor 1 mei hun financiële verslaggeving kunnen publiceren.[15] Volgens de AFM heeft de verspreiding van het coronavirus forse implicaties voor de financiële markten. Vanwege de uitzonderlijke omstandigheden waarmee de financiële sector momenteel wordt geconfronteerd, heeft de AFM besloten grote gegevensuitvragen aan financiële ondernemingen op te schorten. De AFM wil de financiële sector hiermee ruimte geven om zich volledig te richten op de uitdagingen van deze crisis en op de behoeften van de klanten. Hierop zijn enkele uitzonderingen, waaronder de naleving van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Maar ook bij die onderzoeken zal de AFM rekening houden met de omstandigheden waarmee financiële ondernemingen momenteel te maken hebben.[16]

Scenario 3: de crisis leidt tot de criminalisering van meer ondernemingsgedrag

In crisissituaties is het gemakkelijk om hoge prijzen te vragen voor gewilde artikelen (denk aan de eerder genoemde woekerprijzen voor mondkapjes). Hoewel dit niet gewenst is, gaat het hier niet (altijd) om crimineel gedrag. De sociale reactie op dit soort gedrag is echter interessant. Zo geeft het Openbaar Ministerie aan hard op te zullen treden

13 Financieel Dagblad 24 april 2020, zie https://fd.nl/ondernemen/1342132/fraudegevoeligheid-now-subsidie-leidt-tot-onrust-onder-accountants.
14 De Accountant 15 juni 20120, zie https://www.accountant.nl/nieuws/2020/6/200-meldingen-van-mogelijke-fraude-met-coronasubsidies/.
15 Zie www.esma.europa.eu/sites/default/files/library/esma80-187-546_public_statement_external_audit_bmr_april_2020.pdf.
16 AFM, *AFM schort uitvragen deels op tot 1 juni*, 26 maart 2020, zie www.afm.nl/nl-nl/professionals/nieuws/2020/mrt/afm-schort-uitvragen-deels-op-tot-1-juni.

doi: 10.5553/JV/016758502020046002002

tegen mensen die misbruik maken van de situatie[17] en besteedden media veel aandacht aan farmaceut Roche, de marktleider voor de machines waarmee de tests voor het coronavirus worden uitgevoerd. Door de grote vraag was het voor Roche niet mogelijk voldoende materiaal te leveren waardoor de tests niet konden worden uitgevoerd. Een van de materialen, een speciale vloeistof, kan door de laboratoria zelf worden gemaakt – Roche weigerde in eerste instantie echter het geheime recept prijs te geven (Follow the Money 2020). Onder andere omstandigheden wordt dergelijk gedrag vaak niet als crimineel gezien. Mocht het, in dit voorbeeld, strafbaar worden om in een dergelijke situatie bedrijfsgeheimen geheim te houden, dan kunnen we spreken van een situatie waarin de formele criminalisering (in de wet) van het gedrag volgt op een informele criminalisering ervan (maatschappelijke verontwaardiging). Waar dit voor veel crimineel gedrag een veelvoorkomende volgorde is, komt het criminaliseringsproces in de wereld van organisatiecriminaliteit echter vaker andersom tot stand (Huisman 2009). De vraag is dus ten zeerste of dit het geval zal zijn. Toch zien we in de coronacrisis tekenen van maatschappelijke onrust over het gedrag van bedrijven ontstaan. Om bij het voorbeeld van Roche te blijven: een Nederlandse vestiging van de farmaceut is beklad met de tekst 'Hoeveel doden?'.[18]

Levi (2008) stelt dat er voor het criminaliseren van financieel wangedrag echter meer nodig is dan maatschappelijke onrust. Hij stelt dat een morele paniek noodzakelijk is, een buitenproportionele uitbarsting van maatschappelijke angstreacties gericht op vermeende daders (Cohen 2011), maar dat morele paniek niet snel ontstaat rondom financieel-economische criminaliteit. Hoewel veel van Levi's argumenten ook gelden in de huidige coronacrisis (bijvoorbeeld dat er vanuit de politiek juist *geen* behoefte is aan grootschalige onrust), zien wij wel een verschil met de kredietcrisis: waar we normaliter van financieel-economische criminaliteit inderdaad kunnen aannemen dat deze minder bedreigend is voor individuele burgers dan commune criminaliteit, gaat de coronacrisis over de volksgezondheid. Dit is iets wat de samenleving, en de mensen daarin, direct en persoonlijk raakt. Hoewel wij dus wel de door Levi aangehaalde politieke strategie van

17 NOS, 25 maart 2020, zie https://nos.nl/artikel/2328299-om-zware-straffen-en-snelrecht-voor-misbruikers-van-coronacrisis.html..

18 AD, 27 maart 2020, zie www.ad.nl/binnenland/gebouw-coronatestmaker-roche-in-almere-beklad-met-tekst-hoeveel-doden~afe34f3a/..

doi: 10.5553/JV/016758502020046002002

risicomanagement verwachten en ook al terugzien in de aanpak van fraude in de coronacrisis, kunnen wij wellicht ook rekenen op een morele paniek. Dit laatste is echter wel deels afhankelijk van de vraag in hoeverre er echte 'folk devils' (vijanden van het volk) kunnen worden geïdentificeerd als focuspunt voor de morele paniek. Hoewel, zoals Huisman (2009) aangeeft, de (voornamelijk) mannen in de witte boorden niet aan ons traditionele boefbeeld voldoen, is dit beeld sinds de kredietcrisis wel aan enige verandering onderhevig. De bankensector, de accountancy, maar ook de farmaceutische industrie lijken al een tijdje te lijden onder een reputatieprobleem. En oplichters en ondernemers die uit winstbejag de veiligheid van zorgmedewerkers, breed gezien als de 'helden' van de huidige crisis, op het spel zetten, kunnen als 'coronahufters' rekenen op de toorn van het volk en het strafrechtelijk apparaat.

Scenario 4: door de crisis zal meer financieel-economische criminaliteit aan het licht komen

De kredietcrisis van 2008 leidde onder meer tot de ontdekking van piramidespellen (zoals die van Madoff) en andere vormen van beleggingsfraude (Huisman 2009). Zolang er meer inleg is dan uitgaven zal een piramidespel kunnen overleven. Op het moment dat dit echter niet meer het geval is, en de inleg opdroogt en investeerders hun geld opeisen, zal het piramidespel aan het licht komen. De verregaande maatregelen die op dit moment over de hele wereld worden genomen zullen naar verwachting een groot effect hebben op de wereldwijde economie. Veel bedrijven hebben reeds bij de overheid aangeklopt voor steun. In een recente publicatie over economische scenario's stelt het Centraal Plan Bureau te verwachten dat de economie hard zal worden geraakt (CBP 2020). Het is nog te vroeg om hier veel over te zeggen, maar wij kunnen wel de verwachting uitspreken dat een dergelijke economische crisis gevallen van financieel-economische criminaliteit aan het licht zal brengen.
Zoals gezegd is ook hoogconjunctuur geassocieerd aan hogere niveaus van fraude. Tijdens hoogconjunctuur worden investeerders overmoedig en verwachten ze hoge opbrengsten terwijl ze minder kritisch zijn ten aanzien van informatiebronnen die gouden bergen beloven. Volgens Davidson (2011) is het risico op fraude twee jaar voor en na

doi: 10.5553/JV/016758502020046002002

een economische piek hoog en wordt het steeds moeilijker de hoog gespannen verwachtingen van investeerders waar te maken. Opgeblazen, 'bull' markten verleiden gevestigde, bonafide spelers om excessieve risico's te nemen, terwijl deze markten ook malafide spelers aantrekken. Beide scenario's kunnen leiden tot frauduleuze praktijken die de markten verder doen imploderen (Simspon en Rorie 2016).
Vlak voor het toeslaan van de coronacrisis was sprake van hoogconjunctuur. Het valt dus te verwachten piramide-achtige en frauduleuze beleggingsconstructies in de problemen komen nu het de initiatiefnemers niet meer lukt nieuw geld aan te trekken met hun wervende verkooppraktijken.

Afsluitend

We zitten momenteel midden in de situatie die we beschrijven. Bovenstaande bespiegelingen zijn dan ook niet meer dan 'educated guesses'. De toekomst zal moeten uitwijzen wat de coronapandemie voor effecten heeft gehad op het gebied van fraude en andere financieel-economische criminaliteit. Het lijkt er nu in elk geval op dat de coronacrisis motivaties en gelegenheden biedt voor fraude, waaronder nieuwe vormen. De voorzitter van het College van Procureurs-Generaal heeft aangekondigd dat criminelen die misbruik maken van de coronacrisis met supersnelrecht zullen worden berecht en zware gevangenisstraffen tegen zich zullen horen eisen.[19] Ondanks dit supersnelrecht zal een zelf ook door de crisis getroffen strafrechtelijk apparaat nog wel jaren bezig zijn met de strafrechtelijke nasleep. De coronacrisis is niet voorbij wanneer iedereen is gevaccineerd. Door uitgestelde behandelingen zal de crisis in de gezondheidszorg voortduren. Het Centraal Plan Bureau voorspelt dat de economische gevolgen van de coronacrisis nog jaren lang voelbaar zijn. Dat kan dus ook gelden voor samenhangende financieel-economische criminaliteit. Net als na de kredietcrisis kan verwacht worden dat er nog lang onderzoek zal worden gedaan en gepubliceerd worden over criminaliteit en de coronacrisis (Will e.a. 2013).

19 NOS, 25 maart 2020, zie https://nos.nl/artikel/2328299-om-zware-straffen-en-snelrecht-voor-misbruikers-van-coronacrisis.html.

doi: 10.5553/JV/016758502020046002002

Literatuur

Agnew e.a. 2009
R. Agnew, N. Leeper Piquero & F.T. Cullen, 'General Strain Theory and White- Collar Crime', in: D. Weisburd & S. Simpson (eds.), *The Criminology of White-Collar Crime*, New York: Springer 2009, p. 35-60.

Agnew & Brezina 2010
Agnew, R., & Brezina, T., 'Strain theories', in: E. McLaughlin & T. Newburn (eds.), *The Sage Handbook of Criminological Theory*, Thousand Oaks: Sage Publications 2010, p. 96-113.

CBP 2020
CBP, *Economische scenario's corona,* Den Haag: Centraal Planbureau 2020. www.cpb.nl/sites/default/files/omnidownload/CPB-Infographic-Economische-scenarios-corona-26mrt2020.pdf.

Cohen 2011
S. Cohen, *Folk devils and Moral panics. The creation of the Mods and Rockers*, Abingdon, Oxon: Routledge 2011.

Davidson 2011
R. Davidson, *Accounting Fraud: Booms, Busts, and Incentives to Perform*, Chicago: The University of Chicago 2011.

Europol 2020
Europol, *Pandemic profeteering. How criminals exploit the Covid-19 crisis*. Den Haag: Europol 2020. www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

Follow the Money 2020
Follow the Money, '"Testen, testen, testen" – alleen als het farmaceut Roche behaagt', 27 maart 2020, www.ftm.nl/artikelen/roche-corona-lysisbuffer.

Friedrichs 2009
D.O. Friedrichs, *Trusted Criminals: White-Collar Crime in Contemporary Society*, Belmont, CA: Wadsworth Cengage Learning 2009.

Huisman 2009
W. Huisman, 'Kredietcrisis en organisatiecriminaliteit: vier mogelijke relaties', *Justitiële Verkenningen* (35) 2009-6, *p.* 26-42.

Levi 2008
M. Levi, 'Suite revenge? The shaping of folk devils and moral panics about white-collar crimes', *British Journal of Criminology,* (48) 2008, p. 1-20.

doi: 10.5553/JV/016758502020046002002

Nguyen e.a. 2010
T.H. Nguyen & H.N. Pontell, 'Mortgage Origination Fraud and the Global Economic Crisis', *Criminology & Public Policy* (9), p. 591-612.
Passsas 2005
N. Passas, 'Lawful but awful: 'Legal Corporate Crimes', *The Journal of Socio-Economics* (34) 2005-6, p. 771-786.
Simpson & Rorie 2016
S.S. Simpson & M. Rorie, 'Economic Fluctuations and Crises', in: S. Van Slyke, M. Benson & F.T. Cullen (eds.), *Oxford Handbook of White- Collar Crime*, Oxford: Oxford University Press 2016, p. 326-344.
Sutherland 1949
E.W. Sutherland, *White Collar Crime*, New York: Dryden 1949.
Van Dijk e.a. 2018
J. van Dijk, W.Huisman & P. Nieuwbeerta, *Actuele criminologie*, Den Haag: Sdu uitgevers 2018.
Wilcox & Cullen 2018
P. Wilcox & F.T. Cullen, 'Situational opportunity Theories of Crime', *Annual review of Criminology* (1) 2018-1, p. 123-148.
Will e.a. 2013
S. Will, S. Handelman & D.C. Brotherton (eds), *How They Got Away With It: White collar Criminals and the Financial Meltdown*, New York: Columbia University Press 2013.

doi: 10.5553/JV/016758502020046002002

Vissen met een nieuwe hengel: een onderzoek naar betaalverzoekfraude

Joke Rooyakkers en Marleen Weulen Kranenbarg*

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 Kranenbarg is universitair docent Criminologie aan de Vrije Universiteit Amsterdam. Persoonlijke pagina: https://research.vu.nl/en/persons/marleen-weulen-kranenbarg.

doi: 10.5553/JV/016758502020046002003

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 phishingpanel, 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

doi: 10.5553/JV/016758502020046002003

wordt onderzocht hoe deze relatief nieuwe benaderingsvorm van phishing eruitziet 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 phishinge-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

doi: 10.5553/JV/016758502020046002003

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[1] 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.

doi: 10.5553/JV/016758502020046002003

(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-betaalverzoekfraude wordt immers gebruik gemaakt van een valse identiteit (meestal een gehackt Marktplaatsaccount[2]) om door middel van social engineering die specifiek op de persoon gericht is (ingaan op een Marktplaatsadvertentie 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.

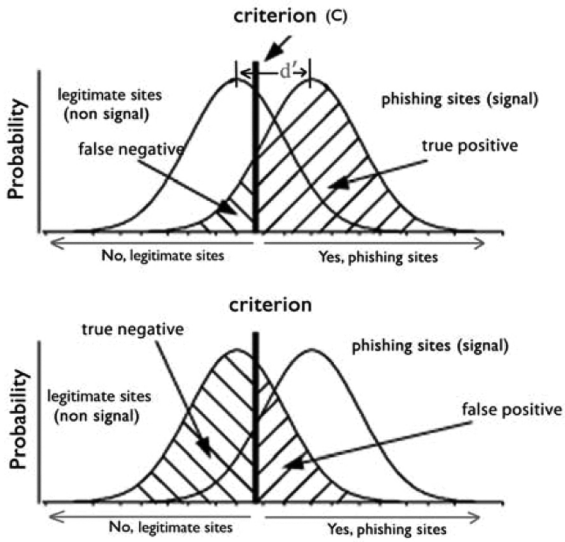
doi: 10.5553/JV/016758502020046002003

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 phishinge-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 phishinge-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 phishinge-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 phishingsites in plaats van e-mails, maar dit is op gelijke wijze van toepassing op phishinge-mails. Daarnaast linken phishinge-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 phishinge-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,

doi: 10.5553/JV/016758502020046002003

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.

doi: 10.5553/JV/016758502020046002003

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/leidinggevende 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 phishinge-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

doi: 10.5553/JV/016758502020046002003

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 phishinge-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 phishinge-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 phishinge-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.

doi: 10.5553/JV/016758502020046002003

Methode

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. Dit omdat online alleen aangifte gedaan kan worden van de 'tech support scam' en 'aan- of verkoopfraude'.[3] 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.[4] 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.
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.

doi: 10.5553/JV/016758502020046002003

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, overtuigingstechnieken en slachtofferkenmerken), namelijk: of het een poging betreft (ja of nee), de benaderingswijze van de fraudeur (social engineering, drie mogelijkheden), gebruik van WhatsApp of Marktplaatschat in de communicatie, het bedrag dat zogenaamd overgemaakt wordt op de phishingsite, 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.[5] 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.

doi: 10.5553/JV/016758502020046002003

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.

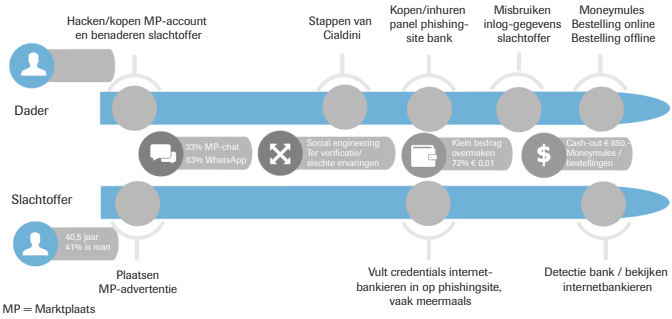
Resultaten

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

doi: 10.5553/JV/016758502020046002003

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 specifieker 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

doi: 10.5553/JV/016758502020046002003

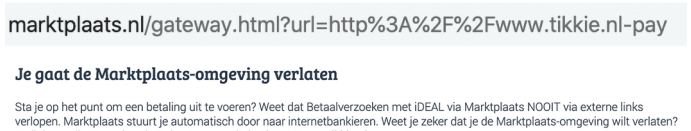
Figuur 4 **Voorbeelden van gateway-URL's van illegitieme en legitieme betaalverzoeken**

https://betaalverzoek.rabobank.nl/betaalverzoek?/id=	https://rabobank.overboeking.online
https://tikkie.me/pay/	https://betaalverzoek-tikkie.nl
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 phishingsite (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 verstuurde niet-legitieme betaalverzoeklink om het bedrag over te maken, komt het slachtoffer op een phishingwebsite. Deze phishingsite 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 phishingsite met de 'betaalomgeving van de gekozen bank'. Ook dit is echter weer een phishingsite 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-phishingsite 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

doi: 10.5553/JV/016758502020046002003

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



informatie die het slachtoffer invoert op de phishingsite daar binnenkomen. De phishingsite 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*,[6] 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 verstuurde 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.

doi: 10.5553/JV/016758502020046002003

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.

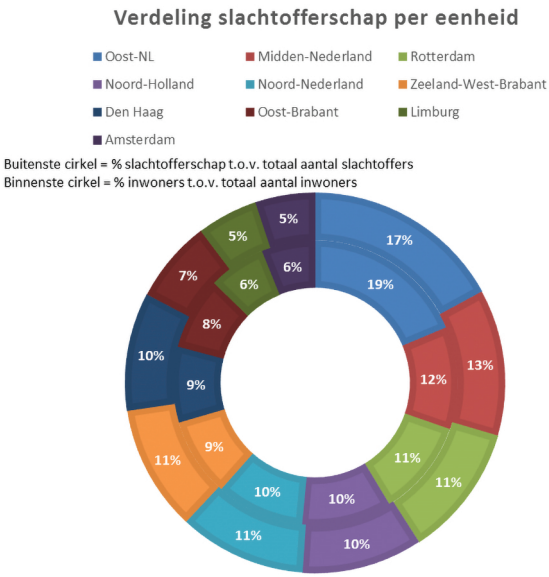
Slachtofferkenmerken

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,[7] 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.

doi: 10.5553/JV/016758502020046002003

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

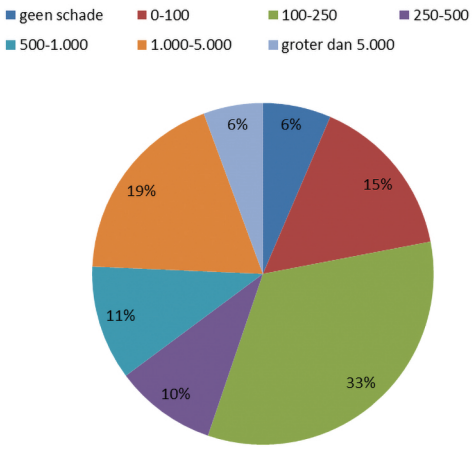


Conclusie

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 spearphishing 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 ontplooien (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.

doi: 10.5553/JV/016758502020046002003

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.

doi: 10.5553/JV/016758502020046002003

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 phishingsite 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

doi: 10.5553/JV/016758502020046002003

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 phishingpogingen. 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 phishingslachtofferschap (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 ontplooien 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

doi: 10.5553/JV/016758502020046002003

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

doi: 10.5553/JV/016758502020046002003

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.

doi: 10.5553/JV/016758502020046002003

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.

doi: 10.5553/JV/016758502020046002003

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 nieuw 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.

doi: 10.5553/JV/016758502020046002003

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. Lenzini (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. Kawauchi 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.

doi: 10.5553/JV/016758502020046002003

F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger

Robby Roks en Nahom Monshouwer*

De NOS meldt op 3 september 2018 dat er op sociale media als Instagram en Telegram honderden accounts met namen als 'snelgeldverdienen' of 'moneymakers' actief zijn die op grote schaal berichten plaatsen in de trant van 'Wil je snel geld verdienen en ben je 18+? Stuur me dan snel een privéberichtje.'[1] In deze berichten, die vooral gericht lijken op jongeren, wordt gevraagd om tegen betaling bankpassen en pincodes aan te leveren om fraude met pinpassen mogelijk te maken, een fenomeen dat in de wetenschappelijke literatuur ook wel wordt aangeduid als phishing (Lastdrager 2014). Bij banken bestaan er grote zorgen om deze activiteiten, omdat hier de nodige financiële schade mee gepaard gaat. Uit jaarcijfers van de Nederlandse Vereniging van Banken blijkt dat het schadebedrag door phishing in 2019 met bijna € 8 miljoen ruim verdubbeld bleek te zijn ten opzichte van 2018.[2]

Hoewel de geleden schade door consumenten in veel gevallen door de banken wordt vergoed, hebben we hier te maken met vormen van online fraude die een grote financiële schade met zich meebrengen. Deze cybercriminele activiteiten zijn in Nederland eerder onderwerp van studie geweest door Soudijn en Zegers (2012) en Leukfeldt (2014). Beide studies zijn gebaseerd op een wetenschappelijke analyse van

* Dr. R.A. Roks is als universitair docent verbonden aan de sectie Criminologie van de Erasmus Universiteit Rotterdam. R.N. Monshouwer MSc is CCD Analist bij Rabobank. De huidige bijdrage is gebaseerd op het onderzoek dat laatstgenoemde verrichtte in het kader van zijn masterscriptie aan de Erasmus Universiteit Rotterdam.

1 Gortworst e.a. 2018; zie https://nos.nl/artikel/2248735-politie-waarschuwt-voor-ronselaars-op-instagram-en-telegram.html, laatst geraadpleegd op 1 april 2020.

2 Van Teeffelen 2020; zie www.trouw.nl/binnenland/opnieuw-flink-meer-schade-door-phishing-doen-banken-genoeg~b64f36f0/, laatst geraadpleegd op 21 april 2020.

doi: 10.5553/JV/016758502020046002004

afgeronde politieonderzoeken. Soudijn en Zegers beschrijven de modus operandi van phishing op basis van een online cardingforum dat door de politie offline gehaald werd. Op basis van een analyse van de informatie op het forum concluderen Soudijn en Zegers (2012, p. 127) dat fysieke locaties zoals restaurants en clubs waar criminelen elkaar ontmoeten en kennis en informatie uitwisselen – zogeheten *offender convergence settings* (Felson 2006) – langzamerhand lijken over te zijn gegaan naar virtuele ontmoetingsplaatsen. Online, zoals op forums, ontmoeten mensen elkaar, worden goederen, diensten of informatie uitgewisseld en worden nieuwe criminele activiteiten besproken en uitgedacht. Soudijn en Zegers (2012, p. 127) concluderen om die reden dat 'whoever gains admission to the forum thereby opens the doors to an enormous source of contacts'.

Op basis van een analyse van een opsporingsonderzoek naar een cybercrimineel netwerk dat zich bezighield met phishing in Amsterdam laat Leukfeldt (2014) echter zien dat ook de offline wereld een onmisbare rol blijft spelen tijdens cybercriminaliteit. Niet een online forum, maar de straten van Amsterdam waren in de studie van Leukfeldt (2014, p. 235) de offender convergence setting waar de kernleden van het criminele netwerk elkaar hebben ontmoet en waar geldezels werden gerekruteerd om hun bankgegevens ter beschikking te stellen. Het rekruteringsproces vond daarbij zowel plaats in de fysieke straten van Amsterdam alsook op wat Lane (2019) de 'digitale straat' noemt: op socialemediaplatforms (Leukfeldt 2014, p. 231). Een analyse van het gebruik van sociale media door een problematische jeugdgroep uit de Rotterdamse wijk Spangen laat eveneens zien hoe jongeren platforms als Twitter gebruiken om naar specifieke bankpassen te vragen en om te poseren met verschillende betaalpassen (Roks & Van den Broek 2017, p. 40).

Bovenstaande studies illustreren het gebruik van virtuele ontmoetingsplaatsen zoals online fora en socialemediaplatforms in het *crime script* van phishing. Tot op heden zijn er echter geen studies geweest waarin specifiek aandacht wordt besteed aan phishing op Telegram Messenger, ofschoon diverse berichten in de media wijzen op het gebruik van Telegram voor online vormen van fraude en oplichting alsmede voor de handel in allerhande andere criminele goederen en diensten. Telegram lijkt hiervoor geschikt omdat deze gratis berichtendienst gebruikers de mogelijkheid biedt om versleutelde berichten, foto's en videobestanden te delen die, bovendien, een zelfvernieti-

doi: 10.5553/JV/016758502020046002004

gingsfunctie toegewezen kunnen krijgen (Moyle e.a. 2019, p. 102). Op Telegram worden berichten en bestanden versleuteld opgeslagen en daarnaast hebben gebruikers de mogelijkheid middels end-to-endencryptie[3] in de zogenaamde Secret Chats nog anoniemer te kunnen communiceren. Door deze functionaliteiten presenteert Telegram zich als een veilige berichtendienst, die bovendien laagdrempeliger is in termen van toegang en gebruik dan bijvoorbeeld fora op het darkweb.

In deze bijdrage doen wij verslag van een verkennend onderzoek naar online fraude en oplichting op Telegram op basis van een afgeronde masterscriptie (Monshouwer 2019). Ons doel is daarbij om een bijdrage te leveren aan de wetenschappelijke kennis over de modus operandi van online fraude en oplichting, de rol van online offender convergence settings en, ten slotte, het verrichten van wetenschappelijk onderzoek op socialemediaplatforms als Telegram. In deze bijdrage belichten we de volgende onderwerpen. We beginnen met een toelichting op het verrichten van *netnografisch* onderzoek op Telegram. Vervolgens geven we op basis van onze analyse van berichten op Telegram een illustratie en interpretatie van de zogenaamde F-game, een term die verwijst naar verschillende vormen van online fraude en oplichting. We besluiten deze bijdrage met een reflectie op de betekenis van deze bevindingen en het benoemen van enkele theoretische en methodologische implicaties, alsmede enkele suggesties voor vervolgonderzoek.

Netnografisch onderzoek op Telegram

Het berichtenplatform Telegram Messenger werd in 2013 door de Rus Pavel Durov opgericht na een langlopend conflict met de Russische autoriteiten over het afstaan van gebruikersgegevens van VKontakte, een andere succesvolle applicatie die Durov ontwikkelde. Door strenge controles vanuit Rusland en als antwoord op de conflicten met de autoriteiten ontwikkelde Durov met Telegram een socialemedia-

3 Door de end-to-endencryptie in de Secret Chats van Telegram kunnen alleen de zender en ontvanger van het bericht de versleutelde date lezen, waardoor 'no nobody else can decipher them, including us here at Telegram', aldus een antwoord op een van de Frequently Asked Questions op de website van Telegram Messenger (https://telegram.org/faq#secret-chats).

doi: 10.5553/JV/016758502020046002004

platform waarbij *encrypted messaging* en privacy centraal staan.[4] Telegram vertoont bepaalde gelijkenissen met de populaire berichtenservice WhatsApp, niet alleen wat betreft vormgeving, maar ook omdat een account op Telegram gelinkt is aan het telefoonnummer van de gebruiker, waarmee gecommuniceerd kan worden met opgeslagen contacten.

