Online fraude in beeld

Fenomeenbeeld 2024

Online fraude in beeld

Fenomeenbeeld 2024

In opdracht van de Nationaal Intelligencecoördinator van de politie en de Politiechef van de Eenheid Landelijke Expertise en Operaties zijn in 2024 strategische fenomeenbeelden opgesteld. Deze hebben betrekking op de geprioriteerde veiligheidsthema's van de politie zoals opgenomen in de Nationale Intelligence Agenda (NIA). Het rapport Online fraude in beeld is onderdeel van deze reeks.

Inhoud

Samenvatting

In deze samenvatting worden de belangrijkste uitkomsten van dit fenomeenbeeld beschreven. De focus ligt op de ontwikkeling, omvang en gevolgen van elf belangrijke vormen van online fraude. De hierna vermelde cijfers zijn afkomstig uit analyses van de politiesystemen en opsporingsonderzoeken. In verschillende hoofdstukken is uitgelegd dat veel burgers aangifte achterwege laten, waardoor de werkelijke aantallen slachtoffers en financiële schade aanzienlijk hoger zullen zijn. Voor meer informatie wordt de lezer verwezen naar de aparte hoofdstukken.

Online fraude in cijfers

70.000
aangiften en meldingen
in 2023

1 op de 5 doet aangifte
verschilt per fraudevorm: aankoopfraude
20% en bankhelpdeskfraude 82%

€ 109 miljoen
aan schadebedragen in 2023

Criminele inkomsten voor luxe goederen en financiering andere delicten

Criminele groeperingen

vaak op Nederlands grondgebied

Criminele groeperingen plegen meer soorten online fraude naast traditionele criminaliteit

GROTE IMPACT
financieel en emotioneel

Online fraude
laagdrempelig
groot bereik

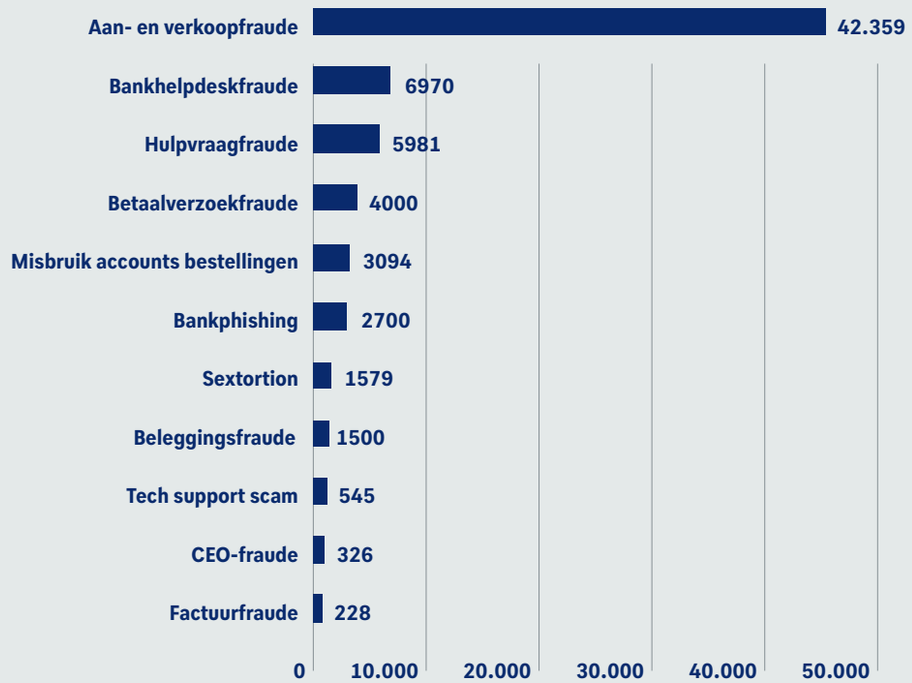
Cybercrime-as-a-service

tools en leads met persoonsgegevens
te koop op sociale media

Online fraude neemt al jaren sterk toe

Online fraude is sterk toegenomen, wat kan worden toegeschreven aan de explosieve groei van internetgebruik en de toenemende digitalisering in vrijwel alle aspecten van ons dagelijks leven. Meer dan ooit vertrouwen individuen, bedrijven en overheden op digitale systemen voor communicatie, financiële transacties en opslag van gevoelige informatie. Deze afhankelijkheid heeft cybercriminelen nieuwe kansen geboden om kwetsbaarheden te exploiteren. Het aantal registraties is sinds 2014 sterk toegenomen met een flinke piek in 2020. Daarna liepen de registraties terug, maar bleven op het hoge niveau van voor 2020. Het hoge niveau vertaalt zich ook in het flinke aandeel dat online fraude heeft in het totaal aantal registraties dat bij de politie binnenkomt. De frequentie van online fraudevormen varieert wel naar type fraude. Verschillende vormen zijn opgekomen en sommige zijn na een piek teruggelopen in frequentie. Daarom kan niet in algemene termen worden gesproken over een afname (of een toename) van de online fraude, maar wel dat het aantal registraties substantieel is. Bovendien kan de emotionele en financiële schade bij verschillende vormen aanzienlijk zijn, zoals nog blijkt.

Figuur 1. Aantal registraties per online fraudevorm
Bron: BVH, BlueIntel

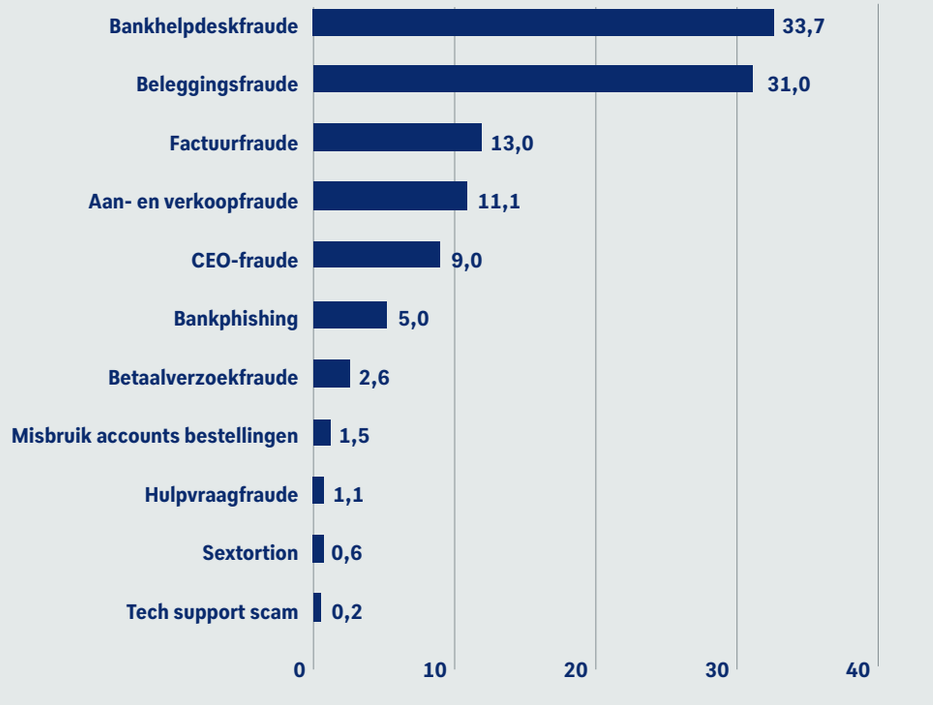


Online fraude veroorzaakt veel slachtoffers en schade

In dit rapport worden de omvang en gevolgen beschreven van elf belangrijke vormen van online fraude (met als uitzondering sextortion, dat om afpersing gaat). Hierbij ging het in 2023 in totaal om bijna 70.000 aangiften en meldingen die bij de politie binnenkwamen[1].
Per fraudevorm lopen de aantallen sterk uiteen, variërend van enkele honderden tot enkele tienduizenden registraties (Figuur 1).

Dit geldt ook voor de totale financiële schade die burgers en bedrijven als slachtoffer oplopen (Figuur 2). Deze ligt voor de fraudevorm tech support scam rond de € 200.000,- en loopt op tot enkele tientallen miljoenen euro's voor beleggingsfraude en bankhelpdeskfraude. Wat hierbij opvalt, is dat de delicten met de meeste registraties in totaal niet per se de grootste financiële schade veroorzaken. Bij sommige vormen van fraude leidt een enkel incident al tot een hoog schadebedrag. Daarbij investeren de daders wel relatief veel tijd en energie in het verleiden van het beoogde slachtoffer.

Figuur 2. Totale financiële schade per fenomeen in miljoenen euro's
Bron: BVH, BlueIntel



1 Uitzonderingen zijn betaalverzoekfraude en bankphishing, waarvoor de vermelde cijfers uit 2022 komen.

Tot slot is de impact van slachtoffers van online fraude niet beperkt tot financiële schade en worden de persoonlijke gevolgen voor slachtoffers nog vaak onderschat. Uit verschillende onderzoeken blijkt dat de impact van online criminaliteit niet onderdoet voor die van traditionele criminaliteit, en in sommige opzichten zelfs groter is. De schade beperkt zich vaak niet alleen tot de directe slachtoffers, maar strekt zich soms uit tot gezinnen of complete families. Dat komt omdat het verdwijnen van spaartegoeden, oudedagvoorzieningen en potentiële erfenissen de toekomst van families kan ontwrichten.

Online fraude vaak door georganiseerde groepen met jeugdige leden

De criminele groeperingen die online fraude plegen, bestaan uit meerdere leden die elkaar vaak al jaren kennen en zich niet beperken tot één type fraude. Ze plegen vaak in wisselende samenstelling verschillende vormen van fraude, zoals bankhelpdeskfraude en betaalverzoekfraude. De groepsleden zijn overwegend jong (twee derde is jonger dan 30 jaar) en nieuwe leden komen uit hun vertrouwde en lokale kring. De structuur van deze groeperingen is vaak fluïde, met een vaste kern en een losse groep van faciliteerders en uitvoerders, zoals bellers en phishers. Er is een duidelijke rolverdeling en hiërarchie binnen groepen. De kernleden coördineren en zorgen voor de samenwerking door voorbereidingen te treffen en afspraken te maken over de uitvoering.

Veel samenloop van zowel online als traditionele delicten

Criminele groeperingen ontplooien een scala aan criminele activiteiten voor financieel gewin. Onderzoek naar antecedenten van verdachten en opsporingsonderzoeken laten zien dat de overstap van de ene naar de andere online fraudevorm klein is. Bankhelpdeskfraude, bankphishing en hulpvraagfraude gaan vaak samen. Door het doorverkopen van buitgemaakte goederen en het veiligstellen van de criminele opbrengsten, gaan online fraude en traditionele delicten zoals diefstal, heling of witwassen vaak hand in hand. Online fraudeurs blijken soms ook betrokken bij drugs- en mensenhandel, zij het in mindere mate. Incidenteel worden online frauderende groepen met geweld, aanranding, moord en wapen(bezit) geassocieerd. Dit beeld sluit aan bij trends die de laatste jaren worden gesignaleerd, waarbij criminele (jeugd)groepen zich bezighouden met zowel online fraude als traditionele delicten. De instap om cybercrime te plegen is eenvoudiger geworden, onder andere doordat cybercrime-as-a-service de technische drempels heeft verlaagd, en criminelen op internetfora kennis delen en verhandelen. Om deze samenloop beter te kunnen duiden, is meer gericht onderzoek nodig, bijvoorbeeld naar de rollen van verdachten en naar recidive.

Criminele opbrengst voornamelijk besteed aan luxegoederen

Een groot deel van de criminele opbrengst wordt besteed aan luxe of statusverhogende goederen zoals horloges, sieraden, designerkleding, telefoons en laptops. Deze aankopen verhogen niet alleen de status van de criminelen, maar dienen ook als middel om geld wit te wassen Ook worden er reizen, hotelovernachtingen en casinobezoeken mee bekostigd. Contant geld heeft ook statuswaarde binnen deze groepen. De aankopen worden vaak betaald met cash, anonieme prepaidkaarten of via rekeningen van geldezels of slachtoffers. Cryptovaluta speelt vaak een rol bij het wegsluizen van criminele opbrengst, waarbij meerdere transacties, omzettingen (cryptomunten) en mixerdiensten worden gebruik om de herkomst te verhullen. Tot slot zijn er enkele aanwijzingen dat criminele opbrengsten worden gebruikt als kapitaal om andere misdrijven te financieren of voor de aankoop van onroerend goed in het buitenland.

Nieuwe werkwijze: overnemen wat werkt en steeds gerichtere benadering van slachtoffers

Online fraude kent vele verschijningsvormen en ontwikkelt zich continu. De elf vormen die in dit fenomeenbeeld worden beschreven kennen verschillende werkwijzen die naast elkaar bestaan of elkaar soms verdringen. Vaak vindt een kruisbestuiving plaats waarbij de oplichters succesvolle werkwijzen kopiëren en toepassen in andere online of hybride (fraude)vormen. Dit is terug te zien in het veelvuldig gebruik van Remote Access Tools (RAT's) die in steeds meer online fraudevormen worden ingepast en die oplichters gebruiken om bijvoorbeeld mee te kijken in de bankomgeving van slachtoffers, of om allerlei financiële handelingen mee te verrichten. Daarnaast worden ook zogenaamde leads, digitale lijsten met persoonsgegevens, in verschillende online fraudevormen gebruikt om steeds gerichter verschillende doelgroepen te benaderen (70+'ers, alleenstaande dertigers, hoogopgeleide veertigers). De komende jaren zal deze ontwikkeling vermoedelijk versnellen onder invloed van kunstmatige intelligentie en het zoeken naar steeds effectievere manieren om slachtoffers door middel van social engineering te beïnvloeden.

Aanpak zaak van samenwerken met publieke en private partners

In de afgelopen jaren zijn door publieke en private partijen veel inspanningen geleverd om online fraude te bestrijden, zoals opsporingsonderzoeken en technische barrières. Ondanks deze inspanningen worden nog steeds veel burgers en bedrijven het slachtoffer van deze praktijken. Om deze reden probeert de huidige integrale aanpak online fraude bestaande en toekomstige online fraudevormen effectiever tegen te gaan. Deze aanpak bundelt krachten van politie, Openbaar Ministerie (OM) en (private) partners, en richt zich naast opsporing en vervolging op preventie, kennisdeling, snelle interventies, en innovatieve oplossingen.

Voor veelvoorkomende fraudevormen zoals aan- en verkoopfraude, identiteitsfraude, bankhelpdeskfraude, betaalverzoekfraude en hulpvraagfraude zijn en worden specifieke interventies ontwikkeld. De uitbreiding van deze aanpak zal de komende jaren een bijdrage leveren om online fraude effectiever te bestrijden.

2

Aanleiding en onderzoeks-vragen

Begin 2021 besloot de dienstleiding van de Dienst Landelijke informatieorganisatie (DLIO) om vierjaarlijks een fenomeenbeeld te maken op de geprioriteerde thema's uit de Nationale Intelligence Agenda. Er is behoefte aan kennis over deze thema's ten behoeve van een nationale en internationale fenomeenstrategie van de politie. De huidige geprioriteerde thema's zijn: Serious and organised Crime (SOC) Drugs, SOC Geweld, Mensenhandel, Cybercrime, Milieucriminaliteit, Contraterrorisme, Extremisme en Radicalisering (CTER) en Openbare orde en veiligheid (OOV).

Het voorliggende rapport brengt cybercrime in kaart, maar cybercrime is een breed fenomeen dat verschillende cyberdelicten omvat. Over het algemeen worden er twee benaderingen gebruikt om cybercriminaliteit te categoriseren. Bij de eerste benadering, die bekend staat als cybercrime in enge zin, gebruiken criminelen ICT om aanvallen uit te voeren op ICT-infrastructuur, zoals met ransomware en DDoS-aanvallen. Binnen de politie richten onder andere het Team High Tech Crime (THTC), het Landelijk Operationeel Cybercrime Overleg (LOCO) en diverse cyberteams zich op de bestrijding van deze vorm van cybercriminaliteit. De tweede benadering betreft gedigitaliseerde criminaliteit, waarbij de ICT een handig hulpmiddel is om burgers financieel op te lichten. Voorbeelden zijn hulpvraagfraude en bankhelpdeskfraude. In de praktijk overlappen beide benaderingen elkaar, waardoor ze niet strikt afgebakend kunnen worden (DLIO & DRIO, 2022b).

De politie en het OM investeerden de laatste jaren veel in het verbeteren van de aanpak van gedigitaliseerde criminaliteit. Om dit te bespoedigen, richtten zij op 1 januari 2022 het project Centurion op. Dit project heeft als doelstelling om met politie en OM tot een gezamenlijke en landelijk gecoördineerde aanpak van gedigitaliseerde criminaliteit binnen de politie te komen. Dit gebeurt onder andere door de opvolging van aangiftes in de basisteams te ondersteunen en door informatie bijeen te brengen waardoor criminele verbanden in beeld gebracht en aangepakt kunnen worden. Binnen de politie is er vaak sprake van schaarste, ook bij de aanpak van gedigitaliseerde criminaliteit, waardoor het prioriteren van zaken noodzakelijk is. Een landelijk veiligheidsbeeld kan daarom helpen landelijke prioriteiten vast te stellen.

Dit fenomeenbeeld geeft hier invulling aan en stelt de politie en partners in staat om keuzes voor belangrijke thema's binnen gedigitaliseerde criminaliteit te onderbouwen. Dit gebeurt onder meer door de aard, omvang en kenmerken van criminele groeperingen en verdachten voor elf verschillende verschijningsvormen van online fraude in kaart te brengen. Dit zijn: aan– en verkoopfraude, phishing (bankphishing en betaalverzoekfraude), tech support scam (TSS), bankhelpdeskfraude, hulpvraagfraude, beleggingsfraude, misbruik seksueel beeldmateriaal (sextortion), misbruik accounts voor bestellingen en Business E-mail Compromise (CEO-en factuurfraude). Het gaat vooral om vormen van online fraude die qua aantallen registraties de hoofdmoot vormen (ongeveer 75 procent) van wat bij de politie binnenkomt (Willekers et al., 2024).

De keuze voor de fraudevormen die in dit fenomeenbeeld aan bod komen, is onder meer gemaakt op basis van al gestelde prioriteiten binnen *Centurion* en de Veiligheidsagenda van het OM, waarin gedigitaliseerde criminaliteit vanaf 2023 weer is opgenomen (Ministerie van Justitie en Veiligheid, 2023). Binnen *Centurion* ligt de focus op vier verschillende thema´s, namelijk, aan- en verkoopfraude, phishing, bankhelpdeskfraude en hulpvraagfraude. Aanvullend hierop is vanuit de projectleiding van Centurion gevraagd om twee extra thema's mee te nemen in het fenomeenbeeld, namelijk misbruik seksueel beeldmateriaal (specifiek sextortion)[2] en beleggingsfraude. De aanleiding hiervoor waren signalen dat deze vormen van afpersing en oplichting in toenemende mate slachtoffers maakten. De nieuwe Veiligheidsagenda richt zich primair op vier vormen van gedigitaliseerde criminaliteit: fraude met onlinehandel, online fraude met betaalproducten, online voorschotfraude en online identiteitsfraude. Op het eerste gezicht lijken de fraudevormen in de Veiligheidsagenda en die van Centurion te verschillen, maar na de inhoudelijke uitwerking blijkt er veel overlap te zijn. In de uitwerking van dit fenomeenbeeld leggen we de verbinding tussen de thema's van Centurion en de bijbehorende speerpunten in de Veiligheidsagenda uit, waardoor duidelijk wordt dat de onderzochte fraudevormen grotendeels de speerpunten uit de Veiligheidsagenda dekken. Tot slot zijn aan deze geprioriteerde thema's en wensen de volgende vormen toegevoegd: misbruik accounts voor bestellingen, Business E-mail Compromise (BEC)-fraude en tech support scam. Deze vormen zijn eerder beschreven (o.a. *Nationaal dreigingsbeeld* 2017 (NDB) en *Nationaal Cyberbeeld* 2019 (NCB)), vanwege de impact op burgers en bedrijven. Om dit fenomeenbeeld volledig te maken, zijn ze nogmaals opgenomen.

Met dit fenomeenbeeld kan de politie betere keuzes maken en al gestelde prioriteiten beter onderbouwen. De onderzoeksvragen zijn uitgebreid beschreven in bijlage 1 en worden hierna kort samengevat. Tot slot is gebruik gemaakt van de Landelijke Cyber Query (LCQ), die dagelijks registraties van cybercrime uit de politiesystemen haalt. De bronnen en werkwijze van de LCQ worden beschreven in bijlage 2 van dit document.

Onderzoeksvragen en methode

De volgende onderzoeksvragen komen aan de orde:

1. Hoe heeft het fenomeen zich ontwikkeld (in termen van modus operandi)?
2. Hoe heeft de omvang zich ontwikkeld? Wat zeggen externe bronnen hierover?
3. Wat zijn kenmerken van criminele groeperingen?
4. Wat zijn kenmerken van slachtoffers? Indien bekend, wat zijn de gevolgen voor slachtoffers?
5. Bestaat er een aanpak van het fenomeen (door de politie en publiek-private partijen)?
6. Wat zijn de verwachtingen in relatie tot de aanpak?
7. Welke ontwikkelingen zijn er te verwachten?

Voor het beantwoorden van de onderzoeksvragen is zoveel mogelijk gebruik gemaakt van politiegegevens, zoals informatie afkomstig uit opsporingsonderzoeken, onderzoeksdossiers en politieregistraties. Verder zijn verschillende (interne) databronnen geraadpleegd, zoals de Basis Voorziening Handhaving (BVH), Blueview, Summ-IT en FIU-gegevens. In veel hoofdstukken is gebruik gemaakt van kennisdocumenten die door het Project VAK zijn opgesteld. In deze kennisdocumenten zijn crimescripts van de verschillende online fraudevormen uitvoerig beschreven. Project VAK is een interne afdeling binnen de politie en in 2021 opgericht om de domeinkennis op gedigitaliseerde criminaliteit en cybercrime te vergroten. In de teksten wordt verwezen naar project VAK, maar de verschillende (interne) documenten zijn niet opgenomen

2 In dit beeld spreken we over online fraude in plaats van gedigitaliseerde criminaliteit. Sextortion is de uitzondering hierop, omdat om online afpersing gaat en niet zozeer over fraude. Het is nog niet duidelijk of sextortion onder zeden gaat vallen of onder Centurion.

in de literatuurlijst. De informatie in dit fenomeenbeeld is verder aangevuld met zowel interne als externe rapportages (o.a. veiligheidsbeelden uit verschillende eenheden en rapporten van het CBS, het WODC en NVB). Tot slot zijn op verschillende thema's interviews afgenomen en is feedback verkregen van inhoudsdeskundigen.

Leeswijzer

Dit rapport gaat in op allerlei vormen van online fraude en de wijze waarop deze zich de afgelopen jaren hebben ontwikkeld. In hoofdstuk 3 *Historie van online fraude* worden achtereenvolgens de ontwikkeling van horizontale fraude naar online fraude geschetst en de publiek-private samenwerkingsverbanden die de politie heeft op het gebied van financieel-economische criminaliteit.

In het daaropvolgende hoofdstuk *Online fraude in Nederland* worden in tien aparte onderdelen de onderzoeksvragen beantwoord voor de volgende verschijningsvormen:

Hoofdstuk 4.1: Aan – en verkoopfraude
Hoofdstuk 4.2: Phishing (Bankphishing en betaalverzoekfraude)
Hoofdstuk 4.3: Tech support scam
Hoofdstuk 4.4: Bankhelpdeskfraude
Hoofdstuk 4.5: Bankhelpdeskfraude: verdachtenbeeld
Hoofdstuk 4.6: Hulpvraagfraude
Hoofdstuk 4.7: Misbruik seksueel beeldmateriaal (sextortion)
Hoofdstuk 4.8: Beleggingsfraude
Hoofdstuk 4.9: Misbruik accounts voor bestellingen
Hoofdstuk 4.10: Business E-mail Compromise (BEC)(CEO– en factuurfraude)

In hoofdstuk 5 *Overeenkomsten in werkwijzen* wordt ingegaan op de gemeenschappelijke kenmerken van veel online fraudevormen, zoals de georganiseerdheid, social engineering, de inzet van geldezels en het witwassen van de opbrengsten.

