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