Anders dan WhatsApp biedt Telegram echter de mogelijkheid om lid te worden van verschillende groepen. Een zoekfunctie maakt het mogelijk om verschillende groepen op Telegram te vinden waar de gebruiker lid van kan worden om de gedeelde berichten te lezen en bestanden (afbeeldingen, video's, audio) op te slaan. In de groepen op Telegram hebben gebruikers, net als in de groepchatfunctie op WhatsApp, de mogelijkheid om met alle gebruikers in de groep te communiceren. De Telegramgroepen kunnen tot maximaal 200.000 leden bevatten en beheerders kunnen bots toevoegen om de (in)formele gedragsregels in de desbetreffende groep te handhaven. Gebruikers die zich niet houden aan de (in)formele regels van de groepen lopen het risico om voor een bepaalde tijdsduur verbannen te worden. Als de interactie niet geschikt is voor het grote publiek, hebben gebruikers bovendien de mogelijkheid om op een profiel van een andere gebruiker te klikken en een privébericht te sturen.

De eerste stap tijdens het verzamelen van data in het scriptieonderzoek van de tweede auteur was het selecteren van relevante groepen op Telegram. Het gebruik van de zoektermen 'swipen' en 'bonken' – twee specifieke aanduidingen voor online fraude en oplichting die in het vervolg van deze bijdrage nader toegelicht worden – in combinatie met de plaats 'Utrecht' resulteerde in een aantal groepen. Na uitgebreid rond te hebben gekeken in diverse groepen werd de tweede auteur lid van de groepen 'Swipe en Bonk' (886 leden[5]) en 'UTRECHT + OMGEVING HANDELSGROEP 030' (943 leden). Hiernaast werden ook enkele andere groepen, 'The Hustlers Handelgroep' (3.239 leden), 'Swipers United' (134 leden) en '[Y] SWIPEHANDEL' (796 leden), op regelmatige basis bezocht zonder hier lid van te worden.

Vanaf begin april tot eind juli 2019 verrichtte de tweede auteur netnografisch onderzoek in deze groepen. De term netnografie is schat-

4 Hakim 2014; zie www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html, laatst geraadpleegd op 1 april 2020.

5 Het gaat hier om het aantal leden van de groepen tijdens het verrichten van de dataverzameling. Opgemerkt dient echter te worden dat de hoeveelheid leden per groep van dag tot dag, en zelfs van uur tot uur, kan veranderen.

doi: 10.5553/JV/016758502020046002004

plichtig aan Kozinets (2002, p. 62), die het begrip introduceerde om te verwijzen naar 'a new qualitative research methodology that adapts ethnographic research techniques to the study of cultures and communities emerging through electronic networks'. Ondanks dat het *being there*, dat aangemerkt kan worden als een kernbeginsel van dit etnografisch onderzoek, op het internet op een andere manier vormt krijgt, biedt de digitale wereld wel degelijk mogelijkheden om de etnografische traditie online voort te zetten. Urbanik en Roks (2020) beschrijven op basis van hun ervaringen met het incorporeren van onderzoek op sociale media tijdens meer klassiek offline veldwerk dat de traditionele rollen op het participant-observantcontinuüm van Gold (1958) ook online door onderzoekers kunnen worden uitgevoerd. Sociale media bieden immers verschillende functionaliteiten om actief en zichtbaar te participeren, onder andere door te reageren op *posts* en *comments* van andere gebruikers.

De online wereld biedt echter vooral de mogelijkheid om anoniem te observeren, zonder zelf deel te nemen. In de wetenschappelijke literatuur wordt dit ook wel aangeduid als *cyber stealth* (Murthy 2008), *lurken* (Richman 2007; Ferguson 2017) of *creepen* (Trottier 2012). De tweede auteur verkoos deze variant, in het bijzonder omdat de groepen op Telegram de mogelijkheid bieden om de inhoud van de posts en gesprekken te zien, zonder dat de gebruiker zijn aanwezigheid of identiteit kenbaar hoeft te maken. Bovendien biedt Telegram, anders dan bijvoorbeeld socialemediaplatform Snapchat, de mogelijkheid om screenshots van conversaties te maken zonder dat andere gebruikers hier een melding van krijgen. In de onderhavige studie is ervoor gekozen om screenshots te maken van de inhoud van de groepen op Telegram zonder de andere gebruikers hiervan op de hoogte te stellen, in het bijzonder omdat het gaat om delen van het internet die voor iedereen met een internetverbinding en telefoonnummer toegankelijk zijn. Al het verzamelde materiaal dat gebruikt is in de uiteindelijke masterscriptie van Monshouwer (2019) is geanonimiseerd en in sommige gevallen, wanneer een conversatie tussen gebruikers meer gedetailleerd werd beschreven, voorzien van pseudoniemen.

De data zijn verzameld door om de twee dagen de geplaatste berichten in de eerdergenoemde groepen te lezen en screenshots te maken van conversaties en berichten die te maken hadden met phishing. Er is bewust gekozen om niet alle informatie in de groepen in één keer volledig te downloaden, ofschoon deze functie wel beschikbaar is in de

doi: 10.5553/JV/016758502020046002004

Desktop-versie van Telegram. Hier lagen twee redenen aan ten grondslag. De eerste reden had te maken met cybersecurity. Door alles uit een groep te downloaden bestond het risico dat er ook afbeeldingen en bestanden met een zogeheten *encrypted* Remote Access Tool (RAT) – software waarmee je computer of mobiele telefoon voor hackdoeleinden gebruikt kan worden – tussen zouden kunnen zitten, iets waar door diverse gebruikers in de groepen voor werd gewaarschuwd (Monshouwer 2019, p. 22). Ten tweede zou het downloaden van alle informatie resulteren in een enorme hoeveelheid aan data, omdat er meerdere keren per dag dezelfde berichten door gebruikers werden gedeeld. Bovendien werd er ook allerlei content geplaatst die geen betrekking had op fraude, zoals berichten waarin wapens, drugs en designerkleding werden gevraagd of aangeboden. De content over het fenomeen phishing, en fraude meer in het algemeen, in de groepen werd opgeslagen door het maken van screenshots om zo een letterlijke tekstuele weergave van de berichten vast te kunnen leggen. In de periode april tot juli 2019 werden op deze manier meer dan 1.650 screenshots verzameld, die met behulp van Atlas.ti werden geanalyseerd (Monshouwer 2019, p. 25-26).

De F-game op Telegram

In de studie van Monshouwer (2019) lag de primaire focus op het beschrijven van de manieren waarop fraudeurs en oplichters gebruik maken van Telegram. In de geanalyseerde groepen passeerden diverse aan fraude en oplichting gerelateerde activiteiten de revue, waarbij gebruikers specifieke goederen en diensten om deze cybercriminele activiteiten te verrichten aanboden en vroegen. We lichten dit in het vervolg nader toe door meer zicht te geven op de vorm en inhoud van de berichten in de groepen. Vervolgens zoomen we in op de diverse modi operandi die in de bestudeerde groepen werden gedeeld.

'Op zoek naar iemand die dagelijks ECHTE jobs heeft?'

Afgaande op de berichten in de bestudeerde groepen lijkt Telegram dienst te doen als een marktplaats voor een veelvoud aan criminele goederen en diensten. Naast specifieke berichten en conversatie over fraude en oplichting in de vorm van het aanbieden of vragen van cre-

doi: 10.5553/JV/016758502020046002004

ditcardgegevens, bankpassen en methoden om geld afkomstig van phishingaanvallen te gebruiken, passeerden ook afbeeldingen van (vuur)wapens en diverse hard- en softdrugs de revue. De berichten worden gekenmerkt door het veelvuldige gebruik van emoji's en hoofdletters en een doorgaans adverterende stijl, zoals het volgende bericht illustreert:

> 'Yo F-gamers, Op zoek naar iemand die dagelijks ECHTE jobs heeft? Geen praatjesmaker die je kaart dagen lang houd? Dan ben je bij het juiste adres! WAT IS ER NU AAN? CRELAN BELGIE. ING BELGIE. ING NL. Ik meld elke dag welke jobs er zijn en wat je daar voor vangt.' (*The Hustlers Handel*, mei 2019)

De informatie uit het bovenstaande bericht vereist een zekere 'insider knowledge' om te ontcijferen waar door de gebruiker op wordt gedoeld. 'F-game', allereerst, is een term die zowel op straat als online wordt gebruikt als verwijzing naar activiteiten die kunnen worden geclassificeerd als fraude of oplichting. Opmerkelijk hierbij is dat het wordt aangemerkt als een 'game', een term die in de vorm van 'the crack game' op de straten van de Verenigde Staten ook wel wordt gebruikt voor het aanduiden van betrokkenheid bij de handel in specifieke verdovende middelen (Draus & Carlson 2009). In het gebruik van de term 'job' herkennen we bovendien eufemistisch taalgebruik waarbij criminaliteit wordt gezien als werk (Roks 2016, p. 160). Met welke 'jobs' – of 'djoen' of 'djunta', dat zich ook laat vertalen als werk (SMIB 2017, p. 98) – specifiek geld kan worden verdiend, is afhankelijk van wat er 'aan' is, oftewel waar vraag naar is of welke mogelijkheden zich voordoen, zoals in het bovenstaande geval bankpassen uit zowel België (Crelan en ING) als Nederland (ING).
Naast dat er diensten of 'jobs' worden aangeboden, zijn er ook gebruikers die op zoek zijn naar specifieke goederen of diensten. Er wordt daarbij gevraagd naar betaalpassen met bijbehorende pincodes van diverse Europese banken, maar in de geanalyseerde groepen zijn het voornamelijk Nederlandse banken. ABN AMRO wordt daarbij vanwege de groene betaalpassen aangeduid als 'green', ING als 'orra of orange' vanwege de oranje kleur van de pas en 'baro' wordt gebruikt om te verwijzen naar Rabobank. Bovendien gaat de voorkeur uit naar zogenaamde '18+'- of zakelijke kaarten, omdat ze een limiet kennen tot € 10.000 in tegenstelling tot 'kinderkaarten', die 'slechts gevuld

doi: 10.5553/JV/016758502020046002004

kunnen worden tot €5.000'. Naast dat de meeste gebruikers expliciteren wat ze aanbieden of vragen, benoemen ze daarbij ook vaak waar ze niet naar op zoek zijn. Een gebruiker schrijft bijvoorbeeld dat hij of zij niet op zoek is 'naar afhakers, grappenmakers, kleine kinderen en bledders'. Er wordt verwezen naar mensen die hun afspraken niet nakomen, zoals 'afhakers' en 'grappenmakers', naar 'infotrekkers', die enkel vragen stellen, en 'bledders': mensen die enkel praatjes hebben maar de daad niet bij het woord voegen.
Een groot aantal van de bovengenoemde woorden en termen illustreert de veelvuldige aanwezigheid van straattaal in de geanalyseerde groepen op Telegram. Dit valt eveneens te herkennen in het gebruik van specifieke termen voor phishinggerelateerde activiteiten. Naast de eerdergenoemde 'green', 'orra' en 'baro', wordt er meer in het algemeen gevraagd om 'sappies' en 'nip'. In deze termen herkennen we de linguïstische praktijk van 'talking backwards' (Lefkowitz 1989), waarbij woorden omgekeerd worden geschreven, zoals in 'sappies' van 'passen' en 'nip' van 'pinnen'. In Nederland kan deze omgang met taal in het bijzonder worden herleid naar de Amsterdamse Bijlmer, waar het wordt aangeduid als 'Sbimese', een omkering van de verbasterde aanduiding voor het stadsdeel als 'Bims' (SMIB 2017). Meer in het algemeen lijkt deze manier van praten en schrijven te zijn geïnspireerd door het *verlan* uit de banlieues van Frankrijk (Slooter 2019, p. 49).

De modus operandi van 'mapsen', 'swipen' en 'bonken'

We zien het gebruik van straattaal en de omkering van woorden eveneens terugkomen in de beschrijving van een aantal modi operandi die in de bestudeerde Telegramgroepen worden gedeeld, te weten 'mapsen', 'swipen' en 'bonken'. De benaming van de eerste werkwijze wordt nader toegelicht in het volgende bericht:

> 'Nu gaan we ons verdiepen in het Mapsen. Wat is Mapsen? Mapsen is het woord voor spammen. Dat houd in dat je een bericht in één keer verstuurd naar een groot aantal mensen. Bij het mapsen hoort phishen. Bij het phishen krijg je informatie van mensen doormiddel van oplichting.' (*Swipers United*, juli 2019)

doi: 10.5553/JV/016758502020046002004

Allereerst is het opvallend dat er op Telegram een toelichting wordt gegeven op de betekenis van de gehanteerde termen. 'Mapsen', de meervoudsvorm van de omkering van het woord 'spam', houdt in dit geval in dat er berichten worden gestuurd naar zo veel mogelijk telefoonnummers van potentiële slachtoffers. Er wordt hierbij een onderscheid gemaakt tussen zogenaamde gewone 'leads', bestaande uit mensen met een telefoonabonnement bij een specifieke provider, en 'target leads' in de vorm van mensen van wie bekend is dat ze bijvoorbeeld een creditcard hebben. Naar deze 'leads' worden 'nepberichten' gestuurd die afkomstig lijken te zijn van een verzender die wordt vertrouwd, zoals een Nederlandse bank. De berichten bevatten een hyperlink en zodra een slachtoffer daarop klikt, krijgt hij een pagina te zien die identiek lijkt aan de website van zijn eigen bank en wordt hem gevraagd zijn inloggegevens in te voeren. Op het moment van invoeren verkrijgt iemand anders echter ook toegang tot de financiële gegevens van het slachtoffer en wordt het aanwezige geld op de spaar- of bankrekening overgemaakt naar andere rekeningen, om vervolgens zo snel mogelijk contant uit een betaalautomaat te worden gehaald (vgl. Leukfeldt 2014, p. 234).

Opvallend aan de berichten in de geanalyseerde groepen is dat zowel wordt beschreven wat de specifieke activiteit inhoudt, alsook dat gebruikers meer inzicht wordt gegeven in welke handelingen ze stapsgewijs moeten verrichten om dit tot een succesvol einde te brengen. We zien dit terugkomen bij de tweede modus operandi die beschreven werd in de groepen op Telegram: 'swipen'. Met deze term wordt verwezen naar een manier om online producten te bestellen in webshops en te laten leveren, zonder voor de bestelde producten te betalen. In de Telegramgroep 'Swipe en Bonk' wordt uitgebreid beschreven welke stappen achtereenvolgens moeten worden doorlopen om accounts op Zalando, Bol.com of andere e-commercepartijen te 'swipen'.

De eerste drie stappen geven een nadere toelichting op de apparatuur en software die vereist zijn. Opmerkelijk hierbij is dat expliciet wordt benoemd welke software hiervoor gebruikt moet worden, waar deze kan worden gedownload en welke functie dit heeft. Bij 'swipen' wordt bijvoorbeeld benoemd dat gebruik moet worden gemaakt van NordVPN om het IP-adres en de fysieke locatie van de gebruiker te verbergen, en dat er een softwareprogramma moet worden gedown-

doi: 10.5553/JV/016758502020046002004

load om cookies te wissen. Na het doorlopen van deze stappen is het volgens het bericht tijd voor stap 4:

> 'Vervolgens ga je naar de website toe, je logt in en gaat net als elk willekeurig persoon even op de site rond surfen je gaat cookies opbouwen even hier kijken even daar kijken enzovoort enz enzz. Je gaat nooit gelijk inloggen iets opzoeken aanklikken en bestellen. Zodra je een aantal cookies hebt opgebouwd heb je meer slagingspercentage. Oke nu we dit hebben gedaan gaan we naar ons artikel toe… We klikken het aan en zorg altijd dat je net onder de €200 besteld. Op de bestelpagina staan gegevens je MOET NOOOOIT GEGEVENS AANPASSEN VAN EEN ACCOUNT DAN BLOKEERD AFTERPAY. je laat alles precies zoals het is want je gaat bestellen en laten leveren op een afhaalpunt en daarvoor heb je weer een ID kaart nodig. Als het pakketje op het afhlaapunt ligt stuur je iemand erheen of jij zelf met een id kaart en de track en trace code en dan krijg je je pakketje mee!! Veel success' (*Swipe en Bonk*, juli 2019)

Naast deze stapsgewijze toelichting wordt er in de groepen ook expliciet gevraagd om contacten bij PostNL of bezorgers werkzaam bij DHL om deze producten vervolgens tegen vergoeding af te leveren, maar bieden bezorgers zelf ook hun diensten aan in deze groepen om wat extra's te verdienen.

De derde en laatste modus operandi die in de geanalyseerde groepen op Telegram kan worden waargenomen, staat bekend als 'bonken', een term die in deze context gebruikt wordt als synoniem voor het 'gooien' van geld op een pas. 'Bonkers' zijn met andere woorden mensen die toegang hebben tot online bankgegevens van anderen en op zoek zijn naar manieren om de virtuele valuta om te zetten in contant geld. Het cashen van dit geld gebeurt door zogenaamde 'geldezels' (Leukfeldt 2014, p. 239-241). Ook deze modus operandi wordt uitgebreid toegelicht en onderverdeeld in een aantal stappen. Om te 'bonken' is een 'schone' telefoon nodig die niet eerder voor deze activiteit is gebruikt of waarvan de fabrieksgegevens zijn gewist. In tegenstelling tot 'swipen' wordt er bij 'bonken' opgeroepen om geen gebruik te maken van VPN.

Anders dan bij de andere modi operandi is bovendien dat er in het geval van 'bonken' een duidelijke afstemming is vereist tussen verschillende actoren en speelt een wezenlijk deel zich niet online af, maar in de fysieke wereld. Naast mensen die het geld van de rekenin-

doi: 10.5553/JV/016758502020046002004

gen van slachtoffers in juiste verhoudingen overmaken naar andere accounts, moeten de 'nippers' ('pinners') onder flinke tijddruk bij een pinautomaat aanwezig zijn om het overgemaakte geld uit de muur te halen. In het bericht wordt daarbij gespecificeerd dat het geld opgenomen moet worden in delen van € 1.200. Ten slotte wordt aangegeven dat de telefoon waarmee contact is geweest tussen de 'bonker' en de 'nipper' moet worden weggegooid.

Conclusie

In deze bijdrage hebben we een beschrijving gegeven van de modi operandi van online fraude en oplichting op het platform Telegram Messenger. Onze resultaten illustreren dat Telegram, net als cryptomarkten (Martin 2014; Aldridge & Decary-Hétu 2016) of specifieke online fora (Holt & Lampke 2010; Soudijn & Zegers 2012), lijkt te fungeren als een criminele marktplaats. In de bestudeerde groepen op Telegram zijn enerzijds gebruikers actief die goederen en diensten aanbieden en anderzijds gebruikers die op zoek zijn naar specifieke goederen of diensten. Bovendien illustreren de resultaten in deze bijdrage dat er op Telegram uitgebreide en stapsgewijze handleidingen ter beschikking worden gesteld om specifieke criminele activiteiten op een succesvolle manier uit te voeren, en dat gebruikers elkaar informeren over wat er wel en niet lijkt te werken. Het gaat daarbij niet enkel om een toelichting op de modus operandi, maar ook om meer nadrukkelijke informatie over de technologische kanten en benodigdheden om online fraude en oplichting mogelijk te maken. Telegram kan hierdoor worden beschouwd als een *digital offender convergence setting*.

Om toegang te krijgen tot de informatie in de groepen op Telegram hoeft er, anders dan op cryptomarkten, geen verbinding te worden gemaakt met een TOR-netwerk (Martin 2014; Ferguson 2017) en bovendien hoeven gebruikers zich niet te registreren om toegang te krijgen zoals op een online forum gebruikelijk is (Holt & Lampke 2010; Soudijn & Zegers 2012). Wel biedt de encryptie op Telegram gebruikers de mogelijkheid om op basis van een *plastic identity* (Yar 2005) anoniem en veilig te communiceren met anderen. Een wezenlijk verschil met de eerdergenoemde digital offender convergence settings is daarmee de ogenschijnlijke laagdrempeligheid van Telegram, die te

doi: 10.5553/JV/016758502020046002004

vergelijken is met andere, meer conventionele socialemediaplatforms zoals Twitter en Instagram.

De resultaten uit deze verkennende studie roepen de vraag op wie er in deze groepen actief zijn. Het veelvuldige gebruik van straattaal in de berichten en conversatie doet daarbij vermoeden dat het gaat om personen die zijn ingebed in een straatcultuur en hun werkterrein lijken te hebben verplaatst van de fysieke straat naar de digitale straat (Lane 2019). Tot op heden wijzen de beschikbare studies over de digitalisering van straat- en gangculturen vooral op het expressieve gebruik van het internet door (groepen) jongeren op straat, zoals het opbouwen en managen van reputatie, individuele en collectieve identiteitsconstructie en de veranderende dynamiek van geweld (zie voor een overzicht Irwin-Rogers e.a. 2018). De bevindingen uit deze studie illustreren echter dat sociale media ook een gedigitaliseerde kansenstructuur bieden om geld te verdienen, en dat er zelfs sprake lijkt van een diversificatie van traditionele delicten op straat, van de handel in drugs tot betrokkenheid bij cybercriminele activiteiten zoals phishing (Leukfeldt & Roks 2020).

Deze verkennende studie waar de onderhavige bijdrage op is gebaseerd, kent een aantal beperkingen. Allereerst is het onderzoek beperkt tot het volgen van enkele groepen op Telegram gedurende een periode van vier maanden. Een bijkomende beperking is dat we niet weten of ook offline navolging wordt gegeven aan het besprokene in de geanalyseerde Telegramgroepen. Eerdere studies naar de digitale straat wijzen immers op de centrale rol van het wekken van indrukken en discrepanties tussen online en offline identiteiten en gedragingen (Lane 2019; Urbanik & Roks 2020). Wel wekken de negatieve ervaringen in de berichten van sommige gebruikers, die bijvoorbeeld aangeven dat bepaalde aanbieders van goederen of diensten niet te vertrouwen zijn, de indruk dat vraag en aanbod dankzij de Telegramgroepen bij elkaar komen. Bovendien vertonen de gedetailleerde beschrijvingen van de modi operandi in deze bijdrage veel gelijkenissen met de crimescripts van phishing die worden beschreven in eerdere wetenschappelijke studies (Soudijn & Zegers 2012; Leukfeldt 2014).

De relatieve openheid van deze informatie biedt kansen voor zowel opsporingsdiensten als banken en e-commercebedrijven die geconfronteerd worden met de vormen van online fraude en oplichting die in deze bijdrage tot in detail werden beschreven. Bovendien onder-

doi: 10.5553/JV/016758502020046002004

streept dit artikel wat ons betreft de mogelijkheden die Telegram Messenger biedt voor het verrichten van wetenschappelijk onderzoek, temeer omdat er ook groepen zijn die zich specifiek richten op de handel in verdovende middelen, wapens, namaakkleding en andere criminologisch relevante thema's. Onze aanbeveling zou daarbij zijn om vervolgonderzoek niet enkel te beperken tot een observerende rol, maar de ingebouwde beveiligde berichtenservice te gebruiken om te communiceren met zowel aanbieders als vragers van illegale goederen en diensten. Een aanverwant thema dat daarbij bovendien nader uitgediept kan worden, is hoe er op Telegram wordt omgegaan met vertrouwen, omdat er, anders dan op cryptomarkten en online fora, niet gewerkt wordt met rating- en reviewsystemen om gebruikers te laten beoordelen of kopers of verkopers betrouwbaar zijn (Soudijn & Zegers 2012; Holt e.a. 2015).

Literatuur

Aldridge & Decary-Hétu 2016
J. Aldridge & D. Decary-Hétu, 'Cryptomarkets and the future of illicit drug markets', in: EMCDDA (red.), *The Internet and drug markets, EMCDDA insights*, Luxemburg: European Union 2016, p. 23-32.

Draus & Carlson 2009
P.J. Draus & R.G. Carlson, '"The game turns on you": Crack, sex, gender, and power in small-town Ohio', *Journal of Contemporary Ethnography* (38) 2009, afl. 3, p. 384-408.

Felson 2006
M. Felson, *The ecosystem for organized crime* (HEUNI paper No. 26), Helsinki: HEUNI 2006.

Ferguson 2017
R.H. Ferguson, 'Offline "stranger" and online lurker: Methods for an ethnography of illicit transactions on the darknet', *Qualitative Research* (17) 2017, afl. 6, p. 683-698.

Gold 1958
R. Gold, 'Roles in sociological field observation', *Social Forces* (36) 1958, p. 217-223.

Gortworst e.a. 2018
J. Gortworst, A. Pruis & D. Simons, 'Politie waarschuwt voor ronselaars op Instagram en Telegram', *NOS* 3 september 2018, https://nos.nl/artikel/2248735-politie-waarschuwt-voor-ronselaars-op-instagram-en-telegram.html.

doi: 10.5553/JV/016758502020046002004

Hakim 2014
D. Hakim, 'Once celebrated in Russia, the programmer Pavel Durov chooses exile', *New York Times* 2 december 2014, www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html.

Holt & Lampke 2010
T.J. Holt & E. Lampke, 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies* (23) 2010, afl. 1, p. 33-50.

Holt e.a. 2015
T.J. Holt, O. Smirnova, Y.T. Chua & H. Copes, 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime* (16) 2015, afl. 2, p. 81-103.

Irwin-Rogers e.a. 2018
K. Irwin-Rogers, J.A. Densley & C. Pinkney, 'Gang violence and social media', in: J.L. Ireland, P. Birch & C.A. Ireland (red.), *The Routledge international handbook of human aggression*, Londen: Routledge 2018, p. 400-410.

Kozinets 2002
R.V. Kozinets, 'The field behind the screen: Using netnography for marketing research in online communities', *Journal of Marketing Research* (39) 2002, afl. 1, p. 61-72.

Lane 2019
J. Lane, *The digital street*, New York: Oxford University Press 2019.

Lastdrager 2014
E.E. Lastdrager, 'Achieving a consensual definition of phishing based on a systematic review of the literature', *Crime Science* (3) 2014, afl. 1, p. 9.

Lefkowitz 1989
N.J. Lefkowitz, 'Verlan: talking backwards in French', *The French Review* (63) 1989, afl. 2, p. 312-322.

Leukfeldt 2014
E.R. Leukfeldt, 'Cybercrime and social ties', *Trends in Organized Crime* (17) 2014, afl. 4, p. 231-249.

Leukfeldt & Roks 2020
E.R. Leukfeldt & R.A. Roks, 'Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes', *Deviant Behavior* (geaccepteerd, te verschijnen).

Martin 2014
J. Martin, 'Lost on the Silk Road: Online drug distribution and the "cryptomarket"', *Criminology & Criminal Justice* (14) 2014, afl. 3, p. 351-367.

Monshouwer 2019
N. Monshouwer, *'Kom met je spa en we vullen em.' Een netnografisch onderzoek naar het gebruik van Telegram door F-gamers* (masterscriptie Rotterdam), 2019.

doi: 10.5553/JV/016758502020046002004

Moyle e.a. 2019
L. Moyle, A. Childs, R. Coomber & M.J. Barratt, '# Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs', *International Journal of Drug Policy* (63) 2019, p. 101-110.

Murthy 2008
D. Murthy, 'Digital ethnography: An examination of the use of new technologies for social research', *Sociology* (42) 2008, afl. 5, p. 837-855.

Richman 2007
A. Richman, 'The outsider lurking online', in: A.L. Best (red.), *Representing youth*, New York: New York University Press 2007, p. 182-202.