In hoofdstuk 6 komen de *niet-financiële gevolgen voor slachtoffers* aan bod voor slachtoffers van een aantal (maar niet alle) fraudevormen, zoals bankhelpdeskfraude en sextortion (dat online afpersing betreft).

Hoofdstuk 7 *Toekomstige ontwikkelingen* gaat onder meer in op de gevolgen van artificiële intelligentie voor de uitvoering van fraudevormen.

In de bijlagen zijn de onderzoeksvragen en methode terug te vinden, evenals een overzicht van de stakeholders en een onderzoek wat is uitgevoerd naar de verschillende witwasmethoden van online fraude. Tot slot is een woordenlijst en een lijst met afkortingen opgenomen.

3

Historie van online fraude

Van horizontale fraude naar gedigitaliseerde criminaliteit (online fraude)

Horizontale fraude is een term voor fraudevormen waarbij burgers, bedrijven en organisaties het slachtoffer worden[3]. De vormen die hieronder vallen, zoals voorschotfraude en beleggingsfraude, bestaan al vele jaren en zijn reeds in verschillende deelrapporten *Horizontale fraude* voor het *Nationaal dreigingsbeeld* (NDB) beschreven (o.a. Bloem & Harteveld, 2012; Bloem, Harteveld & De Heus, 2017). Onder andere is geconstateerd dat horizontale fraude in het afgelopen decennium sterk van aard is veranderd. De digitalisering van de samenleving speelt daarbij een belangrijke rol en leidde tot veranderingen in de modus operandi van bestaande horizontale fraudevormen, maar ook tot het ontstaan van nieuwe vormen en mogelijkheden om dit soort fraude te plegen, zoals phishing, het misbruiken van accounts voor bestellingen of hulpvraagfraude. Hieronder zal kort bij deze (langdurige) ontwikkeling worden stilgestaan, waarbij ook aandacht is voor de vastlegging van deze vormen in de politiesystemen.

Horizontale fraude is steeds meer gedigitaliseerd of wordt gepleegd met behulp van cybercrime. Daarbij is door het gebruik van digitale middelen het bereik van daders veel groter geworden (Bloem et al., 2017). Vroeger kregen potentiële slachtoffers frauduleuze aanbiedingen per post, bijvoorbeeld over een erfenis (Bloem & Harteveld, 2012), maar nu heeft bijna iedereen een e-mailadres en/of sociale media-account, waardoor aanschrijven veel gemakkelijker gaat en grootschaliger plaatsvindt. Een internationaal onderzoek waarin ook Nederlandse inwoners zijn bevraagd, bevestigde dit: e-mail was het gebruikelijke medium voor oplichters om contact te zoeken, daarna de telefoon en ook sms en berichtenapps (Abraham et al., 2023). Daarnaast worden digitale hulpmiddelen en kennis om online fraude te plegen al enige jaren aangeboden op het darkweb en via sociale media (zoals Telegram) (OM & politie, 2024). Waar de criminelen vroeger de deur uit moesten, kunnen ze nu achter hun computer, laptop of telefoon online fraude plegen.

De introductie en het toenemende gebruik van sociale media[4] bieden uitgelezen kansen voor online fraude, doordat criminelen daar gemakkelijk toegang hebben tot veel persoonlijke informatie. Veel mensen beseffen niet dat het delen van hun privéleven op deze platforms hen kwetsbaar maakt voor oplichting. Tien jaar geleden werden mensen nog benaderd via datingsites, nu vinden oplichters veel informatie op verschillende soorten sociale media. Het gaat niet alleen om persoonlijke gegevens (telefoonnummers, e-mailadressen, familieleden en vrienden), maar ook bieden sociale media inzicht in relaties, voorkeuren en interesses van mensen. Deze gegevens misbruiken cybercriminelen om contact te leggen en mensen te overtuigen om mee te werken. Door het grote bereik en de voortdurende technologische ontwikkelingen, zoals tools waarmee bankrekeningen kunnen worden geplunderd of naaktfoto's kunnen worden gestolen voor chantage, wordt online fraude beschouwd als een nieuwe vorm van high impact crime (HIC) of veelvoorkomende criminaliteit (VVC) (DLIO, 2022a).

Online fraude veroorzaakt niet alleen aanzienlijke financiële schade, maar het leidt ook vaak tot emotionele schade en een verlies van vertrouwen in internet en medemensen. Vanwege de grote aantallen wordt online fraude beschouwd als een van de meest voorkomende vormen van criminaliteit. Ter illustratie: in 2023 onderzocht de Eenheid Noord-Holland hoe groot het aandeel van cybercrime en gedigitaliseerde criminaliteit (inclusief fraude in online handel) was in het totaal van veelvoorkomende criminaliteit, zoals fietsendiefstal, winkeldiefstal, eenvoudige mishandeling en afpersing. Het bleek dat dit ongeveer een derde van het totaal was. De Eenheid Den Haag kwam in 2020 tot een soortgelijke conclusie. Online vormen van criminaliteit waarvan vooral burgers en organisaties de dupe waren, kwamen vaker voor dan andere vormen van criminaliteit. Van alle misdrijven uit het Wetboek van Strafrecht bestond 18 procent uit horizontale fraude met een digitale component. Dit was het hoogste percentage binnen de categorieën van veelvoorkomende criminaliteit, waaronder ook geweld en vernieling vallen (Hesseling, 2021). In een recent onderzoek (Willekers et al., 2024) is het aandeel online fraude in het totale werkaanbod aan registraties onderzocht (die verder vooral bestaan uit incidenten van en overlast door kwetsbare personen). De voorzichtige schatting was dat het aandeel registraties met een overduidelijk digitale component 12 tot 14 procent bedroeg van het totale aanbod aan registraties, [5]wat als substantieel wordt gezien.

Horizontale fraude waarbij burgers, bedrijven en organisaties worden opgelicht, vormt al jaren een probleem in termen van het aantal gedupeerden en de gevolgen die zij ondervinden in de vorm van financiële en emotionele schade. In het laatste decennium gebeurt dit vooral digitaal en veel vormen van horizontale fraude komen nu terug onder de noemer gedigitaliseerde criminaliteit (en sinds kort als online fraude, dat is de term die in dit beeld wordt gehanteerd). In het deelrapport *Horizontale fraude* 2017 (Bloem et al., 2017) werden in totaal tien horizontale fraudevormen onderzocht. Daarbij werd ook gekeken naar de rol van de digitale techniek binnen het plegen van deze fraudes. De conclusie was dat de digitale technologie het grootschalig benaderen van potentiële slachtoffers faciliteerde bij alle fraudevormen, behalve faillissementsfraude.

Het afgelopen decennium blijkt dat het aantal registraties van horizontale fraude in de politiesystemen flink is toegenomen. Dit is op te maken uit de ontwikkeling van de omvang van de vier grootste fraudecategorieën. In 2014 werden bijna 28.000 gevallen van oplichting

3 Dit in tegenstelling tot verticale fraude waarbij voornamelijk de overheid het slachtoffer is.

4 Er zijn veel verschillende socialemediaplatformen. Een van de eerste grote en populaire was Facebook. In de loop van de tijd zijn er verschillende bij gekomen, zoals Telegram, Instagram, TikTok, SnapChat en YouTube. Deze platformen delen vergelijkbare doelen, namelijk interactie tussen gebruikers mogelijk maken, met elkaar communiceren, informatie, foto's en video's delen. Om gebruikers vast te houden, maken de platformen gebruik van algoritmes, waardoor ze verleid worden om langer en vaker op het platform te blijven. Advertentie-inkomsten zijn een belangrijke inkomstenbron van de platformen en voor gerichte reclames worden ook algoritmes gebruikt. De platformen trekken uiteraard ook kwaadwillenden en worden misbruikt om fraude te plegen, bijvoorbeeld met phishingberichten, via nep-accounts en nep-vriendschapsverzoeken, berichten dat mensen zogenaamde prijzen hebben gewonnen, romantische berichten et cetera. Al deze berichten zijn bedoeld om mensen persoonlijke gegevens en geld afhandig te maken. De platformen verschillen in de mate waarin ze hier actief tegen optreden en de maatregelen die ze daar tegen nemen.

5 Het aantal registraties met een digitale component bedroeg naar schatting tussen de 83.300 en 95.100. Het totaal aantal registraties was ruim 672.700. Dit was met de kanttekening dat voorzichtigheid geboden was omdat een volledige vergelijking niet mogelijk is, omdat kleine verschillen mogelijk zijn wanneer verschillende bronnen gebruikt worden.

geregistreerd, wat toen in de politiesystemen alleen als oplichting kon worden vastgelegd. Aangezien er nauwelijks onderscheid kon worden gemaakt tussen de verschillende vormen van horizontale fraude, is in 2015 besloten om een opsplitsing te maken in 15 verschillende fraudecategorieën[6]. Het gros van de registraties horizontale fraude (rond de 95%) komt terug in maar vier algemene fraudecategorieën, namelijk fraude met online handel[7], overige horizontale fraude, fraude met betaalproducten en identiteitsfraude (Figuur 3). De ontwikkeling van deze vier fraudecategorieën geven een goede indicatie van de ontwikkeling van horizontale fraude in het algemeen. Daarnaast is op basis van het doornemen en labelen van registraties die in deze vier categorieën voorkomen, vastgesteld dat ze vooral vormen van online fraude bevatten. Daardoor wordt de impact van digitalisering goed zichtbaar en ook dat horizontale fraude steeds meer is verschoven richting online fraude.

In 2014 zag de politie bijna 28.000 registraties van oplichting. Dit aantal was meer dan verdubbeld in 2017 naar ruim 62.000 registraties horizontale fraude. Deze toename is voornamelijk toe te schrijven aan de opkomst van verschillende online fraudevormen, zoals de tech support scam en online handel. In de jaren daarna neemt deze stijging verder toe en piekt in 2020 tot meer dan 125.000 registraties, vooral door de opkomst van nieuwe werkwijzen (betaalverzoekfraude en hulpvraagfraude). Na 2022 zet een daling in en deze stabiliseert in 2023 op het hoge niveau van voor 2020. Vanaf 2023 is weer een lichte stijging te zien en de komende jaren moet blijken of deze stijging doorzet (Figuur 3)[8].

Een enkele verklaring is niet goed te geven voor de daling die inzette na 2020 na de lange periode van sterke stijging. In de Veiligheidsmonitor van 2024 constateert het CBS voor dezelfde periode ook een daling van online criminaliteit (CBS, 2024). De piek in 2020 en daling in de twee jaren daarna dienen wel in perspectief geplaatst te worden. Zo valt deze periode samen met het begin van de corona-uitbraak en de maatregelen om het coronavirus terug te dringen, zoals een lockdown en het sluiten van horeca, scholen en kinderopvang.

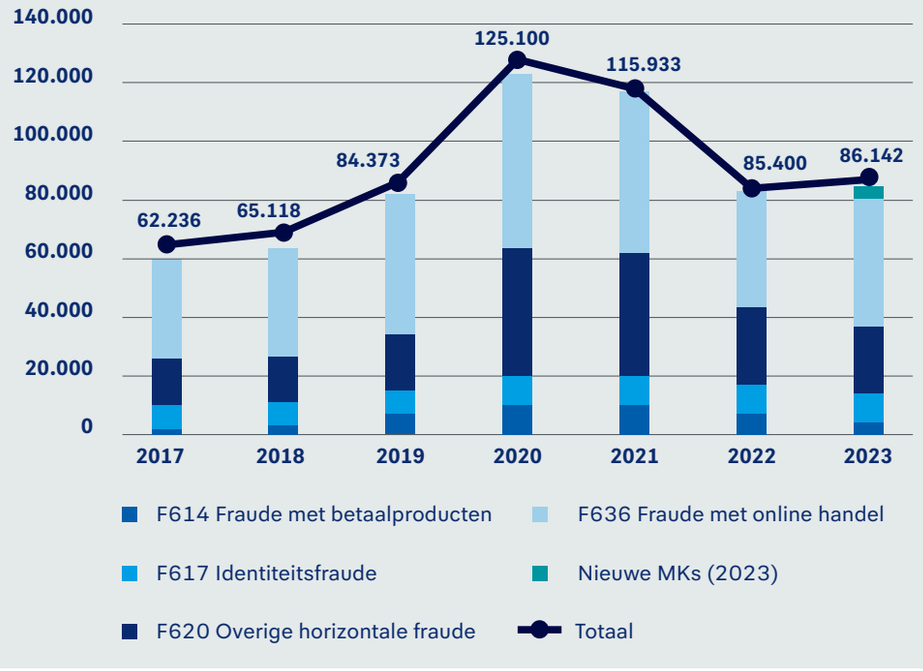
De toename van het aantal slachtoffers in de coronajaren (2020 en 2021) is vooral toe te wijzen aan de fraudecategorieën fraude met online handel (F636) en overige horizontale fraude (F620). Hoewel de fraude met tickets op Marktplaats sterk terugliep door de maatregelen, nam tegelijkertijd de handel toe in essentiële en gewilde producten zoals medicijnen, mondkapjes en spelcomputers. Omdat het voor consumenten moeilijker was om de legitimiteit van verkopers te verifiëren, creëerde dit gunstige omstandigheden voor criminelen om valse aanbiedingen te plaatsen en betalingen te ontvangen zonder de beloofde producten te

6 Elf categorieën zijn hier buiten beschouwing gelaten omdat ze minder dan honderd registraties bevatten. Het gaat hierbij om fraude met namaakgoederen, verzekeringsfraude, faillissementsfraude, voorschotfraude, fraude in de zorg, kilometerfraude, krediet-, hypotheek- en depotfraude, telecomfraude, beleggingsfraude, vastgoedfraude en acquisitiefraude.

7 Dit betreffen hoofdzakelijk aangiften via het internet die terechtkomen bij het Landelijk Meldpunt Internetoplichting (LMIO).

8 In 2023 zijn wederom enkele fraudecategorieën toegevoegd, namelijk telefonische helpdeskfraude, online identiteitsfraude en hulpvraagfraude. Deze zijn in 2023 opgeteld bij het totaal, omdat deze registraties anders in een van de vier grote categorieën zouden zijn ondergebracht.

Figuur 3. Ontwikkeling aantallen registraties in fraude-MK's
Bron: Cognosrapportage (intern)



leveren. Daardoor werden veel mensen slachtoffer van aan- en verkoopfraude. Over de toename van andere online fraudevormen bestaat geen duidelijke verklaring. Daar is geen onderzoek naar gedaan en hierover kan slechts worden gespeculeerd. Voor de afname na 2020 geeft een eenheid als verklaring dat het moeilijker is om aangifte te doen. Soms moeten mensen een afspraak maken, soms moeten ze naar een andere locatie en zit daar veel tijd tussen, soms worden oudere slachtoffers gevraagd aangifte te doen via internet, terwijl ze dat liever bij de balie doen en, tot slot, als de bank niet vergoedt komen slachtoffers geen aangifte meer doen. Een breder onderzoek onder alle eenheden zou moeten uitwijzen of dit een landelijke (zorgelijke) tendens is en of deze tendens in dat geval de afname kan verklaren.

Om horizontale fraude of specifieke vormen van online fraude goed uit de politiesystemen te krijgen, wordt in dit rapport niet alleen gekeken naar de registraties in de verschillende fraudecategorieën. Sinds 2016 wordt de Landelijke Cybercrime Query (LCQ) gebruikt om vormen van cybercrime beter uit de politiesystemen te halen. De LCQ zoekt dagelijks binnen de BVH-data naar verzamelingen van trefwoorden die op zichzelf of in combinatie kunnen duiden op cybercrime. Hiermee worden ook vormen van online fraude opgehaald die met cybercrime worden gepleegd. De registraties die de LCQ dagelijks ophaalt, worden in de eenheden gelezen en gecategoriseerd op diverse kenmerken en vastgelegd in een Excel-database (BlueIntel). Het

doel is om onder andere overzichten en beelden te maken. De categorieën in de database komen overeen met de fenomenen zoals in dit rapport weergegeven en onderzocht. De aantallen uit deze database gebruiken we om een beeld van de omvang te geven (per fenomeen). Zie bijlage 2 (methode) voor een uitgebreidere uitleg hiervan.

Politie en publiek-private samenwerking

In 2021 publiceerden Staats et al. een literatuuroverzicht over de publiek-private samenwerkingen op het gebied van financieel-economische criminaliteit en cybercrime over de periode 2015 - 2020. Het doel was deze samenwerkingsverbanden voor het eerst in kaart te brengen, de behaalde resultaten te onderzoeken en de succesfactoren en knelpunten te benoemen. Het overzicht benadrukt het belang van samenwerken bij de aanpak van deze vormen van ondermijnende (en slecht zichtbare) criminaliteit. Daarnaast biedt het inzicht in de gezamenlijke projecten die er al zijn en wat deze hebben opgeleverd.

De auteurs vonden 36 publiek-private samenwerkingsverbanden, waarbij het onderscheid financieel-economische misdaad en cybercrime niet altijd even scherp is. Er bestaan ook mengvormen, zoals samenwerkingsverbanden die gaan over cybercrime maar zich meer richten op de bestrijding van financieel gewin. Het volledige overzicht geven Staats et al. in een tabel. Hierna volgt een beschrijving van een aantal verbanden dat relevant is voor de aanpak van online fraude en cybercrime. Onder andere worden genoemd de Electronic Crimes Taskforce (ECTF; een samenwerking tussen politie en banken), het Landelijk Meldpunt Internetoplichting (LMIO; een samenwerking tussen politie en Marktplaats) en het Knooppunt Finec (expertiseknooppunt politie). Op het gebied van de aanpak van cybercrime zijn NoMoreDDoS en NoMoreRansom in het leven geroepen. Beide bestaan uit meerdere samenwerkende organisaties, zoals De Nederlandsche Bank, VNO-NCW, Belastingdienst, diverse beveiligingsbedrijven, en niet te vergeten de politie, Team High Tech Crime (THTC) en Europol. In het hoofdstuk over misbruik seksueel beeldmateriaal zijn onder andere genoemd Meldknop.nl, een samenwerking met de organisatie Veilig Internetten en Meldpunt Kinderporno. Daarnaast is Sh!tzooi (voorkomen van sexting op scholen) genoemd, waarin politie, scholen en welzijnsinstellingen samenwerken. Hack Right is opgericht om te voorkomen dat jonge daders van cybercrime een strafblad krijgen. Onder meer politie, Raad voor de Kinderbescherming, ministerie van Justitie en Veiligheid, bedrijven, wetenschappers en ethische hackers werken samen. Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een samenwerkingsverband tussen de overheid en het bedrijfsleven, opgericht om criminaliteit tegen bedrijven aan te pakken. Naast VNO-NCW, MKB-Nederland, Verbond van Verzekeraars en Koninklijke Horeca nemen ook een aantal ministeries deel (Economische Zaken en Justitie en Veiligheid).

Sommige samenwerkingsverbanden bestaan niet meer, omdat de samenwerking succesvol was, zoals de Brede coalitie ter verstoring van tech support scam. TSS is daardoor flink afgenomen en de activiteiten zijn mogelijk verschoven naar andere varianten (hoewel dat niet onderzocht is). In geval van TSS werden slachtoffers door een namaak helpdesk (zoals Microsoft) gebeld of zochten zij zelf een helpdesk omdat ze problemen met de computer hadden. Vervolgens bewoog de ‘medewerker’ de slachtoffers om geld over te maken voor de niet bestaande diensten of bood aan om met een Remote Access Tool mee te kijken en maakte het geld zelf over. Andere samenwerkingsverbanden, zoals Business E-mail Compromise (BEC; samenwerking tussen OM, politie, bedrijfsleven en grootbanken) bestaan niet meer omdat ze niet goed van de grond kwamen.

De onderzoekers hebben de samenwerkingsverbanden ook aan een evaluatie op effectiviteit onderworpen. Ze zijn ingedeeld in vier categorieën: informatie- en kennisdeling, ondersteuning publieke instanties, geen specifieke rol en rol is projectafhankelijk. De knelpunten en succesfactoren worden uitgebreid beschreven. Doel van de samenvatting in dit fenomeenbeeld is om te laten zien dat het niet altijd noodzakelijk is om nieuwe samenwerkingsverbanden in het leven te roepen en wanneer dit wel noodzakelijk is, de knelpunten en succesfactoren in beschouwing te nemen.

4

Online fraude in Nederland

In dit fenomeenbeeld worden verschillende online fraudevormen beschreven aan de hand van antwoorden op de onderzoeksvragen. Een aantal fraudevormen komt overeen met die in de Veiligheidsagenda (Ministerie van Justitie en Veiligheid, 2023), namelijk aan- en verkoopfraude, phishing, bankhelpdeskfraude en hulpvraagfraude. Deze zijn ook door Centurion geprioriteerd. Daarnaast zijn aanvullend enkele fenomenen beschreven op verzoek van Centurion, namelijk misbruik van seksueel beeldmateriaal (sextortion) en beleggingsfraude. Tot slot zijn aan deze geprioriteerde thema's en wensen de volgende vormen nog toegevoegd: misbruik accounts voor bestellingen, Business E-mail Compromise (BEC)-fraude en tech support scam. Deze vijf fenomenen worden korter in de vorm van een update weergegeven.

4.1 Aan- en verkoopfraude

Bij aankoopfraude bieden oplichters producten aan op handelsplaatsen, sociale media of malafide webshops en vragen om vooruitbetaling, of laten betalen voor niet-bestaande producten, maar leveren vervolgens niet. Bij verkoopfraude kopen of bestellen oplichters een product en vragen aan de verkoper om vooruit te leveren, maar betalen vervolgens niet.

Aan- en verkoopfraude in cijfers

Veel aangiften

met veelal lage schadebedragen

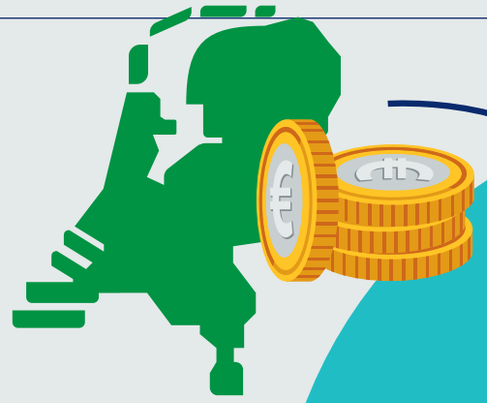
€ €

€ 250

Gemiddeld schadebedrag 250 euro per registratie.

20%

Het CBS meldt dat 20% aangifte doet van aankoopfraude



45.000

Sinds 2010 jaarlijks gemiddeld 45.000 aangiften

Stijging

in het overmaken van criminele gelden naar het buitenland

Vooruit betalen niet leveren

toename online bestellen via valse webshops, afname via Marktplaats dankzij maatregelen

Totale schade bedraagt gemiddeld

€ 11 miljoen per jaar

De informatie in dit hoofdstuk is tot stand gekomen met medewerking van het Landelijk Meldpunt Internetoplichting (LMIO). Aan- en verkoopfraude, voorheen bekend als online handelsfraude, is een belangrijk speerpunt in de Veiligheidsagenda en gaat voornamelijk over het niet nakomen van leverings- en/of betalingsverplichtingen. Oplichters bieden producten aan op handelsplaatsen, sociale media of malafide webshops en vragen om vooruitbetaling, of laten betalen voor niet-bestaande producten, maar leveren vervolgens niet. Dit is aankoopfraude. Het is ook mogelijk dat oplichters een product kopen of bestellen, aan de verkoper vragen om vooruit te leveren, maar vervolgens niet betalen. Dit is verkoopfraude. Deze vorm van fraude, vooruitbetalen-niet leveren, begon op Marktplaats, dat in 1999 werd opgericht. Omdat het aantal aangiften hand over hand toenam, is in 2010 het Landelijk Meldpunt Internetoplichting (LMIO) opgericht, dat sindsdien jaarlijks enkele tienduizenden aangiften ontvangt (Bloem & Harteveld, 2012; 2017). Het ging en gaat nog steeds vaak om tickets voor concerten, navigatiesystemen, internetspellen en mobiele telefoons.

Hoe heeft het fenomeen zich ontwikkeld?

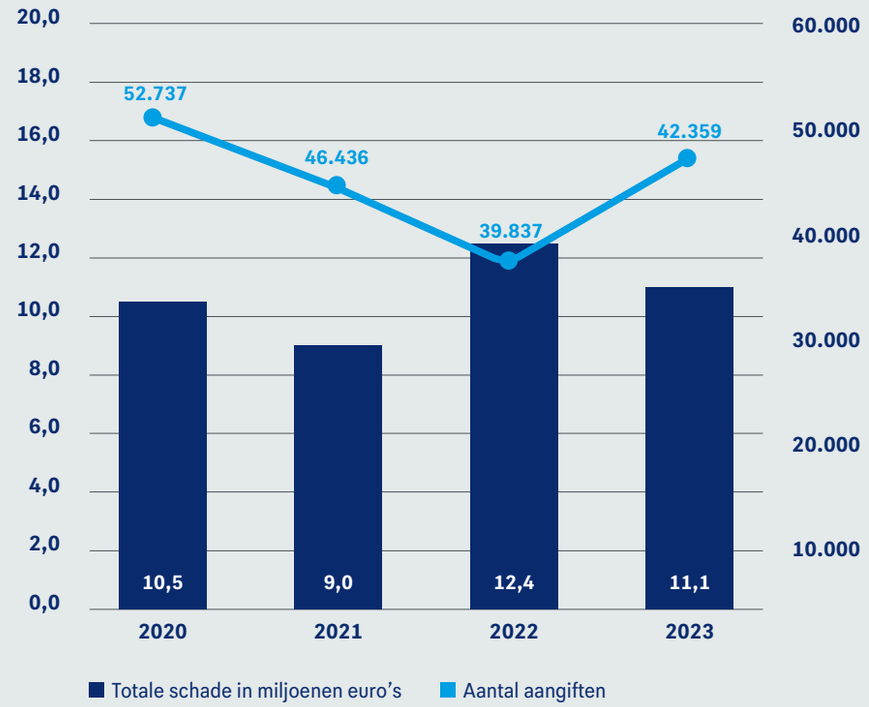
Er zijn twee trends waarneembaar die al enkele jaren bestaan. Ten eerste verschoof aan- en verkoopfraude van Marktplaats naar andere online handelsplaatsen, zoals malafide en nepwebshops. Nepwebshops, die soms sterk lijken op bestaande webshops, gingen producten aanbieden die niet geleverd worden. Ten tweede is er een hardnekkige trend waarbij oplichters verkopers ervan overtuigen om buiten de beveiligde chat- en betaalomgeving van Marktplaats te gaan. Ze sturen dan een betaalverzoek met een link via berichtenapps zoals WhatsApp, waardoor slachtoffers op een nepwebsite van de bank terechtkomen en worden opgelicht. Dit is een vorm van phishing en wordt als zodanig beschreven in hoofdstuk 4.2. Deze MO is nog steeds actueel, ondanks de vele waarschuwingen in diverse media en door politie en Marktplaats.

In de loop der jaren was de ene trend wat meer actueel dan de andere, maar uit contact met het LMIO blijkt dat niet leveren via online handelsplaatsen als Marktplaats en niet leveren via nepwebwinkels naar elkaar toe groeien. Aankoopfraude komt het meest voor (bijna 98%). Naast fraude op de bekende online handelsplatformen, ziet het LMIO ook steeds vaker fraude via nepwebshops en sociale media. Bij een deel van de fraudes die via sociale media verlopen, komen de slachtoffers uiteindelijk ook bij een malafide webshop terecht. Het overgrote deel van die oplichtingen gaat via een groot sociale media platform door op een advertentie te klikken. Slachtoffers worden vervolgens doorgeleid naar een malafide webshop, waar dan de daadwerkelijke oplichting plaatsvindt. Het zicht op de aantallen ontbreekt en is nog in onderzoek bij het LMIO.

Hoe heeft de omvang zich ontwikkeld?

Aangiften en meldingen worden rechtstreeks naar het LMIO gestuurd via een aangifteformulier. Het aantal registraties is al jaren aan het stijgen. In 2011 waren er ongeveer 35.000 registraties, in 2015 waren dat er in totaal 44.000 (niet in figuur) en in 2020 is dat aantal gestegen naar 53.000 (afgerond, zie figuur 4). Deze piek hangt deels samen met de uitbraak van de coronapandemie, waardoor mensen vaker online aankopen deden en het moeilijker was om de legitimiteit van verkopers of websites te verifiëren. Tegelijkertijd kwam er een grotere vraag naar essentiële en gewilde producten zoals medicijnen, mondkapjes en spelcomputers. Vooral in het eerste jaar (2020) creëerde dit gunstige omstandigheden voor criminelen om valse aanbiedingen te plaatsen of (nep)webshops op te zetten en betalingen te ontvangen zonder de beloofde producten te leveren. Vanaf 2021 daalde het aantal registraties tot bijna 40.000 in 2022, om daarna weer te stijgen in 2023.

Figuur 4. Ontwikkeling aantal registraties en totale financiële schade aan-en verkoopfraude
Bron: BVH, BlueIntel



Uit eerdere contacten met het LMIO blijkt dat de variant van aan- en verkoopfraude waarbij er wel betaald wordt, maar niet geleverd via Marktplaats, is afgenomen. Die afname moet in perspectief gezien worden. Lang niet iedereen doet aangifte en advertenties worden steeds vaker op sociale media zoals Facebook of Instagram geplaatst. Sinds 2017 heeft Facebook zijn eigen Marketplace, maar helaas heeft het LMIO geen zicht op het aantal fraudes dat hierop wordt gepleegd (hierna wordt dit uitgelegd). Het aantal fraudes met webshops is daarentegen flink toegenomen (DLIO, 2022) en dat heeft twee oorzaken. Ten eerste treft Marktplaats, verantwoordelijk voor de meeste registraties, regelmatig maatregelen om fraude te voorkomen, waardoor fraude steeds moeilijker wordt. Ten tweede liep de verkoop van tickets voor concerten tijdens de coronalockdowns sterk terug. Fraude met tickets was een belangrijk onderdeel van de registraties, en hoewel er nu weer volop tickets worden aangeboden, blijven de cijfers lager dan vóór corona. Daarnaast heeft de werkwijze zich verplaatst naar fraude met apps voor berichten als opstap om slachtoffers te vinden. Van deze

gewijzigde werkwijze kan er geen internetaangifte bij het LMIO worden gedaan, omdat de internetaangifte alleen bedoeld is voor aan-en verkoopfraude. Ondanks de toename van fraude met webshops zijn de aantallen lager gebleven dan in de jaren ervoor, maar het totale schadebedrag is wel toegenomen. Deze vorm van fraude kenmerkt zich door veel registraties met gemiddeld lage schadebedragen. De gemiddelde schade bedraagt 250 euro per registratie.

Geschatte omvang van aan– en verkoopfraude

In het deelrapport *Horizontale Fraude* 2017 (Bloem & Harteveld, 2017) werd de omvang van horizontale fraude geschat op €16 miljoen per jaar (voor gemiddeld 43.000 registraties per jaar). Bij dergelijke schattingen wordt doorgaans rekening gehouden met *dark numbers*: het deel van de slachtoffers dat geen melding of aangifte doet, bijvoorbeeld uit schaamte of omdat het betaalde bedrag zo laag was dat het niet de moeite waard was om aangifte te doen. Een methode om een beeld te krijgen van deze *dark numbers*, is het volgen van geldstromen naar bankrekeningnummers van oplichters en te onderzoeken hoe groot het verschil is tussen het aantal betalers en het aantal aangevers. Het volgen van geldstromen levert een accuraat beeld op van het aantal aangiften en hetgeen betaald is, waardoor een beter beeld van de financiële schade kan worden gegeven.

Voor het deelrapport 2017 heeft het Landelijk Meldpunt Internet Oplichting (LMIO) dit gedaan voor aan- en verkoopfraude. Daaruit bleek dat 50 procent van de slachtoffers aangifte deed. Sindsdien houdt het Centraal Bureau voor de Statistiek (2022) dit bij op basis van zelfrapportage. Daaruit blijkt dat circa 20% van de gedupeerden aangifte doet van aankoopfraude (19% voor alle online criminaliteit). Wanneer dit percentage wordt geëxtrapoleerd naar de schade over het jaar 2022 (12,4 miljoen euro), dan zou de financiële schade afgerond €50 miljoen bedragen.

Aan– en verkoopfraude in het perspectief van alle online aankopen

Bij aan-en verkoopfraude is sprake van het zogenaamde *many-little-principe.* Oplichters plaatsen veel aanbiedingen op online handelsplaatsen voor relatief lage bedragen of voor bedragen die te mooi zijn om waar te zijn (zoals voor te goedkope smartphones van dure merken). Onder online handelsplaatsen vallen bijvoorbeeld Marktplaats, eBay, Vinted en Speurders, maar advertenties worden steeds vaker op sociale media zoals Facebook (Marketplace) of Instagram geplaatst. De oplichters bereiken veel slachtoffers en het risico is laag. Vanwege de anonimiteit op internet kunnen oplichters heel lang ongestraft hun gang gaan.

Marktplaats is nog steeds een van de grote Nederlandse online handelsplatforms. Voor 2017 bezochten ruim 1,3 miljoen mensen per dag Marktplaats, anno 2023 maakt Marktplaats melding van maandelijks 8 miljoen unieke bezoekers. Toen werden gemiddeld 350.000 nieuwe advertenties op de website geplaatst, van kleding en verzamelobjecten tot auto's en huisraad. In 2017 stonden op een gemiddelde dag ruim 9 miljoen advertenties op Marktplaats. Anno 2023 is dat verdubbeld naar 18,7 miljoen. Dit hangt samen met een flinke toename van het totaal aantal online kopers (alle aankopen die Nederlanders online doen). Het percentage Nederlanders dat online bestelt, steeg van 77 procent (CBS, 2015) voor 2017 naar 97 procent in 2022 en Nederlanders gaven gezamenlijk 33,3 miljard euro online uit. Ter vergelijking, in 2021 was dat 30,6 miljard euro. De stijging zat vooral in aankopen van tickets voor attracties, evenementen en reisgerelateerde aankopen, hetgeen niet onlogisch is na de lockdowns gedurende de coronaperiode (Thuiswinkel.org, 2023). Nederland is koploper in Europees verband met het doen van online aankopen. De helft van de Nederlanders koopt regelmatig tweedehands spullen online en ruim een derde biedt ze zelf aan. Populairste sites zijn Facebook (Marketplace) en Vinted, gevolgd door Marktplaats (Marketing Tribune, 2022).

Bezoekers van online handelsplaatsen zijn niet de enige gedupeerden van aan- en verkoopfraude, ook webshops hebben veelvuldig met fraude te maken. Uit een onderzoek van Thuiswinkel.org onder 107 webshops en retailers die online artikelen verkopen, kwam naar voren dat 80 procent wel eens met fraude te maken heeft. Meest voorkomend is de claim dat een besteld artikel met achterafbetaling niet is ontvangen[9]. Tweede meest voorkomende fraudevorm is misbruik van (bestaande) accounts voor bestellingen zoals beschreven in hoofdstuk 4.9. Vooral grote shops die gewilde artikelen verkopen ondervinden hiervan veel hinder. Zij treffen dan ook vaak maatregelen om fraude te voorkomen, waarbij klantvriendelijkheid zwaar weegt, en soms beschikken ze zelfs over fraudeteams (persoonlijke informatie, 21 augustus 2024).

Externe bronnen

De geraadpleegde externe bronnen bevestigen het beeld uit de politiesystemen, namelijk dat aan- en verkoopfraude het meest voorkomende delict is met gemiddeld een lage financiële schade. Het CBS deed in 2021 voor het eerst onderzoek naar de financiële schade van allerlei delicten (CBS, 2022). Fraude met online aankopen kwam met 1,3 miljoen delicten het vaakst voor en had tegelijkertijd het laagste gemiddelde schadebedrag: de helft ervan lag onder de 50 euro (totaal was de schade 238 miljoen euro).

De Fraudehelpdesk[10] (FHD) heeft een hoofdcategorie voor marktplaats- en webwinkelfraude, maar het aantal meldingen blijft redelijk stabiel en is veel lager dan bij de politie. Jaarlijks worden er ongeveer 5000 meldingen gedaan en de totale schade is meestal rond één miljoen euro, wat neerkomt op gemiddeld 400 euro per melding. Gedupeerden worden door de FHD naar het LMIO verwezen en dit verklaart de grote verschillen met de aantallen bij de politie.

Junger et al. (2022)[11] verbonden aan de Universiteit van Twente constateerden een daling in traditionele criminaliteit en een stijging in fraude. Winkeldiefstal is vervangen door online handelsfraude en fraude wordt nu gepleegd met bankpassen in plaats van dat banken worden overvallen, aldus de onderzoekers. Voor het onderzoek is een eigen categorisering gebruikt, maar aankoopfraude is vergelijkbaar met alle andere bronnen (politie en extern). Bijna 3000 willekeurig geselecteerde leden uit een panel (*LISS - Longitudinal Internet Stu-*

9 Vanuit het standpunt van de shops is dit geformuleerd als verkoopfraude. In de aangiften van het LMIO is dit niet terug te zien en verder is niet onderzocht hoe vaak shops hiervan aangiften doen.

10 De cijfers zijn door de FHD via mailings verstrekt, waardoor een concrete bronvermelding ontbreekt.

11 Gefinancierd door de politie, de Nederlandse Vereniging van Banken (NVB), International Card Services (ICS) en St. Achmea slachtoffer en samenleving (SAS).

dies for the Social Sciences) hebben een vragenlijst ingevuld voor het onderzoek. Aankoopfraude kwam het vaakst voor met gemiddeld lage schadebedragen.

Wat zijn kenmerken van criminele groeperingen?

Er is weinig bekend over de ontwikkeling van kenmerken van plegers en/of criminele groeperingen als het gaat om aan- en verkoopfraude. Hoewel er wel iets bekend is over de inzet van geldezels, zijn details over criminele groeperingen alleen indirect bekend. Het LMIO volgt financiële stromen via bankrekeningnummers en vordert het bankrekeningnummer waarnaar het geld is overgemaakt bij de bank. Hierdoor komen geldezels in beeld die hun rekeningnummer ter beschikking stellen. Uit de overzichten die het LMIO bijhoudt, blijkt dat voornamelijk minderjarige jongeren (12-17 jaar) hun rekening beschikbaar stellen en daartoe worden ze geronseld op schoolpleinen en via sociale media. Soms stellen de geldezels vervolgens de eigen rekening of pinpas beschikbaar aan de criminelen, soms hebben ze een meer actieve rol en nemen ze het crimineel verkregen geld op, sluizen het door naar rechtspersonen, naar het buitenland of naar de criminele leiding. Op deze manier werken ze mee aan belastingfraude en het witwassen van de criminele inkomsten. Ze krijgen hiervoor een geringe vergoeding en zijn vaak niet op de hoogte van hun aandeel in de fraude.

Het LMIO is gevraagd naar de ontwikkeling in het gebruik van geldezels, omdat het gegevens hierover bijhoudt. Het is echter moeilijk om iets te zeggen over trends, om verschillende redenen. Niet altijd is duidelijk of de katvanger en de uitvoerder van de oplichting dezelfde persoon zijn. Ook staat niet bij alle aangiften een bankrekeningnummer vermeld. De aantallen per jaar verschillen sterk, waardoor geen uitspraak kan worden gedaan over een trend. Geldezels spelen bij nagenoeg alle online fraudevormen een rol en de problematiek en aantallen zijn al jaren groot.

Wat betreft het overmaken van criminele gelden naar het buitenland, constateert het LMIO dat steeds vaker gebruik wordt gemaakt van buitenlandse Payment Server Providers (PSP's), vergelijkbaar met het Nederlandse iDeal. Het aantal meldingen over PSP's is gestegen van 4600 in 2020 naar 9073 in 2023 De stijging hangt samen met de toename van oplichting via valse webshops, waarbij gebruik werd gemaakt van PSP's. Eerder was een stijging zichtbaar in het overmaken van criminele gelden naar buitenlandse bankrekeningnummers, maar dit lijkt te dalen in 2023. Gewone bankrekeningnummers worden gebruikt bij oplichting via Marktplaats, zowel binnen als buiten de beveiligde betaalomgeving van Marktplaats of via betaalverzoeken.

Het LMIO merkt al enige tijd op dat grotere criminelen, die waarschijnlijk deel uitmaken van groeperingen, betrokken zijn bij valse webshops. Deze criminelen zijn ook betrokken bij geweldsdelicten en drugshandel. Hoewel het LMIO dit ziet, houdt het nog geen overzichten van groeperingen bij, waardoor geen uitspraak over de ontwikkeling kan worden gedaan. Eerder werd geconstateerd in het deelrapport *Horizontale Fraude* 2017 (Bloem & Harteveld, 2017) dat multidisciplinaire groeperingen zich bezighouden met allerlei vormen van fraude, waaronder aan- en verkoopfraude. Een voorbeeld in het deelrapport was een webshop voor consumentenelektronica waartegen 1700 aangiften waren gedaan en waarvoor geldezels uit Griekenland werden ingezet.

Destijds zag het LMIO dat criminelen zich gingen toeleggen op andere criminaliteitsvormen. Criminelen stapten over van woninginbraken naar oplichting via handelsplaatsen, vanwege de combinatie van een lage pakkans en een snel resultaat. Vaak is er sprake van individuele oplichters die 'het kunstje' doorleren. Ook is er sprake van oplichters die in georganiseerd verband opereren, maar het exacte aantal kan het LMIO niet uit zijn systemen halen. Uit breder onderzoek (o.a. Roks et al., 2020) blijkt dat criminele netwerken zich ook met online fraude bezighouden. Naast traditionele offline delicten gaat het om cyberdelicten, waarbij ze gebruik maken van de digitale omgeving. In dergelijke groeperingen hebben verschillende actoren hun eigen rollen en gaat het vaak om complexe logistieke processen.

Wat zijn kenmerken van slachtoffers?

Uit onderzoek is gebleken dat slachtoffers van aan-en verkoopfraude over het algemeen jonger zijn dan slachtoffers van andere fraudevormen, zoals TSS of bankhelpdeskfraude. Het gemiddelde slachtoffer is 43 jaar oud en hoger opgeleid, en het merendeel is werkend (Borwell, 2017). In lijn hiermee liet een onderzoek van het CBS uit 2015 zien dat ouderen veiliger gedrag vertoonden op internet dan jongeren en dus minder vaak slachtoffer waren. Echter, latere onderzoeken hebben aangetoond dat ouderen vaker slachtoffer zijn van andere vormen van online fraude, vooral wanneer social engineering technieken werden ingezet, zoals bij phishing, betaalverzoekfraude en hulpvraagfraude.

Wat zijn de verwachtingen in relatie tot de aanpak?

In twee achtereenvolgende deelrapporten *Horizontale Fraude* (Bloem et al., 2012; 2017) was de conclusie:

Internet maakt de drempel tot fraude met online handel laag. Op dit moment wordt veel aan preventie gedaan, door Marktplaats, het LMIO en de Fraudehelpdesk. Het is echter wel noodzakelijk dat een aantal stelselmatig frauderende groeperingen in kaart wordt gebracht en aangepakt. Wanneer dit achterwege blijft, dan is de verwachting dat fraude met online handel niet zal afnemen.

Marktplaats werkt sinds de oprichting samen met het LMIO en heeft veel maatregelen getroffen om fraude tegen te gaan, zoals de al genoemde beveiligde betaalomgeving. Dit heeft gemaakt dat de aantallen registraties bij het LMIO wel iets teruggelopen zijn, maar het gaat nog steeds om enkele tienduizenden per jaar. Daar komt bij dat lang niet iedereen zich meldt bij de politie en dat circa 20 procent van de registraties naderhand door de aangever/melder of de politie worden teruggetrokken (opgave LMIO). In het algemeen bestaat de aanpak uit een combinatie van preventie en voorlichting en incidenteel het opsporen van geldezels.

In de loop der jaren heeft Marktplaats steeds meer maatregelen moeten nemen om fraude op of via haar website te voorkomen en beschikt zij inmiddels over een flinke fraudeafdeling, die werkt aan het blokkeren van accounts, het verwijderen van advertenties, het creëren van een 'veilige oversteek' (koopbescherming en beveiligde betaalverzoekmogelijkheid) en het geven van voorlichting. Het LMIO heeft ervoor gezorgd dat kopers de gegevens van de verkoper kunnen controleren op de site van Politie.nl, zoals bankrekening, url, telefoon-

nummer en e-mailadres[12]. Ook doet het LMIO zogenaamde *notice-and-take-down* procedures, dat wil zeggen dat nepwepshops gemeld worden bij providers die ze dan uit de lucht halen. Recentelijk is van de grond gekomen dat geldezels civiel aangepakt worden: met de hulp van een deurwaarder dienen ze de schade aan het slachtoffer terug te betalen. Dit is aan een aantal voorwaarden verbonden: de verdachte moet meerderjarig zijn en er moeten aangiftes tegen deze persoon zijn gedaan. Daarnaast is de geldezel niet kwetsbaar , zoals verslaafd en/of dakloos, en mag niet voorkomen in een centraal curatele systeem.

Het project Centurion en LMIO hebben samen verschillende initiatieven gerealiseerd om aan- en verkoopfraude tegen te gaan, terwijl er nog andere initiatieven in ontwikkeling zijn. Een van deze initiatieven is het automatisch bundelen en doorsturen (zogenaamd routeren) van aangiften naar de eenheid van de rekeninghouder. Dit betekent dat als er meer aangiften tegen hetzelfde bankrekeningnummer worden gedaan, deze aangiften zichtbaar worden in Betere Opsporing door Sturing op Zaken (BOSZ) en dat een *casescreener* een besluit moet nemen over het vervolg van de zaak. Dit geldt alleen voor aangiften met een Nederlands bankrekeningnummer waarbij de rekeninghouder is geïdentificeerd en woonachtig is in Nederland, en niet voor PSP-rekeningen of verzamelrekeningen. Dit proces is van toepassing op ongeveer 30 procent van alle aangiften van aan- en verkoopfraude. De overige 70 procent wordt momenteel handmatig verwerkt of gaat naar de Basis Voorziening Handhaving (BVH) van de Landelijke Eenheid. Er zijn plannen om dit te veranderen, zodat aangiften naar de BVH van de eenheid gaan waar het slachtoffer woont, maar het is nog niet duidelijk wanneer dit zal gebeuren.

Het LMIO heeft onlangs een samenwerking opgezet met een Nederlandse Payment Service Provider om fraude tegen te gaan. Wanneer er een aangifte of melding wordt gedaan waarin deze PSP is betrokken, worden identificerende gegevens opgevraagd bij de Kamer van Koophandel en banken. Er is ook samengewerkt met een kleine online bank, omdat die in onevenredig veel registraties voorkwam. Het doel was om de bank aan te sporen meer te doen aan beveiliging. Verder zijn er plannen om samenwerking op te zetten met banken en PSP's in het buitenland, onder andere door overleg met een partij die online betalingen faciliteert en door het afsluiten van een convenant.

In het kort zijn er veel maatregelen genomen door zowel LMIO als Marktplaats om fraude tegen te gaan. Echter, er wordt geen inzicht verkregen in criminele groeperingen die actief zijn in deze fraudevorm (en andere fraudevormen, zoals zal blijken uit de beschrijving van andere fenomenen). Hoewel voorspellingen moeilijk blijven, blijft de conclusie uit eerdere dreigingsbeelden nog steeds geldig: als de verantwoordelijke groeperingen niet in kaart worden gebracht en aangepakt, zullen de aantallen registraties onverminderd hoog blijven.

12 Zie: https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html

4.2 Phishing

Phishing is een tactiek die cybercriminelen gebruiken om onrechtmatig persoonlijke gegevens van iemand te verkrijgen en/of toegang te krijgen tot een apparaat of account van die persoon. Phishing heeft meestal een faciliterende rol en de onrechtmatig bemachtigde gegevens worden gebruikt om andere vormen van fraude te plegen.

Phishing in cijfers

Bankphishing

(sms belastingdienst): 2700 registraties met 5 miljoen euro schade in 2022.