Roks 2016
R.A. Roks, *In de h200d. Een eigentijdse etnografie over de inbedding van criminaliteit en identiteit* (diss. Rotterdam), 2016

Roks & Van den Broek 2017
R.A. Roks & J.B.A. van den Broek, '#HOUHETSTRAAT: Straatcultuur op social media?', *Tijdschrift over Cultuur en Criminaliteit* (7) 2017, afl. 3, p. 31-50.

Slooter 2019
L.A. Slooter, *The making of the banlieue: An ethnography of space, identity and violence* Londen: Palgrave Macmillan 2019.
SMIB, *Smibanese woordenboek*, Amsterdam: Uitgeverij Pluim 2017.

Soudijn & Zegers 2012
M.R. Soudijn & B.C.H.T. Zegers, 'Cybercrime and virtual offender convergence settings', *Trends in Organized Crime* (15) 2012, afl. 2-3, p. 111-129.

Van Teeffelen 2020
K. van Teeffelen, 'Opnieuw flink meer schade door phishing. Doen banken genoeg?', *Trouw* 21 april 2020, www.trouw.nl/binnenland/opnieuw-flink-meer-schade-door-phishing-doen-banken-genoeg~b64f36f0/.

Trottier 2012
D. Trottier, 'Interpersonal surveillance on social media', *Canadian Journal of Communication* (37) 2012, p. 319-332.

Urbanik & Roks 2020
M.M. Urbanik & R.A. Roks, '#GangstaLife: Fusing urban ethnography with netnography in gang studies', *Qualitative Sociology* 2020, p. 1-21.

Yar 2005
M. Yar, 'The novelty of "cybercrime". An assessment in light of routine activity theory', *European Journal of Criminology* (2) 2005, AFL. 4, p. 407-427.

doi: 10.5553/JV/016758502020046002004

Helpdeskfraude in Nederland

Jildau Borwell*

Helpdeskfraude (*tech support scam*) is een cybercrimevorm die in 2011 in Nederland opkwam. Vanwege de impact en het grote aantal slachtoffers is in 2018 gestart met een integrale aanpak om helpdeskfraude te bestrijden. Bij helpdeskfraude heeft een slachtoffer telefonisch contact met een oplichter die zich voordoet als medewerker van een software- of socialmediabedrijf. Dit contact komt op drie mogelijke manieren tot stand:

a. Het slachtoffer wordt gebeld over zogenaamde problemen (virussen of verlopen licenties) met diens computer.
b. Er verschijnt een schermvullende pop-up met een virusmelding op de pc van het slachtoffer met het verzoek een telefoonnummer te bellen.
c. Het slachtoffer zoekt een helpdesk van een software- of socialmediabedrijf en vindt een telefoonnummer op een nep-helpdeskwebsite van de oplichters, of dit telefoonnummer wordt per ongeluk doorgegeven door een legitiem bedrijf.

Daders van helpdeskfraude gebruiken 'social engineering', waarmee ze door misleiding toegang krijgen tot de systemen en vertrouwelijke gegevens van slachtoffers. De oplichters overtuigen slachtoffers ervan om via een *Remote Access Tool*[1] de besturing van de pc over te nemen (zodat computervredebreuk plaatsvindt), zogenaamd om de problemen op te lossen. Vervolgens wordt vaak toegang verkregen tot de online bankomgeving van het slachtoffer en wordt veel geld afgeschreven.

De oudere leeftijdsgroepen zijn onder slachtoffers van helpdeskfraude oververtegenwoordigd. Van de aangevers en melders tussen 2016 en 2019 is bijna de helft (46%) tussen de 60 en 79 jaar (N=4.184). Het aantal aangiftes

* J. Borwell MSc werkt binnen de politie als senior cybercrimeanalist bij het cybercrimeteam van de Eenheid Noord-Nederland. Vanuit een landelijke themaverdeling heeft zij zich gespecialiseerd in helpdeskfraude, waarbij zij onder andere de rapportages schreef waarop deze kadertekst gebaseerd is. Daarnaast doet zij vanuit het lectoraat Cybersafety van de NHL Stenden Hogeschool in Leeuwarden promotieonderzoek naar de impact van cybercrime op slachtoffers.

1 Het gaat hier meestal om legitieme software, die bijvoorbeeld vaak door ICT-afdelingen wordt gebruikt om de besturing van computers van medewerkers binnen het bedrijf over te nemen voor ondersteuning.

doi: 10.5553/JV/016758502020046002005

en meldingen van helpdeskfraude piekte in 2017, nam in 2018 af en in 2019 weer toe. In deze periode is echter een daling in gemelde schadebedragen te zien, met een totaal van tegen de € 5 miljoen in 2017, tegen de € 3 miljoen in 2018 en € 2,6 miljoen in 2019. De schade van slachtoffers wordt meestal niet vergoed. Naast financiële impact rapporteren slachtoffers bovendien psychologische, sociale en lichamelijke impact, zoals stress, slaapproblemen en verlies van vertrouwen in andere mensen.

Vanwege het grote aantal slachtoffers en de impact van helpdeskfraude geven politie, Openbaar Ministerie en partners prioriteit aan de bestrijding ervan. In maart 2018 tekenden vertegenwoordigers van publieke partijen en private partijen uit de telecom-, software- en financiële sector daartoe een intentieverklaring, waarmee het startsein werd gegeven voor de Brede Coalitie ter verstoring van Tech Support Scams in Nederland. Doordat de opsporing bij helpdeskfraude moeizaam is (daders bevinden zich veelal in India en gebruiken anonimiseringstactieken in hun communicatie en financiële infrastructuur), ligt de nadruk op preventieve en verstorende maatregelen. Deze maatregelen worden genomen op basis van een gezamenlijke intelligencepositie, waarmee een barrièremodel is opgesteld om het criminele bedrijfsproces te verstoren. De aanpak bestaat bijvoorbeeld uit mediacampagnes, blokkeren van gebruikte telefoonnummers, offline halen van websites, blokkeren van transacties en aanpassen van misbruikte functionaliteiten van RAT's.

Toen de coalitie startte, kwam de variant waarbij slachtoffers door de oplichters gebeld werden verreweg het meest voor. Sindsdien is de prevalentie hiervan sterk gedaald. In 2019 vond een verschuiving plaats naar de variant waarbij slachtoffers zelf een telefoonnummer van een helpdesk zochten en bij de oplichters uitkwamen. Hoewel onzeker is of de verschuiving het gevolg is van de maatregelen, illustreert deze dat politie en haar partners alert moeten blijven op daders en hun modus operandi. Criminele bedrijfsprocessen moeten blijvend worden gemonitord om tot een succesvolle aanpak te komen. Dat geldt temeer bij cybercrime, waarbij criminelen hun werkwijzen snel ontwikkelen, aanpassen en onderling delen.

doi: 10.5553/JV/016758502020046002005

Het verlies van geld, geluk en gezicht

Romance scams, datingfraude en 'sweetheart swindles'

Raoul Notté*

Onze samenleving is sterk gedigitaliseerd. Het internet is de arena waarin wij werken, onze financiën regelen, boodschappen doen, waar ons sociale leven plaatsvindt en we liefde zoeken.[1] Als gevolg van deze digitalisering is cybercriminaliteit in toenemende mate een probleem. De prevalentie van deze 'nieuwe' vormen van criminaliteit overstijgt inmiddels de 'traditionele' vormen van criminaliteit. Statistieken over de gehele wereld laten een vergelijkbaar beeld zien.
Onderzoek laat zien dat slachtoffers van cybercriminaliteit negatieve (financiële, psychologische en emotionele) gevolgen ondervinden (bijv. Cross e.a. 2016; Jansen & Leukfeldt 2018; Worsley e.a. 2017; Reyns & Randa 2015). Deze gevolgen worden geregeld versterkt door onbegrip voor het slachtoffer, gebrek aan ondersteuning (Worsley e.a. 2017; Cross e.a. 2016; Notté e.a. 2020) en onvoldoende kennis en mogelijkheden vanuit de politie en justitie om zaken succesvol aan te pakken (Leukfeldt e.a. 2013a; 2013b; 2018). Het bestaande slachtofferbeleid is gebaseerd op kennis over en onderzoek naar de ervaringen van slachtoffers van offline criminaliteit (zie bijv. Leukfeldt e.a. 2018). Het is van belang om meer kennis over deze vormen van slachtofferschap te genereren en te delen over de hele linie van wetenschap, beleid, opsporing, vervolging en ondersteuning.

* R.J. Notté MSc is als researcher/lecturer verbonden aan The Hague University of Applied Sciences (Faculteit IT & Design/Centre of Expertise Cyber Security). Hij is tevens promovendus bij het International Victimology Institute (INTERVICT) van Tilburg University.

1 Het CBS constateerde in 2013 al dat een op de drie vrijgezellen doet aan online dating en 14% van alle Nederlandse stellen elkaar kent via het internet, zie www.cbs.nl/nl-nl/nieuws/2014/25/steeds-vaker-relatie-via-internet.

doi: 10.5553/JV/016758502020046002006

Een eerste verkennend onderzoek[2] naar de gevolgen van cybercriminaliteit voor slachtoffers laat zien dat datingfraude of *romance scams*[3] zeer grote impact op slachtoffers hebben (Leukfeldt e.a. 2018; Notté e.a. 2020).
Dit artikel poogt inzicht te bieden in het nog vaak onbegrepen fenomeen van romance scams. Dit wordt gedaan door te kijken naar wat het inhoudt, hoe vaak het voorkomt en wat de impact ervan is. Hiervoor wordt gebruik gemaakt van beschikbare (inter)nationale data en onderzoeken over dit onderwerp. Ter illustratie zijn casussen en quotes van slachtoffers toegevoegd, opgedaan in interviews door de auteur van dit artikel. De aangehaalde citaten zijn afkomstig uit Leukfeldt e.a. 2018.

Wat zijn romance scams en hoe vaak komt zoiets voor?

Romance scams, datingfraude, 'sweetheart swindle' zijn alle benamingen voor dezelfde fraude. Het gaat om een emotioneel ingrijpende vorm van fraude waarbij de fraudeur, of scammer, het slachtoffer laat geloven dat hij sterke gevoelens voor het slachtoffer heeft. Het romantische aspect van deze vorm van fraude dient als het aas waar het slachtoffer mee wordt gelokt, voordat de dader overgaat op andere vormen van fraude, zoals voorschot- of identiteitsfraude.
Romance scams onderscheiden zich van andere vormen van fraude door in te spelen op het medeleven van mensen en de wens om liefgehad te worden. De romance scam bestond al in een predigitaal tijdperk: via contactadvertenties in de krant werden slachtoffers geworven. Door het internet is de schaal aanzienlijk toegenomen (Rege 2009), het biedt de mogelijkheid om informatie over het slachtoffer te vinden en een leugen te ensceneren via nepwebsites en profielen (Notté e.a. 2020). Dit laatste kan een effect creëren dat doet denken aan de Amerikaanse film *The Truman Show* (1998), waarin Jim Carrey als Truman Burbank zonder het te weten al zijn gehele leven de hoofdrol speelt in een realityshow.

2 Daarbij zijn vier slachtoffers van romance scams geïnterviewd en twee internationale wetenschappers die meerdere tientallen slachtoffers hebben gesproken, en is gesproken met vijf medewerkers van slachtofferhulporganisaties die slachtoffers en zogenaamde 'lotgenotengroepen' voor romance scams begeleiden.
3 Er zijn wereldwijd verschillende benamingen in omloop, in dit artikel zal de term 'romance scam' gebruikt worden om naar al deze zaken te verwijzen.

doi: 10.5553/JV/016758502020046002006

Onderzoeken (Rege 2009; Whitty 2013) laten zien hoe romance scams een vast proces volgen. De eerste fase is de constructie van een geloofwaardig nepprofiel dat niet van echt te onderscheiden is. Naast profielen op datingsites maken fraudeurs gebruik van nepprofielen van 'bekenden',[4] vervalste websites van bedrijven en andere organisaties.[5] In de tweede fase wordt contact met het slachtoffer gelegd, en worden een vertrouwensbasis en gevoelens van liefde gecreëerd. In de derde fase wordt om geld gevraagd via een tragisch narratief, zoals de diefstal van identiteitsdocumenten, plotselinge ziekte of een ernstig ongeluk. Wanneer de fraudeur succesvol is, zal dit verhaal zich verder ontspinnen en het slachtoffer meer geld overmaken. Dit proces zet zich voort totdat het geld op is of het slachtoffer stopt met betalen. Door de aanzienlijke tijd en aandacht die fraudeurs in scams stoppen,[6] hebben veel slachtoffers lange tijd niet door dat zij worden opgelicht (Rege 2009).

Casus 1: Sara (42), schade € 220.000

Via de datingapp Tinder ontmoet Sara een buitenlandse man, die een succesvol eigen bedrijf heeft. De twee hebben al gauw dagelijks contact en het slachtoffer ontwikkelt sterke romantische gevoelens na het delen van passies, angsten, pijn en liefde. Alle informatie die het slachtoffer krijgt over de man klopt wanneer ze dit online controleert. Wanneer de man in het buitenland wat problemen heeft met zijn bankpas, laat hij het slachtoffer inloggen op zijn (achteraf blijkt valse) bankrekening om van daar geld over te maken. Dit vergroot het vertrouwen van het slachtoffer. Ondertussen maken ze, na maandenlang intensief contact, plannen om samen een woning te zoeken als hij, na afloop van zijn project in het buitenland, terug in Nederland is. Wanneer de man in de problemen komt met justitie in het buitenland, maakt het slachtoffer geld over (ze heeft op zijn 'bankrekening' immers gezien dat hij kredietwaardig is) en stopt hier pas mee wanneer alles op is en haar baas haar een lening weigert. Door een web van leugens, liefde en financiële afhankelijkheid van de investeringen die ze in de man heeft gedaan,

4 Zoals gefingeerde familie, vrienden, collega's en andere 'stakeholders' in het fraudeverhaal.
5 Zoals bijvoorbeeld een volledig geënsceneerde maar functionerende internetbankieren-omgeving, inclusief inlogscherm en saldo- en overschrijvingenoverzicht.
6 Het is niet ongewoon om maandenlang dagelijks (telefonisch) contact te hebben voordat er om geld wordt verzocht.

doi: 10.5553/JV/016758502020046002006

verliest ze uiteindelijk meer dan € 200.000 en haar huis. Sara woont tijdelijk op een camping in het Oosten van het land.
(Leukfeldt e.a. 2018)

Whitty (2013) komt tot een uitgebreidere beschrijving van het proces (zie figuur 1), waarbij een aanzienlijke tijd besteed wordt aan fase 2 en 3 om vertrouwen te creëren. In de 'grooming'-fase wordt het slachtoffer het hof gemaakt, waarbij niet alleen vertrouwen, maar ook sterke emoties van verliefdheid worden opgewekt:

> 'Ik kreeg een gigantische bos met rozen, bonbons (…) dan gaan ze je inpakken, je krijgt continu berichten: "Je bent de vrouw van mijn leven." Hij zegt eigenlijk precies wat je wilt horen. Je wordt gewoon hartstikke verliefd op zo'n man.' (slachtoffer, in: Leukfeldt e.a. 2018)

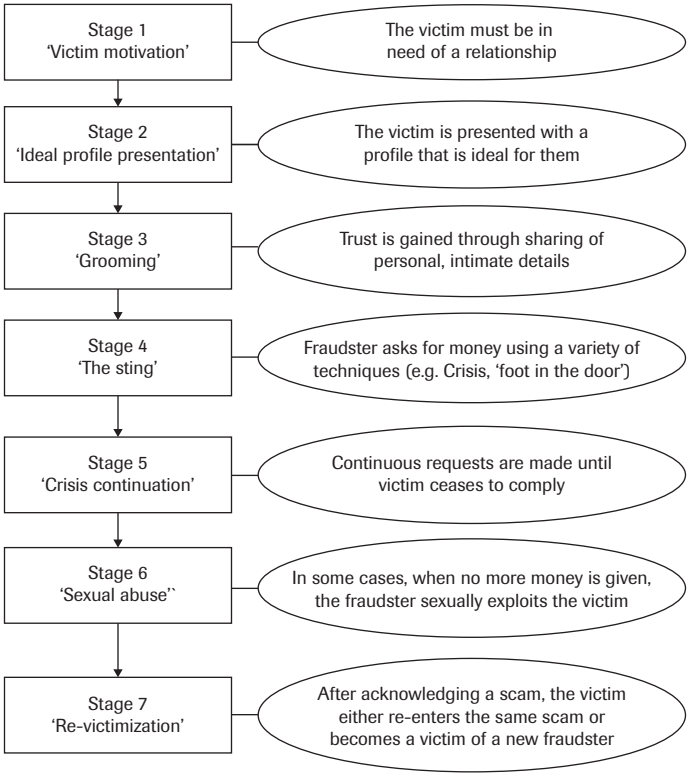
Wanneer er voldoende fundament is gelegd, wordt overgegaan op 'the sting': het slachtoffer wordt geconfronteerd met een crisissituatie die zonder het slachtoffer niet opgelost kan worden. Dit werkt tweeledig. Enerzijds geven slachtoffers aan vereerd te zijn om de persoon te zijn die door 'hun geliefde' benaderd wordt. Anderzijds worden slachtoffers mede-eigenaar gemaakt van het probleem dat de fraudeur schetst (Notté e.a. 2020). De fraudeur oefent grote druk uit op het slachtoffer om geld over te maken. Deze cyclus herhaalt zich totdat het slachtoffer weigert nog meer geld over te maken.
Doordat slachtoffers midden in de leugen leven en gevangen zijn in de spanning stopt het betalen pas vaak als al het geld op is. Dit wordt mede veroorzaakt doordat slachtoffers 'pot committed' zijn, stoppen met betalen betekent het verlies van alles wat geïnvesteerd is:

> '[Ik zat] er middenin en dacht als ik niet stop ben ik mijn geld kwijt (…) Ik kon de één procent hoop niet opgeven.' (slachtoffer, in: Leukfeldt e.a. 2018)

In sommige gevallen worden slachtoffers na confrontatie met de dader op nieuwe manieren tot slachtoffer gemaakt, via identiteitsfraude, door afpersing met naaktbeelden, of zij worden benaderd door fraudeurs die zich bijvoorbeeld voordoen als de politie die persoonsinformatie of geld van het slachtoffer nodig heeft om de daders van de initiële oplichting te pakken (Whitty 2013).

doi: 10.5553/JV/016758502020046002006

Figuur 1 De zeven fasen van romance scam



Bron: Whitty 2013

Een volledig beeld van de prevalentie van romance scams is lastig te schetsen als gevolg van de lage aangiftebereidheid (Van de Weijer e.a. 2019; Hesseling & Versteegh 2016; Domenie e.a. 2012) en doordat politie en justitie niet per definitie als aanspreekpunt voor cybercrimes worden gezien (Domenie e.a. 2012; Jansen & Leukfeldt 2018; Jong e.a. 2018). Ook gevoelens van schaamte en eigen verantwoordelijkheid bij slachtoffers spelen een rol (King & Thomas 2009).
Voor data zijn we daarom afhankelijk van de Fraudehelpdesk, waar de meeste meldingen binnenkomen. In de afgelopen vijf jaar ging het om 700 meldingen met financiële schade. In totaal is er melding gemaakt

doi: 10.5553/JV/016758502020046002006

Tabel 1 Romance-scammeldingen en slachtoffers bij Fraudehelpdesk

Jaar	2017	2018	2019
Meldingen	313	412	639
Slachtoffers (financieel)	134	180	412
Totale schade	€ 1.651.769	€ 3.259.507	€ 3.744.300
Gemiddelde schade	€ 12.326	€ 18.108	€ 16.469

van € 12,5 miljoen, een gemiddelde van € 17.850 per persoon (Fraudehelpdesk 2020; zie tabel 1).

Een uitvraag via het EUCPN leert dat in Europese landen geen aangiftes van romance scams worden bijgehouden.[7] De Deense politie weet via toegekende tags te herleiden dat er in het laatste jaar 272 gevallen zijn gemeld.
Online zijn meer data beschikbaar over romance scams. De Verenigde Staten en met name Australië houden een vrij volledige registratie bij. In 2018 werden meer dan 378.000 meldingen gedaan in Australië met een totale schade van A$ 489 miljoen, een toename van 44% ten opzichte van het jaar ervoor. Romance scams hebben aldaar de op een na grootste financiële impact met een schadebedrag van A$ 60 miljoen (ACCC 2019). In de Australische registratie is te zien dat met name Instagram en Tinder in deze periode veel gebruikt zijn om contact te leggen, betalingen zijn vooral gedaan via de bank, bedrijven als Western Union, bitcoin of iTunes cards. Voorts signaleren zij in toenemende mate het gebruik van sextortion[8] in romance scams (ACCC 2019). Statistieken van de FBI (IC3) laten een vergelijkbaar beeld zien: romance scams[9] als de vorm van fraude met de een na grootste financiële impact, met meer dan 18.000 slachtoffers en een totaal schadebe-

7 European Crime Prevention Network; het netwerk wil het lokale, nationale en Europese niveau verbinden en de kennis en praktijken inzake criminaliteitspreventie in alle EU-lidstaten bevorderen en is in 2001 bij besluit van de Raad van de Europese Unie opgericht. Er is een uitvraag gedaan onder alle Europese lidstaten. Een reactie van Oostenrijk, Duitsland, Frankrijk, Hongarije, Luxemburg, Portugal en Roemenië leert dat deze landen geen specifieke registratie van romance scams of datingfraude bijhouden.

8 Waarbij het slachtoffer wordt afgeperst op basis van het (dreigen met) verspreiden van naaktfoto's of -video's.

9 Het Internet Crime Complaint Center registreert deze als 'confidence and romance fraud'.

doi: 10.5553/JV/016758502020046002006

drag van meer dan $ 362 miljoen in 2018. Een toename van meer dan 70% ten opzichte van het voorgaande jaar (IC3 2019).
Het is eveneens interessant te kijken naar de achtergrond van slachtoffers. Data uit Australië laten zien dat zowel mannen als vrouwen slachtoffer worden van romance scams, vrouwen rapporteren daar over het algemeen meer absolute financiële schade (ACCC 2019). Dit komt overeen met Brits onderzoek onder 200 slachtoffers van romance scams (Whitty 2018), waarbij 60% van de vrouwen slachtoffer is ten opzichte van 40% van de mannen. Slachtofferschap in dit onderzoek ligt aanzienlijk hoger (63%) in de leeftijdsgroep tussen 35-54 jaar dan bij jongeren (21%) en ouderen (16%). Slachtoffers in het verkennende Nederlandse onderzoek waren eveneens hoofdzakelijk (driekwart) vrouw en tussen de 35 en 55 jaar (Leukfeldt e.a. 2018). Over het algemeen zijn slachtoffers hoger opgeleid en qua karaktereigenschappen scoren zij hoger op impulsiviteit en lager op zelfcontrole (Whitty 2018).

Casus 2: Jeanine (51), schade € 67.000

Jeanine ontmoet een man uit de VS op Tinder. Zij is zelf net gescheiden van haar man en de man uit Amerika heeft onlangs zijn vrouw verloren. In de periode van december tot juni hebben de twee innig contact. Ze delen angsten, liefde en passie. De man werkt voor een bedrijf dat containerschepen vervoert. Hij toont foto's van de schepen, de officiële documenten lijken te kloppen, en de man houdt rekening met het tijdsverschil dat er zou moeten zijn tussen Nederland en de landen waar hij zegt te bivakkeren. De twee ontwikkelen een romantische relatie waarin plannen ontstaan om na verloop van tijd samen naar een nieuwe woning te gaan zoeken. Hij toont haar een (nep)banksite om haar vertrouwen te wekken met betrekking tot zijn geld en zijn bedrijf. Zij wisselt voor hem (nep)cheques in die op zijn (nep)rekening verschijnen. Dan komt hij in de problemen met de douane, waardoor een van zijn containerschepen vastligt en zijn project ernstige vertraging oploopt. Ook hiervan zijn officieel lijkende douanepapieren. Op dit moment heeft het slachtoffer contact met een (geënsceneerde) koerier, een VN-diplomaat, een bank, douane en het Tinder-profiel. Het slachtoffer ontwikkelt het gevoel dat zijn probleem ondertussen ook haar probleem is. Om te voorkomen dat hij wordt opgepakt, springt zij bij met een eerste betaling, zij heeft zijn financiële middelen gezien en gaat ervan uit dat zij uiteindelijk haar betaling terugontvangt. Het slachtoffer geeft vanaf dit moment aan

doi: 10.5553/JV/016758502020046002006

gehersenspoeld te zijn en er geld in te hebben zitten ('pot committed'), waardoor ze steeds verder gaat in zijn (uiteindelijke) leugens en meer geld overmaakt. Op het moment dat haar geld op is, leent ze van haar moeder en uiteindelijk van haar baas; die vraagt haar waar het geld voor is, en geeft haar aan dat dit waarschijnlijk een oplichter betreft.
(Leukfeldt e.a. 2018)

Romance-scamslachtoffers staan er vaak alleen voor

De belangrijkste behoefte van slachtoffers is zorgen dat de scam stopt. Slachtoffers behoeven hulp om in te zien dat ze slachtoffer zijn van fraude middels een duidelijk verhaal over wat ze is overkomen:[10]

> '[Ik moet] weten hoe het zit, of je inderdaad slachtoffer bent van fraude. Zonder een heel verhaal en oordeel eromheen.' (slachtoffer, in: Leukfeldt e.a. 2018)

Door hun vindbaarheid, hun specifieke kennis over dit fenomeen en hun begrip van de situatie spelen organisaties als de Fraudehelpdesk en Slachtofferhulp Nederland een belangrijke rol hierin (Leukfeldt e.a. 2018). Voor slachtoffers is het belangrijk erkend te worden als slachtoffer en hun verhaal te kunnen doen. Dit is het startpunt voor verwerking van slachtofferschap. Deze erkenning vinden slachtoffers vaak niet bij de politie, waar zij weggestuurd worden en geen aangifte kunnen doen (Leukfeldt e.a. 2018). Uit eerder onderzoek blijkt dat dit te wijten is aan gebrek aan kennis bij politiemedewerkers (Leukfeldt e.a. 2013b). Dit is in lijn met buitenlandse studies, waaruit blijkt dat de politie fraudedelicten onvoldoende serieus neemt (Bossler e.a. 2019). Als resultaat wordt geen aangifte opgenomen, vindt er geen registratie plaats van criminaliteit en voelen slachtoffers zich niet serieus genomen (Leukfeldt e.a. 2018; 2020; Cross e.a. 2016).
De politie benadrukt in haar afwijzing geregeld dat het slachtoffer zelf verantwoordelijk is, doordat het uit eigen beweging of 'vrijwillig' geld heeft overgemaakt (Leukfeldt e.a. 2018). De directe sociale omgeving

10 Internationale experts op het onderwerp onderschrijven dit belang: 'The biggest challenge is, to convince them that it is real (…) [because] once you are engaged, financially and emotionally, it is hard to quit' (onderzoeker, in: Leukfeldt e.a. 2018).

doi: 10.5553/JV/016758502020046002006

houdt slachtoffers ook verantwoordelijk,[11] iets wat in de literatuur wordt omschreven als *victim blaming* (zie bijv. Cross 2016). De noodzakelijkheid van (een mate van) coöperatie van het slachtoffer voor het slagen van de fraude maakt het slachtoffer gevoelsmatig medeverantwoordelijk (Titus & Gover 2001). De dominantie van dit idee van eigen verantwoordelijkheid wordt geïllustreerd door de wijze waarop het slachtoffer ook zichzelf de schuld geeft:

> 'Achteraf neem ik mezelf dat heel kwalijk, ik ben mijzelf hierdoor minder waard gaan vinden (…) hoe heb ik zo stom kunnen zijn?' (slachtoffer, in: Leukfeldt e.a. 2018)

Uit schaamte lopen slachtoffers het risico zichzelf te isoleren en zich terug te trekken uit (delen van) de samenleving:

> '[Ik heb het] verzwegen voor mijn omgeving, hoongelach, dat krijg je gewoon (…) Je kunt ook een voorwerp van spot worden, dat wil je niet.' (slachtoffer, in: Leukfeldt e.a. 2018)

Dit isolement maakt slachtoffers extra kwetsbaar.

Een financiële strop voor slachtoffers, familie en vrienden

De gevolgen die slachtoffers van romance scams melden, variëren van het verlies van enkele honderden euro's tot bedragen van honderdduizenden euro's. De uiteindelijke impact die deze financiële gevolgen hebben op het leven van slachtoffers verschilt door de financiële situatie en de sociale omgeving van slachtoffers (Notté e.a. 2020; Cross e.a. 2016). Dit varieert van een fikse tegenvaller tot het verlies van alles wat iemand had, schulden en verlies van huisvesting:

> 'Ik heb niks meer! Ik heb mijn laatste cent overgemaakt! (…) In een paar weken tijd ben je alles kwijt wat je in al die jaren hebt opgebouwd.' (slachtoffer, in: Leukfeldt e.a. 2018)

11 Slachtoffers worden niet zelden door hun eigen sociale omgeving veroordeeld, omdat er ook vaak geld van anderen is verloren en de financiële schade niet alleen het slachtoffer raakt.

doi: 10.5553/JV/016758502020046002006

De reden dat de schade zo groot is, lijkt te zijn dat de fraude lang aanhoudt. Zo verliezen veel slachtoffers ook geld dat zij hebben geleend (Leukfeldt e.a. 2018; Cross e.a. 2016).
Financiële schade kan langdurig aanhouden voor slachtoffers die door de emotionele impact van de fraude niet langer kunnen werken of ziek worden (Leukfeldt e.a. 2018; Cross e.a. 2016). Door het ontbreken van een aangifte, opsporingsonderzoek en daarmee veroordeling van een dader is het onmogelijk voor slachtoffers om een financiële schadevergoeding te ontvangen (Notté e.a. 2020). Banken en andere financiële instellingen kunnen weinig voor de slachtoffers betekenen. Hier is uiteraard, door de vaak grote financiële schade, wel veel behoefte aan. Slachtoffers zijn nu puur aangewezen op financiële hulp vanuit de omgeving om te voorzien in hun levensonderhoud en onderdak (Leukfeldt e.a. 2018).

Een financiële en emotionele 'double hit'

De financiële schade van romance scams is evident, empirische studies tonen ook emotionele en psychologische gevolgen aan (Leukfeldt e.a. 2018; Button e.a. 2009; Kerr e.a. 2013; Richards & Cross 2018; Buchanan & Whitty 2014). Deze gevolgen hangen samen met de weerbaarheid van slachtoffers (Button e.a. 2009; Cross e.a. 2016). De combinatie van financiële en emotionele gevolgen wordt een *double hit* genoemd (Whitty & Buchanan, 2015).
De emotionele impact van romance scams is groot. In Australisch onderzoek worden ze als '*devastating*' omschreven (Cross e.a. 2016), in Nederlandse studies spreken slachtoffers en hulpverleners eveneens over depressies, PTSS en suïcidaliteit (Leukfeldt e.a. 2018). Mildere gevolgen van romance scams zijn een verlies van vertrouwen, schuldgevoel en schaamte, woede en frustratie, stress, angst, verdriet en teleurstelling (Leukfeldt e.a. 2020; Notté e.a. 2020; Cross e.a. 2016), en deze impact kan zich gedurende een lange periode doen gelden (Cross e.a. 2016). Slachtoffers spreken ook over een fysieke impact, zoals slapeloosheid, misselijkheid en gewichtsverlies door de grote emotionele impact (Cross e.a. 2016; Leukfeldt e.a. 2018).
De ervaring kan voor slachtoffers dermate traumatisch zijn dat zij de wijze waarop het slachtoffer zichzelf en de wereld ziet fundamenteel verandert. De basisassumpties over het leven lijken aangetast, of

doi: 10.5553/JV/016758502020046002006

shattered,[12] waardoor het slachtoffer niet meer gelooft in een goede wereld en het gevoel voor eigenwaarde is verdwenen:

> 'Ik durf mijn gevoelens niet meer te uiten, ik durf niets meer te zeggen, ik durf niet meer voor mezelf op te komen.' (slachtoffer, in: Leukfeldt e.a. 2018)

De aantasting van deze basisassumpties bij getraumatiseerde slachtoffers is problematisch, omdat deze een negatieve invloed hebben op het verloop van het verdere leven en het succes daarin (Janoff-Bulman 1992). Het verlies van vertrouwen in zichzelf en de wereld om het slachtoffer heen heeft een sterke negatieve invloed op het maken van plannen voor de toekomst, het doen van investeringen en het aangaan van connecties. Het vertrouwen dat hiervoor nodig is, lijkt door het slachtofferschap te zijn verdwenen:

> 'Vreemde mensen die hou ik op afstand. Je vertrouwen is weg. Je moet eerst opbouwen en daarna kan ik je vertrouwen.' (slachtoffer, in: Leukfeldt e.a. 2018)

Conclusie en discussie

De afgelopen jaren is er een toename te zien in romance scams, zowel in het aantal slachtoffers als wat betreft de financiële schade die wordt geleden. Vaak bestaan er geen mogelijkheden voor financiële compensatie. De grootste groep slachtoffers lijkt over het algemeen hoger opgeleid en van middelbare leeftijd.
Grote financiële verliezen gaan gepaard met gevoelens van schaamte, schuld en het verdriet om het verlies van een (ingebeelde) liefdesrelatie. Deze ingrijpende gevolgen worden versterkt als blijkt dat de politie niet actief op zoek gaat naar de dader en het slachtoffer zelf verantwoordelijk gehouden wordt.
Eerder slachtofferonderzoek laat zien dat een gebrek aan deze sociale ondersteuning, het ontbreken van een opsporingsonderzoek en geen mogelijkheden voor compensatie van de geleden schade allemaal bij-

12 Zoals voor het eerst beschreven in de *shattered assumptions theory* van Janoff-Bulman (1992).

doi: 10.5553/JV/016758502020046002006

dragen aan het vergroten van de negatieve impact op het slachtoffer (Shapland e.a. 1985).
In Nederlands onderzoek wordt door twee slachtoffers zelfs de parallel getrokken met seksueel misbruik en mishandeling:

> 'Ik ben fysiek nooit verkracht, toch had ik het gevoel dat ik verkracht was.' (slachtoffer, in: Leukfeldt e.a. 2018)

In Australisch onderzoek vergeleken slachtoffers eveneens de impact van romance scams met verkrachting (Cross 2016). Gelet op de impact van romance scams hebben slachtoffers meer ondersteuning en empathie nodig om te voorkomen dat zij geïsoleerd raken en om te leren omgaan met de gevolgen van een romance scam. Meer kennis is nodig om burgers weerbaarder te maken en de ondersteuning van slachtoffers te verbeteren. Registraties moeten worden verbeterd om de aard en omvang beter in kaart te brengen. Internationale samenwerking lijkt noodzakelijk om opsporing en vervolging mogelijk te maken, datingapps en sociale media aan te spreken op hun verantwoordelijkheden als platform en meer begrip en erkenning voor slachtoffers te creëren. Om tot een betere voorlichting en preventie te komen is meer (kwantitatief) onderzoek nodig naar de kenmerken van slachtoffers.

Literatuur

ACCC 2019
ACCC, *Targeting scams: Report of the ACCC on scams activity 2018*, Canberra: Australian Competition and Consumer Commission 2019.

Bossler e.a. 2019
A. Bossler, T.J. Holt, C. Cross & G.W. Burruss, 'Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness', *Security Journal* 2019, doi: 10.1057/s41284-019-00187-5.

doi: 10.5553/JV/016758502020046002006

Buchanan & Whitty 2014
M. Buchanan & M.T. Whitty, 'The online dating romance scam: Causes and consequences of victimhood', *Health, Risk & Society* (20) 2014, afl. 3, p. 261-283.

Button e.a. 2009
M. Button, C. Lewis & J. Tapley, *A better deal for fraud victims: Research into victims' needs and experiences*, Londen: National Fraud Authority 2009.

Cross 2016
C.A. Cross, '"They're very lonely": Understanding the fraud victimisation of seniors', *International Journal for Crime, Justice and Social Democracy* 2016, p. 60-75.

Cross e.a. 2016
C.A. Cross, K.M. Richards & R. Smith, 'The reporting experiences and support needs of victims of online fraud', *Trends and Issues in Crime and Criminal Justice* 2016, p. 1-14.

Domenie e.a. 2012
M.M.L. Domenie, E.R. Leukfeldt, J. van Wilsem & W.P. Stol, 'Slachtofferschap van cybercrime in kaart gebracht. Hacken, e-fraude, identiteitsfraude en voorschotfraude', *Tijdschrift voor Veiligheid* (11) 2012, afl. 2, p. 47-56.

Fraudehelpdesk 2020
Fraudehelpdesk, *Fraude in het afgelopen decennium*, www.fraudehelpdesk.nl/thema/fraude-in-het-afgelopen-decennium/.

Hesseling & Versteegh 2016
R. Hesseling & P. Versteegh, 'Politiecijfers: meten is weten, maar doe vooral ook meer met ongeveer', in: E. Devroe, E. De Raedt, H. Elffers & D. Schaap (red.), *Meten is weten*, Apeldoorn: Maklu 2016, p. 25-42.

IC3 2019
IC3, *2018 Internet crime report*, Washington: Internet Crime Complaint Center, Federal Bureau of Investigation 2019.

Janoff-Bulman 1992
R. Janoff-Bulman, *Shattered assumptions*, New York: Free Press 1992.

Jansen & Leukfeldt 2018
J. Jansen & E.R. Leukfeldt, 'Coping with cybercrime victimization: An exploratory study into impact and change', *Journal of Qualitative Criminal Justice & Criminology* (2) 2018, afl. 2, p. 205-228.

Jong e.a. 2018
L. Jong, E.R. Leukfeldt & S. van de Weijer, 'Aangiftebereidheid na slachtofferschap van cybercrime', Tijdschrift voor Veiligheid. 17(1-2) 2018, p. 66-78.

doi: 10.5553/JV/016758502020046002006

Kerr e.a. 2013
J. Kerr, R. Owen, C. McNaughton-Nicolls & M. Button, *Research on sentencing online fraud offences*, Londen: Sentencing Council 2013.

King & Thomas 2009
A. King & J. Thomas, 'You can't cheat an honest man: Making ($$$ and) sense of the Nigerian e-mail scams', in: F. Schmalleger & M. Pittaro (red.), *Crimes of the internet*, Upper Saddle River, NJ: Pearson Prentice Hall 2009, p. 206-224.

Leukfeldt e.a. 2013a
E.R. Leukfeldt, S. Veenstra, M. Domenie & W.P. Stol, *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime*, De Bilt/Leeuwarden: PAC/NHL 2013.

Leukfeldt e.a. 2013b
E.R. Leukfeldt, S. Veenstra, M. Domenie & W.P. Stol, 'High volume cyber crime and the organization of the police. The results of two empirical studies in the Netherlands', *International Journal of Cyber Criminology* (7) 2013, afl. 1, p. 1-17.

Leukfeldt e.a. 2018
E.R. Leukfeldt, R.J. Notté & M. Malsch, *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*, Den Haag: WODC 2018.

Leukfeldt e.a. 2020
E.R. Leukfeldt, R.J. Notté & M. Malsch, 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes', *Victims & Offenders* (15) 2020, afl. 1, p. 60-77, doi: 10.1080/15564886.2019.1672229.

Notté e.a. 2020
R.J. Notté, E.R. Leukfeldt & M. Malsch, 'Double, triple or quadruple hits? Exploring the impact of cybercrime on victims', *International Review of Victimology* (in review).

Rege 2009
A. Rege, 'What's love got to do with it? Exploring online dating scams and identity fraud', *International Journal of Cyber Criminology* (3) 2009, afl. 2, p. 494-512.

Reyns & Randa 2015
B. Reyns & R. Randa, 'Victim reporting behaviors following identity theft victimization: Results from the National Crime Victimization Survey', *Crime & Delinquency* (63) 2015, doi: 10.1177/0011128715620428.

doi: 10.5553/JV/016758502020046002006

Richards & Cross 2018
K.M. Richards & C.A. Cross, 'Online fraud victims' experiences of participating in qualitative interviews', *Criminal Justice Studies* 2018, p. 95-111.
Shapland e.a. 1985
J. Shapland, J. Willmore & P. Duff, *Victims in the criminal justice system*, Aldershot: Gower Publishing 1985.
Titus & Gover 2001
R.M. Titus & A.R. Gover, 'Personal fraud: The victims and the scams', *Crime Prevention Studies* (12) 2001, p. 133-151.
Van de Weijer e.a. 2019
S.G.A. van de Weijer, R. Leukfeldt & W. Bernasco, 'Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking', *European Journal of Criminology* (16) 2019, afl. 4, p. 486-508.
Whitty 2013
M.T. Whitty, 'The Scammers Persuasive Techniques Model: Development of a stage model to explain the online dating romance scam', *The British Journal of Criminology* (53) 2013, afl. 4, p. 665-684.
Whitty 2018
M.T. Whitty, 'Do you love me? Psychological characteristics of romance scam victims', *Cyberpsychology, Behavior, and Social Networking* 2018, p. 105-109.
Whitty & Buchanan 2015
M. Whitty & T. Buchanan, 'The online dating romance scam: The psychological impact on victims – both financial and non-financial', *Criminology and Criminal Justice* (16) 2015, doi: 10.1177/1748895815603773.
Worsley e.a. 2017
D.J. Worsley, J. Wheatcroft, E. Short & R. Corcoran, 'Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses', *SAGE Open* (7) 2017, doi: 10.1177/2158244017710292.

doi: 10.5553/JV/016758502020046002006

Wie krijgt zijn geld terug?

Acties van slachtoffers tot schadevergoeding bij bankfraude

Johan van Wilsem, Take Sipma en Esther Meijer-van Leijsen*

Bankfraude is een ernstig maatschappelijk probleem. Regelmatig klinken er waarschuwingen voor oplichtingstrucs waarmee slachtoffers via manipulatieve communicatie geld afhandig wordt gemaakt. Zo kwam recent in het nieuws oplichting via misleidende WhatsApp-berichtjes die zogenaamd van een familielid afkomstig waren. Ook via andere vormen van identiteitsfraude, zoals diefstal van een username en password, kunnen illegaal bedragen van de bankrekening van een slachtoffer worden afgeschreven. Grote hoeveelheden gebruikersnamen en wachtwoorden zijn in bulk verkrijgbaar op illegale markten en vormen tegenwoordig populaire illegale handelswaar (Holt & Lampke 2010). Persoonsinformatie is een *hot product* geworden voor fraudeurs (Pratt e.a. 2010). Bankfraude wordt, in al haar verschijningsvormen, niet apart geregistreerd, maar in slachtofferenquêtes wordt wel gevraagd naar verschijnselen die er deel van uitmaken, zoals ongeautoriseerde bankafschrijvingen en identiteitsdiefstal. Uit die informatie wordt duidelijk dat, op jaarbasis, enkele procenten van de volwassen bevolking met deze fenomenen te maken hebben (Paulissen & Van Wilsem 2015; Sipma & Van Leijsen 2019), en in de Verenigde Staten zelfs tot 10% (Langton 2019). Bovendien zijn veel mensen bezorgd om slachtoffer te worden van identiteitsdiefstal, diefstal van bankpas of online bankfraude, namelijk 70% van de Europese bevolking (Eurobarometer 2018). In het meest recente supplement identiteitsdiefstal van de *National Crime Victimization Survey* (2016) rapporteerde Langton (2019) dat het gemiddelde aanvankelijke financiële verlies voor identiteitsfraudeslachtoffers (bij ontdekking) $ 850 was (mediaan $ 300). Voor Nederland constateerden Paulissen en Van

* Dr. J. van Wilsem is strateeg-onderzoeker bij de Algemene Rekenkamer. Dr. T. Sipma is als onderzoeker verbonden aan het WODC. Dr. E. Meijer-van Leijsen is als onderzoeker werkzaam bij de Algemene Rekenkamer.

doi: 10.5553/JV/016758502020046002007

Wilsem (2015) dat het gemiddelde verlies voor slachtoffers, voor de periode 2010-2012, € 375 bedroeg (mediaan € 100).
Slachtoffers kunnen proberen de ondervonden financiële schade vergoed te krijgen. Zowel in de Verenigde Staten als in Nederland lukt dit meestal. Volgens Langton (2019) bleef niettemin 12% van de Amerikaanse slachtoffers met restschade zitten na pogingen tot schadevergoeding. Van hen ging het bij 15% om verliezen van $ 1.000 of meer. Sipma en Van Leijsen (2019) melden dat in Nederland bijna 20% van de slachtoffers van identiteitsfraude door onterechte bankafschrijving geen schadevergoeding ontvangt. De mediane schade die deze groep uiteindelijk leed, was € 99. In een beperkt aantal gevallen is het geleden verlies hoog – meer dan € 1.000 – en in uitzonderlijke gevallen meer dan € 10.000.
De omvang van de schadevergoeding voor slachtoffers bepaalt de uiteindelijke financiële gevolgen die zij ondervinden. In aanvulling daarop is de verwachting dat de *sociale* weerslag van identiteitsfraude meestal ernstiger is naarmate de schadevergoeding geringer is. In een grootschalig onderzoek onder Amerikaanse slachtoffers van identiteitsdiefstal geven Golladay en Holtfreter (2017) aan dat de emotionele gevolgen, zoals gevoelens van depressie, woede, verwarring en gebrek aan vertrouwen, groter zijn naarmate het bedrag dat zij kwijt zijn hoger is – na correctie voor een groot aantal alternatieve variabelen, zoals eerder slachtofferschap en sociaal-demografische kenmerken. Ook in andere studies worden de sociale gevolgen van slachtofferschap van bankfraude en identiteitsfraude onder de aandacht gebracht (Button e.a. 2014; Leukfeldt e.a. 2018; Randa & Reyns 2019; Sipma & Van Leijsen 2019). Het beperken van de financiële gevolgen hiervan via schadevergoeding lijkt dan ook een tweesnijdend zwaard: het beperkt zowel de financiële als de sociale schade onder slachtoffers. Als zodanig is het belangrijk om meer kennis te krijgen over de determinanten van schadevergoeding. In dit artikel richten wij ons daarop. Daarbij kijken we ook naar een stap die vaak voorafgaat aan de schadevergoeding: de beslissing om het incident te melden bij de formele instanties. Wat bepaalt of slachtoffers dat doen?

doi: 10.5553/JV/016758502020046002007

Contact opnemen met instanties

Naar het wel of niet melden van een misdrijf bij de politie is veel criminologisch onderzoek verricht (zie voor een overzichtsstudie Xie & Baumer 2019), maar niet zozeer op het gebied van fraude (zie echter Copes e.a. 2001; Schoepfer & Piquero 2009). In dit artikel over onterechte bankafschrijvingen kijken we echter niet alleen naar het wel of niet melden van een incident bij de politie, maar – gezien het financiële belang ervan – ook naar het melden bij de bank. Het melden van het incident zien we daarbij als een keuze door de burger om actie te ondernemen. Over dit bredere fenomeen heeft de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) een belangwekkende studie gepubliceerd, *Weten is nog geen doen* (Bovens e.a. 2017). De vruchten die burgers kunnen plukken van beleid, of de sancties die ze riskeren, hangen vaak samen met hun *doe-vermogen*, hun vermogen om in actie te komen. Belastingaangifte doen, tijdig betalen van verkeersboetes en doorgeven van gegevens om in aanmerking te komen voor toeslagen zijn voorbeelden hiervan. Een belangrijk thema in *Weten is nog geen doen* (hierna: Wingd) is dat het doe-vermogen ongelijk verdeeld is tussen burgers – en daarmee ook de verdeling van gewenste en ongewenste uitkomsten die zij ervaren. Als ze afzien van actie, hebben ze daar vaak last van. De mate waarin burgers behept zijn met doe-vermogen hangt samen met uiteenlopende kenmerken. In Wingd wordt de link gelegd met opleidingsniveau, maar wordt tegelijkertijd met klem benadrukt dat er ook onder hoogopgeleiden mensen zijn met een laag doe-vermogen, en dat er onder lageropgeleiden ook veel mensen zijn met een hoog doe-vermogen. Niettemin kunnen we nagaan in hoeverre onder lageropgeleiden minder vaak actie wordt ondernomen, in dit geval naar aanleiding van een indicatie van identiteitsfraude – een onterechte afschrijving van de bankrekening.
Een andere link die in Wingd wordt gelegd in relatie tot doe-vermogen heeft betrekking op persoonlijkheidskenmerken, met name het vermogen om vooruit te kijken en het langetermijnbelang van beslissingen te zien. Indien dit vermogen laag is, vindt men het moeilijker te anticiperen op doelen die verder verwijderd zijn in de tijd en focust men meer op kortetermijndoelen. Dit idee is ook toegepast in de slachtofferliteratuur, maar dan vooral op de vraag wie er slachtoffer wordt (Holt e.a. 2018; Schreck 1999; Sipma & Van Leijsen 2019; Van

doi: 10.5553/JV/016758502020046002007

Wilsem 2013) en minder op hoe slachtoffers reageren na slachtofferschap (maar zie Turanovic & Pratt, 2014; Van Wilsem 2016). Wij stellen in dit artikel dat lage zelfcontrole ook verband kan houden met het melden van een incident bij slachtoffers van identiteitsfraude, vanwege de link met een lager doe-vermogen. Een belangrijk doel om te melden is tenslotte om het gestolen geld terug te krijgen – een langetermijndoelstelling waarvoor (soms aanzienlijk) doorzettingsvermogen nodig is. We verwachten dat slachtoffers met lage zelfcontrole minder naar dit langetermijndoel zullen handelen. Uiteindelijk zullen ze daardoor minder vaak schadevergoeding ontvangen en zal voor deze groep slachtoffers de financiële schade groter zijn. Mogelijk speelt voor deze groep slachtoffers ook dat zij meer aansprakelijk worden gesteld voor de geleden schade door hun bank. Banken zijn mogelijk minder geneigd om terug te betalen als ze van mening zijn dat de onterechte bankafschrijving verband houdt met impulsieve online besluitvorming door het slachtoffer. De exacte redenen voor slachtoffers om niet te melden of voor banken om niet terug te betalen staan niet geregistreerd in de gegevens die we voor dit onderzoek analyseren. We kunnen echter wel onderzoeken of lage zelfcontrole gerelateerd is aan het melden van het incident bij de bank en het wel of niet ontvangen van schadevergoeding.

Enquêtedata: een nadere analyse

In dit artikel gebruiken we gegevens uit het LISS-panel, een representatieve enquête onder huishoudens die in 2007 is gestart door onderzoeksbureau CentERdata. Voor het huidige onderzoek hebben we gegevens gebruikt uit vijf edities van LISS-paneldata, verzameld tussen februari 2010 en februari 2018 met tweejaarlijkse intervallen. Elke editie bestond uit ongeveer 5.000 tot 6.000 respondenten. In totaal hebben in deze periode 11.028 respondenten ten minste eenmaal geparticipeerd, waarvan 63% meerdere malen. De respondenten gaven voor diverse vormen van slachtofferschap op of ze dit het afgelopen jaar hadden ervaren. Een van die vragen ging over een vorm van bankfraude, namelijk ongeautoriseerde geldopname (‘Geld van uw bankrekening afgeschreven zonder uw toestemming’). Een kanttekening bij de beantwoording van deze vraag is dat sommige respondenten zich mogelijk niet hebben gerealiseerd dat geld ten onrechte is afgeschre-

doi: 10.5553/JV/016758502020046002007

ven van hun bankrekening. In dit artikel beperken we ons tot de 636 respondenten (bijna 6%) die tussen 2010 en 2018 eenmaal of meermaals een ongeautoriseerde bankafschrijving hebben meegemaakt in het jaar voorafgaand aan de enquête.

Incidentkenmerken

De *aanvankelijke financiële schade* bij slachtoffers werd bepaald door te vragen: 'Hoeveel geld (in euro's) werd van uw rekening afgeschreven?' Slachtoffers konden het relevante bedrag invullen. Vervolgens werd gevraagd of zij erin waren geslaagd dit bedrag terug te krijgen. Antwoordcategorieën hierop waren (1) 'ja, volledig', (2) 'ja, gedeeltelijk' en (3) 'nee'. We hercodeerden dit tot een variabele of het slachtoffer wel of niet geheel werd terugbetaald, ook omdat de tweede categorie een heel kleine groep betrof. Als een volgende stap werd de *uiteindelijke financiële schade* vastgesteld. Slachtoffers bij wie de schade volledig werd vergoed, scoorden een waarde van nul op deze variabele. Voor slachtoffers die meldden dat het bedrag in zijn geheel niet werd terugbetaald, staat de uiteindelijke schade gelijk aan de aanvankelijke schade. Aan de slachtoffers die meldden gedeeltelijk te zijn terugbetaald, werd gevraagd welk bedrag zij hadden ontvangen. Het resterende verschil werd geclassificeerd als de uiteindelijke schade voor deze groep. Om vast te stellen of het incident was gemeld bij officiële instanties, werd gevraagd: 'Heb je maatregelen genomen naar aanleiding van dit incident?' Twee categorieën waren 'gemeld bij de politie' en 'contact met de bank' (beide 0-1). 11% meldde zich bij de politie en 63% nam contact op met hun bank.

Slachtofferkenmerken

Naast incidentkenmerken zijn van de respondenten ook persoonskenmerken bekend. Dat zijn om te beginnen een aantal achtergrondkenmerken – geslacht, leeftijd, burgerlijke staat (partner of niet), opleidingsniveau en inkomenscategorie. Opleidingsniveau werd opgenomen als een ordinale variabele met zes categorieën, variërend van basisonderwijs tot universiteit. Voor wat betreft het maandelijks huishoudensinkomen werden vijf categorieën onderscheiden: laag inkomen (€ 1.150 of minder), laag tot gemiddeld inkomen (€ 1.151-1.800),

doi: 10.5553/JV/016758502020046002007

gemiddeld tot hoog inkomen (€ 1.801-2.600), hoog inkomen (meer dan € 2.600) en inkomen onbekend.
De mate van zelfcontrole van respondenten werd vastgesteld via elf items, die een subschaal vormen van de *Dickman Impulsivity Inventory* over disfunctionele impulsiviteit. Aan alle respondenten in de gehele steekproef werd hiervoor gevraagd of een aantal verschillende gedragingen van toepassing is op hen. Voorbeeldvragen zijn: 'Ik zeg vaak wat er in mij opkomt zonder eerst na te denken', 'Ik geniet ervan langzaam en zorgvuldig te werken aan problemen' (omgekeerd gecodeerd) en 'Ik maak vaak afspraken zonder na te denken of ik in staat ben me eraan te houden'. Betrouwbaarheidsanalyses op de gehele steekproef laten zien dat er per editie van het LISS-panel afdoende interne consistentie is tussen de items voor zinvolle schaalconstructie (Cronbach's alpha variërend van 0,72 tot 0,75). Tot slot is herhaald slachtofferschap van onterechte bankafschrijvingen in kaart gebracht aan de hand van de longitudinale gegevens. 13% van de slachtoffers gaf tijdens meerdere edities aan dat ze dit incident hebben meegemaakt. Voor hen hebben we de kenmerken van het meest recente incident gebruikt.[1]

Analyse

We beginnen onze analyse met een beschrijving van de hoeveelheid geld dat van slachtoffers is gestolen – in eerste instantie nadat ze het incident hadden ontdekt, en uiteindelijk nadat ze contact hadden opgenomen met instanties en probeerden te worden vergoed. Vervolgens onderzoeken we de relatie tussen initiële en uiteindelijke schade door ze te relateren aan incident- en slachtofferkenmerken. Het initiële en uiteindelijke verlies hebben we ingedeeld in vijf categorieën. Voor *aanvankelijk verlies* zijn deze categorieën: (1) minder dan € 50, (2) tussen € 50 en 99, (3) tussen € 100 en 249, (4) tussen € 250 en 999, en (5) € 1.000 of meer. Voor *uiteindelijk verlies* onderscheiden we ook vijf categorieën, maar rekening houdend met de verdeling (later weergegeven in tabel 1), met iets andere waarden: (1) geen verliezen, (2) minder dan € 50, (3) tussen € 50 en 99, (4) tussen € 100 en 249, en (5) € 250 of meer. Deze categorieën hebben we onder andere onderscheiden omdat er enkele waarnemingen in de steekproef zaten met

1 Een overzicht met *descriptives* van de gebruikte variabelen is beschikbaar op aanvraag bij de eerste auteur.

doi: 10.5553/JV/016758502020046002007

Tabel 1 Hoogte van financiële schade na onterechte bankafschrijving, in categorieën (N=636)

	Aanvankelijke schade(%)	Definitieve schade(%)
€ 0	-	82,2
Minder dan € 50	27,5	7,4
€ 50-99	16,5	3,0
€ 100-249	13,5	2,8
€ 249-999	14,0	1,7
€ 1.000 of meer	10,1	0,9
Onbekend	18,4	1,9
Hoogste schade	€ 35.000	€ 10.500

zeer hoge waardes die zonder categorisering anders disproportioneel veel invloed op de resultaten zouden hebben. Voor beide afhankelijke variabelen wordt ordinale regressieanalyse gebruikt. Tot slot beoordelen we de relatie tussen incident- en slachtofferkenmerken met de door het slachtoffer ondernomen acties (melding bij de politie, contact met de bank) en met het in aanmerking komen voor schadevergoeding. Voor deze analyses zijn de afhankelijke variabelen dichotoom (ja-nee), daarom wordt gebruik gemaakt van logistische regressieanalyses.