Betaalverzoekfraude

(1 cent betalen): 4000 registraties met 2,6 miljoen euro schade in 2022

Exacte cijfers over 2023 niet bekend

Nieuwe trend in 2023

nepberichten van de belastingdienst via sms of app

Verkrijgen persoonlijke bankgegevens via een link naar

valse website van de bank

Drie typen

betaalverzoekfraude
bankphishing
nepfacturen

In dit fenomeenbeeld worden twee vormen van online fraude besproken, waarin phishing de centrale werkwijze is. Het gaat om bankphishing en betaalverzoekfraude. Betaalverzoekfraude is in de Veiligheidsagenda opgenomen (Ministerie van Veiligheid & Justitie, 2023)[13].

Hoe heeft het fenomeen zich ontwikkeld?

Bij bankphishing ontvangen slachtoffers in eerste instantie een mail met een link die afkomstig lijkt te zijn van de bank. Met de ontwikkeling van korte digitale berichten op de telefoon zijn deze mails vervangen door sms-berichten of app-berichten, zoals via Telegram of WhatsApp. Wanneer het slachtoffer op de link klikt, wordt hij of zij doorgeleid naar een website die lijkt op die van de bank. Hier wordt vervolgens gevraagd om persoonlijke gegevens, zoals inloggegevens. Hiermee krijgt de oplichter toegang tot de bankrekening van het slachtoffer. Dit is een technisch middel om persoonlijke e-banking of cryptogegevens te bemachtigen en daarmee wordt computervredebreuk gepleegd of gepoogd te plegen tegen de systemen van de bank (CCT Limburg, 2020).

In 2023 werd een nieuwe trend zichtbaar in bankphishing. Mensen klikken niet op de link, maar betalen het bedrag dat ze in de sms- of app-berichten ontvangen. Strikt genomen betreft het geen bankphishing, omdat het slechts gaat om het voldoen aan een betaalverzoek of het betalen van een valse factuur (in oudere rapporten worden ze ook wel ‘spooknota’s’ genoemd).

Betaalverzoekfraude is een andere vorm van phishing die rond 2018 is opgekomen. Deze vorm van online fraude vindt vaak plaats via allerlei online handelsplatformen. De oplichter probeert bijvoorbeeld via Marktplaats contact te zoeken met personen die een product te koop aanbieden. Vervolgens worden deze verkopers overgehaald om het gesprek en de betaling buiten de beveiligde chat- en betaalomgeving van Marktplaats voort te zetten. Daar vragen de oplichters meestal om een klein bedrag van 1, 2 of 5 cent over te maken, onder het voorwendsel dat zij eerder zijn opgelicht en zeker willen weten dat het goed zit. Dit betaalverzoek wordt bijvoorbeeld via berichtenapps gestuurd en is met een link gekoppeld aan een phishingsite. Na betaling komen kopers op een site die eruitziet als een betrouwbare bank en worden allerlei persoonlijke gegevens gevraagd, zoals inloggegevens. Hierdoor krijgen de oplichters toegang tot de bankrekening van het slachtoffer.

Met de opkomst van e-mail ontstond phishing, maar met de intrede van online platforms ontstonden allerlei nieuwe vormen van criminaliteit met een digitale component. Toen Marktplaats en WhatsApp (in plaats van e-mail) en nieuwe digitale betaalmethoden populair werden, kwamen voor oplichters kansen om betaalverzoekfraude te plegen. Veel mensen hadden inmiddels hun e-mail beveiligd met een spamfilter, maar waren niet opgewassen tegen deze nieuwe vorm van fraude. Oplichters maken vaak gebruik van *social engineering* om vertrouwen te winnen bij hun slachtoffers. Dit kan variëren van kortdurend contact tot langdurige interacties. Zodra het vertrouwen is gewonnen, sturen de oplichters direct een betaalverzoek. Hoewel deze vorm van fraude technisch klinkt, is er weinig technische kennis vereist en kan het op grote schaal worden gepleegd. Alle benodigde onderdelen, zoals gehackte Marktplaatsaccounts en phishingpanels[14], kunnen voor een lage prijs worden gekocht of ingehuurd via internet. Het enige wat nog rest, is het benaderen van potentiële slachtoffers en het verdiende geld op een anonieme manier weg te sluizen (de cash-out) (Rooyakkers & Weulen Kranenbarg, 2020).

Hoe heeft de omvang zich ontwikkeld?

Betaalverzoekfraude en bankphishing kennen geen aparte categorieën in de politiegegevens, maar vallen beide onder de algemene categorie fraude met bankgegevens en/of internetbankieren. Daarom is het moeilijk om aan exacte aantallen te komen. In de periode van 2016 tot en met 2018 stond fraude met bankgegevens op de tweede plaats in een landelijke top 10 van online fraudevormen met de meeste registraties (meer dan 2600 registraties). In deze periode ging het voornamelijk om phishing via e-mail en in mindere mate om phishing via sms-berichten (de precieze aantallen zijn nooit onderzocht). Tussen 2016 en 2018 vond er een verdubbeling plaats van het aantal registraties, gevolgd door een nog grotere toename in 2019. In deze periode werden verschillende aanpassingen gedaan in de Landelijke Cyber Query (LCQ) om wijzigingen in de werkwijze op te vangen en ook om betaalverzoekfraude op te sporen (een nieuw fenomeen in die tijd). Hierdoor nam het aantal registraties van fraude met bankgegevens sterk toe, waardoor het niet meer mogelijk was om een goede vergelijking te maken met de cijfers van voor die tijd (Borwell et al., 2020). Wel is duidelijk dat betaalverzoekfraude de meest voorkomende werkwijze is binnen deze algemene categorie.

Om iets te zeggen over betaalverzoekfraude zijn verschillende bronnen gebruikt. Om die reden is geen tabel gemaakt en is het niet mogelijk om een trend te schetsen. De aantallen gaan over heel Nederland. Een analyse van het cybercrimeteam Limburg over het jaar 2020 liet zien dat er toen ongeveer 6000 registraties van betaalverzoekfraude waren (12% van alle registraties uit de LCQ; 14% betrof een poging). Een handmatige analyse in 2021 leverde ruim 10.000 registraties op, waarvan 85 procent via Marktplaats waren gegaan (betaalverzoekfraude) (Van der Plas, 2020). In 2022 ging het om ruim 4000 aangiften en meldingen. Dit aantal is afkomstig uit het Cyberintelligencejaarbeeld van de Inteltafel Cyber (2023) en betreft gecontroleerde registraties. De conclusie was dat bij zeven van de tien eenheden betaalverzoekfraude op de derde plaats stond en 80 procent via Marktplaats was gegaan. De schade over die 4000 registraties bedroeg 2,6 miljoen euro.

Uit de samenwerking tussen Marktplaats en het cybercrimeteam van Limburg bleek dat de aantallen flink zijn teruggelopen (hierna beschreven onder aanpak). Alleen betaalverzoekfraude via Marktplaats scoort hoog bij de meeste eenheden en dit is al een aantal jaren zo. Het advies is om gedetailleerd onderzoek te doen naar de verschillende fraudevormen die onder fraude met bankgegevens/internetbankieren vallen, zodat inzichtelijk wordt of meer

13 Betaalverzoekfraude is hierin opgenomen onder een andere naam (WhatsApp-fraude) onder een algemene categorie (online voorschotfraude). Een opvallende indeling, waarbij de Veiligheidsagenda het begrip ‘voorschotfraude’ onjuist hanteert. In geval van voorschotfraude ontvangen slachtoffers mails waarin een erfenis of prijs in een loterij in het vooruitzicht wordt gesteld, maar om deze te ontvangen, moeten bedragen (voorschotten) vooruitbetaald worden.

14 Bijlage 4, woordenlijst

fraudevormen dan betaalverzoekfraude en bankphishing in deze categorie voorkomen. In de overgang van BlueIntel naar het nieuwe programma Helios is een voorstel voor nieuwe categorieën gedaan, zodat de verschillende vormen beter kunnen worden onderscheiden. In de toekomst is het daarmee mogelijk om een consistenter beeld te geven dan nu in de voorgaande alinea is beschreven.

Bij bankphishing gaat het bijna altijd om e-mails of sms-berichten die schijnbaar namens de bank zijn verzonden (Inteltafel Cyber, 2023). De oplichters sturen dit soort phishingberichten in grote hoeveelheden en ongericht. In 2022 kreeg de politie ruim 2700 registraties binnen over phishing-e-mails of -sms'jes die zich voordeden als afkomstig van de bank. De schade bedroeg vijf miljoen euro. De e-mails spelen vaak in op trends in de maatschappij, zoals de energietoeslag of e-mails die bij mensen binnenkomen als zij hun vakantiegeld hebben ontvangen. Niet alle berichten zijn van de bank, maar ook van andere organisaties. In 2021 waren er bijvoorbeeld ruim 1000 phishingmails over de verlenging van de inschrijving van Woningnet, die in 2022 alweer flink gedaald waren. Op de website van Woningnet was informatie gegeven over phishing, wat de oplichters kennelijk inspireerde om nepmails namens deze organisatie te sturen. Uit een analyse over 2022 bleek dat één op de drie registraties betrekking had op phishing vanuit een bank en dat de nepwebsites steeds beter leken op echte bankwebsites. De andere registraties gingen over berichten van de overheid of het was niet bekend. De Inteltafel Cyber heeft voor het Cyberintelligencejaarbeeld deze analyse uitgevoerd over 2022; analyses over eerdere jaren ontbreken, waardoor geen uitspraak kan worden gedaan over het verloop.

In 2023 kwam een nieuwe variant van bankphishing op. In dat jaar kreeg de politie hiervan 1431 registraties (opgave Oost-Nederland). Slachtoffers kregen een bericht en klikten niet op de link, maar maakten het bedrag over. Het ging bijvoorbeeld om achterstallige betalingen van de belastingdienst, maar ze konden ook schijnbaar van het Centraal Justitieel Incassobureau (CJIB) of de Kamer van Koophandel afkomstig zijn. Vanwege de betaling vallen deze registraties strikt genomen niet onder bankphishing. De betaalverzoeken of valse facturen kregen mensen binnen via een sms-of app-bericht.

Externe bronnen

Vanwege het gebruik van verschillende indelingen en termen door externe bronnen, is het lastig om vergelijkingen te maken, zowel onderling als met de categorisering van de politie.

Het CBS heeft in 2021 voor het eerst onderzoek gedaan naar de financiële schade van diverse delicten. Het CBS noemt niet apart betaalverzoekfraude en bankphishing, maar hanteert een algemene term genaamd spoofing, dat op de tweede plaats staat na aan- en verkoopfraude (CBS, 2022). Het CBS definieert spoofing als alle vormen van fraude waarbij de dader zich voordoet als een vertrouwde instantie of persoon, zoals een medewerker van de bank of een helpdesk, een goede vriend/familielid, of een nieuwe aanbidder, om mensen geld afhandig te maken. Via spoofing verschaft de dader zich toegang tot de bankrekening, of hackt een account of apparaat van het slachtoffer. In veel gevallen maakt het slachtoffer ook zelf geld over naar de dader. In totaal waren er 97.000 slachtoffers van spoofing onder personen van 15 jaar en ouder, met een totale schade van 261 miljoen euro (gemiddeld 2700 euro). Dit was 11 procent van de totale financiële schade door alle criminaliteit. Driekwart van de slachtoffers maakte zelf het geld over naar de oplichter (187 miljoen euro).

De cijfers van de Fraudehelpdesk laten zien dat het aantal meldingen van cybercriminaliteit (waar phishing, malware en helpdeskfraude onder vallen) tussen 2021 en 2022 met de helft afnam, van ruim 12.000 naar 6200 meldingen. Onder phishing verstaat de FHD alle vormen van hengelen naar vertrouwelijke gegevens door links te sturen die naar valse websites leiden. Dit gebeurt via allerlei kanalen, zoals emails, berichtenapps, sms, ook telefonisch en via persoonlijk contact. De aantallen meldingen zijn redelijk stabiel: zowel in 2022 als in 2023 schommelen ze rond de 3200, zij het dat de totale schade in 2022 ruim 250.000 euro was en in 2023 lager, namelijk ruim 145.000 euro. De schade per melding was in 2022 gemiddeld 2050 euro (122 slachtoffers) en in 2023 iets lager, namelijk gemiddeld 1250 euro (117 slachtoffers). Zoals de FHD meldt, kunnen de aantallen hoger liggen, omdat phishingmails voor andere doeleinden kunnen worden gebruikt, waardoor de gevolgen niet altijd duidelijk zijn. Ook de FHD ziet dat oplichtingen waarbij via een valse link in een e-mail om gegevens wordt gevraagd, die eerder onder cybercriminaliteit vielen, zijn verplaatst naar nieuwe trends zoals hulpvraagfraude en bankhelpdeskfraude. In hoofdstuk 4.4 over bankhelpdeskfraude zijn nadere details beschreven.

De Nederlandse Vereniging van Banken meldt dat de schade van phishing tussen 2021 en 2022 halveerde van 6,1 miljoen euro naar 3,6 miljoen euro. De NVB (2023, 29 maart) stelt dat de oplichters persoonlijke informatie in handen proberen te krijgen door valse e-mails te sturen (phishing) en ze proberen met malware in te breken op computers.

Wat zijn kenmerken van criminele groeperingen?

Het lijkt erop dat er momenteel geen specifieke informatie beschikbaar is over criminele groeperingen die zich bezighouden met betaalverzoekfraude. In 2020 zijn in het NCB (Bloem & Harteveld, 2019) thema's benoemd op basis van een top 10 van meest voorkomende online fraudevormen en aanvullend onderzoek naar de meeste impact en schade. Deze thema's zijn belegd bij verschillende eenheden om een informatiepositie op te bouwen en een aanpak te ontwikkelen samen met de teams[15]. Op verschillende thema's is succesvol samengewerkt tussen intelligenceafdelingen van de politie en verschillende publiek-private partijen. Op andere thema's zijn uitgebreide beelden opgeleverd, inclusief barrièremodellen. Alleen voor phishing was dat niet het geval. Daarna hebben eenheden (hierna uitgewerkt) dit als thema opgenomen en is er gewerkt aan verbetering van de informatiepositie. Een beeld van plegers, rollen of groeperingen, laat staan van een ontwikkeling hierin is helaas niet tot stand gekomen.

Casus: functies binnen criminele groepering

In onderstaande casus worden de rollen binnen een criminele groepering beschreven aan de hand van een opsporingsonderzoek naar betaalverzoekfraude. Daarin zijn bij uitzondering de rollen beschreven die de verschillende leden hadden. Het is waarschijnlijk dat meer groepen op deze wijze te werk gaan.

15 De thema's waren helpdeskfraude, phishing, factuur- en CEO-fraude, ransomware, DDoS en account take over (ATO, dat toen hacken accounts voor bestellingen heette). Later kwamen daar betaalverzoekfraude en sextortion bij.

Verschillende vormen van online fraude en verschillende rollen in de groepering.

Er zijn vier verdachten, 3 mannen en een vrouw, en 30 aangiften van online fraude: ViN-fraude, betaalverzoekfraude, bankphishing en bankhelpdeskfraude. De vier leden hadden verschillende rollen (ronselaar, pinner, bonker):

Het vrouwelijke lid ronselde geldezels om bankpassen beschikbaar te stellen en boekte hotelkamers. Een mannelijk lid deed hetzelfde en was ook verantwoordelijk voor het plaatsen van nepadvertenties op Marktplaats. Hij stelde zijn pas beschikbaar en nam het geld op dat afkomstig was van de oplichtingen. De tweede man had dezelfde taken maar ronselde daarbij geldezels om hun bankpassen beschikbaar te stellen. De derde man deed soortgelijke taken, zoals het beschikbaar stellen van zijn bankpas, het boeken van hotelkamers en het opnemen van geld afkomstig van internetoplichting. Hij hield zich echter ook bezig met het verkrijgen van leadlijsten en panels[16], en het daadwerkelijk frauderen.

De verdachten verbleven elke week in familiekamers in een groot hotel met laptops en 'panels' (illegale software waarmee o.a. nepbetaallinken worden aangemaakt) om mensen op te lichten. Bij het plegen van de oplichtingen volgden handelingen elkaar snel op: als het geld was overgeboekt, belde de oplichter gelijk naar de 'pinner', om het geld van de rekening van de katvanger te pinnen. Er werd vaak van simkaart gewisseld. Ze gebruikten geweld om geldezels te dwingen om bankrekeningen te openen. Een van de mannen zou over een automatisch vuurwapen beschikken. De verdachten gaven veel geld uit aan roomservice en prostituees. Ze namen geld op in het casino om het aldaar te besteden en kochten cryptovaluta.

Wat zijn de verwachtingen in relatie tot de aanpak?

Deze paragraaf gaat over de aanpak van phishing in het algemeen. Dit beeld is divers aangezien uit de aanpak van banken en het project BigPhish[17] blijkt dat phishing via email sterk is teruggelopen. Dit is slechts één vorm van phishing, aangezien andere vormen, zoals betaalverzoekfraude en bankphishing, nog steeds tot de meest voorkomende behoren. Deze vormen veroorzaken veel schade en hinder bij burgers. In hoofdstuk 4.1 over aan-en verkoopfraude is al de aanpak van betaalverzoekfraude beschreven, omdat het contact met slachtoffers veelal via een advertentie op Marktplaats plaatsvindt.

16 Bijlage 4, woordenlijst

17 Het project BigPhish betreft een samenwerking tussen de eenheid Noord-Nederland, de Electronic Crime Task Force (ECTF) en de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) en heeft als doel om criminaliteit met behulp van phishing aan te pakken.

Tussen 2013 en 2015 is de financiële schade van phishing bij de banken flink afgenomen van 9,6 miljoen euro naar 3,7 miljoen euro (Bloem et al., 2017). Toen was skimmen[18] verantwoordelijk voor een groot deel van de schade. Door de integrale aanpak van de politie en banken, waarbij opsporing en wijziging van techniek werden gecombineerd, was het niet langer mogelijk om te skimmen. Er was ook een flinke daling in het aantal registraties te zien. Hierdoor was de verwachting dat er in de navolgende jaren weinig zou veranderen, maar dit was onzeker vanwege mogelijke verschuivingen en nieuwe ontwikkelingen in het betaallandschap. Op dat moment stapten consumenten nog niet massaal over naar nieuwe betaalvormen en was er vertrouwen in de beveiliging van de nieuwe technieken. Inmiddels is dit sterk veranderd.

Zoals eerder beschreven is het op basis van politiedata moeilijk om een duidelijke trend te schetsen, aangezien de categorie fraude met bankgegevens en/of internetbankieren uit ruwe data bestaat, waarin alle vormen van phishing zijn opgenomen. Hierdoor zegt de enorme stijging die tussen 2016 en 2021 te zien was niet zoveel. Ook bankhelpdeskfraude, bijvoorbeeld, werd tot eind 2023 onder deze algemene categorie weggeschreven. Daarnaast zijn er onjuist gescoorde registraties, die niet worden gecontroleerd. Bovendien zijn er aanpassingen in de Landelijke Cyber Query (LCQ) gemaakt om betaalverzoekfraude beter te kunnen identificeren, wat heeft geleid tot een flinke stijging na 2017. Om tot juiste uitspraken over trends te komen, verdient het aanbeveling om de gehele categorie nader te onderzoeken en te kijken naar de verschillende vormen die deze bevat en hoe deze veranderen.

In het *Jaarbeeld Cybercrime 2021* van de Eenheid Rotterdam is de verwachting over 2022 uitgesproken dat phishing zal toenemen om verschillende redenen. Ten eerste is er *'Phishing-as-a-service'*, waarbij kant-en-klare tools op sociale media worden aangeschaft en laagdrempelig worden gebruikt voor het uitvoeren van online fraude. Ten tweede zal phishing toenemen doordat steeds meer malware via sms/e-mail op mobiele apparaten terechtkomt, zoals bijvoorbeeld Flubot[19], een bancaire malware die gericht is op het stelen van privégegevens uit Android-toestellen. Ten derde is er het toenemend gebruik door cybercriminelen van technieken waarmee het moeilijker wordt voor antivirusprogramma's om de malware te ontdekken. Ten vierde zullen vaker aanvallen plaatsvinden gericht op het stelen van cryptovaluta. Deze voorspelling lijkt uit te komen. In 2023 waren er 355 registraties van diefstal van cryptomunten met een totale schade van 65 miljoen euro. (Bron: BVH, BlueIntel)[20].

18 Skimmen was het op onrechtmatige wijze kopiëren van betaalkaartgegevens.

19 Flubot is sinds voorjaar 2022 niet meer waargenomen en het is niet dat dit type malware terugkomt. Sinds voorjaar 2024 worden nieuwe vormen van bancaire malware gezien, zoals Vulture. De malware wordt gedownload via een bekende virusscanner en valt apps van banken aan die werken op Android.

20 Diefstal cryptomunten omvat verschillende type delicten waarbij uiteindelijk de dader toegang krijgt tot het wallet account van het slachtoffer en de crypto eruit overboekt naar een eigen rekening of rekening van een katvanger. Bijvoorbeeld een bankhelpdesk die belt en wel even helpt met crypto overmaken naar een veilige rekening. Zogenaamd Bitvavo die belt dat men nog crypto heeft op een rekening en dat men meer crypto moet inleggen om dat geld terug te krijgen (opgave Oost-Nederland).

Als laatste is er de ontwikkeling van Chat GPT, een chatbot die met behulp van kunstmatige intelligentie moeiteloos en zeer snel gesprekken en teksten kan genereren. Experts verwachten dat er een flinke toename zal zijn van phishingmails, omdat de chatbot heel gemakkelijk echt lijkende e-mails van bijvoorbeeld banken kan genereren. Vooral ouderen en kleine ondernemers worden verwacht het doelwit te worden. In hoofdstuk 7 van dit rapport is een uitgebreidere beschrijving te vinden van de cybercriminele mogelijkheden die kunstmatige intelligentie biedt.

Aanpak banken

De omvang van de schade als gevolg van phishing bij banken is flink gedaald, vooral phishing door middel van mails met een link naar een nagemaakte bankomgeving. Dit komt volgens de Nederlandse Vereniging van Banken enerzijds doordat mensen de mails beter herkennen door de vele voorlichting, en anderzijds doordat banken steeds beter worden in het herkennen van phishing. Zo zijn systemen ontwikkeld die signalen geven als een afwijkend bedrag wordt afgeschreven of overgemaakt. Vaak neemt de bank dan contact op om te controleren of het klopt en als dat niet het geval is, wordt de betaling tegengehouden. Banken vergoeden de schade onder bepaalde voorwaarden, tenzij er sprake is van grove nalatigheid, fraude of opzettelijk handelen.

De banken kennen een heel pakket aan maatregelen die onder de verschillende fraudevormen worden beschreven. Door één van de maatregelen is het voor cybercriminelen bijna onmogelijk geworden om toegang te krijgen tot betaalrekeningen van slachtoffers. Een voorbeeld hiervan is dat sommige banken iedere paar seconden een andere gekleurde QR-code aanbieden.
Een van de belangrijkste maatregelen is echter de *notice-and-takedown*-procedure die sterk is geprofessionaliseerd. Daardoor kunnen banken nepsites snel uit de lucht halen, waardoor geen slachtoffers meer gemaakt kunnen worden.

Aanpak politie: BigPhish

Binnen de politie zijn verschillende initiatieven ontwikkeld om phishing aan te pakken en navraag heeft enige informatie opgeleverd[21]. In het project BigPhish, een samenwerking tussen de eenheid Noord-Nederland, Electronic Crime Task Force (ECTF) en de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), kwam een opvallende aanpak tot stand. Dit project liep tussen 2018 en 2022 en begon met het verzamelen van informatie door TNO. Het cybercrimeteam van Noord-Nederland selecteerde vervolgens een phishing kit[22] en ontleedde deze, waarna de bouwer ervan kon worden geïdentificeerd.

Daarnaast zijn meerdere andere kits ontleed, wat ertoe leidde dat digitale specialisten domeinen gingen volgen waarop kenmerken van deze kits zichtbaar waren. In totaal zijn bijna 47.000 domeinen gevolgd. Daarbij bleek dat er per dag 200-250 phishing sites online waren. Besloten werd om deze te verstoren met de hulp van de ECTF binnen de politie.

21 De informatie over BigPhish is verkregen door een gesprek met een collega van Team Digitale Opsporing van Noord-Nederland.

22 Bijlage 4, woordenlijst

Dat ging als volgt: de Nederlandse banken zijn aangesloten bij een internationaal bedrijf dat tegen betaling analyses van webhosting aanbiedt, waaronder phishing detectie, cybercrime disruptie en het neerhalen van sites. De ECTF leverde iedere phishing site aan en dit internationale bedrijf haalde ze neer, waarbij de kosten voor rekening van de banken kwamen. Nederland werd niet opgemerkt door de detectiewerkzaamheden van dit internationale bedrijf, omdat deze voornamelijk gericht waren op de Verenigde Staten.

De actie heeft een flinke slag toegebracht aan de criminele activiteiten die met behulp phishing werden gepleegd, zoals verschillende online fraudes. Phishing zou sindsdien in Nederland met 90 procent zijn afgenomen. In totaal zijn vijf bouwers van phishing kits geïdentificeerd, waarvan er vier zijn veroordeeld (één van de bouwers bevond zich in België en bleef buiten beeld). Deze aanpak heeft vermoedelijk geleid tot een verschuiving naar andere online fraudevormen, zoals bankhelpdeskfraude. Dit heeft er echter wel voor gezorgd dat verdachten sneller in beeld komen, omdat ze meer contactmomenten hebben met slachtoffers en daarbij social engineering inzetten. Dit maakt het voor de opsporing iets gemakkelijker om hen op te sporen. Zie verder hoofstuk 4.4. over Bankhelpdeskfraude.

Aanpak politie: thema phishing bij Eenheid Zeeland-West-Brabant

Vijf eenheden hadden thema's onder zich met als doel een informatiepositie op te bouwen en een aanpak te ontwikkelen. De Eenheid Zeeland-West-Brabant kreeg phishing als thema. Dit heeft nog niet geleid tot een veel betere informatiepositie, onder andere omdat dit thema lastig was af te bakenen. Overzicht en inzicht binnen de gehele organisatie ontbraken, bijvoorbeeld op het gebied van opsporingsonderzoeken en verdachten. De eenheid zag voor zichzelf een taak als aanspreekpunt of 'expertisecentrum' en de informatie werd gedeeld via kennisdocumenten op het intranet van de politie. Het project VAK heeft deze kennisdocumenten verzameld en up-to-date gehouden door middel van interviews met collega's. De aanpak die door de eenheid is ontwikkeld bestond uit het samenstellen van een crimescript, waaruit twee opsporingsonderzoeken zijn voortgekomen. Eén onderzoek richtte zich op phishing via e-mails met een link naar een valse bankomgeving en het andere onderzoek richtte zich op de bouwers van phishing kits.

Aanpak politie: thema betaalverzoekfraude bij Eenheid Limburg

In 2020 kreeg het cybercrimeteam van de politie Limburg betaalverzoekfraude als thema. Het team heeft zijn kennis op dit thema verwerkt in een zogeheten 'Book of Crime', waarin wordt beschreven hoe een criminaliteitsvorm wordt gepleegd en dat alleen intern te raadplegen is. Voor het thema betaalverzoekfraude heeft het cyberteam onderzoek gedaan naar het aantal slachtoffers en de omvang van de schade. Gezien de toename in het aantal gevallen van betaalverzoekfraude, heeft het team samengewerkt met Marktplaats om verdere maatregelen te nemen om dit te verstoren. Zo zijn bijvoorbeeld telefoonnummers niet langer zichtbaar bij advertenties en wordt er een uitleg over fraude gegeven wanneer gebruikers dit willen. Daarnaast heeft het team via een brede mailingcampagne meer voorlichting gegeven en mensen opnieuw gewaarschuwd. Volgens een bericht op Politie.nl is het aantal geval-

len van betaalverzoekfraude in twee jaar tijd met 76,5 procent afgenomen (januari 2021 t/m december 2022),[23] wat overeenkomt met de gemelde aantallen in de paragraaf over de ontwikkeling van de omvang.

23 Zie: https://www.politie.nl/nieuws/2023/februari/3/00-politie-en-marktplaats-bundelen-krachten-betaalverzoekfraude-met-ruim-75-afgenomen.html#:~:text=Met%20als%20doel%20het%20aantal,met%2076%2C5%25%20afgenomen.

4.3 Tech support scam

Tech support scam (TSS) is een vorm van oplichting waarbij telefonisch contact plaatsvindt tussen het slachtoffer en een oplichter die zich voordoet als medewerker van een bekend (internationaal) softwarebedrijf. Deze oplichter communiceert vaak in het Engels en beweert dat het slachtoffer technische problemen heeft met zijn computer, e-mail of sociale media-accounts. Om dit te verhelpen, wordt het slachtoffer overgehaald een Remote Access Tool (RAT) te installeren, zodat het probleem op afstand kan worden opgelost. Met de RAT verkrijgt de oplichter toegang tot de computer en dus de bankrekening van het slachtoffer, die vervolgens wordt leeggehaald.

Tech support scam in cijfers

Gesprek
in het Engels, meestal vanuit *callcenters* in India

2854
Van 2854 registraties in 2021 naar 545 in 2023

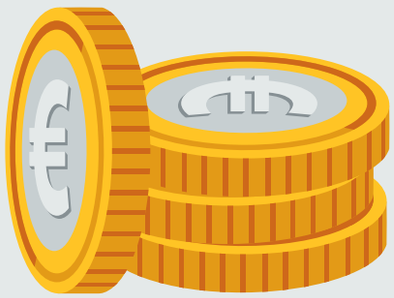
Eerste online fraudevorm met gebruik
Remote Access Tool

Een zogenaamde helpdesk
van een softwarebedrijf belt dat er iets mis is met de computer

€ 350
Gemiddeld schadebedrag van 1600 naar 350 euro per registratie

Tegen vergoeding is dit te verhelpen

TSS afgenomen dankzij internationale aanpak door publiek-private partijen)



€ 200.000
Totale schade van 4,7 miljoen euro in 2020 (piek) naar 200.000 euro in 2023

In dit rapport worden twee varianten van telefonische helpdeskfraude beschreven. De tech support scam wordt in dit hoofdstuk beschreven en bankhelpdeskfraude in het volgende. Telefonische helpdeskfraude omvat alle vormen van oplichting waarbij het slachtoffer via de telefoon wordt benaderd. De oplichter biedt tijdens het gesprek hulp of ondersteuning aan om zogenaamd vreemde of zorgelijke problemen op te lossen. De oplichter doet zich voor als medewerker van de helpdesk of fraudeafdeling van een bank, of van een technologie – of softwarebedrijf, of een andere organisatie. Meestal beweert de oplichter dat er verdachte activiteiten op de bankrekening van het slachtoffer zijn gesignaleerd of dat de computer van het slachtoffer besmet is met een virus. Tech support scam staat niet in de Veiligheidsagenda.

Hoe heeft het fenomeen zich ontwikkeld?

Tech support scam (TSS) is een vorm van oplichting waarbij telefonisch contact plaatsvindt tussen het slachtoffer en een oplichter die zich voordoet als medewerker van een bekend (internationaal) softwarebedrijf. Deze oplichter communiceert vaak in het Engels en beweert dat het slachtoffer technische problemen heeft met zijn computer, e-mail of sociale media-accounts. Om dit te verhelpen, wordt het slachtoffer overgehaald een Remote Access Tool (RAT) te installeren, zodat het probleem op afstand kan worden opgelost. Met de RAT verkrijgt de oplichter toegang tot de computer en dus de bankrekening van het slachtoffer, die vervolgens wordt leeggehaald (project VAK, 2022; 2023, Inteltafel Cybercrime, 2022; Borwell et al., 2020).

Registraties van TSS verschenen in Nederland vanaf 2011 sporadisch in de politiesystemen, maar rond 2017 was dit uitgegroeid tot een van de meest voorkomende en wijdverspreide vormen van cybercrime (Borwell et al., 2018; 2020). Voor zover bekend was het een van de eerste vormen van gedigitaliseerde criminaliteit waarbij RAT's grootschalig werden ingezet. Sindsdien is deze werkwijze terug te zien in verschillende andere fraudevormen.

Aanvankelijk werden slachtoffers vooral gebeld door iemand die zich voordeed als medewerker van de Microsoft-helpdesk. Later gebruikten oplichters namen van verschillende andere grote techbedrijven om contact te leggen.

De wijze van contact leggen tussen oplichter en slachtoffer is ook veranderd. Er zijn drie hoofdvarianten te onderscheiden:

1. **Slachtoffer wordt gebeld.**
Dit is de klassieke modus operandi. De oplichter belt en doet zich voor als medewerker van Microsoft of een ander techbedrijf. Ze leggen de slachtoffers uit dat er problemen zijn ontdekt op de computer, zoals virussen, hackers, verlopen licenties of verouderde software.
2. **Slachtoffer neemt zelf contact op.**
Slachtoffers zoeken zelf hulp vanwege computerproblemen of valse e-mails. Ze vinden een (nep)telefoonnummer online, bijvoorbeeld voor de helpdesk van Gmail, Facebook of Microsoft. Ze bellen en krijgen een oplichter aan de lijn die zich voordoet als medewerker van het bedrijf.
3. **Slachtoffer krijgt een pop-up op zijn scherm.**
Er verschijnt een pop-up op het scherm met de boodschap dat de computer is geïnfecteerd met een virus. Daarin wordt het slachtoffer gevraagd een (vaak) Nederlands telefoonnummer te bellen.

Tot 2019 werd het gros van de slachtoffers nog gebeld, maar daarna verschoof dit meer naar slachtoffers die zelf contact opnamen. Soms kregen de slachtoffers het valse telefoonnummer per ongeluk doorgegeven van een legitiem bedrijf. Eind 2019 is dit tijdelijk de meest voorkomende modus operandi (Borwell et al., 2020). Van 2020 tot 2023 werden de meeste slachtoffers weer gebeld, maar bleef het aantal wat zelf contact opnam hoger dan voor 2019 (Inteltafel Cybercrime, 2023). De pop-up variant bleef beperkt.

Bij alle varianten beweren de oplichters de computerproblemen te kunnen oplossen tegen betaling. Vervolgens wordt op verschillende manieren bij het slachtoffer geld buitgemaakt. Zo wordt voor de geboden 'hulp' vaak een vergoeding verlangd of er moeten zogenaamd licenties aangekocht worden. De vergoeding die in rekening wordt gebracht, is doorgaans erg hoog of de betaling wordt gemanipuleerd zodat slachtoffers veel meer geld kwijt zijn dan waarmee zij akkoord zijn gegaan. Het slachtoffer heeft dit vaak niet door omdat de oplichters het scherm op zwart zetten of de informatie op het scherm manipuleren. Daarnaast wordt geld overgeboekt naar (buitenlandse) bankrekeningen, worden bitcoins gekocht die bij de dader terechtkomen of giftcards (zoals iTunes- of andere prepaidkaarten) aangeschaft die de dader verzilvert (Inteltafel Cybercrime, 2023; Borwell et al., 2020, project VAK 2022).

Hoe heeft de omvang zich ontwikkeld?

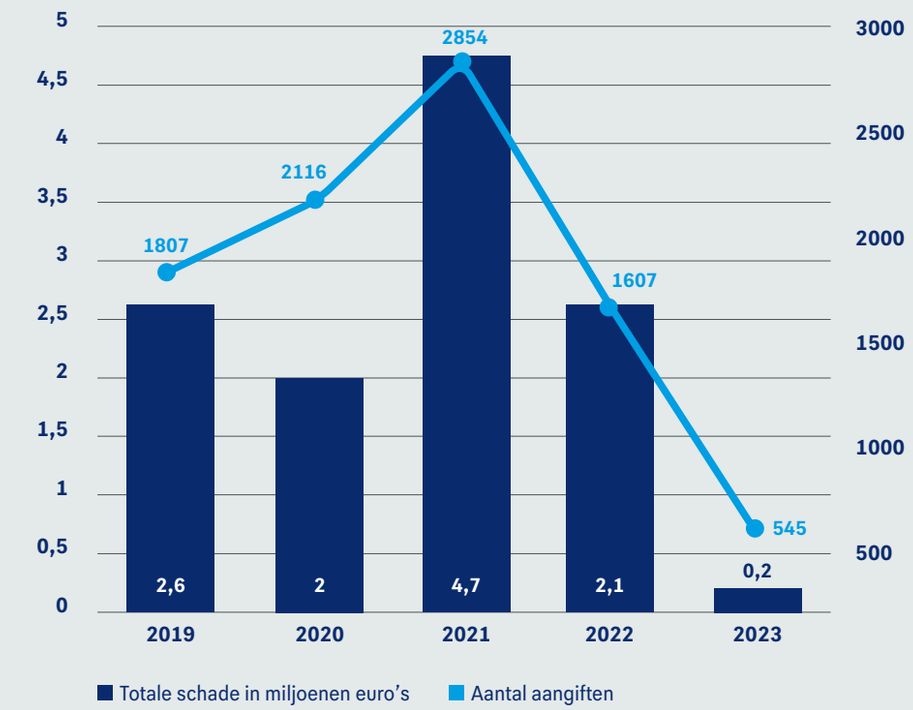
Cijfers over TSS zijn niet direct uit de politiesystemen te halen, daarom is gebruik gemaakt van BlueIntel en de Landelijke Cyber Query (LCQ). Binnen BlueIntel is tech support scam een aparte subcategorie waarin registraties die onder dit fenomeen vallen worden gescoord. De LCQ haalt niet alle registraties op, maar wel de meeste en geeft daarom een goed beeld van de ontwikkeling van de omvang. De gerapporteerde cijfers zijn dan ook een ondergrens van het aantal slachtoffers dat door dit fenomeen is gemaakt.

In figuur 5 is te zien dat er in 2019 ruim 1800 registraties binnenkwamen. In de jaren daarna neemt dit aantal flink toe met een piek in 2021, waarna een daling inzet. In 2023 is het aantal registraties het laagst van alle jaren in de onderzoeksperiode. Uit de politieregistraties blijkt verder dat bij bijna 75 procent van deze registraties financiële schade is geleden. In de eerste jaren bedroeg de geleden financiële schade enkele miljoenen euro's per jaar, met een duidelijke piek in 2021, maar daarna loopt die sterk terug naar twee ton in 2023. Na 2021 is ook het gemiddelde schadebedrag sterk teruggelopen. Dit is het gevolg van de succesvolle aanpak, die verderop in dit hoofdstuk wordt beschreven.

Externe bronnen

De omvang van TSS is moeilijk te vergelijken met de omvang uit andere bronnen vanwege verschillen in afbakening, rapportagecyclus en methode. In de Veiligheidsmonitor rapporteert het CBS tweejaarlijks over de omvang van verschillende (online) delicten, zoals voor verschillende vormen van phishing, waar alle telefonische helpdeskfraude onder valt, ook TSS (CBS, 2024; 2022). Het CBS schat de omvang van helpdeskfraude op basis van zelf gerapporteerde slachtoffers. Dan blijkt dat er in 2021 en 2023 rond de 7000 incidenten waren, veel meer dan er bij de politie binnenkwamen. Een groot deel hiervan wordt waarschijnlijk niet bij de politie gemeld omdat de financiële schade zelden wordt vergoed.

Figuur 5. Ontwikkeling aantal registraties en totale financiële schade TSS
Bron: BVH, BlueIntel



Volgens het CBS kregen slachtoffers van TSS in 20 tot 40 procent van de gevallen hun geld terug van de bank. Net als de Politie ziet ook het CBS een dalende trend in het aantal incidenten. Het is nog niet zeker of deze trend doorzet.

De Fraudehelpdesk (FHD) publiceert jaarlijks cijfers over allerlei vormen van fraude. Over een deel van deze vormen wordt niet elk jaar gerapporteerd, of er wordt niet ieder jaar consequent uitgesplitst naar verschillende verschijningsvormen. Hierdoor is een vergelijking met de politiecijfers niet mogelijk. Zo wordt in 2022 een toename van telefonische oplichting gerapporteerd, maar zijn er geen cijfers voor 2021 en 2023 (Fraudehelpdesk, 2022; 2023; 2024).

Wat zijn kenmerken van criminele groeperingen?

De oplichters achter de TSS lijken voornamelijk vanuit India te opereren en werken vrijwel altijd in georganiseerd verband (Miramirkhani et al., 2017). Dit is indirect ook gebleken uit andere bronnen. Door de afscherming die ze hanteren is dit niet helemaal met zekerheid te zeggen. Digitale en financiële sporen die werden onderzocht in een aantal Nederlandse politieonderzoeken, bleken naar India te leiden (Werkgroep TSS, 2021). Slachtoffers spraken vaak urenlang met verschillende oplichters, waarbij de niet-technische leden van het oplichtersteam verantwoordelijk waren voor het lokken en overtuigen van de slachtoffers. Dat doen ze door middel van social engineering. Zodra een potentieel slachtoffer overtuigd is, neemt een meer technisch onderlegde collega het gesprek over.

Om dit delict te plegen, moeten de oplichters meerdere voorbereidingen treffen en gebruik maken van verschillende kennis en diensten, zoals het beheren en maken van websites, Search Engine Optimization (SEO)[24], pop-ups en RAT's. Voor hun criminele werkzaamheden zetten ze een callcenter op en werven medewerkers hiervoor. Deze expertise of andere benodigdheden worden veelal (extern) ingewonnen. Tot slot moeten de oplichters weten hoe ze hun identiteit kunnen afschermen en de criminele opbrengst kunnen witwassen (project VAK, 2023; Borwell et al, 2020).

Wat zijn kenmerken van slachtoffers?

De slachtoffers van TSS zijn voornamelijk ouderen. Meer dan de helft van de slachtoffers is 60 jaar of ouder, zoals blijkt uit een verdiepende analyse over de periode 2016 tot en met 2020 (Werkgroep TSS, 2021; project VAK, 2023). Dit beeld wordt bevestigd door gegevens van slachtoffers die zich in 2023 bij de politie hebben gemeld. De meeste pogingen van telefonische helpdeskfraude zijn ongericht. De daders bellen niet op basis van leads, maar naar willekeurige telefoonnummers. Daarnaast worden de oplichters ook gebeld door burgers die bijvoorbeeld een pop up in beeld hebben gekregen (project VAK, 2022). Hierdoor lijkt de samenstelling van de slachtoffers meer toevallig tot stand te komen, bijvoorbeeld doordat zij een vaste telefoonlijn hebben, vaker problemen met de computer ervaren en eerder bereid zijn om hulp te aanvaarden bij het oplossen van computerproblemen.

Wat zijn verwachtingen in relatie tot de aanpak?

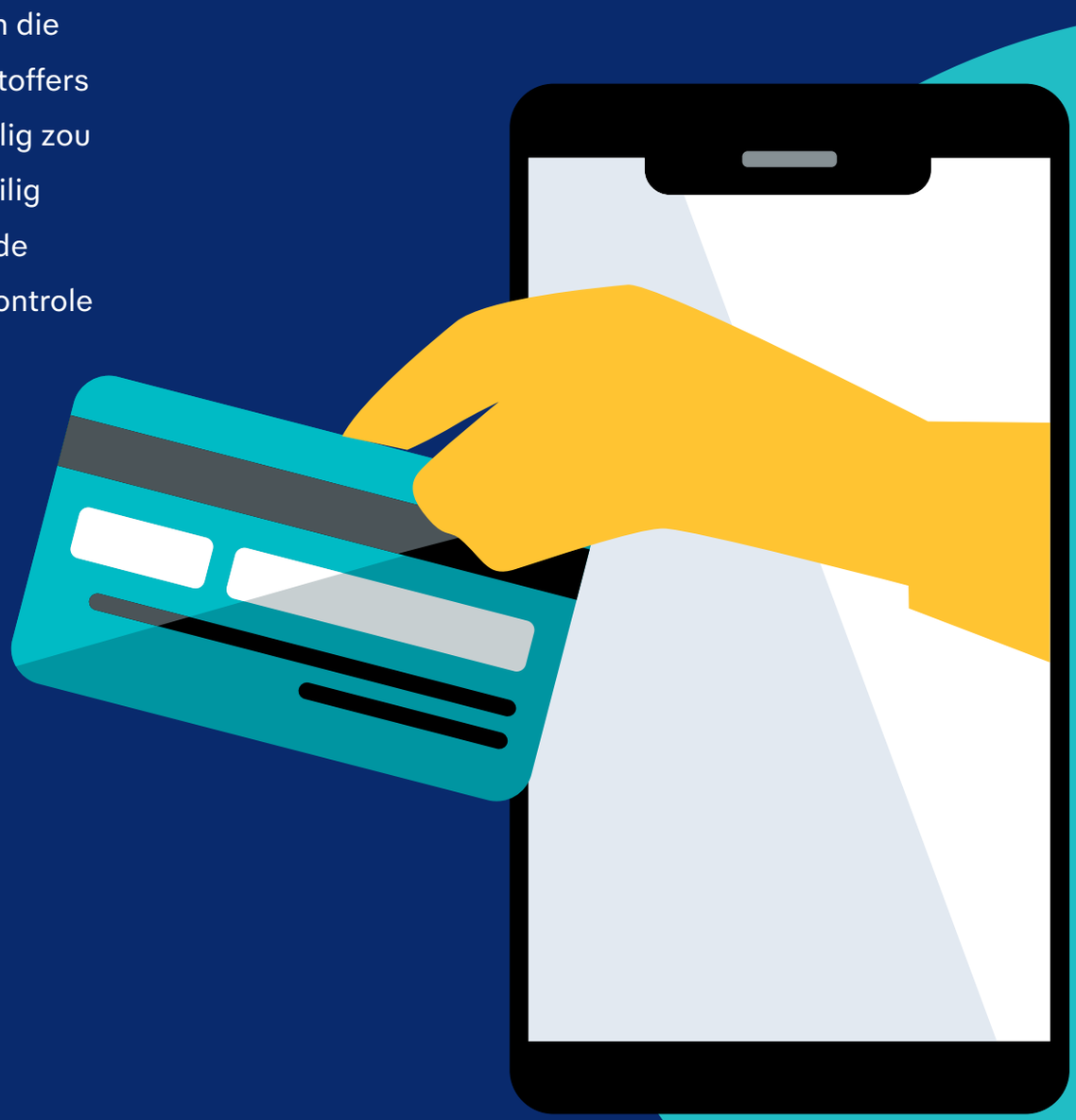
Tech support scam was tussen 2016 en 2018 de meest voorkomende vorm van online fraude bij de politie (Borwell et al., 2020). Dit leidde tot de oprichting in maart 2018 van de Brede Coalitie ter Verstoring van Tech Support Scams in Nederland. De coalitiepartners bestonden uit het ministerie van Justitie en Veiligheid, het Openbaar Ministerie, de politie, de Autoriteit Consument en Markt en private partijen op telecom-, software- en financieel gebied. Omdat de daders vooral vanuit India opereerden, was de opsporing moeilijk. Op basis van een barrièremodel richtte de coalitie zich vooral op preventie en verstoring van de criminele werkwijze, door bijvoorbeeld frauduleuze telefoonnummers en websites te blokkeren, misbruikte functionaliteiten van RAT's aan te passen, transacties te blokkeren en mediacampagnes te voeren. Deze maatregelen hadden aanvankelijk effect, maar criminelen pasten hun werkwijze aan om de beperkingen te omzeilen, bijvoorbeeld door het gebruik van andere RAT's of door mensen zelf contact te laten leggen (Borwell et al., 2020; project VAK, 2022; Eenheid Rotterdam, 2021). Het aantal aangiften nam na een daling in 2019 weer toe, maar de financiele schade bleef lager dan daarvoor. De impact van TSS is sinds 2021 flink teruggelopen en de coalitie is al enige tijd niet meer actief. Veel elementen van de aanpak op TSS worden nu

24 Bijlage 4, woordenlijst

breder toegepast in het Actieplan Integrale Aanpak Online Fraude, waarin een gezamenlijke (publiek-private) strijd wordt aangegaan om aan- en verkoopfraude, phishing met betaalgegevens, hulpvraagfraude, (bank)helpdeskfraude en identiteitsfraude in te dammen. Het is echter belangrijk om te blijven monitoren of criminelen een nieuwe modus operandi bedenken.