Resultaten

Tabel 1 biedt een overzicht van de bedragen die slachtoffers van onterechte bankafschrijvingen verliezen. De linkerkolom toont de initiële verliezen na het ontdekken van het incident. Voor ongeveer een kwart van de slachtoffers zijn de verliezen vrij klein met bedragen van minder dan € 50. Bijna 40% verliest een bedrag van meer dan € 100, terwijl een op de tien slachtoffers € 1.000 of meer kwijt is. De rechterkolom toont de verdeling na schadevergoeding. Het is vrij duidelijk dat de meeste slachtoffers uiteindelijk geen financiële verliezen lijden, aangezien meer dan 80% volledig wordt vergoed. Er blijft nog 7% over met kleine verliezen van minder dan € 50. Een kleine groep kampt met vrij grote verliezen, bijna 3% loopt een schade op van € 250 of meer.

doi: 10.5553/JV/016758502020046002007

Analyses omtrent de hoogte van het aanvankelijke verlies bij een onterechte bankafschrijving levert nauwelijks patronen op voor de onderscheiden incident- en slachtofferkenmerken. Dit wijst erop dat de verdeling van de schadebedragen vrij willekeurig is. Een uitzondering is leeftijd. Oudere slachtoffers worden geconfronteerd met wat grotere aanvankelijke schade.

In tabel 2 wordt de relatie getoond tussen acties van het slachtoffer – contact opnemen met de bank en politie – en slachtoffer- en incidentkenmerken. Daarnaast wordt in de laatste kolom van deze tabel getoond hoe deze kenmerken zich verhouden tot het ontvangen van schadevergoeding. De beslissing om contact op te nemen met de bank blijkt samen te hangen met verschillende kenmerken. Zo nemen hoger opgeleide slachtoffers duidelijk vaker contact op met de bank dan lager opgeleide slachtoffers – een bevinding die overeenkomt met de verwachting uit Wingd. Voor slachtoffers met lage inkomens geldt dat zij ook vaker contact opnemen met de bank – gecontroleerd voor opleidingsniveau. De hypothese over lage zelfcontrole wordt bevestigd, omdat slachtoffers met lage zelfcontrole minder vaak contact opnemen met hun bank. Een andere factor van belang is de hoogte van het aanvankelijk afgeschreven bedrag. Niet verrassend blijkt hieruit dat hoe hoger dit bedrag, des te groter de kans dat het slachtoffer contact opneemt met de bank. Voor de beslissing om contact op te nemen met de *politie* (tweede kolom), lijkt de hoogte van de aanvankelijke schade de dominante factor te zijn, met opnieuw hogere kansen bij slachtoffers met hoge schade. Slachtoffers met een laag tot gemiddeld inkomen melden het incident vaker bij de politie. Aanvullende analyses (niet getoond) wijzen erop dat terugbetaling een rol lijkt te spelen in de beslissing om het incident aan de politie te melden: slachtoffers die niet worden vergoed, hebben een grotere kans om te melden. Tot slot, met betrekking tot wel of niet schadevergoeding ontvangen (laatste kolom) zien we dat hoger opgeleide slachtoffers een wat hogere kans hebben om dit te ontvangen – een bevestiging van onze verwachting. Het inkomensniveau is niet gerelateerd aan het ontvangen van een vergoeding (met uitzondering van slachtoffers van wie het inkomen onbekend is: die hebben een kleinere kans om vergoed te worden). Bovendien hebben slachtoffers met een lage zelfcontrole, in overeenstemming met onze hypothese, minder kans deze te ontvangen.

doi: 10.5553/JV/016758502020046002007

Tabel 2 Contact opnemen met de bank, aangifte doen bij de politie en schadevergoeding, logistische regressie

	Contact opnemen met de bank 0–1		Melden bij de politie 0–1		Schade-vergoeding 0–1	
	B	SE	B	SE	B	SE
Opleidingsniveau[a]	.157**	.066	-.011	.106	.152*	.089
Inkomen: laag	.692*	.377	1.031	.588	.110	.484
Inkomen: laag tot gemiddeld	.210	.296	1.135*	.469	-.568	.371
Inkomen: gemiddeld tot hoog	-.384	.248	-.311	.455	-.164	.361
Inkomen: hoog	Ref.		Ref.		Ref.	
Inkomen: onbekend	-.935**	.342	1.027	.583	-.867*	.422
Lage zelfcontrole[a]	-1.446**	.593	.880	1.002	-1.635*	.724
Aanvankelijk verlies (AV) minder dan € 50	Ref.		Ref.		Ref.	
AV € 50-99	.043	.265	1.496	.856	.243	.345
AV € 100-249	.437	.288	1.469	.889	.361	.370
AV € 250-999	1.180**	.316	3.288**	.779	1.018*	.436
AV € 1.000 of meer	1.317**	.375	4.564**	.776	.769	.486
AV onbekend	.795**	.275	2.219**	.791	1.239**	.420
Nagelkerke R^2	15,9%		32,2%		14.0%	
N	621		623		610	

* $p<0,05$; ** $p<0,01$.
[a] Eenzijdig getoetst.
NB In deze modellen is tevens gecontroleerd voor geslacht, leeftijd, partner, herhaald slachtofferschap van onterechte bankafschrijving en jaartal, via dummyvariabelen.

Ten slotte bespreken we de bevindingen uit tabel 3, die laten zien hoe incident- en slachtofferkenmerken gerelateerd zijn aan de hoogte van de uiteindelijk geleden financiële schade. In Model 1 zien we onze hypothese bevestigd rond opleidingsniveau – de schade is doorgaans lager voor hoger opgeleide slachtoffers. Voor wat betreft inkomen laten de resultaten zien dat slachtoffers met een laag tot gemiddeld inkomen geconfronteerd worden met meer schade in vergelijking met slachtoffers met een hoog inkomen. Lage zelfcontrole is daarentegen niet gerelateerd aan de hoogte van de uiteindelijke schade. Verder zien we dat de uiteindelijke schade hoger is voor slachtoffers die een hoog aanvankelijk verlies leden (€ 1.000 of meer). In Model 2 wordt een kenmerk toegevoegd aan de regressievergelijking, namelijk of het slachtoffer al dan niet contact heeft opgenomen met de bank. De resultaten

doi: 10.5553/JV/016758502020046002007

Tabel 3 Uiteindelijke financiële schade, ordinale regressie

	Model 1		Model 2	
	B	SE	B	SE
Opleidingsniveau[a]	-.140*	.084	-.109	.085
Inkomen: laag	.397	.441	.508	.447
Inkomen: laag tot gemiddeld	.833**	.348	.883*	.349
Inkomen: gemiddeld tot hoog	.342	.336	.282	.340
Inkomen: hoog	Ref.		Ref.	
Inkomen: onbekend	1.047*	.410	.948*	.413
Lage zelfcontrole[a]	.947	.690	.773	.702
Aanvankelijk verlies (AV) minder dan € 50	Ref.		Ref.	
AV € 50-99	.615	.317	.581	.320
AV € 100-249	.407	.346	.424	.350
AV €250-999	.118	.372	.289	.378
AV € 1.000 of meer	.781*	.373	.993**	.381
Contact opgenomen met bank	-	-	-.798**	.240
Nagelkerke R^2	8,5%		10,8%	
N	613		612	

* $p<0,05$; ** $p<0,01$.
[a] Eenzijdig getoetst.
NB In deze modellen is tevens gecontroleerd voor geslacht, leeftijd, partner, herhaald slachtofferschap van onterechte bankafschrijving en jaartal, via dummyvariabelen.

wijzen erop dat dit contact sterk samenhangt met kleinere schade. De samenhang met opleidingsniveau valt hierdoor weg, wat erop duidt dat de hogere uiteindelijke schade onder lageropgeleiden teruggevoerd kan worden tot het feit dat zij minder melding maken bij de bank. Andere kenmerken in het model worden niet wezenlijk beïnvloed door deze toevoeging.[2]

2 Omdat grote definitieve schade weinig voorkomt bij dit delict hebben we robuustheidschecks uitgevoerd op onze analyses door de resultaten ook na te gaan voor een afhankelijke variabele met drie categorieën (met € 50 of meer als de hoogste schadecategorie) en vier categorieën (met € 100 of meer als de hoogste categorie) – in aanvulling op de huidige vijf categorieën. Dit leverde zeer vergelijkbare resultaten op, met uitzondering van de relatie voor 'aanvankelijk verlies tussen € 50 en 99'. In deze alternatieve schattingen had deze categorie hogere uiteindelijke schade.

doi: 10.5553/JV/016758502020046002007

Conclusie

Gezien de groeiende zorg over bankfraude in een gedigitaliseerde samenleving, is het belangrijk om inzicht te krijgen in de ernst van de gevolgen ervan. Dit artikel draagt hieraan bij door voor het fenomeen van ongeautoriseerde bankafschrijvingen na te gaan in hoeverre slachtoffers met financiële schade blijven zitten en in hoeverre ze in actie komen om iets aan deze schade te doen. Het beperken van financiële schade bij identiteitsfraude is op zichzelf belangrijk, maar helpt ook om negatieve sociale gevolgen ervan – mentale problemen, gebrek aan vertrouwen in anderen – te minimaliseren. In dit artikel beschouwden we de acties die slachtoffers ondernamen en de schade die ze uiteindelijk leden als een uitvloeisel van hun doe-vermogen, een concept ontleend aan de WRR-studie *Weten is nog geen doen* (Bovens e.a. 2017). We verwachtten dat slachtoffers van identiteitsfraude minder vaak melding doen bij de bank en de politie als ze een lager opleidingsniveau en minder zelfcontrole hadden. Omdat schadevergoeding minder waarschijnlijk is indien er door het slachtoffer geen melding wordt gemaakt, verwachten we bij deze groepen slachtoffers ook meer financiële schade.

Aan de hand van representatieve slachtoffergegevens verzameld over een periode van acht jaar – tussen 2010 en 2018 – onder de Nederlandse bevolking hebben we patronen van financiële schade, melding maken bij bank en politie en schadevergoeding geanalyseerd bij 636 slachtoffers van een onterechte bankafschrijving. Daaruit kwamen een paar hoofdbevindingen naar voren. Ten eerste blijkt dat, nadat er soms aanzienlijke aanvankelijke bedragen gestolen zijn, de meeste slachtoffers volledige schadevergoeding krijgen, namelijk ruim 80%. In die zin is er, los van de aanvankelijke schrik, geen sprake van blijvende financiële schade onder een groot deel van deze groep slachtoffers. Niettemin blijft ongeveer 15% uiteindelijk met financiële schade achter. Voor een kleine groep gaat het hierbij om aanzienlijke bedragen van € 1.000 of meer.

Wat betreft melding maken bij de bank zagen we inderdaad dat lager opgeleide slachtoffers en mensen met weinig zelfcontrole dit minder vaak deden, conform verwachtingen uit Wingd. Hierbij hielden we rekening met de omvang van de schade, een factor die naast opleidingsniveau en zelfcontrole ook van belang is. Het melden van het incident bij de politie lijkt alleen te worden bepaald door finan-

doi: 10.5553/JV/016758502020046002007

ciële motieven, de kans daarop hing af van de hoogte van het aanvankelijk gestolen bedrag en of de schade werd vergoed door de bank. Rondom het wel of niet ontvangen van schadevergoeding zagen we de patronen terug zoals bij de beslissing om wel of niet bij de bank te melden, met minder vaak schadevergoeding onder lageropgeleiden en onder slachtoffers met lage zelfcontrole. Al met al was er meer schade voor slachtoffers met een lagere opleiding en slachtoffers met een laag tot gemiddeld inkomen, maar niet onder slachtoffers met lagere zelfcontrole. Voor lageropgeleiden lijkt dit terug te voeren tot het minder vaak melden van het incident. Voor de lage-inkomensgroep bleef een effect over nadat we rekening hielden met het melding maken bij de bank, hetgeen suggereert dat het contact met de bank voor deze groep minder effectief is om financiële schade te voorkomen.
Een aantal patronen in deze studie duidt op ongewenste uitkomsten. Bepaalde groepen – lageropgeleiden en mensen met lage zelfcontrole – komen minder vaak in actie nadat ze te maken hebben gehad met een onterechte bankafschrijving, soms van een aanzienlijk bedrag. Hiermee hangt samen dat deze groepen minder vaak in aanmerking komen voor schadevergoeding. In navolging van Wingd pleiten we in dit kader voor begrijpelijke communicatie en gerichte ondersteuning. Als er eenmaal sprake is van schade, is het voor ieder slachtoffer – maar met name voor hen wier doe-vermogen op de proef wordt gesteld – van belang dat het incident geen zoektocht is om de schade bij het juiste loket te melden, zowel bij banken als bij de politie. Slachtofferhulp Nederland probeert hierbij op een laagdrempelige manier ondersteuning te bieden. Onderzoek onder slachtoffers van financiële cyberdelicten laat zien dat deze groep veel behoefte heeft aan herstel van de schade en dat het sommigen maar moeilijk lukt, onder andere door moeilijkheden om het delict te kunnen aangeven bij de politie (Leukfeldt e.a. 2018). Toegankelijkheid van communicatie en helderheid waar een slachtoffer met schade terechtkan, zorgen voor duidelijkheid in de 'keuzearchitectuur' (Bovens e.a. 2017) en zijn daarbij voor het gericht kunnen ondernemen van actie door slachtoffers van groot belang. Deze duidelijkheid helpt ook slachtoffers voor wie 'doen' een uitdaging is om daadwerkelijk stappen te zetten. Omdat veel van de voorlichting hierover online plaatsvindt, is het van belang om na te gaan in hoeverre burgers bij diverse typen problemen – zoals slachtofferschap – over voldoende internetvaardigheden

doi: 10.5553/JV/016758502020046002007

beschikken om hun weg naar de juiste informatiekanalen te vinden en zodoende tot een plan van aanpak te kunnen komen.

Literatuur

Bovens e.a. 2017
M. Bovens, A.G. Keizer & W. Tiemeijer, *Weten is nog geen doen. Een realistisch perspectief op redzaamheid* (WRR-rapporten nr. 97), Den Haag 2017.

Button e.a. 2014
M. Button, C. Lewis & J. Tapley, 'Not a victimless crime: The impact of fraud on individual victims and their families', *Security Journal* (27) 2014, p. 36-54.

Copes e.a. 2001
H. Copes, K.R. Kerley, K.A. Mason & J. van Wyk, 'Reporting behavior of fraud victims and Black's theory of law: An empirical assessment', *Justice Quarterly* (18) 2001, p. 343-363.

Eurobarometer 2018
Eurobarometer, *Europeans' attitudes towards Internet security*, Brussel 2018.

Golladay & Holtfreter 2017
K. Golladay & K. Holtfreter, 'The consequences of identity theft victimization: An examination of emotional and physical health outcomes', *Victims & Offenders* (12) 2017, p. 741-760.

Holt & Lampke 2010
T.J. Holt & E. Lampke, 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies* (23) 2010, p. 33-50.

Holt e.a. 2018
T.J. Holt, J. van Wilsem, S. van de Weijer & R. Leukfeldt, 'Testing an integrated self-control and routine activities framework to examine malware infection victimization', *Social Science Computer Review* 2018.

Langton 2019
L. Langton, *Victims of identity theft 2016*, Washington: Bureau of Justice Statistics 2019.

Leukfeldt e.a. 2018
R. Leukfeldt, R. Notté & M. Malsch, *Slachtofferschap van online criminaliteit*, Den Haag: WODC 2018.

Paulissen & Van Wilsem 2015
L. Paulissen & J. van Wilsem, *Dat heeft iemand anders gedaan. Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland*, Amsterdam: Reed Business Information 2015.

doi: 10.5553/JV/016758502020046002007

Pratt e.a. 2010
T.C. Pratt, K. Holtfreter & M.D. Reisig, 'Routine online activity and Internet fraud targeting: Ending the generality of routine activity theory', *Journal of Research in Crime and Delinquency* (47) 2010, p. 267-296.

Randa & Reyns 2019
R. Randa & B.W. Reyns, 'The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey', *Deviant Behavior* 2019, p. 1-15.

Schoepfer & Piquero 2009
A. Schoepfer & N.L. Piquero, 'Studying the correlates of fraud victimization and reporting', *Journal of Criminal Justice* (37) 2009, p. 209-215.

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

Sipma & Van Leijsen 2019
T. Sipma & E. van Leijsen, *Slachtofferschap van cyber- en gedigitaliseerde criminaliteit onder burgers*, Den Haag: WODC 2019.

Turanovic & Pratt 2014
J.J. Turanovic & T.C. Pratt, '"Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization', *Journal of Quantitative Criminology* (30) 2014, p. 29-56.

Van Wilsem 2013
J. van Wilsem, '"Bought it, but never got it". Assessing risk factors for online consumer fraud victimization', *European Sociological Review* (29) 2013, p. 168-178.

Van Wilsem 2016
J. van Wilsem, 'Exploring the possibility of "moral hazard" among victims of identity fraud: The relation between reimbursement for unauthorized cash withdrawals and risky online behavior', in: T.J. Holt (red.), *Cybercrime through an interdisciplinary lens*, Londen: Routledge 2016, p. 106-118.

Xie & Baumer 2019
M. Xie & E.P. Baumer, '"Crime victims" decisions to call the police: Past research and new directions', *Annual Review of Criminology* (2) 2019, p. 217-240.

doi: 10.5553/JV/016758502020046002007

Resultaten van een awareness-training in het herkennen van phishingmails

Dieke Miltenburg*

Een probleem bij digitale criminaliteit is dat slachtoffers vaak niet weten dat ze slachtoffer zijn en ook als ze dat wel weten, geen aangifte doen bij de politie. Derhalve is weinig informatie beschikbaar over de kenmerken van slachtoffers van digitale criminaliteit. Verscheidene onderzoekers hebben getracht hier meer inzicht in te verkrijgen door aan respondenten scenario's voor te leggen. Hierbij is respondenten gevraagd om phishingmails van legitieme mails te onderscheiden, zowel voorafgaand aan als na afloop van een training over dit onderwerp. Probleem bij dit soort onderzoek is dat de respondenten weten dat ze aan een test meewerken. Het is dan ook goed mogelijk dat zij in het dagelijks leven andere keuzes zouden maken dan in het testscenario.

Derhalve is voor een andere aanpak gekozen bij een onderzoek naar het klikgedrag van ondernemers bij het ontvangen van phishingmails voor en na een *awareness*-training. De deelnemers konden zich inschrijven voor een 'weerbaarheidstest', waarbij niet werd verteld dat het een phishingtest betrof. De deelnemers aan de test ontvingen, verspreid over drie rondes, in totaal zes phishingmails. Na het versturen is bijgehouden of, en zo ja, wie van de ondernemers op een link in een of beide mails hadden geklikt en of zij gegevens achterlieten op de websites waar de link in de mail naartoe verwees. De eerste ronde van twee phishingmails vond plaats in de week voorafgaand aan de training (Ronde 1). Na Ronde 1 volgde een *awareness*-training, waarbij is stilgestaan bij het voorkomen van slachtofferschap van cybercrime in het algemeen en phishing in het bijzonder. De trainer gaf tips en liet zien waar ondernemers op dienen te letten bij het ontvangen van (phishing)mails, en hij beantwoordde tevens vragen vanuit de zaal. Een week na de training vond Ronde 2 plaats, waarin wederom twee phish-

* D. Miltenburg MSc behaalde recent haar wo-master Opsporingscriminologie aan de Vrije Universiteit Amsterdam. Deze bijdrage is gebaseerd op haar afstudeerscriptie, zie www.ubvu.vu.nl/pub/fulltext/scripties/14_2650385_0.pdf.

doi: 10.5553/JV/016758502020046002008

ingmails zijn verstuurd. Tot slot vond een maand na het volgen van de training Ronde 3 plaats, waarin de laatste twee phishingmails zijn verstuurd naar de deelnemende ondernemers.

Toen het klikgedrag van Ronde 1 vergeleken werd met Ronde 2, bleken in Ronde 2 significant minder ondernemers te hebben geklikt op een phishinglink dan in Ronde 1 (van 40,2% naar 25,0%). Eenzelfde significant verschil was zichtbaar bij de vergelijking tussen Ronde 1 en Ronde 3 (van 40,2% naar 26,0%). Tussen Ronde 2 en Ronde 3 was geen significant verschil aanwezig. Het aantal keer dat gegevens zijn achtergelaten op een phishingmail is afgenomen van 34 (Ronde 1) naar 14 (Ronde 2) en 16 (Ronde 3) keer. Uit het onderzoek is verder een significant verschil gebleken tussen mannen en vrouwen, waarbij, in tegenstelling tot eerder onderzoek, onder de groep mannen een hoger percentage op een link klikte dan onder de groep vrouwen. Man zijn bleek tevens een significante voorspeller voor het klikken op een link in ten minste een van de zes phishingmails. Het ontbreken van significante verschillen in leeftijd, opleidingsniveau, sector waarin iemand werkzaam is, en of iemand een eerdere *awareness*-training heeft gevolgd op het gebied van cybercrime, komt mogelijk door het beperkte aantal respondenten (n=92).

Naast het beperkte aantal respondenten ontbrak een controlegroep en is gebruik gemaakt van zelfbedachte bedrijven en scenario's, waarbij respondenten de phishingmails mogelijk voor spam hebben aangezien en niet voor phishing. Dit blijft gissen omdat met de respondenten geen terugkoppeling is geweest omtrent beweegredenen voor het wel of niet klikken. Een aanbeveling voor toekomstig onderzoek is dan ook om het kwantitatieve deel van het klikgedrag te combineren met een kwalitatief deel. Door respondenten achteraf te bevragen over de keuzes die zij hebben gemaakt bij het ontvangen van een (phishing)mail, waar zij op hebben gelet en wat bij hen de doorslag heeft gegeven voor het wel of niet klikken, wordt inzicht verkregen in het beoordelingsproces. Daarnaast kan meer informatie worden verkregen over waarom de ene groep klikt en de andere niet, zodat duidelijk wordt welke groepen extra bescherming nodig hebben om slachtofferschap te voorkomen. Om dit te bewerkstelligen wordt aanbevolen om gebruik te blijven maken van een phishingtest in combinatie met een fysieke training, zodat gewerkt wordt met echte mensen, echte situaties en echte trainingen.

doi: 10.5553/JV/016758502020046002008

Social engineering: digitale fraude en misleiding

Een meta-analyse van studies naar de effectiviteit van interventies

Jan-Willem Bullée en Marianne Junger*

Onderzoek toont aan dat online criminaliteit in de afgelopen jaren een grote bedreiging is gaan vormen voor zowel individuen (Henson e.a. 2016; Internet Crime Complaint Center 2018; Marinos & Sfakianakis 2012; Reep-van den Bergh & Junger 2018) als organisaties (Klahr e.a. 2017). Veel online gepleegde delicten bevatten een element van fraude en misleiding, ofwel '*social engineering*' (Blakeborough & Correia 2017; Verizon Risk Team 2018). Aanvallers gebruiken misleiding, bedrog en andere overtuigingstechnieken als aanvalstactiek om slachtoffers gevoelige informatie te laten delen of kwaadwillige acties uit te laten voeren (Gupta e.a. 2011). Door slimme trucs proberen zij iets van je te verkrijgen, zoals persoonlijke informatie en logininformatie, maar uiteindelijk komt het meestal neer op: geld.

Social engineering wordt beschouwd als een van de grootste cybergevaren, omdat mensen erg bevattelijk blijken te zijn voor misleiding. Social-engineeringaanvallen lijken op het eerste gezicht legitiem en ongevaarlijke berichten of verzoeken te betreffen. De computergebruiker heeft vaak niet door dat hij slachtoffer is van een dergelijke aanval (Hadnagy & Wilson 2010). Daarom wordt vaak gesteld dat de mens de zwakste schakel is in informatiebeveiliging (Happ e.a. 2016; Schneier 2000).

Er zijn eindeloos veel mogelijkheden voor social engineers. De enige beperking is de verbeelding van de aanvallers. Het succes van social engineering hangt vooral af van de 'kwaliteit' en de wijze waarop zij

* Dr. J.-W. Bullée is werkzaam bij Awareways, Computer & Network Security. Hij promoveerde in 2017 op het proefschrift *Experimental social engineering* aan de Universiteit Twente. Prof. dr. M. Junger is hoogleraar Cyber Security en Business Continuity aan de Universiteit Twente.

doi: 10.5553/JV/016758502020046002009

wordt uitgevoerd. De resultaten kunnen dan ook erg variëren. In de context van e-mailphishing loopt het slagingspercentage uiteen van bijna 0% tot meer dan 80% (Sokol e.a. 2017; Vishwanath 2015; Wright e.a. 2014; Yang e.a. 2017). In persoonlijke verhalen vertellen professionele *penetration testers*[1] vaak dat de kans dat zij ergens binnenkomen nagenoeg 100% is.

Vandaar dat het beperken van de kans op succes zo belangrijk is. Echter: mensen leren weerstand te bieden is niet eenvoudig. Daarnaast is er nog niet veel ervaring met de effectiviteit van interventies opgedaan. Sommige auteurs zijn negatief over het mogelijk succes: Bada en collega's (2015) gaven hun onderzoek de titel mee 'Cyber security awareness campaigns: Why do they fail to change behaviour?' Een gefundeerd oordeel over de effectiviteit van interventies die social engineering moeten bestrijden, is er niet. Om hierop een antwoord te vinden hebben wij een overzicht van de literatuur gemaakt en een meta-analyse verricht. Onze onderzoeksvraag luidt: welke vormen van interventies en specifieke elementen hierin, om social engineering tegen te gaan, zijn het meest succesvol?

Hieronder geven wij een overzicht van de relevante literatuur en beschrijven wij beknopt de methode en de resultaten van de meta-analyse uitgevoerd op deze literatuur. Voor meer gegevens over de literatuur en meta-analyse verwijzen wij naar Bullée en Junger (2020a; 2020b).

Methodiek van de meta-analyse

Om relevante studies op te sporen is de Scopus-database geraadpleegd. Vervolgens is voor alle zoekresultaten gekeken of deze bruikbaar waren. De zoekopdracht leverde 418 resultaten op. Na het controleren op geschiktheid, bleven er 19 studies over voor de analyse. Een studie kan een of meerdere interventies testen. In totaal zijn er 37 interventies gevonden, en voor iedere interventie is de effectgrootte berekend. Deze maat geeft het verschil aan in kwetsbaarheid tussen proefpersonen in de controle en die in de interventiegroep. Specifiek is Cohen's *d* (van 'difference') gebruikt; deze maat is het verschil

1 Penetration testers zijn ethische hackers die een geautoriseerde gesimuleerde cyberaanval ('pentest') op een computersysteem uitvoeren om de beveiliging van het systeem te evalueren.

doi: 10.5553/JV/016758502020046002009

Tabel 1 Beoordeling van effectomvang volgens Cohen (2013)

Categorisering	Effectgrootte
Klein	0,2 en lager
Middelgroot	0,5
Groot	0,8 en groter

tussen de twee gemiddelden gedeeld door de standaardafwijking (Cohen 2013). Voor een indeling naar de omvang van het effect, zie Tabel 1.

De studies zijn beschreven aan de hand van een aantal kenmerken:
1. de context van de studies;
2. de karakteristieken van de interventie;
3. de kenmerken voor de evaluatiestudie.

Effectiviteit van interventies

In totaal zijn 19 studies in de analyse betrokken, met gezamenlijk N=23.146 proefpersonen en 37 observaties (d.w.z. effectgrootten). De gemiddelde effectgrootte van een interventie om social engineering tegen te gaan, is 0,54 (95% CI=[0,359, 0,719], I^2=89,31%, 37 studies). Dit wordt beschouwd als een middelgroot effect (Cohen 2013). De I^2-statistiek is een maat voor heterogeniteit, de variantie in een meta-analyse (Higgins e.a. 2003). Voor een overzicht van de effectgrootte per studie wordt verwezen naar Bullée en Junger (2020b).

Type social engineering

De geselecteerde studies maakten gebruik van verschillende typen schijnaanvallen om de vaardigheid van hun deelnemers te testen. Een relatief groot deel van de interventies was gericht op phishing en daarom gebruikten deze studies e-mail als 'schijnaanval'. Daarnaast is gebruik gemaakt van persoonlijk contact (face to face), de telefoon, sms of een phishingwebsite. De wijze waarop interventies werden getest, heeft impact op de effectiviteit (F(4, 32)=5,53, p=,002). Interventies die via sms of een website werden getest, gingen gepaard

doi: 10.5553/JV/016758502020046002009

met relatief grote effecten op slachtofferschap (respectievelijk EG=1,37 en 1,25).[2] Interventies die werden getest via e-mail, face to face of de telefoon werden geassocieerd met kleinere effecten (respectievelijk EG=0,35, 0,30 en 0,27).

Preslachtofferschap

Interventies en trainingsmateriaal hebben tot doel het bewustzijn te vergroten en gedrag te veranderen met betrekking tot een bepaald onderwerp. Het ingrijpen bij iemand die het gewenste gedrag al uitvoert, is echter verspilling van tijd en middelen. In plaats daarvan is het efficiënter om de interventie alleen te verstrekken aan degenen die deze nodig hebben. Daartoe dient '*pre-victimisation*': alleen gebruikers die 'vallen' voor de aanval wordt een interventie aangeboden. Daarnaast dient preslachtofferschap bij een schijnaanval om een gebruiker te motiveren: als ze voor de social-engineeringaanval zijn gevallen, zullen ze worden gemotiveerd om te leren hoe ze dit in de toekomst kunnen voorkomen. Daarom gebruiken securityonderzoekers vaak een tweefasebenadering. Die bestaat eruit dat alle proefpersonen bijvoorbeeld een nepphishingmail ontvangen. Vervolgens worden degenen die het gewenste gedrag hebben uitgevoerd (bijvoorbeeld niet op de link klikken) 'met rust gelaten'. Degenen die slachtoffer zijn geworden (bijvoorbeeld op de link hebben geklikt), worden doorverwezen of uitgenodigd om deel te nemen aan een bewustmakingscursus over social engineering (Kumaraguru e.a. 2007a).
De combinatie van preslachtofferschap met een interventie wordt een 'embedded' training of interventie genoemd. Verschillende onderzoeken toonden aan dat deze previctimisatie een relevant aspect was van interventies in zowel laboratoriumonderzoeken (Kumaraguru e.a. 2009; Mayhorn & Nyeste 2012; Sheng e.a. 2007) als reallife (Kumaraguru e.a. 2008). In tegenstelling tot de verwachting was het effect van ingebedde interventies kleiner dan het effect van niet-ingebedde interventies ($Q(1)=9{,}38$, $p=,002$). De gemiddelde effectgrootte van ingebedde interventies was 0,18 en van de niet-ingebedde interventies 0,70.

2 Wanneer wordt gesproken over effecten, zijn het effecten in de verwachte richting, namelijk dat de interventie leidt tot minder slachtofferschap. Zo niet, dan wordt dit expliciet vermeld.

doi: 10.5553/JV/016758502020046002009

Modaliteit van de interventie

Interventies werden aangeboden op verschillende wijzen: soms werd een gebruiker getraind tijdens een gesprek, of er werd een fysiek document verstrekt om kennis of online waarschuwingen over te dragen om te informeren over potentieel gevaar. Soms is de training interactief, bijvoorbeeld wanneer gebruikers in een klaslokaal communiceren met een trainer (Mayhorn & Nyeste 2012; Lastdrager e.a. 2017). Er is gesuggereerd dat het gebruik van interactieve antiphishingtraining een effectievere manier is om gebruikers in staat te stellen phishing-URL's te identificeren dan het gebruik van passieve zelfstudies over phishing (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Andere 'trainingsmodaliteiten' bestonden uit het verzenden van nepphishingmails naar gebruikers: de eerste antiphishingstudies bevatten geen opleidingsonderdeel (Dodge e.a. 2007). In plaats daarvan testten deze onderzoeken het effect van een 'ik heb je'-moment. Wanneer een gebruiker slachtoffer werd van een nepphishingmail, ontving deze de melding dat hij 'slachtoffer' was geworden. Het idee is dat medewerkers beseffen hoe kwetsbaar ze zijn en daarom in de toekomst voorzichtiger handelen. Door het herhaaldelijk verzenden van nepphishingmails kan het aantal slachtoffers geleidelijk worden verminderd (Dodge e.a. 2007; Aburrous e.a. 2010).
De modaliteit maakt uit voor de effectiviteit ($F(2, 34)=3{,}57$, $p={,}039$). Interventies die mondeling werden gepresenteerd of gebruik maakten van een interactieve inhoud hadden een relatief groot effect (EG=1,00 en 0,94). Degenen die alleen tekst gebruikten, hadden een kleiner effect (EG=0,36).

Priming op gevaar

Mensen reageren vaak sneller op bepaalde tekens, woorden of gewaarwordingen als zij deze eerder hebben waargenomen (Dolan e.a. 2010; Kenrick e.a. 2005). In de fysieke wereld steunt veel onderzoek op het bestaan van zogeheten *priming*-effecten (Cameron e.a. 2012). Online hebben verschillende interventies ook gebruik gemaakt van vormen van priming (Acquisti e.a. 2012; Grazioli 2004; Parsons e.a. 2015). Zo informeerden Stockhardt en collega's (2016) en Parsons en collega's (2015) van tevoren dat de interventie over phishing ging. Acquisti en

doi: 10.5553/JV/016758502020046002009

collega's (2012; niet in de meta-analyse) 'primeden' respondenten door een verschil in lay-out van de website, 'slordig/deviant' versus 'netjes/professioneel'. Maar de resultaten laten niet altijd positieve effecten zien (Sundar e.a. 2013; Grazioli & Wang 2001). Over het algemeen lijken de resultaten niet overtuigend over de impact van priming in een online context. In onze meta-analysestudie bleek dat interventies die gebruik maakten van priming effectiever waren (EG=1,01) dan interventies die geen gebruik maakten van priming (EG=0,38; Q(1)=10,42, p=,001).

Waarschuwing voor gevaar (warning)

Waarschuwingen zijn een directere manier om een boodschap over te brengen dan priming. Traditionele offline waarschuwingen zijn succesvol geweest in het beïnvloeden van gedrag (Argo & Main 2004; Wogalter e.a. 2012). Richtlijnen voor adequate offline waarschuwingen zijn samengevat door Wogalter en collega's (2012). Waarschuwingen kunnen gebruikers in beginsel ook helpen zich online veiliger te gedragen; maar veel gebruikers pasten hun gedrag echter niet aan wanneer geldbeloningen in het geding waren (Barth e.a. 2019; Kirlappos & Sasse 2012; Christin e.a. 2011). In de huidige studie vinden wij dat waarschuwingen, alleen of in combinatie met een training, geen invloed hadden op het effect van een interventie (EG (F(2, 34)=0,17, p=,848).

Focus van de inhoud op de interventie

De focus van interventies varieert sterk. Phishingmails bevatten vaak links naar kwaadaardige websites. De meeste gebruikers zijn echter niet op de hoogte van de structuur van URL's en domeinnamen (Herzberg & Jbara 2008). Het gevolg is dat oplichters er vaak in slagen om gebruikers ertoe te verleiden op deze links te klikken. Dienovereenkomstig richten veel antiphishingspellen zich op het herkennen van phishing-URL's. Andere antiphishinginterventies leggen gebruikers enkele meer algemene kenmerken van phishingmails uit. Deze worden bijvoorbeeld beschreven als:

1. Phishingmails vragen vaak om persoonlijke informatie.
2. Phishingmails bevatten vaak een gevoel van urgentie.

doi: 10.5553/JV/016758502020046002009

3. Bij phishingmails komen vaak het e-mailadres van de afzender in het veld 'Van' en de bedrijfsnaam niet overeen.
4. Phishingmails bevatten vaak een bedreiging om een reactie te stimuleren.
5. Phishingmails bevatten vaak verkeerd gespelde woorden, vreemde spaties of slordige grammatica.
6. Phishingmails bevatten vaak links naar phishingwebsites.
7. Door met de muis over een link in een e-mail te bewegen wordt de gekoppelde URL onthuld (Downs e.a. 2006).

Een probleem bij het toepassen van deze kenmerken is dat phishingmails veranderen: ze worden steeds geavanceerder en gepersonaliseerde *spearphishing* maakt het ook moeilijker om ze te herkennen (Bullée e.a. 2017).

De focus van de interventie hangt significant samen met de effectgrootte ($F(5, 31)=3{,}84$, $p={,}008$). Interventies die gericht waren op de URL werden geassocieerd met een groot effect (EG=1,19), interventies gericht op cybercriminaliteit in het algemeen hadden een middelgroot effect (EG=0,60). Interventies gericht op social engineering en interventies gericht op de inhoud van een e-mail hadden een klein tot middelgroot effect (EG=0,34 en 0,34). Interventies die gericht waren op zowel de URL als de e-mail hadden een klein effect (EG=0,28). Tot slot werden de overige interventies geassocieerd met een middelgroot effect (EG=0,52).

Technische aspecten van een interventie

De meeste interventies waren gericht op mensen, omdat mensen informatie kunnen onthullen en kwetsbaar zijn voor aanvallen. Sommige interventies bouwen echter technische tegenmaatregelen in als extra beveiliging. Gebruikers kunnen deze niet omzeilen, ook niet als ze dat willen. Omdat slechts één interventie een dergelijke technische component had, namelijk Margulies en Herzberg (2013), kunnen we hierover geen uitspraken doen.

Formaat van de interventies

Interventies zijn ontwikkeld in veel verschillende formaten. Zo werden antiphishinginterventies aangeboden door gebruikers een sms-bericht

doi: 10.5553/JV/016758502020046002009

te sturen, of een stripverhaal, een combinatie van een stripverhaal en tekst of een spel te geven. Een strip lijkt bijvoorbeeld effectiever dan een tekst met grafische elementen (Kumaraguru e.a. 2007b).
Twee grootschalige reallife-antiphishingstudies onderzochten het effect van ingebedde trainingen (Kumaraguru e.a. 2008; Caputo e.a. 2014). De ene studie gebruikte een cartoon (Kumaraguru e.a. 2008), de andere studie een tekst (Caputo e.a. 2014). De inhoud van de boodschap was vergelijkbaar. De cartoon (met weinig woorden) verbeterde het gebruikersgedrag binnen het bedrijf (Kumaraguru e.a. 2008). De tekst (met veel woorden) verhinderde echter niet dat werknemers het slachtoffer werden van phishing (Caputo e.a. 2014). Er zijn ook spellen ontwikkeld, meestal als een meer uitgebreide vorm van antiphishingtraining. Gaming vergroot de motivatie van gebruikers om te leren (Sheng e.a. 2007). Het positieve effect van leren door gamen wordt bevestigd in de leerwetenschap (Clark & Mayer 2016). Het meest geteste antiphishingspel is Anti-Phishing Phil (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Deze game leert gebruikers onderscheid te maken tussen legitieme URL's en phishing-URL's. De belangrijkste boodschap van het spel is om aandacht te besteden aan URL's; aangezien dit goede indicatoren zijn voor phishing. Phil, het hoofdpersonage in het spel, krijgt punten wanneer hij legitieme wormen eet (d.w.z. URL's), terwijl punten worden afgetrokken wanneer Phil slechte wormen eet. Het spel bestaat uit vier ronden en elke ronde begint met een korte uitleg met antiphishingadvies. Daarnaast bevat de training voorbeelden en oefenvragen (Sheng e.a. 2007). De Anti-Phishing Phil-game is in verschillende onderzoeken getest (Arachchilage e.a. 2016; Davinson & Sillence 2010; Kumaraguru e.a. 2010; Mayhorn & Nyeste 2012; Sheng e.a. 2007). Meer recentelijk is er een game ontwikkeld voor smartphones (Arachchilage & Cole 2011). De meeste antiphishingexperimenten met games lieten positieve resultaten zien bij het leren van gebruikers om phishingaanvallen te identificeren. Het is echter moeilijk om het exacte effect van antiphishingspellen te bepalen in vergelijking met trainingsinterventies omdat veel van de antiphishingspellen zijn getest in kleinschalige pilotstudies (bijv. Sheng e.a. 2007; Yang e.a. 2012).
In onze meta-analyse vonden wij echter geen statistisch significant effect van het interventieformaat op een afname van slachtofferschap ($F(4,32)=2,57$, $p=,057$).

doi: 10.5553/JV/016758502020046002009

Gebruik van tips

Verschillende interventies gaven tips of een specifieke aanbeveling aan gebruikers. Gebruikers kregen onder meer de volgende tips (Kumaraguru e.a. 2007b, p. 75):
– Klik nooit op links in e-mails.
– Typ het websiteadres in de webbrowser.
– Zoek en bel zelf de klantenservice.
– Geef nooit persoonlijke informatie.

In de meta-analyse bleek het geven van tips geen effect te hebben (F(2, 34)=0,18, p=,837).

Intensiteit van de interventie

Sommige interventies waren vrij eenvoudig en sommige waren relatief uitgebreid. Het lijkt plausibel dat intensievere interventies leiden tot sterkere effecten en meer impact op de lange termijn; maar vermoedelijk zijn deze ook meer tijdrovend, moeilijker te implementeren en duurder. Daarom verdient een eenvoudige maar effectieve interventie in het algemeen de voorkeur in termen van kosteneffectiviteit. Intensiteit bleek inderdaad van belang voor de effectgrootte (F(2, 34)=3,60, p=,038). Interventies met een hoge intensiteit hadden een groot tot zeer groot effect (EG=0,97), terwijl interventies met een lage of gemiddelde intensiteit een klein tot middelgroot effect hadden (EG=0,41 en 0,34).

Kenmerken van de evaluatiestudie onderzoeksmethode

In de vorige paragraaf zijn de kenmerken besproken van interventies die potentiële slachtoffers moeten helpen social engineering te weerstaan. Maar de wijze waarop het onderzoek is uitgevoerd, kan ook impact hebben op onderzoeksresultaten.

Langetermijneffecten van de interventie

Ongeacht het onderzoeksdesign en de inhoud of de kwaliteit van de training, blijkt dat het behouden van opgedane kennis moeilijk is voor

doi: 10.5553/JV/016758502020046002009

gebruikers. Sommige studies testten het bewaren van kennis na zestien dagen (Alnajim & Munro 2009), vier weken (Lastdrager e.a. 2017) of een paar maanden (Canova e.a. 2015; Caputo e.a. 2014). De meta-analyse laat zien dat de tijd tussen het verstrekken van de interventie en het testen van de kwetsbaarheid voor social engineering leidt tot een kleine maar significante vermindering van het aantal slachtoffers (p=,047). De effectomvang neemt af (EG=-,0005) voor elk extra uur na het uitvoeren van de interventie.

Omgeving: reallife of lab

In experimenten kan het gedrag van de proefpersonen in een gecontroleerde omgeving worden geobserveerd (Siedler & Sonnenberg 2010). In het lab zijn mensen zich bewust van het feit dat ze meedoen aan onderzoek en zijn zij soms ook ingelicht over het doel van het experiment. Hierdoor kunnen zij vooringenomen zijn in hun gedrag. Het is niet bij voorbaat zeker dat ze buiten het experiment hetzelfde gedrag zouden vertonen en vergelijkbare vermoedens van bijvoorbeeld social engineering hebben. Daarom wordt verwacht dat de effecten van interventies die worden getest in een laboratoriumomgeving groter zijn dan die van interventies die in een veldexperiment worden onderzocht. Dit komt overeen met onze eigen analyses (Q(1)=7,19; p=,007): EG=0,81 in laboratoriumstudies en EG=0,33 in veldexperimenten.
Zich bewust zijn van deelname als onderzoeksonderwerp heeft betrekking op het waarnemereffect. Mensen hebben de neiging om aspecten van hun gedrag te veranderen wanneer ze zich ervan bewust zijn dat ze worden geobserveerd en mogelijk de onderzoeksresultaten kunnen beïnvloeden (Monahan & Fisher 2010). Bij sommige labstudies wisten deelnemers niet precies waar het onderzoek, bijvoorbeeld phishing, over ging, terwijl dit bij andere veldexperimenten wel duidelijk was. Het zich bewust zijn van het onderwerp van het onderzoek en de interventie valt dus niet samen met laboratorium versus veldexperiment en is daarom apart bekeken. Zoals verwacht is het waarnemereffect ook gevonden in onze meta-analyse (F(2,34)=5,06, p=,012). Naarmate de deelnemers zich minder bewust waren van het feit dat zij deelnamen aan onderzoek of van het onderwerp van het onderzoek nam de effectgrootte af (respectievelijk (EG=0,87, EG=0,40 en EG=0,23).

doi: 10.5553/JV/016758502020046002009

Randomisatie

Sterkere onderzoeksdesigns hebben zowel een maximale interne als een maximale externe validiteit (Campbell & Stanley 1963). Het gebruik van gerandomiseerde experimenten is de beste onderzoeksmethode om het effect van interventies te bestuderen (Feder e.a. 2000). Twee studies (Weisburd e.a. 2001; Welsh e.a. 2011) hebben aangetoond, in een overzicht van criminologisch onderzoek, dat betere onderzoekdesigns vaak geringere effecten rapporteerden en minder goede onderzoekdesigns vaak sterkere effecten. Dat pleit ervoor om de sterkste onderzoeksdesigns te gebruiken: het heeft geen nut interventies te implementeren die in feite – indien goed onderzocht – geen effect hebben. Voor online interventies vinden wij echter geen invloed van randomisatie op de effectgrootte ($F(2, 34)=0,09$, $p=,913$). Mogelijk komt dat omdat de zwakkere onderzoekdesigns in onze eigen meta-analyse niet zijn geïncludeerd.

Slotbeschouwing

Het goede nieuws is dat er interventies zijn die helpen om de effecten van social-engineeringaanvallen te beperken.
De ideale interventie, op basis van onze meta-analyse, is een interventie waarin de volgende elementen zitten:
- De interventie is interactief (bijv. een spel).
- Er is contact met gebruikers (bijv. een les).
- De interventie heeft een specifieke focus en behandelt een of twee concrete onderwerpen (bijv. over URL's en phishingmails).
- De interventie is relatief intensief.

Een effectieve interventie is niet het enige dat een organisatie moet doen om veilig te zijn. Een aantal aanvullende tips:
- Voer schijnaanvallen uit, dan weet je hoe je organisatie erbij staat.
- Blijf alert en houd op regelmatige momenten trainingen of vergelijkbare oefeningen.
- Evalueer je beleid regelmatig, dan weet je of je vorderingen maakt.

Tot slot is het anoniem delen van een databank met informatie over beveiliging, over (schijn)aanvallen en over effecten van interventies erg nuttig.

doi: 10.5553/JV/016758502020046002009

Onze studie heeft een aantal beperkingen. De reikwijdte van onze conclusies over de effectiviteit wordt beperkt door een aantal zaken. Er zijn nog niet zoveel experimentele studies die interventies tegen social engineering hebben getest. Dat beperkt de mogelijkheden voor analyses: een multivariate analyse is niet goed mogelijk. Daarnaast is lastig dat er nog niet veel systematiek is in dit veld, zowel bij het ontwikkelen van interventies als bij de wijze waarop ze het best kunnen worden getest. Meer overeenstemming over de eisen die aan het ontwikkelen van interventies kunnen worden gesteld en het adequaat testen ervan zouden winst opleveren voor de groei van de kennis op dit terrein.

Verder zagen wij dat interventies die alleen gericht waren op het uitleggen van de URL zeer effectief waren. Deze uitkomst kan gedeeltelijk het gevolg zijn van het feit dat bij het onderzoek naar de effectiviteit van deze interventies in bijna alle gevallen de respondenten werden ingelicht over het doel van de interventie; terwijl studies die 'blind' testten en dus feitelijk zuiverder onderzoek verrichtten hierdoor minder grote effecten vonden. Omdat wij geen multivariate analyse konden uitvoeren vanwege het grote aantal variabelen ten opzichte van het aantal effectgroottes is het mogelijk dat dit gegeven de uitkomsten heeft beïnvloed.

Daarnaast is er niet evenveel aandacht geweest voor elk type social engineering. Er is – terecht – veel onderzoek gedaan naar phishing en het herkennen van foute URL's. Maar er is jammer genoeg veel minder aandacht geweest voor andere typen social engineering, zoals via de telefoon. Daarnaast blijkt dat sommige tips, bijvoorbeeld over phishing, kunnen verouderen omdat de aanvallers slimmer worden. Zo is de tip dat de aanhef van een e-mail niet specifiek is ('beste klant') als indicatie voor phishing niet meer heel adequaat: met spearphishing lukt het de aanvallers om de e-mailontvanger bij naam te noemen. Terwijl de offline criminaliteit flink afneemt in dit coronatijdperk, lijkt de online criminaliteit alleen maar toe te nemen (Flemming 2020; Banken.nl 2020). Omdat het probleem van social engineering daarmee alleen maar belangrijker lijkt te worden, pleiten wij ervoor dat er meer wordt gedaan aan het systematisch ontwikkelen van interventies en het adequaat testen ervan.

doi: 10.5553/JV/016758502020046002009

Literatuur

Aburrous e.a. 2010
M. Aburrous, M.A. Hossain, K. Dahal & F. Thabtah, 'Experimental case studies for investigating e-banking phishing techniques and attack strategies', *Cognitive Computation* (2) 2010, afl. 3, p. 242-253.

Acquisti e.a. 2012
A. Acquisti, L.K. John & G. Loewenstein, 'The impact of relative standards on the propensity to disclose', *Journal of Marketing Research* (49) 2012, afl. 2, p. 160-174.

Alnajim & Munro 2009
A. Alnajim & M. Munro, 'An anti-phishing approach that uses training intervention for phishing websites detection', *ITIG 2009 – 6th International Conference on Information Technology: New generations*, 2009, p. 405-410.

Arachchilage & Cole 2011
N.A.G. Arachchilage & M. Cole, 'Design a mobile game for home computer users to prevent from "phishing attacks"', *Information Society (i-Society)* 2011, p. 485-489.

Arachchilage e.a. 2016
N.A.G. Arachchilage, S. Love & K. Beznosov, 'Phishing threat avoidance behaviour: An empirical investigation', *Computers in Human Behavior* (60) 2016, p. 185-197.

Argo & Main 2004
J.J. Argo & K.J. Main, 'Meta-analyses of the effectiveness of warning labels', *Journal of Public Policy and Marketing* (23) 2004, afl. 2, p. 193-208.

Bada e.a. 2015
M. Bada, A.M. Sasse & J.R.C. Nurse, *Cyber security awareness campaigns: Why do they fail to change behaviour?*, 2015, www.cs.ox.ac.uk/files/7194/csss2015_bada_et_al.pdf.

Banken.nl 2020
Banken.nl, 'Scherpe toename phishing vanwege corona', 2020, www.banken.nl/nieuws/22291/scherpe-toename-phishing-vanwege-corona.

Barth e.a. 2019
S. Barth, M.D.T. de Jong, M. Junger, P.H. Hartel e.a. 'Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources', *Telematics and Informatics* (41) 2019, p. 55-69.

Blakeborough & Correia 2017
L. Blakeborough & S. Correia, *The scale and nature of fraud: A review of the evidence*, 2017, www.gov.uk/government/publications/the-scale-and-nature-of-fraud-a-review-of-the-evidence.

doi: 10.5553/JV/016758502020046002009

Borenstein e.a. 2010
M. Borenstein, L.V. Hedges, J.P.T. Higgins & H.R. Rothstein, 'A basic introduction to fixed-effect and random-effects models for meta-analysis', *Research Synthesis Methods* (1) 2010, afl. 2, p. 97-111.

Bullée & Junger 2020a
J.H. Bullée & M. Junger, 'Social engineering', in: T.J. Holt & A.M. Bossler (red.), *Palgrave international handbook of cybercrime and cyberdeviance*, Cham, Zwitserland: Palgrave Macmillan 2020, p. 1-28.

Bullée & Junger 2020b
J.H. Bullée & M. Junger, 'Are interventions against social engineering effective, not effective or do they have adverse effects? A meta-analysis', nog niet gepubliceerd.

Bullée e.a. 2017
J.H. Bullée, L. Montoya, M. Junger & P. Hartel, 'Spear phishing in organisations explained', *Information and Computer Security* (25) 2017, afl. 5, p. 593-613.

Cameron e.a. 2012
C.D. Cameron, J.L. Brown-Iannuzzi & B.K. Payne, 'Sequential priming measures of implicit social cognition: A meta-analysis of associations with behavior and explicit attitudes', *Personality and Social Psychology Review* (16) 2012, afl. 4, p. 330-350.

Campbell & Stanley 1963
D.T. Campbell & J.C. Stanley, *Experimental and quasi-experimental designs for research*, Boston, MA: Houghton, Mifflin Company 1963.

Canova e.a. 2015
G. Canova, M. Volkamer, C. Bergmann & B. Reinheimer, *NoPhish app evaluation: Lab and retention study* (NDSS workshop on usable security 2015), 2015.

Caputo e.a. 2014
D.D. Caputo, S.L. Pfleeger, J.D. Freeman & M.E. Johnson, 'Going spear phishing: Exploring embedded training and awareness', *IEEE Security and Privacy* (12) 2014, afl. 1, p. 28-38.

Christin e.a. 2011
N. Christin, S. Egelman, T. Vidas & J. Grossklags, 'It's all about the benjamins: An empirical study on incentivizing users to ignore security advice', *International Conference on Financial Cryptography and Data Security*, 2011, p. 16-30.

Clark & Mayer 2016
R.C. Clark & R.E. Mayer, *E-learning and the science of instruction: Proven guidelines for consumers and designers of multimedia learning*, Hoboken, NJ: John Wiley & Sons 2016.