4.4 Bankhelpdeskfraude

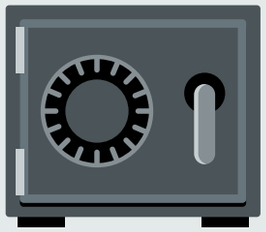
Bankhelpdeskfraude is een vorm van oplichting waarbij slachtoffers telefonisch worden benaderd door personen die zich voordoen als bankmedewerkers. Ze wijzen de slachtoffers erop dat het geld op hun bankrekening(en) niet meer veilig zou zijn en zetten hen vervolgens onder druk om hun geld veilig te stellen (al dan niet met hulp). In werkelijkheid maken de slachtoffers het geld over naar een rekening die onder controle staat van de oplichters.



Bankhelpdeskfraude in cijfers

7000

Van 1450 registraties in 2020 naar 7000 in 2023



Het (spaar)geld moet veilig worden gesteld op een zogenaamde

kluisrekening

In afgelopen jaren toename gebruik

Remote Access Tool

Nieuwe werkwijze

de oplichter haalt bankpas en sieraden op bij de slachtoffers

Zogenaamde bankmedewerker belt

want er is iets mis met de rekening

80%

van de slachtoffers is ouder dan 60 jaar

€ 7000

Gemiddeld schadebedrag gedaald van 14.000 naar 7000 euro per registratie

34 miljoen

Totale schade van 18 miljoen euro in 2020 naar 34 miljoen euro in 2023

In dit rapport worden twee varianten van telefonische helpdeskfraude beschreven. Bankhelpdeskfraude wordt in dit hoofdstuk beschreven en de tech support scam in het vorige. Telefonische helpdeskfraude omvat alle vormen van oplichting waarbij het slachtoffer via de telefoon wordt benaderd. De oplichter biedt tijdens het gesprek hulp of ondersteuning aan om zogenaamd vreemde of zorgelijke problemen op te lossen. De oplichter doet zich voor als medewerker van de helpdesk of fraudeafdeling van een bank, technologie – of softwarebedrijf of een andere organisatie. Meestal beweert de oplichter dat er verdachte activiteiten op de bankrekening van het slachtoffer zijn gesignaleerd of dat de computer van het slachtoffer besmet is met een virus. Bankhelpdeskfraude staat in de Veiligheidsagenda.

Hoe heeft het fenomeen zich ontwikkeld?

Bankhelpdeskfraude is een vorm van oplichting waarbij slachtoffers telefonisch worden benaderd door personen die zich voordoen als bankmedewerkers. Ze wijzen de slachtoffers erop dat het geld op hun bankrekening(en) niet meer veilig zou zijn en zetten hen vervolgens onder druk om hun geld veilig te stellen (al dan niet met hulp). In werkelijkheid maken de slachtoffers het geld over naar een rekening die onder controle staat van de oplichters. De eerste registraties van bankhelpdeskfraude kwamen rond 2019 sporadisch bij de politie binnen, maar halverwege 2020 ging het om dusdanig hoge aantallen dat het kon worden beschouwd als een veelvoorkomende fraudevorm. In de registraties zijn verschillende werkwijzen te onderscheiden:

1. Slachtoffer maakt zelf geld over naar andere rekening.
Slachtoffers worden gebeld en voorgespiegeld dat hun bankrekening is gehackt en dat criminelen toegang hebben tot de rekening, of dat er (al) frauduleuze transacties op de rekening zijn vastgesteld. Daarom moet het volledige rekeningsaldo worden overgeboekt naar een zogenaamde kluisrekening van de bank. Dat doen slachtoffers dan zelf en het geld wordt overgemaakt naar de daders, meestal op een rekening op naam van een katvanger.

2. Slachtoffer geeft toegang tot computersysteem met Remote Access Tools (of RAT).
De oplichter krijgt na toestemming van het slachtoffer op afstand de controle over diens computer met een RAT en verricht binnen de betaalomgeving verschillende handelingen, zoals het verhogen van de daglimieten, het overmaken van het saldo van de spaarrekening naar de betaalrekening en het klaarzetten van verschillende betaalopdrachten. Het slachtoffer ziet dit niet, omdat het beeldscherm op zwart is gezet.

3. Slachtoffer laat pinpas ophalen (en eventueel andere waardevolle spullen meenemen).
Tijdens het telefoongesprek stelt de oplichter voor om de pinpas ‘met spoed’ bij het slachtoffer thuis op te halen, omdat deze een nieuwe bankrekening en pinpas krijgt. Nog tijdens het gesprek verschijnt er een zogenaamde koerier of bankmedewerker aan de deur om de pas en soms ook de paslezer op te halen. Soms moet de pas nog worden doorgeknipt[25], moet de pincode worden opgeschreven en (beide) in een dichtgemaakte enveloppe worden gedaan of wordt er een code afgesproken waarmee de persoon die de spullen komt ophalen zich kan identificeren. Met de gestolen pinpas en pincode wordt zoveel mogelijk geld opgenomen bij geldautomaten in de omgeving of gepind in winkels. Naast de pinpas worden de slachtoffers vaak ook overgehaald om waardevolle spullen af te geven, zoals sieraden of horloges, en soms zelfs schilderijen.

Opsporingsonderzoek: Bankhelpdeskfraude met RAT’s en geld weggesluisd via cadeaukaarten

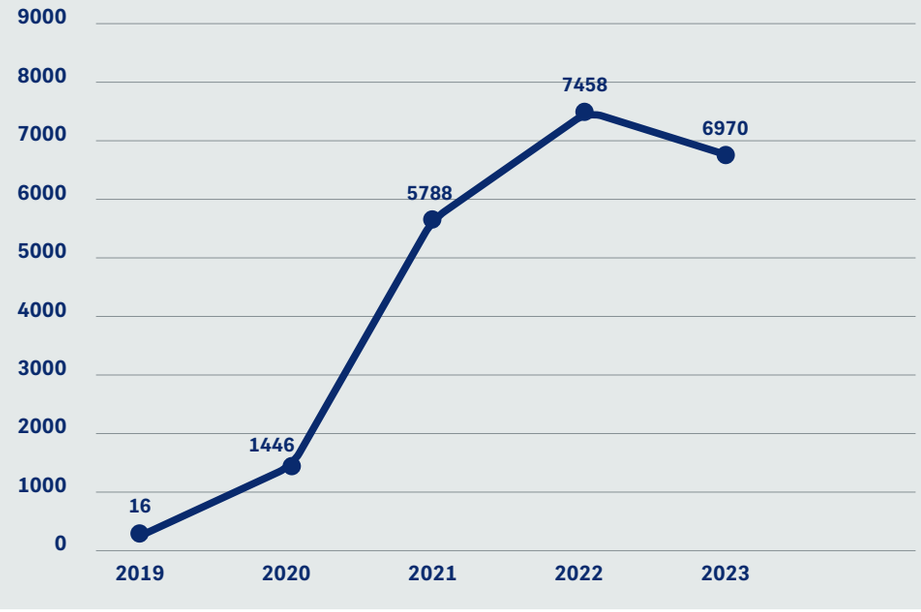
In deze voorbeeldcasus maakten de (hoofd)verdachten zich schuldig aan bankhelpdeskfraude. De fraudeurs belden slachtoffers anoniem met een afgeschermd nummer en deden zich voornamelijk voor als medewerkers van ING Bank of Rabobank. Ze beschikten vaak over verschillende gegevens van het slachtoffer, zoals naam, adres, telefoonnummer, e-mailadres en bankrekeningnummer. Hiermee konden ze vertrouwen wekken en het slachtoffer overtuigen van hun rol als bankmedewerker. De fraudeurs belden de slachtoffers op en vroegen hen of zij recent een grote transactie hadden gedaan. Wanneer het slachtoffer ontkende, beweerde de verdachte dat hun bankrekening gehackt was en dat ze hun geld moesten ‘veiligstellen’. In meerdere aangiftes verklaarden de slachtoffers dat ze door de zogenaamde helpdeskmedewerker vervolgens werden verzocht om een programma op hun computer, tablet of telefoon te installeren. Dit betrof vaak programma’s zoals Anydesk, TeamViewer of TeamViewer QuickSupport, waarmee de fraudeurs de besturing van een apparaat op afstand konden overnemen om illegale handelingen te verrichten.

In deze casus werd het overgemaakte geld niet naar andere betaalrekeningen (van katvangers) gestuurd, maar de groepering liet de slachtoffers cadeaukaarten kopen bij verschillende online webwinkels. Deze kaarten werden soms eerst nog omgewisseld voor andere cadeaukaarten, om daar uiteindelijk iPhones of luxegoederen van te kopen. Deze goederen werden bezorgd bij verschillende adressen in de omgeving van het woonadres van een van de verdachten. Een deel van deze goederen werden vervolgens ‘nieuw in doos’ doorverkocht aan derden. In de loop van het onderzoek veranderde de werkwijze van deze groepering, en kwam het voor dat slachtoffers hun bankpas moesten afgeven aan een zogenaamde bankmedewerker die deze bij hen thuis kwam ophalen.

Ondanks dat de groepering veelvuldig van telefoon en e-mailadres wisselde, kon de politie dankzij overeenkomsten in de aangiften van meerdere slachtoffers en de gebruikte telefoonnummers de verdachten uiteindelijk opsporen. Binnen het onderzoek zijn uiteindelijk 28 aangiften meegenomen, maar de groep was waarschijnlijk bij meer incidenten betrokken. In totaal werd €176.837,58 buitgemaakt. De twee hoofdverdachten in deze zaak zijn 19 en 21 jaar oud.

25 Het doorknippen van de pas krijgen de slachtoffers soms als instructie mee om ze ‘gerust te stellen’. Het doorknippen moet volgens de daders dan wel op een manier gebeuren dat de chip op de pas intact blijft en ze deze later nog kunnen gebruiken.

Figuur 6. Ontwikkeling aantal registraties BHF 2019 – 2023
Bron: BVH, BlueIntel



Hoe heeft de omvang zich ontwikkeld?

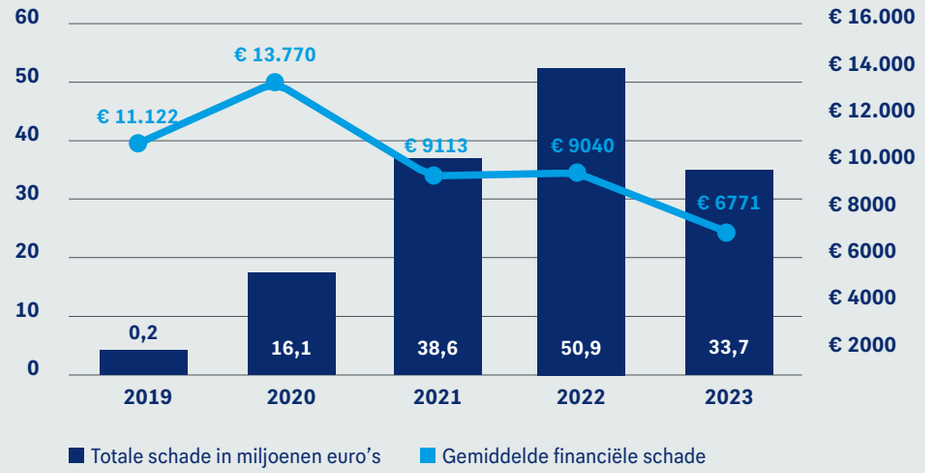
In 2019 waren er nog nauwelijks registraties, maar in 2020 zijn er gemiddeld meer dan 100 registraties per maand (1446 in totaal) en dit verviervoudigt in 2021 (5788).

Het aantal registraties is op zijn hoogst in 2022 (7458) en daarna treedt een lichte daling in, maar met gemiddeld 580 per maand zijn de aantallen nog steeds relatief hoog.

Ook de omvang van de financiële schade is vanaf 2019 opgelopen, zoals is te zien in figuur 7. Jaarlijks gaat het om enkele tientallen miljoenen euro's met in 2022 een piek van ruim 50 miljoen euro. In 2023 is voor het eerst een afname te zien.

Bij ongeveer driekwart van de registraties was er sprake van financiële schade. Dit ligt hoger dan bij veel andere online fraudevormen, vooral omdat banken het doen van aangifte stimuleren door dit als voorwaarde voor restitutie te stellen. In 2023 meldt 60 procent van de slachtoffers een schadebedrag tussen de duizend en tienduizend euro. Tien procent had een schadebedrag onder de 1000 euro en 15 procent meldde een schadebedrag boven de 10.000 euro. Bij 2 procent van de slachtoffers is meer dan 50.000 euro buitgemaakt. Het gemiddelde schadebedrag vertoont inmiddels een dalende trend. Waar het gemiddelde schadebedrag in 2020 nog bijna 14.000 euro bedroeg, is dit in 2023 bijna gehalveerd (afgerond 7000 euro).

Figuur 7. Ontwikkeling gemiddelde en totale financiële schade BHF 2019 - 2023
Bron: BVH, BlueIntel



Uit een intern onderzoek van de Eenheid Limburg blijkt dat de gemiddelde opbrengst twee keer zo hoog is wanneer een RAT wordt gebruikt. In 2019 was er alleen nog sprake van de variant BHF waarbij de slachtoffers zelf het geld overmaakten. Vanaf 2020 neemt het gebruik van RAT's snel toe en wordt dit de dominante werkwijze. In 2022 komt dit terug in ongeveer 67 procent van de registraties en meestal wordt hierbij Anydesk als RAT gebruikt. De variant waarbij de pas wordt opgehaald, is ook sterk gestegen en vertegenwoordigt bijna de helft van de registraties (van 19% in 2021 naar 46% in 2023). En bij 30 procent van de slachtoffers waar de pas wordt opgehaald, worden slachtoffers ook overgehaald om sieraden of contant geld af te staan (Inteltafel Cyber, 2023).

Externe bronnen

Sinds 2019 is bankhelpdeskfraude sterk toegenomen en vanaf 2020 rapporteren de banken hierover. De Nederlandse Vereniging van Banken meldt dat bankhelpdeskfraude vanaf 2020 de grootste schadepost was voor de banken. De schade steeg van ruim 26 miljoen euro in 2020 naar bijna 51 miljoen in 2022, waarna het terugliep tot 28 miljoen euro. De schade voor alle fraude bedroeg in 2022 totaal afgerond 61 miljoen euro.

De gevolgen van bankhelpdeskfraude zijn voornamelijk financieel van aard. Het is moeilijk om de schade precies te verdelen tussen burgers en bedrijven (banken). In de meeste gevallen vergoeden de vier grootbanken de schade aan hun klanten onder de coulanceregе-

ling (NVB, 2021)[26]. Desondanks is de schade voor burgers niet te verwaarlozen en loopt jaarlijks op tot tientallen miljoenen euro's. De banken meldden dat ongeveer 10 procent van de slachtoffers in 2021 en 2022 geen vergoeding kreeg onder de coulanceregeling. In 2023 is dit flink toegenomen naar één op de drie slachtoffers (NVB, 2022, 2023b, 2024). Volgens het CBS werd ongeveer zeven op de tien slachtoffers geheel of gedeeltelijk schadeloosgesteld (CBS, 2022, 22 september).

Het CBS schatte in 2021 de totale schade tussen de 50 en 100 miljoen euro. Dat is een stuk hoger dan de bedragen van de NVB, omdat deze zich beperkt tot alleen de schade van de grootbanken in Nederland, terwijl het CBS ook de schades van burgers meeneemt die niet in aanmerking kwamen voor restitutie van hun bank. De geschatte schade van bankhelpdeskfraude komt volgens het CBS uit een aantal recente rapporten. In eerste instantie uit het rapport De financiële schade van criminaliteit tegen burgers (2022), waarin dit voor het eerst werd onderzocht (voor het jaar 2021). Daarnaast geven de laatste twee Veiligheidsmonitoren (CBS, 2024; 2022) ook enig inzicht in de omvang en impact van bankhelpdeskfraude. In deze rapporten wordt bankhelpdeskfraude beschouwd als een subcategorie van phishing en wordt de term bankspoofing gebruikt, waarbij een oplichter zich voordoet als een medewerker van de bank. De beide Veiligheidsmonitoren laten een vergelijkbaar beeld zien en geven aan dat ongeveer twee op de drie Nederlanders van 15 jaar of ouder (68% om 65%) in de afgelopen 12 maanden te maken hebben gehad met phishing door een telefoontje, e-mail of ander bericht. Een klein percentage (2%) is hier wel eens ingetrapt en minder dan 1 procent is slachtoffer geworden en heeft geld verloren. In respectievelijk 15 en 18 procent van deze gevallen was sprake van bankspoofing (CBS, 2024; 2022). Deze percentages zijn omgerekend naar aantallen en dat betekent dat er in 2021 in totaal 18.000 slachtoffers waren. De helft van deze gedupeerden had ten minste 4000 euro schade geleden. Slachtoffers van bankspoofing doen vaak aangifte, omdat de bank dit stimuleert en in 82 procent van de gevallen is er aangifte gedaan, wat betrekking had op 85 procent van alle schade. De totale schade was 94 miljoen euro, waarvan 70 miljoen euro is vergoed door de financiële instelling en soms door de dader. De resterende 24 miljoen euro schade blijft bij de slachtoffers (CBS, 2022, 22 september).

De Fraudehelpdesk maakt gebruik van hoofdcategorieën om fraudezaken te rapporteren, waarbij verschillende fraudevormen worden onderscheiden, zoals voorschotfraude, acquisitiefraude, cybercrime en ID-fraude rechtspersonen, ook wel bekend als misbruik bedrijfsgegevens. Bankhelpdeskfraude wordt geregistreerd als 'gebeld door de bank' binnen de hoofdcategorie ID-fraude rechtspersonen. Ook de FHD ziet vanaf 2019 een flinke stijging in het aantal meldingen van bankhelpdeskfraude, met een tijdelijke piek van 1454 meldingen in 2021. De laatste drie jaren hebben een wat grilliger verloop, met eerst een lichte daling naar 1309 meldingen in 2022, om vervolgens in 2023 weer te stijgen naar 1547 meldingen De cijfers van de Fraudehelpdesk wijken echter flink af van de cijfers van andere bronnen, waarbij het totaal aantal meldingen lager ligt en er minder vaak financiële schade wordt gemeld. Dit kan komen doordat slachtoffers worden gestimuleerd om aangifte bij de politie te doen.

Wat zijn kenmerken van slachtoffers?

Tussen 2019 en 2023 hebben in totaal 15.950 slachtoffers[27] van bankhelpdeskfraude zich bij de politie gemeld. Het aantal mannelijke en vrouwelijke slachtoffers is ongeveer gelijk en de verschillen zijn minimaal, waarbij er iets meer vrouwen dan mannen zijn (50,9 om 48,9%). De leeftijdsverdeling is echter veel meer uitgesproken. Meer dan de helft (54%) van de slachtoffers is boven de 70 jaar oud en een kwart is tussen 60 en 69 jaar, waaruit blijkt dat de criminelen zich voornamelijk richten op oudere slachtoffers (zie ook: DRIO Eenheid Rotterdam, 2021; Akkermans et al., 2023).

Naast de financiële schade, die al dan niet door de banken wordt vergoed, heeft bankhelpdeskfraude ook andere gevolgen voor de slachtoffers. Deze gevolgen zijn vooral merkbaar in de impact en psychische klachten die slachtoffers en hun directe omgeving ondervinden na een dergelijk delict. De niet-financiële gevolgen voor de verschillende online fraudevormen komen grotendeels overeen en zijn in een apart hoofdstuk 6 Niet financiële gevolgen beschreven.

Wat zijn de verwachtingen in relatie tot de aanpak?

De toename van online fraude in de afgelopen jaren heeft geleid tot veel slachtoffers en schade in de samenleving. Daardoor is er meer prioriteit in de aanpak van deze fenomenen gekomen en komen ze gedeeltelijk terug als thema's in de laatste Veiligheidsagenda 2023-2026. Deze agenda is flexibel genoeg om nieuwe online fraudevormen toe te voegen[28]. Bankhelpdeskfraude is inmiddels een van de primaire aandachtspunten en komt prominent naar voren binnen de integrale aanpak online fraude en in verschillende beleids- of kamerstukken (noot. o.a. Kamerstuk 2020/21, kst-29911-314). De aanpak ervan vereist echter een bredere benadering dan gebruikelijk is voor de politie.

Om bankhelpdeskfraude te voorkomen, te verstoren, op te sporen en te vervolgen worden verschillende stappen gezet. Voorlichting is een belangrijk instrument om bewustzijn en weerbaarheid te creëren bij burgers en bedrijven, om zodoende slachtofferschap te voorkomen. Er is dan ook veel aandacht in de media geweest voor bankhelpdeskfraude.

Daarnaast is het frustreren en bemoeilijken van de werkwijze die oplichters hanteren een doel en hierbij spelen verschillende publieke en private partijen een rol. Zo hebben de ban-

26 Hiervoor gelden toetsingscriteria. Binnen deze criteria blijft het uitgangspunt dat klanten een eigen verantwoordelijkheid hebben. Slachtoffers krijgen echter 100 procent van de schade uit coulance vergoed, tenzij ze medeplichtig zijn aan fraude, al eerder een vergoeding hebben gehad bij dezelfde bank of als ze onvoldoende meewerken aan het fraudeonderzoek van de bank. Bij specifieke omstandigheden kan worden besloten om maar voor een deel, of niet, tot coulance over te gaan.

27 Uit een totaal van 14.725 registraties. Het aantal slachtoffers ligt hoger, omdat in een deel van de incidenten meer slachtoffers zijn en daarvan ook aangifte komen doen. Het gaat dan om een gezamenlijke rekening of het beheer van een rekening voor een familielid (kind of ouder).

28 Aanvankelijk richtte de Veiligheidsagenda zich primair op vier specifieke vormen van gedigitaliseerde criminaliteit, namelijk fraude met online handel, online fraude met betaalproducten, online voorschotfraude en online identiteitsfraude. Om op ontwikkelingen in te kunnen spelen, is hierbij wel een bepaalde flexibiliteit ingebouwd om nieuwe vormen van gedigitaliseerde criminaliteit toe te kunnen voegen of bepaalde vormen te vervangen.

ken de daglimiet standaard verlaagd en een tijdslot ingebouwd bij het verhogen van de daglimiet. Sinds april 2024 bestaat de optie ‘check je gesprek’ waarbij potentiële slachtoffers bij een van de grootbanken direct kunnen checken of ze echt door de bank worden gebeld (NVB, 2024). De vier grote banken hebben de maatregelen doorgevoerd, maar implementatie is niet verplicht en individuele banken maken daarbij altijd een eigen afweging tussen gebruikersvriendelijkheid en veiligheid. Verder is tussen de politie en de vier grootbanken afgesproken dat altijd 112 wordt gebeld bij een heterdaadsituatie.

Ook de telecomsector heeft maatregelen genomen om telefonische spoofing terug te dringen, waardoor oplichters niet meer met zogenaamde nummers van de bank kunnen bellen[29]. Het ministerie van Justitie en Veiligheid werkt aan het verantwoordelijk houden van sociale mediaplatforms voor frauduleuze content (zoals het verspreiden van leadslijsten en belscripts via telegram chatgroepen).[30]

Sinds de opkomst van bankhelpdeskfraude zijn er enkele tientallen (kleine en grote) opsporingsonderzoeken uitgevoerd. Er is flink geïnvesteerd in de opsporing van bankhelpdeskfraude, wat heeft geleid tot meer verdachten die in beeld komen dan bij andere vormen van online fraude. Van alle online fraudevormen worden zaken bankhelpdeskfraude vaker opgepakt. Slechts een beperkt deel van de afgeronde zaken wordt ingezonden naar het Openbaar Ministerie (Willekers et al., 2024). Om een beeld te krijgen van de opgelegde strafmaat is er op de website rechtbank.nl gezocht op de term ‘bankhelpdeskfraude’. Dit leverde in totaal 62 verschillende uitspraken op, waarin bankhelpdeskfraude centraal stond. De (jong)volwassen verdachten met een centrale rol in de uitvoering krijgen straffen opgelegd tussen de 1 en 5 jaar, waarbij 2 à 3 jaar celstraf het meest voorkomt. De strafmaat bij jeugdige verdachten of verdachten met een wat meer faciliterende rol ligt aanmerkelijk lager. Dit is beperkt tot enkele maanden tot een jaar (jeugd)detentie, vaak met aanvullend een proeftijd of werkstraf.