Cohen 2013
J. Cohen, *Statistical power analysis for the behavioral sciences*, New York, NY: Routledge 2013.

doi: 10.5553/JV/016758502020046002009

Davinson & Sillence 2010
N. Davinson & E. Sillence, 'It won't happen to me: Promoting secure behaviour among internet users', *Computers in Human Behavior* (26) 2010, afl. 6, p. 1739-1747.

Dodge e.a. 2007
R.C. Dodge, C. Carver & A.J. Ferguson, 'Phishing for user security awareness', *Computers & Security* (26) 2007, afl. 1, p. 73-80.

Dolan e.a. 2010
P. Dolan, M. Hallsworth, D. Halpern, D. King e.a., *MINDSPACE: Influencing behaviour for public policy*, 2010, www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf.

Downs e.a. 2006
J.S. Downs, M.B. Holbrook & L.F. Cranor, 'Decision strategies and susceptibility to phishing', *Proceedings of the Second Symposium on Usable Privacy and Security*, 2006, p. 79-90.

Feder e.a. 2000
L. Feder, A. Jolin & W. Feyerherm, 'Lessons from two randomized experiments in criminal justice settings', *Crime & Delinquency* (46) 2000, afl. 3, p. 380-400.

Flemming 2020
S. Flemming, 'Threat spotlight: Coronavirus-related phishing', 2020, https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/.

Grazioli 2004
S. Grazioli, 'Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet', *Group Decision and Negotiation* (13) 2004, afl. 2, p. 149-172.

Gupta e.a. 2011
M. Gupta, S. Agrawal & N. Garg, 'A survey on social engineering and the art of deception', *International Journal of Innovations in Engineering and Technology* (1) 2011, afl. 1, p. 31-35.

Hadnagy & Wilson 2010
C. Hadnagy & P. Wilson, *Social engineering: The art of human hacking*, New York, NY: Wiley 2010.

Happ e.a. 2016
C. Happ, A. Melzer & G. Steffgen, 'Trick with treat – Reciprocity increases the willingness to communicate personal data', *Computers in Human Behavior* (61) 2016, p. 372-377.

doi: 10.5553/JV/016758502020046002009

Henson e.a. 2016
B. Henson, B.W. Reyns & B.S. Fisher, 'Cybercrime victimization', in: *The Wiley handbook on the psychology of violence*, Chichester: John Wiley & Sons 2016, p. 553-570.

Herzberg & Jbara 2008
A. Herzberg & A. Jbara, 'Security and identification indicators for browsers against spoofing and phishing attacks', *ACM Transactions on Internet Technology* (8) 2008, afl. 4, p. 1-36.

Higgins e.a. 2003
J.P.T. Higgins, S.G. Thompson, J.J. Deeks & D.G. Altman, 'Measuring inconsistency in meta-analyses', *British Medical Journal* (327) 2003, afl. 7414, p. 557-560.

Internet Crime Complaint Center 2018
Internet Crime Complaint Center, *2017 internet crime report*, 2018, https://pdf.ic3.gov/2017_IC3Report.pdf.

Kenrick e.a. 2005
D.T. Kenrick, S.L. Neuberg & R.B. Cialdini, *Social psychology: Unraveling the mystery*, Boston, MA: Allyn & Bacon 2005.

Kirlappos & Sasse 2012
I. Kirlappos & M.A. Sasse, 'Security education against phishing: A modest proposal for a major rethink', *IEEE Security Privacy* (10) 2012, afl. 2, p. 24-32.

Klahr e.a. 2017
R. Klahr, J. Shah, P. Sheriffs, T. Rossington e.a., *Cyber security breaches survey 2017: A survey detailing business action or cyber security and the costs and impacts of cyber breaches and attacks*, 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf.

Kumaraguru e.a. 2007a
P. Kumaraguru, Y. Rhee, A. Acquisti, L.F. Cranor e.a., 'Protecting people from phishing: The design and evaluation of an embedded training email system', *Conference on Human Factors in Computing Systems – Proceedings*, 2007, p. 905-914.

Kumaraguru e.a. 2007b
P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan e.a., 'Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer', *ACM International Conference Proceeding Series. Vol. 269*, 2007, p. 70-81.

Kumaraguru e.a. 2008
P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor e.a., 'Lessons from a real world evaluation of anti-phishing training', *eCrime Researchers Summit*, 2008, p. 1-12.

doi: 10.5553/JV/016758502020046002009

Kumaraguru e.a. 2009
P. Kumaraguru, J. Cranshaw, A. Acquisti, L.F. Cranor e.a., 'School of phish: A real-world evaluation of anti-phishing training', *SOUPS 2009 – Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, p. 1-12.

Kumaraguru e.a. 2010
P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor e.a., 'Teaching Johnny not to fall for phish', *ACM Transactions on Internet Technology* (10) 2010, afl. 2, p. 1-31.

Lastdrager e.a. 2017
E.E. Lastdrager, I. Carvajal Gallardo, P.H. Hartel & M. Junger, 'How effective is anti-phishing training for children?', *SOUPS 2017 – Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017, p. 229-239.

Marinos & Sfakianakis 2012
L. Marinos & A. Sfakianakis, *ENISA threat landscape 2012*, 2012, www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport.

Margulies & Herzberg 2013
R. Margulies & A. Herzberg, *Conducting ethical yet realistic usable security studies*, www.researchgate.net/publication/253954682_Conducting_Ethical_yet_Realistic_Usable_Security_Studies.

Mayhorn & Nyeste 2012
C.B. Mayhorn & P.G. Nyeste, 'Training users to counteract phishing', *Work* (41) 2012, p. 3549-3552.

Monahan & Fisher 2010
T. Monahan & J.A. Fisher, 'Benefits of "observer effects": Lessons from the field', *Qualitative Research* (10) 2010, afl. 3, p. 357-376.

Parsons e.a. 2015
K. Parsons, A. McCormac, M. Pattinson, M. Butavicius e.a. 'The design of phishing studies: Challenges for researchers', *Computers and Security* (52) 2015, p. 194-206.

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. 1, p. 1555-1570.

Schneier 2000
B. Schneier, 'Crypto-gram, October 15, 2000', 2000, www.schneier.com/crypto-gram/archives/2000/1015.html.

doi: 10.5553/JV/016758502020046002009

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', *SOUPS 2007 – Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007, p. 88-99.

Siedler & Sonnenberg 2010
T. Siedler & B. Sonnenberg, 'Experiments, surveys and the use of representative samples as reference data', *German Council for Social and Economic Data (RatSWD)*, 2010.

Sokol e.a. 2017
P. Sokol, M. Glova, T. Mézešová & R. Hučková, 'Lessons learned from phishing test', *25th interdisciplinary information management talks – Digitalization in management, society and economy* 2017, p. 297-304.

Stockhardt e.a. 2016
S. Stockhardt, B. Reinheimer, M. Volkamer, P. Mayer, e.a., Teaching phishing-security: Which way is best?, 31st IFIP International Information Security and Privacy Conference (SEC), May 2016, Ghent, Belgium. p. 135-149. https://hal.inria.fr/hal-01369549/document.

Sundar e.a. 2013
S.S. Sundar, H. Kang, M. Wu, E. Go e.a., 'Unlocking the privacy paradox: Do cognitive heuristics hold the key?', *CHI'13 extended abstracts on human factors in computing systems*, 2013, p. 811-816.

Verizon Risk Team 2018
Verizon Risk Team, *2018 Annual report*, 2018, www.verizon.com/about/sites/default/files/2018-Verizon-Annual-Report.pdf.

Vishwanath 2015
A. Vishwanath, 'Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack', *Journal of Computer-Mediated Communication* (20) 2015, afl. 5, p. 570-584.

Weisburd e.a. 2001
D. Weisburd, C.M. Lum & A. Petrosino, 'Does research design affect study outcomes in criminal justice?', *The ANNALS of the American Academy of Political and Social Science* (578) 2001, afl. 1, p. u50-70.

Welsh e.a. 2011
B.C. Welsh, M.E. Peel, D.P. Farrington, H. Elffers e.a., 'Research design influence on study outcomes in crime and justice: A partial replication with public area surveillance', *Journal of Experimental Criminology* (7) 2011, afl. 2, p. 183-198.

doi: 10.5553/JV/016758502020046002009

Wogalter e.a. 2012
M.S. Wogalter, K.R. Laughery Sr & C.B. Mayhorn, 'Warnings and hazard communications', in: G. Salvendy (red.), *Handbook of human factors and ergonomics*, Hoboken, NJ: Wiley 2012, p. 868-894.

Wright e.a. 2014
R. Wright, M. Jensen, J. Thatcher, M. Dinger e.a., 'Influence techniques in phishing attacks: An examination of vulnerability and resistance', *Information Systems Research* (25) 2014, afl. 2, p. 385-400.

Yang e.a. 2012
C.C. Yang, S.S. Tseng, T.J. Lee, J.F. Weng e.a., 'Building an anti-phishing game to enhance network security literacy learning', *2012 IEEE 12th International Conference on Advanced Learning Technologies*, 2012, p. 121-123.

Yang e.a. 2017
W. Yang, A. Xiong, J. Chen, R. Proctor e.a., 'Use of phishing training to improve security warning compliance: Evidence from a field experiment', *Proceedings of the hot topics in science of security: Symposium and bootcamp*, 2017, p. 52-61.

doi: 10.5553/JV/016758502020046002009

Wat maakt een cyber awareness-campagne effectief?

Anouk van de Beek*

Hoe zouden *cyber awareness*-campagnes effectiever kunnen worden ingericht en beter kunnen worden afgestemd op risicogroepen van cybercrime? Deze vraag stond centraal in een afstudeeronderzoek naar *cyber awareness*-campagnes.[1] Hiervoor is eerst onderzocht wat er op basis van eerdere onderzoeken bekend is over de effectiviteit van *cyber awareness*-campagnes, om vervolgens geïnventariseerde bestaande campagnes te toetsen aan de eisen van effectiviteit. Allereerst blijkt de mate waarin de campagne haar doelgroep bereikt een belangrijke factor. Dit is afhankelijk van de duur en frequentie van de campagne. Doorgaans werken langdurige campagnes beter dan korte, omdat het bewustzijn van mensen vaak na korte tijd weer verdwijnt. De communicatiestrategie van een campagne kan worden afgestemd op verschillende subgroepen door onderscheid te maken op basis van demografische kenmerken. Ook dienen duidelijke, samenhangende en meetbare doelen worden gesteld en moeten betrokken partijen hun aanpak standaardiseren. Het soort doelstelling is namelijk bepalend voor de strategie van een campagne. Zo blijken de Postbus 51-campagnes vooral effectief te zijn in de verandering van kennis. Gedrags- en houdingseffecten zijn echter veel moeilijker haalbaar.

Bovendien moeten preventie- en *awareness*-interventies aansluiten bij het type cybercrime waartegen de campagne is gericht. Zo zal de 'Say No'-campagne, een internationale campagne gericht tegen online seksuele afpersing en intimidatie, zich specifiek moeten richten op het materiaal (de foto of video) en de bedreiging (het afpersen met seksueel getint materiaal). Ook is het van belang verschillende methoden te hanteren, zodat de campagne beter wordt opgemerkt, onthouden, gewaardeerd en begrepen. Daarbij dienen campagnes zich daadwerkelijk op gedragsverandering te richten, enkel

* A. van de Beek MSc behaalde recent haar wo-master Opsporingscriminologie aan de Vrije Universiteit Amsterdam.

1 Het onderzoek kan worden geraadpleegd via de Online Scriptiedatabase van de Vrije Universiteit Amsterdam via www.ubvu.vu.nl/pub/index_oclc.cfm?SearchObjectId=8&objectid=109&ordering=3&openitem=193913.

doi: 10.5553/JV/016758502020046002010

voorlichting is onvoldoende. Naarmate de boodschap van een campagne complexer is, zal het moeilijker zijn gedragseffecten te bereiken.
Het gebruik van meerdere, invloedrijke communicatiekanalen draagt bij aan het succes van een campagne. Factoren die daarbij een rol spelen zijn bestaande maatschappelijke interesse, frequentie van de boodschap en media-aandacht.
Voorts blijkt samenwerking tussen overheid en private partijen een gunstige invloed te hebben op de effectiviteit van campagnes. Daarnaast is het van belang om praktische kennis te combineren met theoretische gedragswetenschappelijke modellen. Onderzoek naar preventieprogramma's laat echter zien dat veel initiatieven niet gebaseerd zijn op een achterliggende theorie.
Ter illustratie: de campagne 'Bescherm je persoonlijke bestanden tegen internetcriminelen' heeft verschillende kenmerken die de effectiviteit bevorderen. Zo is de campagne in 2018 herhaaldelijk ingezet, richt de campagne zich op een brede doelgroep (het algemene publiek), heeft zij duidelijke en samenhangende doelen (aansporen maatregelen te nemen ter voorkoming van ransomware[2]), worden er meerdere communicatiekanalen en -methoden gebruikt (campagnefilmpjes via social media, radiospots), en richt de campagne zich tegen een specifiek type cybercrime (ransomware). Ook vindt er samenwerking plaats tussen verschillende partijen (ministerie van Justitie en Veiligheid en verschillende mediapartners). Door de campagne te evalueren kan nader inzicht worden gekregen in het daadwerkelijke effect ervan.

2 Ransomware is een type schadelijke software dat een computer infecteert en de controle over het primaire besturingssysteem overneemt of de gegevensbestanden versleutelt. Het programma vraagt de gebruiker dan om losgeld (*ransom*) te betalen om weer toegang te krijgen tot het systeem en/of de gegevensbestanden.

doi: 10.5553/JV/016758502020046002010

Ons cybergedrag is veel onveiliger dan we zelf denken

Implicaties voor effectief beïnvloedingsbeleid door de overheid

Rick van der Kleij, Susanne van 't Hoff-de Goede, Steve van de Weijer en Rutger van de Leukfeldt*

In 2018 gaf 8,5% van de internetgebruikers van 12 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van online criminaliteit (CBS 2019). In totaal zijn dat jaar 1,2 miljoen Nederlanders slachtoffer geworden van online criminaliteit. Zo werd 2,9% van de Nederlanders slachtoffer van fraude met online handel en 1% slachtoffer van identiteitsdiefstal (CBS 2019). Recente studies laten zien dat de impact van slachtofferschap van dergelijke delicten hoog kan zijn en dat slachtoffers naast financiële schade diverse vormen van psychologische en emotionele schade ervaren (Cross e.a. 2016; Jansen & Leukfeldt 2018; Leukfeldt e.a. 2018; 2019).
Slachtofferschap van online fraude komt dus veel voor en de impact ervan kan groot zijn voor slachtoffers. Cybersecurityprofessionals hebben geprobeerd slachtofferschap terug te dringen met technische maatregelen, zoals software voor het detecteren van datalekken. Deze maatregelen hebben veelal maar beperkt effect (bijv. Hauer 2015). Een groot deel van slachtofferschap van cybercriminaliteit is terug te voeren op het online gedrag van mensen (Munnichs e.a. 2017; Ancher e.a. 2019). Dit geldt ook voor slachtofferschap van online oplichting en fraude. Internetgebruikers die onbetrouwbare webshops en phish-

* Dr. R. van der Kleij werkt als senior onderzoeker bij het lectoraat Cybersecurity in het mkb aan de Haagse Hogeschool en als senior onderzoeker bij TNO. Dr. S. van 't Hoff-de Goede is als onderzoeker verbonden aan het lectoraat Cybersecurity in het mkb aan de Haagse Hogeschool. Dr. S. van de Weijer is als onderzoeker verbonden aan het NSCR. Dr. E.R. Leukfeldt werkt als lector Cybersecurity in het mkb aan de Haagse Hogeschool en als senior onderzoeker bij het NSCR. Dit artikel bevat een weergave van de belangrijkste uitkomsten van een recent onderzoek naar cybergedrag dat door de auteurs is uitgevoerd in opdracht van het WODC. Delen van dit artikel zijn ook te vinden in Van 't Hoff-de Goede e.a. 2019. Het doel van dit artikel is om op basis van de belangrijkste uitkomsten implicaties voor beleidsmakers te schetsen.

doi: 10.5553/JV/016758502020046002011

ingmails niet herkennen, hebben een grote kans om opgelicht te worden. Daarnaast kan het veelvuldig delen van persoonlijke gegevens de kans op identiteitsdiefstal verhogen. Een belangrijke vraag is daarom hoe veilig we ons online gedragen, en om slachtofferschap van online oplichting en fraude terug te kunnen dringen, is onderzoek naar het online gedrag van mensen dan ook van wezenlijk belang (Leukfeldt 2017; Rhee e.a. 2009; Talib e.a. 2010).

Zeggen is een, doen is twee

Kennis over hoe gebruikers zich (kunnen) weren tegen online criminaliteit is schaars (zie voor een overzicht bijv. Leukfeldt 2017). Het is tot op heden grotendeels onbekend hoe Nederlanders zich beschermen tegen online criminaliteit, onder andere omdat hoe mensen *zeggen* zich online te gedragen niet altijd hetzelfde is als hoe mensen zich *daadwerkelijk* online gedragen (Crossler e.a. 2013; Debatin e.a. 2009; Warkentin e.a. 2012; Workman e.a. 2008).
Voor het empirisch onderbouwen van eventueel beïnvloedingsbeleid door de overheid op het gedrag van internetgebruikers, zoals een publiekscampagne, is dusdanige kennis echter onontbeerlijk. Daarmee kan slachtofferschap van cybercriminaliteit mogelijk zelfs worden voorkomen. Daarom hebben de Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) een onderzoek uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) om in kaart te brengen hoe veilig Nederlanders zich online zeggen te gedragen, hoe (on)veilig ze zich daadwerkelijk gedragen en welke verklaringen hiervoor zijn (Van 't Hoff-de Goede e.a. 2019). In dit artikel gaan wij in op de belangrijkste uitkomsten van dit onderzoek, en hierbij staan de volgende onderzoeksvragen centraal: Welke factoren hangen samen met veilige online gedragingen? En wat zijn hiervan de beleidsimplicaties om slachtofferschap van cybercriminaliteit te voorkomen?
Om cybergedrag in kaart te brengen maakten we gebruik van het COM-B-gedragsmodel (Capability, Opportunity, Motivation – Behaviour), wat veronderstelt dat Capability, Opportunity en Motivation (COM) gezamenlijk leiden tot Behaviour (B). In het Nederlands: gedrag wordt aangedreven door kennis, gelegenheid en motivatie. Op basis van dit theoretische verklaringsmodel verwachten we aldus dat

doi: 10.5553/JV/016758502020046002011

de mate waarin mensen zich online veilig gedragen, afhangt van de kennis die mensen bezitten over risico's en manieren om zichzelf te beschermen, de gelegenheid die zij daartoe hebben en de mate waarin zij gemotiveerd zijn om zich veilig te gedragen (zie ook Michie e.a. 2011). Deze factoren hebben we meegenomen in ons onderzoek. Dit gedragsmodel is nog niet eerder gebruikt om cybergedrag te onderzoeken. Daarnaast nemen we ook andere factoren mee die in de literatuur worden genoemd als mogelijk relevant voor cybergedrag. In dit artikel bespreken we een selectie van deze factoren, namelijk: gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, type apparaat en tijdsdruk.

De gemoedstoestand kan besluitvorming beïnvloeden en heeft een effect op de strategieën die we kiezen bij het nemen van beslissingen. Gemoedstoestand wordt gedefinieerd als een emotionele toestand die ten minste enige minuten aanhoudt (Matthews e.a. 1995). Deze gemoedstoestand kan positief zijn of negatief. Voorbeelden van positieve dan wel negatieve gemoedstoestanden zijn respectievelijk enthousiast en overstuur. Matthews en collega's (1995) vonden dat informatie die past bij de gemoedstoestand sneller wordt gevonden in het geheugen. Een negatieve gemoedstoestand kan er bijvoorbeeld toe leiden dat mensen minder risico's nemen, omdat zij makkelijker toegang hebben tot negatieve gedachten over de uitkomst van het risicovolle gedrag. Daarnaast kan angst voor slachtofferschap of eerder slachtofferschap verschillende gevolgen hebben voor cybergedrag, zoals vermijdingsgedrag, maar ook het nemen van minder risico's online (Boss e.a. 2015). Ook is het apparaat dat gebruikt wordt om online te gaan van belang. Apparaten die mensen thuis gebruiken voor online activiteiten, zoals een smartphone, tablet, laptop of desktopcomputer, verschillen op een aantal dimensies die van invloed zijn op cybergedrag, en kunnen van invloed zijn op slachtofferschap. Vishwanath (2016) heeft al laten zien dat mobiele gebruikers vaker slachtoffer worden van phishing dan gebruikers van een desktopcomputer. Door de draagbaarheid, het gebruiksgemak en de beschikbaarheid zijn gebruikers van mobiele apparaten meer cognitief ontspannen, zo luidt de verklaring, wat leidt tot meer gewoontegedrag (zoals het klikken op hyperlinks) en daarmee tot verhoogde kans op slachtofferschap. Tot slot zou tijdsdruk ervoor kunnen zorgen dat mensen signalen dat zij risico lopen, negeren en zodoende meer risico's nemen. Een veelgebruikte strategie die mensen hanteren in het omgaan met tijdsdruk is

doi: 10.5553/JV/016758502020046002011

het gebruiken van meer oppervlakkige (heuristische) informatieverwerking (Alison e.a. 2013). Dit kan betekenen dat zij belangrijke cues die kunnen duiden op risico's die zijn verbonden aan het handelen, zoals het klikken op een hyperlink, over het hoofd zien. De huidige studie heeft dan ook onderzocht in hoeverre cybergedrag kan worden verklaard door alle hierboven genoemde factoren.
Dit artikel vat de belangrijkste resultaten samen van het door de auteurs uitgevoerde onderzoek en sluit af met enkele beleidsimplicaties. Wie meer wil lezen over het onderzoek verwijzen we naar het onderzoeksrapport (Van 't Hoff-de Goede e.a. 2019). De volgende paragraaf behandelt de methodologie die is gebruikt voor het onderzoek. In de paragraaf daarna worden de belangrijkste bevindingen van het vragenlijstonderzoek en de gedragsmetingen gepresenteerd. Deze paragraaf focust op het beantwoorden van de belangrijkste onderzoeksvragen, die aan de basis lagen van dit onderzoek. De laatste paragraaf staat stil bij de beleidsimplicaties en vervolgonderzoek.

Methode

Voor de uitvoering van het onderzoek zijn verschillende methoden gebruikt: een vragenlijst, objectieve gedragsmetingen en een discussiebijeenkomst. Op basis van een systematische literatuurstudie is een vragenlijst ontwikkeld die met behulp van een panelbureau is uitgezet. De uiteindelijke steekproef bestaat uit 2.426 personen en is representatief voor de Nederlandse samenleving met betrekking tot geslacht, arbeidsstatus en de provincie waarin men woont. Respondenten zijn echter vaker dan gemiddeld in Nederland hoogopgeleid (50,0% versus 30,0%). Ook zijn respondenten minder vaak dan gemiddeld jonger dan 39 jaar (13,8% versus 29,4%). In de vragenlijst is cybergedrag gemeten door enerzijds vragen, stellingen en vignetten voor te leggen aan de respondenten. Anderzijds zijn objectieve metingen van gedrag gedaan. Tijdens het invullen van de vragenlijst zijn respondenten drie gesimuleerde cyberrisicosituaties tegengekomen, waar zij onwetend van waren. Hierbij hebben wij bekeken hoe de respondenten met deze situaties omgingen. Allereerst is de respondenten aan het begin van de vragenlijst gevraagd om een gebruikersnaam en wachtwoord aan te maken, waarbij wij de sterkte van het gekozen wachtwoord konden achterhalen. Verder verscheen er tijdens de vragenlijst ineens een

doi: 10.5553/JV/016758502020046002011

pop-up, waarin stond dat om verder te kunnen gaan met de vragenlijst er software moest worden gedownload. Deze software was afkomstig uit een onbetrouwbare bron. Ook hier konden we zien welke keuze de respondenten maakten: downloaden, niet downloaden of zelfs helemaal stoppen met de vragenlijst. Tot slot werden de respondenten aan het eind van de vragenlijst nog gevraagd om de volgende gegevens: volledige naam, e-mailadres, e-mailadres van een bekende, geboortedatum, postcode, huisnummer en de laatste drie cijfers van hun rekeningnummer. Voor elk van deze gegevens konden wij inzien of ze waren ingevuld of niet. Door deze combinatie van metingen geeft het onderzoek dan ook inzicht in welke mate mensen denken zich veilig of onveilig te gedragen en in welke mate mensen daadwerkelijk veilig of onveilig cybergedrag vertonen.
Ten slotte zijn de resultaten van de analyses besproken met experts uit verschillende werkvelden tijdens een discussiebijeenkomst. Doel van deze bijeenkomst was om te komen tot een eerste aanzet tot praktisch bruikbare aanbevelingen om cyberrisico's te voorkomen of tegen te gaan. Daarom is voorafgaand aan de bijeenkomst eerst een literatuurstudie gedaan naar bestaande interventies die gedragsverandering bewerkstelligen. Tijdens de bijeenkomst zijn de resultaten bediscussieerd en konden de experts kritisch reflecteren op de gebruikte onderzoeksmethoden, de resultaten en veelbelovende richtingen voor interventies die zorgen voor veilig cybergedrag.

Vragenlijstonderzoek en gedragsmetingen

Slachtofferschap van online criminaliteit

Allereerst tonen wij in deze paragraaf in hoeverre slachtofferschap van online criminaliteit voorkomt binnen de steekproef. Slachtofferschap van online criminaliteit blijkt hoog; bijna de helft van de respondenten (48,1%) is ooit slachtoffer geworden van een online delict (in het afgelopen jaar en/of langer dan een jaar geleden).
In tabel 1 wordt de prevalentie van slachtofferschap per type delict beschreven. In totaal werd 13,6% van de respondenten het afgelopen jaar slachtoffer van online criminaliteit. Respondenten werden afgelo-

doi: 10.5553/JV/016758502020046002011

Tabel 1 Prevalentie van slachtofferschap en geleden schade per type delict

Cybercrime	Ja, <12 maanden	Ja, >12 maanden	Nee	Weet ik niet	Schade (incident <12 maanden)
Phishing	70 (2,9%)	114 (4,7%)	2.110	132	37 (52,9%)
Malware	177 (7,3%)	611 (25,2%)	1.417	221	104 (58,8%)
Online aankoopfraude	48 (2,0%)	190 (7,8%)	2.172	16	45 (93,8%)
Online identiteitsfraude	10 (0,4%)	17 (0,7%)	2.324	75	8 (80,0%)
Voorschotfraude	7 (0,3%)	17 (0,7%)	2.392	10	3 (42,9%)
Profielpagina veranderd	9 (0,4%)	36 (1,5%)	2.336	45	5 (55,6%)
Online account gehackt	16 (0,7%)	61 (2,5%)	2.224	125	11 (68,8%)
Computer gehackt	9 (0,4%)	35 (1,4%)	2.322	60	8 (88,9%)
E-mailaccount gehackt	23 (0,9%)	74 (3,1%)	2.149	180	11 (47,8%)
Bestanden ontoegankelijk	9 (0,4%)	93 (3,8%)	2.206	118	5 (55,6%)
Andere vorm van cybercrime	29 (1,2%)	73 (3,0%)	2.192	132	26 (89,7%)
Totaal (unieke personen)	**330 (13,6%)**	**951 (39,2%)**			**214 (64,8%)**

pen jaar het vaakst slachtoffer van malware[1] (7,3%), gevolgd door phishing[2] (2,9%) en online aankoopfraude[3] (2,0%). Ook werd 39,2% van de respondenten langer dan een jaar geleden één of meerdere keren slachtoffer van online criminaliteit. Ook in deze periode is slachtofferschap het hoogst voor malware (25,2%), online aankoopfraude (7,8%) en phishing (4,7%), gevolgd door 'bestanden zijn ontoegankelijk gemaakt' (bijvoorbeeld door ransomware) (3,8%) en hacking

1 Malware is kwaadaardige software die ongevraagd en meestal ongemerkt op de computer wordt geïnstalleerd. Voorbeelden van malware zijn virussen, Trojan horses, wormen en spyware.
2 Phishing is een vorm van online oplichting, waarbij criminelen e-mails of websites van legitieme instanties namaken om slachtoffers te misleiden, om zodoende inloggegevens te achterhalen en toegang te krijgen tot online accounts.
3 Hierbij wordt een product of dienst via internet gekocht en is ten minste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is.

doi: 10.5553/JV/016758502020046002011

van een e-mailaccount (3,1%).[4] Slachtofferschap van andere vormen van online fraude – identiteitsfraude en voorschotfraude – kwam slechts in beperkte mate voor binnen deze steekproef. Het aantal slachtoffers dat schade heeft ondervonden van het slachtofferschap dat afgelopen jaar heeft plaatsgevonden, is – in lijn met recent onderzoek – zeer groot (Cross e.a. 2016; Jansen & Leukfeldt 2018; Leukfeldt e.a. 2018). Gemiddeld rapporteert 64,8% van de slachtoffers schade, omdat het incident ervoor heeft gezorgd dat zij geld, tijd of bestanden zijn kwijtgeraakt of emotionele schade of andere schade hebben ondervonden (tabel 1). Het percentage slachtoffers dat dergelijke schade ondervindt, is echter afhankelijk van het type delict en varieert tussen 43% tot 94%.