De aanpak van bankhelpdeskfraude is meer dan de som van de afzonderlijke delen en dit geldt ook voor andere vormen van online fraude. Naast opsporing en strafrechtelijke vervolging door politie en OM wordt steeds meer ingezet op alternatieve interventies met publieke en private partijen. Dit is al enige tijd gaande en deze integrale aanpak zal de komende jaren verder worden versterkt en hopelijk impact hebben op de ontwikkeling van bankhelpdeskfraude (zie hoofdstuk 7 Toekomstige ontwikkeling).

29 Zie: https://zoek.officielebekendmakingen.nl/kst-29911-314.html

30 Zie: https://integraleaanpakonlinefraude.nl/page/view/c70107f6-b61c-4838-bfff-6fc4f27d0c05/technische-barrieres-en-interventies

4.5 Bankhelpdeskfraude: verdachtenbeeld

In dit deel wordt een beeld geschetst van de verdachten die betrokken waren bij het plegen van bankhelpdeskfraude. Daarnaast is op basis van politieregistraties onderzocht of deze verdachten eerder al aan dit soort of andere delicten gekoppeld waren door middel van een antecedentenonderzoek. Het onderstaande beeld is gebaseerd op een lijst met verdachten van bankhelpdeskfraude, samengesteld uit twee verschillende bronnen.

Bankhelpdeskfraude: verdachtenbeeld in cijfers

1878

unieke verdachten van bankhelpdeskfraude (BHF)

Fraude

BHF gaat vaak samen met hulpvraagfraude en bankphishing

Traditionele delicten

BHF gaat vaak samen met heling, diefstallen en overvallen. In mindere mate ook met geweldsdelicten en drugs

Twee derde

van de verdachten is jonger dan 30 jaar en driekwart is man

Samenloop delicten

meestal verschillende fraudevormen naast elkaar, maar soms ook samen met traditionele delicten

13.000

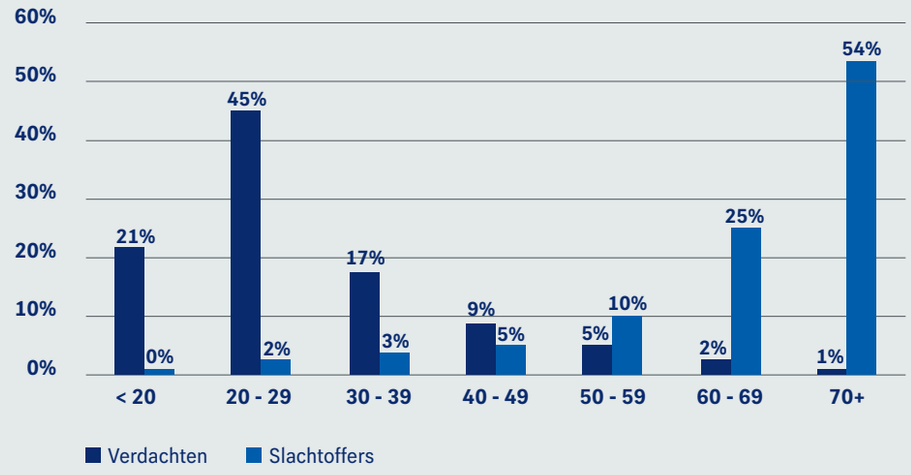
Ze hebben in totaal 13.000 antecedenten, gemiddeld 7 per persoon

De eerste lijst bestaat uit verdachten van bankhelpdeskfraude die gekoppeld zijn aan 14.254 BVH-registraties uit 2021 en 2022. De tweede lijst verdachten is opgesteld aan de hand van de 167 opsporingsonderzoeken die in de periode 2019 -2023 zijn uitgevoerd, waarin bankhelpdeskfraude centraal staat of een belangrijk deel van een onderzoek betreft. Op basis van informatie uit de dossiers en verslagen van deze opsporingsonderzoeken zijn de verdachten (en facilitators) die daarin naar voren kwamen toegevoegd aan de eerste lijst. Het samenvoegen van de twee bestanden leverde een lijst op met 1878 unieke verdachten. Verreweg het grootste deel van de verdachten (ruim 1500, ongeveer 80%) is gekoppeld aan registraties uit BVH. Daarnaast komen 250 verdachten alleen uit de opsporingsonderzoeken naar voren. De overige 120 verdachten (6%) komen in beide verdachtenlijsten terug.

Wat zijn kenmerken van verdachten?

Ruim driekwart van de verdachten is man (1458, 77%) en een vijfde vrouw (401, 21%).[31]
De verdachten zijn overwegend jong, waarbij bijna de helft tussen de 20 en 30 jaar oud is (45%). Samen met de groep jonger dan 20 (22%) is 67 procent van de verdachten jonger dan 30 jaar. Tussen de 30 en 39 jaar loopt het terug (249, 17%), maar naarmate de leeftijd hoger wordt, neemt het aandeel verdachten sterk af.

Figuur 8. Percentage verdachten en slachtoffers per leeftijdscategorie
Bron: BVH, BlueIntel



31 Bij de overige 2 procent is onbekend of het een vrouw of man betreft.

Eerder was er aandacht voor de leeftijdsverdeling van de slachtoffers. Wanneer deze wordt afgezet tegen de leeftijd van de verdachten, die overwegend jong en mannelijk zijn, dan blijkt dat ze zich richten op oudere slachtoffers. Ruim 80 procent van de verdachten is jonger dan 40 jaar, terwijl andersom bijna 80 procent van de slachtoffers ouder is dan 60 jaar (Figuur 8).

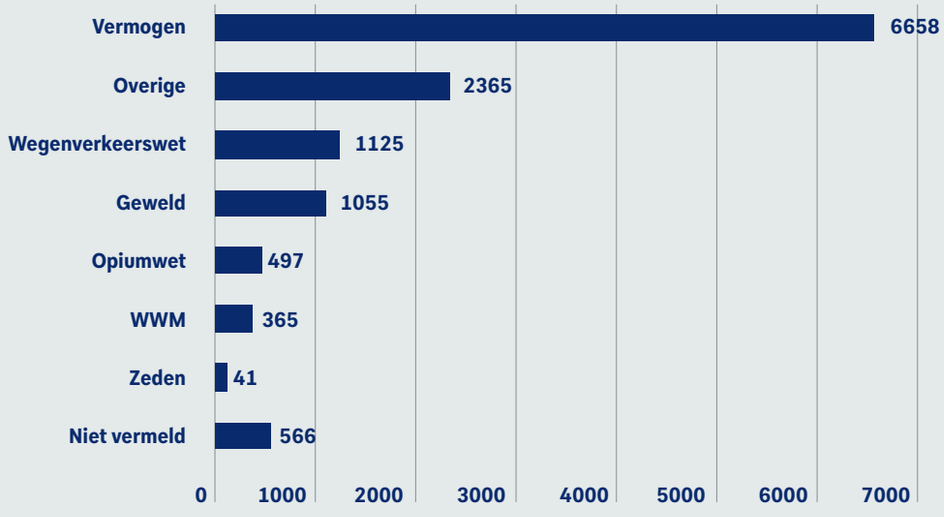
Wat zijn de antecedenten van verdachten?

Daarnaast is onderzocht in hoeverre verdachten betrokken waren bij andere wetsovertredingen. De 1878 personen op de verdachtenlijst leveren in eerste instantie een ruw bestand op met 22.265 politieantecedenten. Een deel hiervan betroffen geseponeerde overtredingen of delicten van voor 2012. Deze zijn niet meegenomen. In totaal blijven dan 12.672 politieantecedenten over en dat is gemiddeld 6,8 antecedenten per verdachte. Een deel van deze verdachten, 388 (bijna 21%), is betrokken bij meer dan 10 antecedenten en is te typeren als veelpleger. Zij zijn samen verantwoordelijk voor 8847 antecedenten, bijna 70 procent van het totaal.

Meer dan de helft van de antecedenten (6411) is van redelijk recente datum, namelijk van 2020 tot en met de helft van 2023. De leeftijd van de meeste verdachten ten tijde van de antecedenten was onder de 30 jaar (72%) met een piek tussen de 18 en 22 jaar (4000 verdachten, 32%).

Vervolgens is eerst onderzocht in welke hoofdcategorieën van de politiesystemen de antecedenten vielen (zie figuur 9). Daarna is gekeken naar de specifieke delicten die gepleegd waren en onder die hoofdcategorieën vielen.

Figuur 9. Antecedenten verdachten bankhelpdeskfraude verdeeld in hoofdcategorieën
Bron: BVH, BlueIntel



In figuur 9 is te zien dat de grootste groep antecedenten is gerelateerd aan de hoofdcategorie vermogen (6658). Een flink aantal antecedenten valt onder overige delicten (2365), de Wegenverkeerswet (1125) en geweld (1055). Ze worden veel minder vaak in verband gebracht met delicten of overtredingen die vallen onder de Opiumwet (497) of de Wet wapens en munitie (365). Tot slot hebben enkele tientallen registraties betrekking op zeden (41).

De antecedenten die onder de hoofdcategorie vermogen vallen, zijn:
- horizontale fraude (1281)
- fraude met betaalproducten (823)
- winkeldiefstal (965)
- heling (502)
- woningdiefstal (320)
- straatroof (195)
- overvallen (124)
- chantage of afpersing (95)

Onder overig vallen vooral antecedenten die betrekking hebben op:
- bedreigingen (475)
- vernielingen (426)
- beledigingen (248)
- computervredebreuk (201). Waarschijnlijk houden ze ook verband met (bank)helpdeskfraude en cybercrime
- huisvredebreuk (89)
- brandstichting (58)
- gijzeling of ontvoering (38)

Antecedenten die vallen onder de Wegen - en verkeerswet gaan over:
- rijden onder invloed van drugs of geneesmiddelen (311)
- of van alcohol (273)
- rijden met een ongeldig rijbewijs (188)
- rijden nadat het rijbewijs is ingevorderd (76)
- doorrijden na een verkeersongeval (102)

Geweld gaat over antecedenten van:
- eenvoudige mishandeling (565)
- openlijke geweldpleging tegen personen (222)
- zware mishandeling (115)
- moord en doodslag (101)

De Opiumwet heeft vooral te maken met:
- bezit van harddrugs (194)
- handel in harddrugs(104)
- bezit van softdrugs (87)
- vervaardigen van softdrugs (56)
- handel in softdrugs (47)

De hoofdcategorie Wet wapens en munitie (WWM) gaat over:
- bezit van vuurwapens (149)
- bezit van overige wapens (213)
- handel in vuurwapens (3)

Antecedenten over zeden komen weinig voor maar zijn wel ernstig:
- aanranding (16)
- verkrachting (14)

De bovenstaande analyse van de politieantecedenten geeft inzicht in de delicten waarbij (individuele) verdachten van bankhelpdeskfraude verder nog betrokken waren. Om te zien of dit terugkomt bij de criminele groepen uit de opsporingsonderzoeken, is aanvullend gekeken naar de samenloop van delicten. Dat is hierna kort uitgewerkt.

Bestaat een samenloop van delicten in opsporingsonderzoeken?

In de onderzoekperiode (2019 tot en met 2023) zijn in totaal 167 opsporingsonderzoeken uitgevoerd naar bankhelpdeskfraude. De samenloop van delicten wordt waarschijnlijk onderschat, omdat de informatie beperkt is tot het hoofddelict en bankhelpdeskfraude niet altijd het hoofddelict is. In een specifiek onderzoek naar drugshandel werd bijvoorbeeld ontdekt dat de verdachte ook betrokken was bij bankhelpdeskfraude op basis van informatie gevonden op in beslag genomen laptops en telefoons. Bijna een kwart van de opsporingsonderzoeken (42) bleek te gaan om meer criminele activiteiten dan alleen bankhelpdeskfraude. Van deze 42 gevallen bleek ruim de helft (26) ook actief te zijn in één of meer andere vormen van online fraude, zoals hulpvraagfraude, smishing en betaalverzoekfraude.

In dertien verschillende onderzoeken komen delicten naar voren die direct of indirect gerelateerd zijn aan bankhelpdeskfraude. In drie onderzoeken komen diefstal en heling naar voren. Het gaat dan om spullen die worden buitgemaakt en doorverkocht bij de pas-ophaalvariant, zoals pinpassen, identiteitsbewijzen, sieraden of andere waardevolle spullen. Daarnaast zijn er onderzoeken waarin de handel in *leads* (2) of phishingpanels[32] (2) naar voren komen. In deze onderzoeken zijn de verdachten dus ook betrokken bij bankhelpdeskfraude. Dit zijn ofwel afnemers die nauwe relaties onderhouden met deze groepering ofwel leden van de groep die zelf ook bankhelpdeskfraude plegen. In een drietal opsporingsonderzoeken naar witwassen is ook een relatie met bankhelpdeskfraude gevonden. Het gaat dan om groeperingen die criminele opbrengsten van bankhelpdeskfraude helpen weg te sluizen door geldezels te ronselen en ze via hun bankrekeningen cryptovaluta aan te laten kopen (zie bijlage 3. Witwassen van criminele opbrengsten).

In negen verschillende opsporingsonderzoeken is een minder directe relatie met bankhelpdeskfraude. In vijf opsporingsonderzoeken kwam een relatie tussen drugs en bankhelpdeskfraude naar voren. In deze onderzoeken waren drugs telkens de aanleiding om het onderzoek op te starten. Het ging daarbij specifiek om drugshandel (2x), de aanhouding van uithalers

32 Bijlage 4, woordenlijst

Verdachtenbeeld

Op basis van 167 opsporingsonderzoeken en 14.254 BVH registraties zijn in totaal 1.878 unieke verdachten geïdentificeerd die betrokken zijn geweest bij het plegen van bankhelpdeskfraude.

van drugscontainers (2x) en een drugsdumping (1x). Bij enkele verdachten was sprake van bankhelpdeskfraude wat naar voren kwam op basis van informatie uit de in beslag genomen telefoons. Ook bij drie opsporingsonderzoeken naar vuurwapens en geweld, waren deze delicten telkens de aanleiding en werd de relatie met bankhelpdeskfraude pas gelegd toen de gegevensdragers in beslag waren genomen. De verdachten waren betrokken bij een schietincident (2x) of de verkoop van vuurwapens en gedurende het onderzoek werd een deel van deze verdachten ook in verband gebracht met het plegen van bankhelpdeskfraude. Tot slot komt in een onderzoek naar mensenhandel een verdachte naar voren die handelt in minderjarige meisjes en ook voorkomt in een onderzoek naar bankhelpdeskfraude.

Samengevat beperken de criminele samenwerkingsverbanden die in beeld komen zich niet tot één specifieke vorm van criminaliteit of fraude. In plaats daarvan tonen zij een brede bereidheid om zich in te laten met diverse criminele activiteiten. Dergelijke groepen plegen afwisselend zowel online als meer traditionele criminaliteit, al dan niet in een verschillende samenstelling. Veel criminelen handelen daarbij vooral opportunistisch en richten zich op de delictsvormen die op dat moment het meest lucratief zijn (Bekkers et al., 2024, Leukfeldt & Holt, 2022)[33].

33 Dit wordt in de literatuur ook wel ‘cafeteria style offending’ genoemd. Dit betreft personen, eerder betrokken bij offline criminaliteit, die gebruikmaken van gelegenheden en criminele kansen om online criminaliteit te plegen, zoals phishing en malware (Leukfeldt & Holt, 2022).

4.6 Hulpvraagfraude

Hulpvraagfraude is een vorm van oplichting waarbij uit naam van een bekende gevraagd wordt snel een betaling te doen. De slachtoffers worden in veruit de meeste gevallen benaderd via WhatsApp. Aan de hand van verschillende overtuigingstechnieken proberen criminelen vervolgens het slachtoffer te overtuigen dat een vriend, zoon of dochter een betaling moet uitvoeren, maar hier zelf niet toe in staat is (vaak met een tragisch verhaal). Het overgemaakte geld komt terecht bij de fraudeur, al dan niet via een katvanger.

Hulpvraagfraude in cijfers

Totale schade in 2023 ruim

€ 1 miljoen

Gebruik van leads

adressen van oude en kwetsbare mensen

Hoi Pap, ben je druk. Mijn telefoon is gevallen.

Ik krijg nu een leentoestel. Kan je me een bericht sturen naar mijn leentoestel? Dit is het nummer (...)

Mijn zoon, althans ik verkeerde in de veronderstelling dat het mijn zoon was, vraagt om een bedrag van 1870 euro over te maken.

Hij belooft het geleende bedrag de volgende dag terug te storten.

Natuurlijk heel dom van mij dat ik in deze valstrik ben getrapt, maar ik wilde hem heel graag ter wille zijn. Hierdoor was ik minder kritisch

Vraag

met spoed om financiële hulp

€ 750

Gemiddeld schade per persoon teruggelopen van 3.200 euro in 2020 naar 750 in 2022

6000

Van 7300 registraties in 2020 naar 6000 in 2023

Hulpvraagfraude valt de beschouwen als de klassieke babbeltruc, maar in een nieuw digitaal jasje (project VAK, 2023). Hulpvraagfraude is in de Veiligheidsagenda opgenomen als voorschotfraude[34].

Hoe heeft het fenomeen zich ontwikkeld?

In 2019 kwam dit fenomeen op onder de naam *whaling*, maar deze naam veranderde al snel in vriend-in-noodfraude en is recentelijk gewijzigd naar hulpvraagfraude, op verzoek van private partijen die deze term al als zodanig hanteerden. In 2019 was *whaling* de vierde meest voorkomende fraudevorm na phishing, account take over (ATO) en helpdeskfraude (voormalig Microsoftfraude). Deze vier online fraudevormen en de aantallen registraties die daarvan bij de politie binnenkwamen, hebben in 2019 geleid tot een flinke stijging in horizontale fraude.

Als slachtoffers een bericht krijgen van een bekende, meestal een kind of ouder, hebben ze vaak niet door dat zij met een oplichter te maken hebben en zijn dan ook bereid om hun 'kinderen' uit de brand te helpen. Ze worden door de cybercriminelen onder druk gezet, er moet altijd snel betaald worden. Daarmee voorkomen ze dat de slachtoffers op een andere manier contact maken met de echte kinderen of bekenden. Urgentie wordt vaker gezien in verschillende fenomenen waar *social engineering* een grote rol speelt. Soms zijn de opgegeven redenen vaag maar plausibel, zoals het moeten kopen van een nieuwe telefoon na waterschade, een vergeten rekening of betrokkenheid bij een verkeersongeval. Dit is terug te zien in de aangiften.

De Eenheid Oost-Nederland heeft in 2020- 2021 hulpvraagfraude als thema geadopteerd en schreef toen een Book of Crime (2021), dat in 2023 verder is gespecificeerd door project VAK (2023). Hierin is een uitgebreid crime script opgenomen over alle stappen die gezet worden om tot de oplichting te komen. Omdat er momenteel geen aanpak bestaat, is in dit fenomeenbeeld alleen de wijze waarop de oplichter in contact komt met het slachtoffer beschreven (veel van de stappen lijken op de die bij andere vormen van fraude en deze zijn opgenomen in hoofdstuk 5 Overeenkomsten in werkwijzen. Daders gebruiken twee technische opties om contact te leggen met slachtoffers, ofwel de oplichter neemt een bestaand account over, of hij maakt een nieuw account aan om zich voor te doen als een vriend, familielid of andere bekende.

Er zijn drie manieren om accounts over te nemen. De eerste is het gebruik van een WhatsApp-hacking platform: op Telegram verkopen ontwikkelaars van phishing-pagina's software en instructies om WhatsApp te hacken. De software stelt de oplichter in staat een bericht te sturen naar een willekeurig ander WhatsApp account met de boodschap 'join private chat [oplichter kan een naam van dit gesprek bedenken]'. De link die bij dit bericht hoort lokt het slachtoffer naar een website die lijkt op de echte omgeving van WhatsApp waarop een QR-code is te zien. Als de gebruiker vervolgens de instructies op die website volgt, stelt hij of zij de hacker in staat het account over te nemen. De hacker krijgt op die manier toegang tot WhatsApp Web, een desktop kopie van het volledige account met inhoud. Zodoende kan de oplichter aanhaken op bestaande conversaties met slachtoffers, waardoor gesprekken en verzoeken nog echter lijken. Een andere methode is een vorm van phishing: de hacker reageert in eerste instantie als geïnteresseerde koper op een Marktplaatsadvertentie of als kandidaat op een dating site. Het gesprek om tot koop over te gaan of om samen af te spreken wordt vervolgens voortgezet via WhatsApp. Daarna krijgt de verkoper het verzoek om de 'code wordt ontvangen' door te geven aan de oplichter. Het verhaal hierbij is meestal dat het per ongeluk naar het nummer van het slachtoffer zou zijn verstuurd. Als de code wordt gedeeld, heeft de oplichter toegang tot het account van de verkoper/dater en krijgt daarmee ook tot zijn gegevens. De derde methode is een voicemail hack. Hierbij maken oplichters wederom misbruik van de mogelijkheden die WhatsApp biedt om toegang te krijgen tot het eigen account. Wanneer iemand opnieuw wil inloggen op zijn WhatsApp-account ontvangt deze in eerste instantie een beveiligingscode via sms. Na een aantal keren die beveiligingscode aan te hebben gevraagd, geeft Whatsapp de mogelijkheid om gebeld te worden om de code te horen of wanneer iemand niet opneemt deze in te spreken op de voicemail. Aangezien voicemails vaak niet of slecht beveiligd zijn, kunnen de oplichters deze beveiligingscodes in veel gevallen afluisteren met een standaard pincode.
Er zijn twee manieren om een nieuw account aan te maken. De eerste manier is het benaderen van een grote groep willekeurige telefoonnummers met een standaard bericht, in de hoop dat een potentieel slachtoffer reageert en overtuigd kan worden. De andere, meer voorkomende en lucratievere methode, is dat de oplichter informatie zoekt om het potentiele slachtoffer te overtuigen dat hij is wie hij zegt dat hij is, namelijk een bekende. Sommige slachtoffers geven aan dat namen (van slachtoffer en geïmiteerde bekende), relatie (tussen die twee) en foto (van de geïmiteerde bekende) in sommige gevallen bekend waren. Cybercriminelen zoeken vooral sociale media af op zoek naar persoonlijke informatie zoals foto's, hobby's en uitspraken, om de boodschap zo echt mogelijk over te laten komen.

Onder de slachtoffers is de leeftijdsgroep van 50 tot 70 jaar oververtegenwoordigd in de politieregistraties. Mogelijk worden zij als doelwit gekozen vanwege bepaalde eigenschappen die mensen in deze leeftijdsgroepen vaak hebben, zoals uitwonende kinderen, enig vermogen, en regelmatig gebruik van berichtenapps zoals WhatsApp. Oplichters die zich op hen richten, hebben naast de eerdergenoemde informatie ook kennis van de leeftijd van het potentiële slachtoffer nodig. Alle informatie wordt op grofweg twee manieren verzameld: kopen of zelf verzamelen.

34 Het OM definieert voorschotfraude onjuist: voorschotfraude omvat namelijk allerlei vormen van oplichting waarbij het slachtoffer onder valse voorwendselen wordt verzocht voorschotten te betalen, met een veel grotere beloning in het vooruitzicht (Bloem, B.A., A. Harteveld & M. de Heus (2017). Deelrapport Horizontale fraude. Nationaal dreigingsbeeld 2017. Politie Intern).

Opsporingsonderzoek: Hulpvraagfraude en bankhelpdeskfraude en verschillende rollen in de groepering

Er zijn vier mannelijke verdachten, en in eerste instantie 74 aangiften van hulpvraagfraude (ViN in het onderzoek). Eén verdachte verbleef in België en er was sprake van Duitse bankrekeningnummers.

Na analyse is het vermoeden dat ieder een taak had:
- Een persoon stuurt zogeheten 'leads' van vaak kwetsbare of oude mensen.
- Een persoon stuurt berichten naar deze mensen met een strekking als "mam, dit is mijn nieuwe telefoon, verwijder mijn oude nummer, ik heb hulp nodig met een factuur".
- Een persoon regelt bankpassen en/of inloggegevens van internetbankieren van geldezels.
- Een persoon geeft opdrachten tot het maken van betaalverzoeken.
- Een persoon maakt betaalverzoeken en stuurt deze vervolgens naar de 'typer'.
- Een persoon pint het van fraude afkomstige geld.