Hoe veilig gedragen Nederlanders zich online?

Dat burgers zich online onveilig gedragen, komt deels naar voren uit de analyses over zelfgerapporteerd gedrag, maar vooral ook tijdens de objectieve metingen van gedrag. Onveilig gedrag blijkt in hoge mate voor te komen. Zo gebruikt meer dan 40% een zwak wachtwoord van zeven of minder tekens,[5] downloadt 40% onveilige software en deelt ongeveer 30% van de respondenten persoonlijke gegevens, zoals hun volledige naam, geboortedatum en e-mailadres.
Het blijkt echter dat er grote verschillen bestaan tussen het zelfgerapporteerde gedrag en het objectieve gedrag. Uit de objectieve metingen blijkt steeds dat mensen zich nog onveiliger gedragen dan ze rapporteren te doen. Respondenten geven, bijvoorbeeld, middels zelfrapportage aan zich (zeer) veilig online te gedragen (bijvoorbeeld niet downloaden uit illegale bron en geen gebruik maken van openbare wifi), terwijl uit objectieve metingen blijkt dat 40% van de respondenten onbekende software downloadt als er een pop-up verschijnt tijdens een video die niet wil afspelen. De resultaten van de huidige studie onderschrijven dan ook het belang van het doen van objectieve metingen van cybergedrag.

4 Hierbij moet worden opgemerkt dat het aantal respondenten dat als antwoord 'weet ik niet' invulde, sterk verschilt per type delict. Bij slachtofferschap van malware, bijvoorbeeld, antwoordden liefst 221 respondenten 'weet ik niet', wat neerkomt op 9,1% van de totale steekproef. Dit betekent dat het percentage respondenten dat slachtoffer is geworden van malware ook toeneemt wanneer alleen gekeken zou worden naar de respondenten die deze vraag wel beantwoord hebben: respectievelijk 8,0% en 27,7% van deze respondenten waren het afgelopen jaar of langer geleden slachtoffer van malware.

5 Zie www.informatiebewust.nl/hoe-maak-je-een-sterk-wachtwoord/.

doi: 10.5553/JV/016758502020046002011

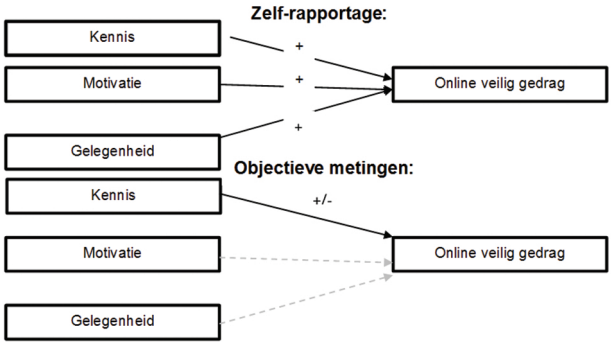
We onderzochten ook of de verschillende cybergedragingen samenhangen. Bijvoorbeeld, gedragen mensen die een sterk wachtwoord kiezen zich gemiddeld ook veiliger op andere cybergedrag? Deze vraag kan eveneens negatief worden beantwoord. De resultaten van de huidige studie wijzen erop dat hoe veilig mensen zich gedragen in een bepaald cybergedragscluster zeer beperkt samenhangt met hoe veilig zij zich gedragen in een ander cybergedragscluster. Wanneer iemand bijvoorbeeld met betrekking tot het omgaan met een phishinge-mail veilig gedrag laat zien, betekent dit niet dat hij zich gemiddeld ook veilig zal gedragen op het gebied van het kiezen van een sterk wachtwoord.
Een kanttekening is hierbij op zijn plaats. Hoewel de methode – een survey met experimenten – heel geschikt is om dit soort onderzoek te doen, hebben we natuurlijk ook te maken met respondenten die zich misschien veilig wanen in de online omgeving van het panelbureau. Hierdoor hebben zij mogelijk sneller onveilige keuzes gemaakt dan anders. Dit kan betekenen dat in de thuissituatie het percentage onveilig gedrag lager is dan door ons is gemeten via het panelonderzoek. Overigens was het juist onze bedoeling om cybergedrag in een veilige omgeving te meten – criminelen bootsen immers altijd een veilige omgeving (van bijvoorbeeld een bank of webshop) na en verleiden mensen hiermee op de hyperlink te klikken of persoonlijke informatie weg te geven –, maar toch kan deze methode tot een vertekening van de resultaten hebben geleid. Daadwerkelijk gedrag zou dus ook in andere contexten moeten worden gemeten. Bijvoorbeeld door het loggen van computers over een langere periode, waardoor oorzaak en gevolg beter bestudeerd kunnen worden.

Kan het cybergedrag worden verklaard door kennis, motivatie of gelegenheid?

Op basis van de literatuur kan worden geconcludeerd dat kennis, gelegenheid en motivatie van gebruikers belangrijke voorspellende factoren van gedrag zijn. De verwachting was dat deze factoren ook samenhangen met cybergedrag. Uit de zelfrapportage komt ook precies dat beeld: zowel kennis als gelegenheid en motivatie hangen positief samen met zelfgerapporteerd veilig cybergedrag. Als we echter kijken naar daadwerkelijk cybergedrag, dan ontstaat er een ander beeld. Alleen kennis blijkt significant samen te hangen met een drietal gedra-

doi: 10.5553/JV/016758502020046002011

Figuur 1 Resultaten COM-B-model



gingen: het delen van persoonlijke gegevens, wachtwoordsterkte en het downloaden van onveilige software. Hoe meer kennis respondenten hebben van online veiligheid, hoe veiliger hun cybergedrag is op het gebied van het delen van persoonlijke gegevens. Het verband tussen kennis en de overige twee gedragingen komt echter niet overeen met de verwachting uit de theorie: deze verbanden zijn negatief. Hoe meer kennis mensen bezitten over risico's en manieren om zichzelf te beschermen, hoe minder sterk het wachtwoord dat ze aanmaken en hoe makkelijker ze onveilige software downloaden. Een mogelijke verklaring is dat mensen zich door deze kennis veilig wanen en bereid zijn meer risico's nemen. Figuur 1 vat de resultaten met betrekking tot het COM-B-model samen.

Welke andere factoren spelen een rol?

Naast kennis, gelegenheid en motivatie zijn op basis van de literatuurstudie verschillende andere factoren meegenomen in de analyses die mogelijk samenhangen met cybergedrag. We bekeken daarom of cybergedrag samenhangt met gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap, type apparaat en tijdsdruk. Om tijdsdruk te manipuleren zijn de respondenten willekeurig toegewezen aan twee tijdsdrukcondities (hoog, laag). In alle analyses is bovendien

doi: 10.5553/JV/016758502020046002011

gecontroleerd voor demografische factoren en de zelfcontrole van respondenten.

Zelfgerapporteerd cybergedrag hangt samen met een aantal van de hierboven genoemde factoren. Een negatieve gemoedstoestand hangt negatief samen met zelfgerapporteerd veilig cybergedrag. Ofwel, hoe groter de negatieve gemoedstoestand van respondenten, hoe minder veilig hun zelfgerapporteerde cybergedrag is. Een positieve gemoedstoestand hangt daarentegen positief samen met de veiligheid van zelfgerapporteerd cybergedrag. Op basis van eerder onderzoek hadden we verwacht dat een positieve gemoedstoestand juist negatief zou samenhangen met veilig gedrag (Isen 2001; Nygren e.a. 1996). Nederlanders met een positieve gemoedstoestand zien de uitkomsten van risicovolle situaties sneller als meer positief en zijn dan ook meer bereid om risico's te nemen, zo was de verwachting. De resultaten laten echter een ander beeld zien. Een verklaring kan op basis van de huidige studie niet worden gegeven. Het type apparaat waarop de vragenlijst is ingevuld, hangt ook samen met zelfgerapporteerd gedrag: respondenten die een pc of laptop gebruikten, geven aan zich veiliger online te gedragen dan respondenten die een tablet gebruikten.

Kijken we echter naar daadwerkelijk gedrag, dan blijven alleen een positieve gemoedstoestand, angst voor slachtofferschap, eerder slachtofferschap en type apparaat over. Een positieve gemoedstoestand hangt samen met zowel de wachtwoordsterkte als het downloaden van software van een onbetrouwbare bron, maar in tegenovergestelde richting. Hoe groter de positieve gemoedstoestand van respondenten, hoe sterker het gekozen wachtwoord. Daarentegen is, in lijn met de literatuur, gevonden dat hoe groter de positieve gemoedstoestand van respondenten, hoe groter de kans is dat zij een onveilige keuze maken bij de softwarepop-up. De positieve gemoedstoestand hangt samengenomen dan ook samen met zowel veilig als onveilig cybergedrag; afhankelijk van het type cybergedrag is dit verband negatief of positief. Angst voor slachtofferschap hangt positief samen met wachtwoordsterkte: hoe meer angst respondenten hebben om slachtoffer te worden van online criminaliteit, hoe sterker het door hen gekozen wachtwoord is. Eerder slachtofferschap daarentegen is negatief gerelateerd aan de veiligheid van daadwerkelijk klikgedrag: respondenten die ooit eerder slachtoffer zijn geworden van online criminaliteit maken significant minder vaak een veilige keuze bij de softwarepop-up. Het type apparaat heeft ook invloed op daadwerkelijk

doi: 10.5553/JV/016758502020046002011

cybergedrag. Respondenten die een pc of laptop gebruiken, kiezen een minder sterk wachtwoord dan respondenten die een tablet gebruiken. Datzelfde geldt voor het wel of niet downloaden van software van een onbetrouwbare bron en het delen van persoonlijke gegevens. Respondenten die een smartphone gebruikten, maken bovendien vaker een veilige keuze dan respondenten op een tablet bij het downloaden. Tot slot vinden we dat tijdsdruk geen effect heeft op het cybergedrag van Nederlanders.

Verschilt het cybergedrag van Nederlanders tussen bevolkingsgroepen?

Enkele van de achtergrondkenmerken van respondenten hangen samen met zelfgerapporteerd cybergedrag. Hoe hoger de leeftijd, hoe veiliger het gerapporteerde cybergedrag en hoe veiliger omgegaan wordt met hyperlinks in phishinge-mails. Voor opleiding is de relatie negatief: hoe hoger de opleiding, hoe minder veilig het zelfgerapporteerde cybergedrag is.
Bij daadwerkelijk cybergedrag vinden we ook een aantal relaties met kenmerken van respondenten, waarvoor we overigens geen verklaring hebben. Zo heeft het hebben van werk een significant verband met zowel wachtwoordsterkte als het wel of niet downloaden van software van een onbetrouwbare bron. Werkenden kiezen een minder sterk wachtwoord en downloaden vaker de software uit onbetrouwbare bron. Daarnaast kiezen respondenten met een hogere opleiding een minder sterk wachtwoord, maar gedragen zij zich wel veiliger op het gebied van delen van persoonlijke gegevens. Het klikgedrag van mannen is gemiddeld minder veilig dan dat van vrouwen en zij delen eveneens meer persoonlijke gegevens. Samenwonenden vertonen daarentegen juist veiliger klikgedrag. Tot slot lijkt het erop dat hoe ouder Nederlanders zijn, hoe meer persoonlijke gegevens zij delen.

Beleidsimplicaties

Heel bewust is er in dit onderzoek voor gekozen om zowel zelfgerapporteerd cybergedrag als daadwerkelijk cybergedrag te meten. We weten immers dat hoewel de meeste mensen aangeven cybersecurity belangrijk te vinden, het werkelijke gedrag van mensen lang niet altijd gelijk is aan hun attitudes of gepercipieerd gedrag. Toch wordt beleid

doi: 10.5553/JV/016758502020046002011

regelmatig gebaseerd op zogenaamde flitspeilingen, ofwel korte enquêtes, onder de Nederlandse bevolking (zie bijv. Paardekoper 2019). Onze studie laat zien dat respondenten een te rooskleurig beeld lijken te hebben van hun eigen cybergedrag wanneer we hun zelfgerapporteerde scores van gedrag vergelijken met hun daadwerkelijke gedrag. Een voorbeeld: daar waar respondenten over het algemeen rapporteren een veilig wachtwoordbeleid te voeren, komt uit de objectieve meting een heel ander beeld naar voren. Meer dan 40% van de respondenten gebruikt een zwak wachtwoord bestaande uit minder dan zeven karakters voor het beveiligen van hun persoonsgegevens in dit onderzoek. Een vergelijkbaar beeld komt naar voren voor wat betreft het downloaden van software van een onbetrouwbare bron. Ook hier zien we dat meer dan 40% van de respondenten onveilig gedrag vertoont door goedkeuring te geven voor het downloaden van software van een onbekende bron. De waarde van flitspeilingen of andere vormen van vragenlijstonderzoek voor het vaststellen van beleid valt daarmee dus te betwisten. Wij pleiten er dan ook voor om beleid te baseren op objectieve metingen van gedrag. Door het gebruik van objectieve metingen van gedrag is de toegevoegde waarde van onderhavig onderzoek dan ook evident: we gaan verder dan bestaande onderzoeken door gepercipieerd en daadwerkelijk gedrag te meten op basis van een representatieve steekproef.

Het belang van meer kennis bij het bestrijden van online criminaliteit wordt bovendien overschat door de overheid, zo blijkt uit de vele zogenaamde bewustmakingscampagnes die door haar worden gefinancierd. Bewustmakingscampagnes worden vaak gelanceerd vanuit de veronderstelling dat kennis over cybersecurity ontbreekt. Terwijl in feite andere factoren leiden tot onveilig digitaal gedrag, zoals slecht ontworpen securitydesign van alledaagse toepassingen of rationaliseringstechnieken die mensen gebruiken om hun eigen onveilige gedrag te rechtvaardigen. Bewustmakingscampagnes zijn dan ook veelal onsuccesvol (Blythe & Coventry 2018). Om goed beleid te ontwikkelen is een gedegen analyse van het onveilige gedrag van mensen nodig. Ten eerste is het van belang te begrijpen waarom mensen zich onveilig gedragen. Op basis van deze inzichten kunnen dan maatregelen worden genomen die de oorzaken wegnemen van het onveilige gedrag. Deze studie laat echter zien dat verschillende mensen zich op verschillende manieren onveilig gedragen. Kennis, gelegenheid en motivatie zijn bovendien nauwelijks gecorreleerd aan de in dit onder-

doi: 10.5553/JV/016758502020046002011

zoek gemeten objectieve gedragingen. Dat maakt het bepalen van geschikte interventies op gedrag nog complexer.
Desalniettemin zou het uitgangspunt bij het ontwerpen van interventies naar onze mening moeten zijn dat het onveilige gedrag van mensen op voorhand wordt verhinderd en veilig gedrag wordt gestimuleerd. Om dit te bereiken is het aanpassen van het securitydesign waarschijnlijk het meest effectief. Door in de ontwerpfase al bewust online diensten in te richten op veilig gebruik wordt de eindgebruiker ontlast of gedwongen veilig te handelen.[6] In de praktijk is momenteel nog onvoldoende aandacht voor het aanpassen van het securitydesign. Bij het ontwerpen van online diensten moet van de grond af aan worden nagedacht over de veiligheid van de eindgebruiker. Dit zogenaamde *security by design*-denken staat echter nog in de kinderschoenen.[7] Om digitaal gedrag van eindgebruikers te beïnvloeden via het design van het systeem is meer kennis nodig. Vervolgens dient deze te worden vertaald naar concrete handvatten voor securityprofessionals in de praktijk.

Literatuur

Alison e.a. 2013
L. Alison, B. Doran, M.L. Long, N. Power, e.a., 'The effects of subjective time pressure and individual differences on hypotheses generation and action prioritization in police investigations', *Journal of Experimental Psychology: Applied, 19*(1), p. 83-93.

Ancher e.a. 2019
M. Ancher, R. van der Kleij & E.R. Leukfeldt, 'Studenten treden in voetsporen cybercrimineel om meer inzicht te krijgen in sociaal engineering', *Informatiebeveiliging Magazine* (19) 2019, afl. 2, p. 26-33.

6 Zie ook KIA veiligheid, oktober 2019, www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/KIA%20Veiligheid%20-%2020191016%20definitief.pdf.
7 Zie www.computable.nl/artikel/opinie/security/6305688/1509029/security-by-design-in-9-stappen.html.

doi: 10.5553/JV/016758502020046002011

Boss e.a. 2015
S.R. Boss, D. Galletta, P.B. Lowry, P. Polak, 'What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users', *MIS Quarterly* 39(4), p. 837.

Blythe & Coventry 2018
J. Blythe & L. Coventry, 'Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, vol. 87 2018, p. 87-97.

CBS 2019
CBS, *Digitale veiligheid & criminaliteit 2018*, Den Haag 2019.

Cross e.a. 2016
C. Cross, K. Richards & R.G. Smith, 'The reporting experiences and support needs of victims of online fraud', *Trends & Issues in Crime and Criminal Justice* 2016, afl. 518, p. 1-14.

Crossler e.a. 2013
R.E. Crossler, A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin & R. Baskerville, 'Future directions for behavioral information security research', *Computers and Security* (32) 2013, p. 90-101.

Debatin e.a. 2009
B. Debatin, J.P. Lovejoy, A.K. Horn & B.N. Hughes, 'Facebook and online privacy: Attitudes, behaviors, and unintended consequences', *Journal of Computer-Mediated Communication* (15) 2009, afl. 1, p. 83-108.

Hauer 2015
B. Hauer, 'Data and information leakage prevention within the scope of information security', *IEEE Access* (3) 2015, p. 2554-2565.

Van 't Hoff-de Goede e.a. 2019
S. van 't Hoff-de Goede, R. van der Kleij, S. van de Weijer & E.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.

Isen 2001
A.M. Isen, 'An influence of positive affect on decision making in complex situations: Theoretical issues with practical implications', *Journal of Consumer Psychology* (11) 2001, afl. 2, p. 75-85.

doi: 10.5553/JV/016758502020046002011

Jansen & Leukfeldt 2018
J. Jansen & E.R. Leukfeldt, 'Coping with cybercrime victimization: An exploratory study into impact and change', *Journal of Qualitative Criminal Justice & Criminology* (6) 2018, afl. 2, p. 205-228.

Leukfeldt 2017
E.R. Leukfeldt (red.), *Research agenda. The human factor in cybercrime and cybersecurity*, Den Haag: Eleven International Publishing 2017.

Leukfeldt e.a. 2018
E.R. Leukfeldt, R. Notté & M. Malsch, *Slachtofferschap van online criminaliteit*, Den Haag: WODC 2018.

Leukfeldt e.a. 2019
E.R. Leukfeldt, R.J. Notté & M. Malsch, 'Exploring the needs of victims of cyber-dependent and cyber-enabled crimes', *Victims and Offenders* (15) 2019, afl. 1, p. 60-77.

Matthews e.a. 1995
G. Matthews, D. Pitcaithly & R.L.E. Mann, 'Mood, neuroticism, and the encoding of affective words', *Cognitive Therapy and Research*, 19, p. 563-587.

Michie e.a. 2011
S. Michie, M.M. van Stralen & R. West, 'The behaviour change wheel: A new method for characterising and designing behaviour change interventions', *Implementation Science* (6) 2011/42.

Munnichs e.a. 2017
G. Munnichs, M. Kouw & L. Kool, *Een nooit gelopen race. Over cyberdreigingen en versterking van weerbaarheid*, Den Haag: Rathenau Instituut 2017.

Nygren e.a. 1996
T.E. Nygren, A.M. Isen, P.J. Taylor & J. Dulin, 'The influence of positive affect on the decision rule in risk situations: Focus on outcome (and especially avoidance of loss) rather than probability', *Organizational Behavior and Human Decision Processes* (66) 1996, afl. 1, p. 59-72.

Paardekoper 2019
A. Paardekooper, 'Flitspeilingen voor burgerparticipatie: de aanpak van Utrecht & Tilburg', *Frankwatching* 2019, www.frankwatching.com/archive/2019/03/22/flitspeilingen-voor-burgerparticipatie-de-aanpak-van-utrecht-tilburg/.

Rhee e.a. 2009
H.S. Rhee, C. Kim & Y.U. Ryu, 'Self-efficacy in information security: Its influence on end users' information security practice behavior', *Computers and Security* (28) 2009, afl. 8, p. 816-826.

doi: 10.5553/JV/016758502020046002011

Talib e.a. 2010
S. Talib, N.L. Clarke & S.M. Furnell, 'An analysis of information security awareness within home and work environments', *ARES 2010 – 5th International Conference on Availability, Reliability, and Security*, 2010, p. 196-203.

Vishwanath 2016
A. Vishwanath, 'Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks', *Computers in Human Behavior, 63*, p. 198-207.

Warkentin e.a. 2012
M. Warkentin, D. Straub & K. Malimage, 'Featured talk. Measuring secure behavior: A research commentary', *Annual Symposium on Information Assurance & Secure Knowledge Management (ASIA & SKM)*, 2012.

Workman e.a. 2008
M. Workman, W.H. Bommer & D. Straub, 'Security lapses and the omission of information security measures: A threat control model and empirical test', *Computers in Human Behavior* (24) 2008, afl. 6, p. 2799-2816.

doi: 10.5553/JV/016758502020046002011

Summaries

Justitiële verkenningen (Judicial explorations) is published six times a year by the Research and Documentation Centre of the Dutch Ministry of Justice and Security in cooperation with Boom juridisch. Each issue focuses on a central theme related to judicial policy. The section Summaries contains abstracts of the internationally most relevant articles of each issue. The central theme of this issue (no. 2, 2020) is .

Corona crisis and fraud: four possible relationships
Clarissa Meerts and Wim Huisman
This contribution contains several concrete examples of 'Corona crime' thereby showing how the current crisis is creating new opportunities for committing crimes. The authors revert to an analysis framework that was previously used to interpret new forms of crime during the banking crisis. It consists of four scenarios that are briefly described. The future will have to show what effects the corona pandemic has had on fraud and other financial and economic crime.

Fishing with a new rod: an investigation into payment request fraud
Joke Rooyakkers and Marleen Weulen Kranenbarg
Online fraudsters seem to adapt to new digital opportunities. While the academic literature about phishing mainly focuses on phishing through emails, fraudsters also appear to use new means of communication and platforms to find and deceive their victims. Based on analysis of 728 police reports from the period from June 20th to August 20th 2019, this article provides a descriptive study on the new phenomenon of payment request fraud on the Dutch advertisement platform Marktplaats.nl (similar to eBay). The article will provide a thorough description of the crime script and its success factors. As fraudsters now use new means of communication, it will also be assessed to what extent they use new persuasion techniques, and to what extent victims may have different characteristics. The research, therefore, focuses on the modus operandi, persuasion techniques used by the fraudsters, and victim characteristics.

Fraud and scams on Telegram Messenger. Results from a netnographic study

Robby Roks and Nahom Monshouwer

In this article, the authors draw on a *netnographic* study conducted between May and July 2019 on phishing on Telegram Messenger. The results indicate that Telegram, just like cryptomarkets and online forums, seems to function as a criminal marketplace. In the groups analyzed the authors see users who both offer and are looking for specific goods and services related to the crime script of phishing. Furthermore, the information on Telegram contains specific modi operandi that are offering comprehensive and step-by-step guides to successfully complete specific financial cybercrimes. Therefore, based on this explorative study the authors argue that Telegram can be seen as a digital offender convergence setting.

Romance scams, dating fraud and 'sweetheart swindles'. The loss of money, happiness and face

Raoul Notté

Romance scams have seen a worldwide increase and are one of the most financially damaging forms of cybercrime. In addition, victims suffer strong emotional impact and are confronted with victim blaming. Research shows how the combination of various emotional and financial impact can induce a 'double-hit' on victims. Knowledge and possibilities for law enforcement are insufficient, which leads to a lack of financial compensation and support for victims.

Who will get their money back? Victims' actions for compensation in bank fraud

Johan van Wilsem, Take Sipma and Esther Meijer-van Leijsen

In the Internet era, banking fraud has become a common way of stealing money. According to victim surveys, this offense has already led to significant numbers of victims. In this article, the authors focus on illegal bank account withdrawals, which are an indication of identity fraud. For this they use data on 636 victims who were surveyed in the LISS panel. Using the concept of 'capability to act', as used in the WRR report *Why knowing what to do is not enough* (2017), the authors model which type of victim takes action to get the stolen amount reimbursed and which type of victim succeeds in doing so. They expect that the less educated and people with low self-control more

often refrain from contact with authorities (bank, police) and therefore more often receive no compensation and remain with higher residual damage. The results show that approximately four in five victims of unauthorized bank debits are fully compensated. For the group of victims for whom this is not the case – remaining with residual damage – most of the hypotheses are confirmed.

Social engineering: digital fraud and deception

Jan-Willem Bullée and Marianne Junger

The prevalence of online crime increases. Social engineering, such as email phishing, is often an important element in an attack. Several interventions have been developed to reduce the success of these types of attacks. The current study investigates whether interventions can help reduce vulnerability to social engineering attacks. The authors investigate which types of interventions and specific elements are most successful. They selected studies with an experimental design that tested at least one intervention. A total of 19 studies with 37 effect sizes, based on a total sample of N=23,146 subjects, were found. The available training courses, intervention materials and effect sizes were analysed. Overall, positive effects of interventions were found. However, there are substantial differences in effect for the different types of interventions. Effective interventions are relatively intensive and have a specific focus. The authors conclude with the design of the best possible intervention given the results of their research.

Our cyber behavior is much more unsafe than we think. Implications for effective government influence policy

Rick van der Kleij, Susanne van 't Hoff-de Goede, Steve van de Weijer and Rutger van de Leukfeldt

The aim of this research was to examine how Dutch citizens behave online and to explain their online behavior. The results of an experimental survey (N=2,426) show that unsafe behavior is highly prevalent. For example, nearly 40% of the respondents use a weak password. However, it appears that there are major differences between self-reported behavior and objective behavior. The objective measurements in the survey show that people behave more unsafely than they self-report. The research further shows that there is no silver bullet for promoting more safe online behavior. Different online behaviors seem

to stem from different sources. Nevertheless, the authors do see a lot of value in interventions that focus on adaptations to the technology that people use for online activities, such that the possibility of unsafe behavior is reduced and the possibility of safe behavior is increased – also known as *security by design*. There is a role here for policy measures encouraging technology manufacturers to make these adjustments.

Wetenschappelijk Onderzoek- en
Documentatiecentrum
Ministerie van Justitie en Veiligheid