Man 1: ronselen geldezels, ophalen passen, sturen leads en betaalverzoeken (in telefoon afbeeldingen van tweeduizend bankpassen gevonden en gesprekken met slachtoffers)
Man 2: ronselen geldezels, ophalen passen, sturen leads en betaalverzoeken en gesprekken met slachtoffers
Man 3: gesprekken voeren met slachtoffers. Er zijn afbeeldingen van bankpassen op telefoon gevonden
Man 4: gesprekken voeren met slachtoffers, leads sturen, ophalen bankpassen en pinnen van geld

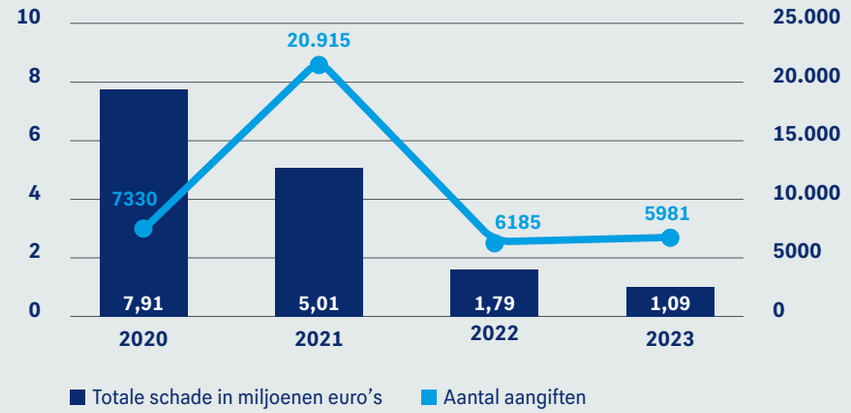
Over de wijze waarop het frauduleus verkregen geld wordt witgewassen, wordt geen melding gedaan. Ook niet of de verdachten meerdere antecedenten hadden. Ze werden aangeklaagd voor computervredebreuk vanwege het in bezit hebben en verspreiden van wachtwoorden en toegangscodes, hacken, oplichting, witwassen en deelname aan een criminele organisatie.

Hoe heeft de omvang zich ontwikkeld?

In 2020 liep hulpvraagfraude op, om in 2021 met enkele tienduizenden meldingen en aangiften sterk toe te nemen, zoals te zien in figuur 10.

Sinds het voorjaar van 2020 is het mogelijk om aangifte via internet te doen, wat de hoge aantallen kan verklaren. Na 2021 liep het aantal aangiften sterk terug en in 2023 leek het te stabiliseren. Ook de gemiddelde schade per registratie liep sterk terug, van ruim 3200 euro in 2020 naar 750 euro in 2022. De gemiddelde schade per registratie is voor 2023 niet bekend.

Figuur 10. Ontwikkeling aantal registraties en totale financiële schade hulpvraagfraude
Bron: BVH, BlueIntel



Verklaringen voor deze sterke daling ontbreken, hoewel gesuggereerd wordt dat een verplaatsing naar bankhelpdeskfraude heeft plaatsgevonden. Dit is moeilijk aan te tonen, omdat fenomenen, trends en werkwijzen voortdurend verschuiven.

Externe bronnen

Het CBS heeft in 2021 voor het eerst onderzoek gedaan naar de financiële schade van allerlei delicten (CBS, 2022). In het rapport gaat het over spoofing: criminelen nemen een andere identiteit aan om het slachtoffer geld over te laten maken. De meeste van deze delicten gaan over fraude in het betalingsverkeer en in 2021 gaven 10 miljoen mensen aan wel eens benaderd te zijn door een oplichter. In totaal gingen 97.000 mensen mee in het verhaal van de oplichter en werden 26.000 personen specifiek slachtoffer van hulpvraagfraude. De helft van hen betaalde minstens 2000 euro aan zogenaamde vrienden of familieleden. De totale schade door dit delict was 73 miljoen euro. Hiervan werd 25 miljoen euro vergoed door de banken.

De Fraudehelpdesk stelt dat bankhelpdeskfraude en hulpvraagfraude vooral opkwamen in 2020 waardoor beide vormen destijds ook veel aandacht kregen in de media. De schade voor beide vormen bedroeg in 2020 4 miljoen euro. Hulpvraagfraude daalde sterk, van ruim 12.000 meldingen in 2020 naar 3500 meldingen in 2022, maar steeg weer in 2023 naar ruim 8700 meldingen. De totale schade bedroeg bijna 200.000 euro en de 197 gedupeerden betaalden gemiddeld 2700 euro. Bankhelpdeskfraude steeg daarentegen fors zoals verder wordt beschreven in hoofdstuk 4.4.

De Universiteit Twente schetst een soortgelijk beeld. Van de 3000 respondenten gaven er 446 aan slachtoffer te zijn geweest van fraude. Specifieke vervolgvragen die aan hen werden gesteld, wezen uit dat aankoopfraude het vaakst voorkwam, gevolgd door hulpvraagfraude

en spoofing. Hoewel de aantallen klein zijn, komen de verhoudingen overeen met de cijfers van de politie, ook wat betreft de schadebedragen. Buiten beleggingsfraude, zijn de schadebedragen van hulpvraagfraude gemiddeld hoger dan van de andere fraudevormen die zijn onderzocht (Junger et al., 2022).

Wat zijn de verwachtingen in relatie tot de aanpak?

De Eenheid Oost-Nederland ontwikkelde een aanpak om geldezels aan te pakken, zaken te draaien en automatisch gegevens te vorderen (na clustering van aangiften), maar deze moest vrijwel direct worden gestopt na januari 2021 vanwege juridische struikelblokken en is sindsdien niet meer opgepakt. Hulpvraagfraude blijft zich echter ontwikkelen en nieuwe succesvolle werkwijzen die het aantal registraties de komende jaren doen toenemen, kunnen de vraag om een aanpak doen versterken. Bijvoorbeeld bij het toenemen van casussen waarbij deep fake-technologie wordt ingezet om stemmen na te bootsen. De hulpvraagfraude verloopt in een dergelijke casus volgens de beschreven werkwijze, waarbij een kind contact opneemt en een urgent probleem heeft waarvoor direct betaald moet worden. In een specifiek geval werd een moeder schijnaar gebeld door haar zoon. De stem van de zoon bleek echter met kunstmatige intelligentie te zijn gekloond. Navraag bij een eenheid leert dat er nog maar weinig aangiften van dit soort gevallen zijn en de tijd zal uitwijzen of dergelijk misbruik zal toenemen. Ontwikkelingen op het gebied van generatieve AI worden beschreven in hoofdstuk 7 Toekomstige ontwikkelingen.

4.7 Misbruik seksueel beeldmateriaal: sextortion

Sextortion is een vorm van online bedreiging, intimidatie en afpersing dat vanaf 2018 toeneemt (CBS, 2022). Sextortion is een samenvoeging van de Engelse woorden ‘sex’ en ‘extortion’ en het houdt in dat seksueel getint (beeld)materiaal als chantagemiddel wordt gebruikt.

Misbruik seksueel beeldmateriaal: sextortion in cijfers

1500

Van 560 registraties in 2020
naar 1500 in 2023

Emotionele
impact is
GROOT

Doel

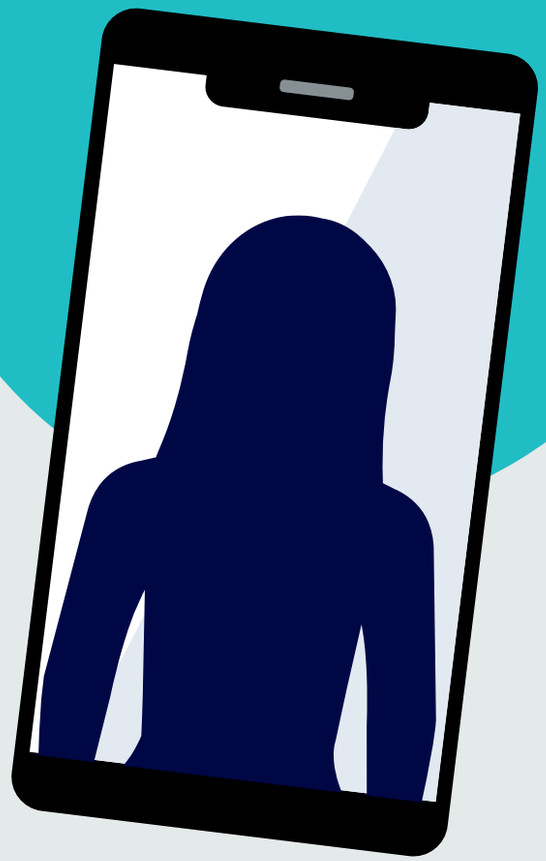
meer foto's, geld,
handelingen
of wraak (relationeel)

75%

hoogte gemiddeld
schadebedrag wisselt
sterk, bij 75% registraties
geen schadebedrag

Totale schade per jaar
€ 500.000

Seksueel getint
beeldmateriaal als
chantagemiddel



In 2019 pakte de Eenheid Amsterdam van de politie dit thema op vanwege de grote impact op kwetsbare en minderjarige slachtoffers en een te geringe aandacht die er op dat moment voor het fenomeen was. Sextortion is niet in de Veiligheidsagenda opgenomen en ook geen geprioriteerd thema van Centurion.

Hoe heeft het fenomeen zich ontwikkeld?

De Eenheid Amsterdam definieert 'sextortion als een vorm van misbruik van seksueel getint (beeld)materiaal, waarbij de redelijke vrees is ontstaan dat het (beeld)materiaal daadwerkelijk is verkregen door een ander en wordt gedreigd met de verspreiding en/of openbaarmaking van dit seksueel getinte (beeld)materiaal om iemand te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen (Eenheid Amsterdam, 2021).

Onderscheid is gemaakt tussen drie varianten:

1. Financiële sextortion.
Bij deze variant moet een slachtoffer één of meerdere financiële transacties doen om verspreiding en/of openbaarmaking van seksueel getint (beeld)materiaal te voorkomen.

2. Sextortion met een seksueel motief.
Hierbij moet een slachtoffer bijvoorbeeld een of meerdere seksuele handelingen verrichten bij de dader en/of moet een slachtoffer meer seksueel getint (beeld)materiaal leveren.

3. Overige sextortion.
In dit geval ligt het motief vaak in de persoonlijke sfeer. Zo kan bijvoorbeeld een ex-partner uit jaloezie dreigen om seksueel getint (beeld)materiaal openbaar te maken om het slachtoffer angst te bezorgen. Wanneer het buiten de persoonlijke/relationele sfeer plaatsvindt, is het vaak gericht op het verkrijgen van een dienst. Een slachtoffer wordt bijvoorbeeld gedwongen om een bankpas en pincode af te geven en op te treden als katvanger om wederrechtelijk verkregen geld door te boeken of te (laten) cashen. Soms wordt om een niet-criminele dienst gevraagd, bijvoorbeeld het ondertekenen van een zakelijk contract.

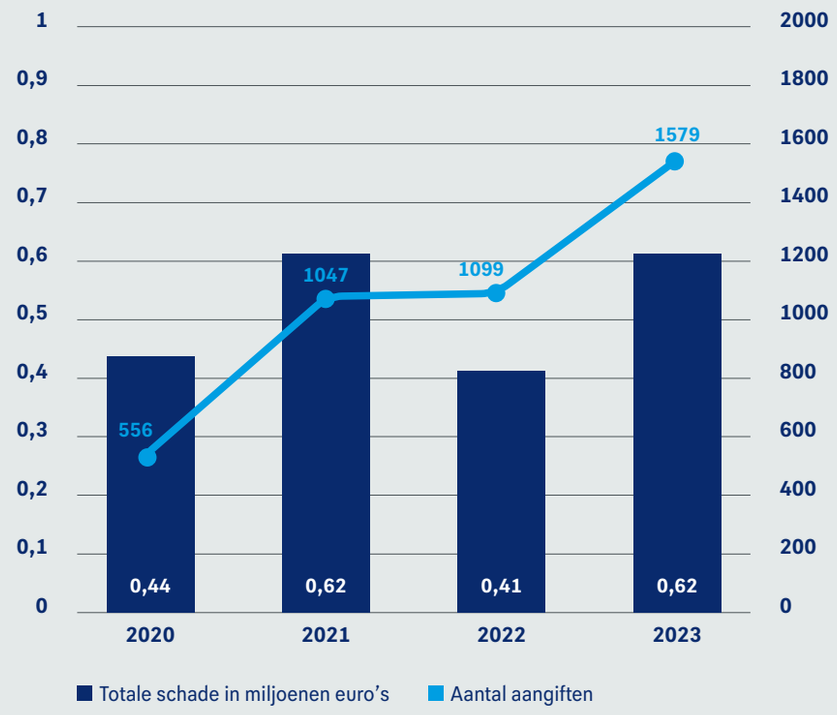
Sinds maart 2023 bestaat in de politiesystemen een nieuwe maatschappelijke klasse Misbruik seksueel beeldmateriaal (F5295), waarin alle registraties van misbruik van beeldmateriaal worden opgenomen. Daar vallen ook sextortion, sexting en exposen[35] onder. Wanneer in dit fenomeenbeeld de term Misbruik seksueel beeldmateriaal wordt gebruikt, gaat het over het brede misbruik zoals hiervoor omschreven, anders wordt de term sextortion gehanteerd.

Hoe heeft de omvang zich ontwikkeld?

Voor het vaststellen van de aantallen en financiële schade van sextortion zijn twee bronnen beschikbaar. Door de politie-eenheden zijn de registraties rechtstreeks in de excel-database BlueIntel vastgelegd over een periode van ruim drie jaar, waardoor iets te zeggen valt over de trend (zie figuur 11). Daarnaast zijn er cijfers uit het Cyberintelligencejaarbeeld 2022 van de Inteltafel Cyber (2023), gebaseerd op gescoorde registraties uit BlueIntel, die daarna zijn gecontroleerd op inhoud, zodat zeker is dat ze sextortion betreffen. Deze registraties vormen het uitgangspunt voor de beschrijving van de financiële schade in de alinea hierna.

Vanaf 2020 is een flinke stijging zichtbaar in het aantal sextortion registraties. Deze zijn in 2023 bijna verdriedubbeld ten opzichte van 2020[36]. Het Cyberintelligencejaarbeeld (Inteltafel Cyber, 2023) spreekt van een verviervoudiging van het aantal registraties in de coronajaren, maar noemt hierbij geen aantallen. In dit jaarbeeld werd de verwachting uitgesproken dat het aantal registraties na die enorme stijging weer zou afnemen in 2022, maar dat was niet het geval. Het aantal gecontroleerde registraties uit 2022 in het jaarbeeld lag op 1259[37], hetgeen iets hoger is dan de scores in BlueIntel zoals opgesomd in figuur 11.

Figuur 11. Ontwikkeling aantal registraties en totale financiële schade sextortion
Bron: BVH, BlueIntel



35 Bijlage 4, woordenlijst.

36 Op de gescoorde registraties vindt geen kwaliteitscontrole plaats, waardoor de aantallen vertekend kunnen zijn.

37 Aantallen registraties over de periode 2020 tot en met 2023 zijn niet gecontroleerd, en worden daarom alleen als trend beschreven.

Het gemiddelde schadebedrag is alleen voor het jaar 2022 berekend en is gebaseerd op het Cyberintelligencebeeld (Inteltafel Cyber, 2023). Het betreffen hier opgeschoonde cijfers, dat wil zeggen dat er alleen is gekeken naar de registraties waarvan een schadebedrag bekend is[38]. In 2022 bedroeg de totale financiële schade 430.500 euro. Van de 1259 registraties was in slechts 340 gevallen een bedrag vermeld. Het gemiddelde schadebedrag voor dit beperkte aantal registraties was 1266 euro. De hoogte van dit bedrag hangt samen met de uitschieters. Het hoogste schadebedrag was 40.000 euro en acht slachtoffers hadden een schade hoger dan 10.000 euro. Ongeveer honderd slachtoffers hadden een gemiddeld schadebedrag van rond de 1200 euro. In totaal tweehonderd slachtoffers betaalden gemiddeld 385 euro.

Uit het Cyberintelligencebeeld blijkt dat de grootste aantallen registraties betrekking hebben op financiële sextortion, waarbij afpersing plaatsvindt voor geld (52%). Hierbij zijn vooral mannen het slachtoffer. Van sextortion met een seksueel motief zijn vooral meisjes slachtoffer (24%). In een klein aantal gevallen (5%) betreft het relationele sextortion, waarbij een ex-partner uit jaloezie of wraak beeldmateriaal dreigt te openbaren om angst te zaaien. Voor de overige 19 procent is het motief niet bekend. Het project VAK (2023) meldt dat deze vorm van afpersing vaak te maken heeft met het leveren van diensten, waarbij het slachtoffer bijvoorbeeld een bankpas en pincode moet afgeven of als katvanger moet functioneren.

Externe bronnen

Het CBS maakt tweejaarlijkse veiligheidsmonitoren die een weerslag zijn van bevolkingsonderzoek naar veiligheid, leefbaarheid en slachtofferschap van veelvoorkomende criminaliteit, traditioneel en online. Aan de laatste twee Veiligheidsmonitoren deden ruim 180.000 respondenten van 15 jaar of ouder mee die een uitgebreide enquête invulden (CBS, 2024; 2022). In beiden komt sextortion terug onder de categorie phishing. Phishing wordt breed gedefinieerd door het CBS, want het gaat het om alle vormen van online oplichting waarbij de dader zich voordoet als iemand anders (een persoon of bedrijf) en via allerlei kanalen personen benadert met valse verhalen om geld te krijgen. Zo vallen hulpvraagfraude, voorschotfraude, beleggingsfraude en bijvoorbeeld factuurfraude allen onder phishing, maar dus ook sextortion.

In beide monitoren geeft 65 procent van de respondenten aan in de laatste twaalf maanden ten minste één keer een telefoontje, e-mail of ander bericht te hebben ontvangen dat (waarschijnlijk) van een oplichter afkomstig was. Een heel klein deel is er wel eens ingetrapt en heeft geld verloren. Van die 65 procent heeft slechts 0,3 procent te maken gehad met sextortion. Het CBS noemt geen concrete aantallen, maar geeft aan dat er wel een stijging is ten opzichte van 2021. In 2021 is in de Veiligheidsmonitor voor het eerst naar directe financiële schade van diverse delicten gevraagd. Sextortion valt daarin onder de categorie overige online fraude. De totale schade voor online delicten bedroeg 62 miljoen euro en 2 procent daarvan kwam voor rekening van overige online delicten als identiteitsfraude, afpersing na hacken of sextortion.

38 Niet alle registraties hebben een schadebedrag en bij sextortion geldt specifiek dat niet altijd een financieel motief ten grondslag ligt aan het delict. Een deel van de registraties heeft daarom geen schadebedrag. Alleen voor 2022 is uitgezocht welk deel van de registraties een schadebedrag had.

Het CBS beschrijft de gevolgen van sextortion niet specifiek, maar geeft aan dat bijvoorbeeld online bedreiging en intimidatie, dus incidenten in de interpersoonlijke sfeer, het vaakst emotionele of psychische problemen veroorzaken. Het is denkbaar dat deze gevolgen ook gelden voor sextortion. Maar ook online oplichting en fraude, hacken, en andere online delicten bezorgen slachtoffers emotionele schade.

Uit onderzoek naar de daders door het CBS (2022) bleek dat daders en slachtoffers elkaar vaak kennen. Van de slachtoffers die online bedreigd werden met geweld zei 38 procent aan de dader(s) te kennen. Van degenen die online gepest werden zei 59 procent te weten wie de dader was. Online pesten gebeurt vaak door medestudenten of scholieren (13%), gevolgd door buurtgenoten (10%) en vrienden (8%).

In 2020 deden Gorissen et al. een literatuuronderzoek naar de aard, omvang en aanpak van online seksueel geweld. De onderzoekers constateerden een zorgwekkende toename van het aantal meldingen van sextortion. Het onderzoek richtte zich op jongeren en zag, ondanks de toename, dat slechts 2 procent van de jongens die te maken heeft gehad met financiële sextortion melding doet bij de politie. De groei van het aantal meldingen van online seksueel geweld wordt deels verklaard doordat jongeren, gebruikers zowel als misbruikers, meer online zijn. Ook de grotere bekendheid van hulplijn Helpwanted.nl droeg hieraan bij.[39] De onderzoekers geven in het rapport een overzicht van organisaties (hierna beschreven) die zich bezighouden met online seksueel geweld en verschillende soorten sextortion, maar benadrukken dat accurate prevalentiecijfers vaak ontbreken.

Wat zijn kenmerken van criminele groeperingen?

Uit een onderzoek in 2021 naar de verdachten van jeugdcriminaliteit en cybercrime (Hesseling, Harteveld & Bloem, 2021) blijkt dat vooral minderjarigen (12-18 jaar) en jongvolwassenen (18–23 jaar) zich bezighouden met afpersing/chantage (na fraude/oplichting) en dan specifiek met sextortion. Hoewel het om kleine aantallen gaat, zijn de jeugdige verdachten vaker betrokken bij sextortion dan de verdachten van 23 jaar en ouder. Als mogelijke verklaring voor de jonge leeftijd stellen de onderzoekers dat jongeren meer betrokken zijn bij het digitaal verspreiden van – al dan niet gehackte – seksueel getinte foto's op sociale media (sexting). Het gaat dan vaak om scholieren onderling, waarbij sommigen de foto's vervolgens zijn gaan gebruiken om een slachtoffer af te persen (sextortion) of om te pesten. Het eerdergenoemde onderzoek door Gorissen et al. laat daarentegen zien dat vooral mannen zich bezighouden met sextortion en dat ze van alle leeftijden kunnen zijn (gemiddelde is 34 jaar in een range van 14 tot 70 jaar).

De Eenheid Amsterdam (2021) constateerde dat de daders van sextortion overwegend individueel opereren. In andere eenheden (bijvoorbeeld Den Haag) werd echter ook gezien dat groeperingen zijn betrokken. Het gaat dan om lokale netwerken, zoals groepen jongeren die elkaar kennen van school of uit de buurt. Deze groepen kennen geen duidelijke rolverdeling. Hierna worden enkele voorbeelden beschreven van een individueel opererende dader en van een groepering.

39 Helpwanted betreft een hulplijn en biedt praktische hulp of persoonlijk advies bij verschillende vormen van online grensoverschrijdend gedrag, waaronder sextortion. Zie: https://www.helpwanted.nl/onderwerpen/sextortion

In 2020 wordt een Turks-Nederlandse verdachte aangehouden voor sextortion. De dader deed zich voor als vrouw om vertrouwen te wekken en vroeg zijn (overwegend Turkse) slachtoffers om seksueel getint beeldmateriaal te versturen. Als deze daarop ingingen, perste de dader vervolgens zijn slachtoffers af. Bij het afpersen misbruikte hij de Turkse schaamtecultuur. De veroordeling was gebaseerd op 23 zaken met een totaal afgeperst bedrag van 50.000 euro. Veel slachtoffers wilden echter geen aangifte doen zodat het aannemelijk is dat het schadebedrag veel hoger was

Begin 2020 werd een groep jonge criminelen veroordeeld voor afpersing met naaktfoto's. De politie kreeg 22 aangiften binnen, terwijl een oproep van hulplijn Helpwanted 260 meldingen opleverde. De achttien verdachten hadden het vooral gemunt op jongens. De daders deden zich op sociale media als Instagram en Snapchat voor als meisje en legden zo contact met potentiële slachtoffers. Ze vroegen hen om naaktfoto's van zichzelf te sturen. Zodra die binnen waren, dreigden de daders de beelden openbaar te maken tenzij de slachtoffers betaalden, maar na betaling werden de slachtoffers niet met rust gelaten en moesten zij steeds opnieuw geld overmaken. De groep was goed georganiseerd en had de taken goed verdeeld, sommigen hielden zich bezig met nepaccounts, anderen deden de afpersing en zochten vrienden of kennissen van slachtoffers, en weer anderen fungeerden als katvanger (Omroepwest, 2020).

Als het om internationale netwerken gaat, wordt gemeld dat netwerken vanuit de Filipijnen en Marokko actief waren en dat daders en slachtoffers elkaar ontmoetten op internationale dating- en chatsites. Recentelijk lijken vooral bendes uit Afrika steeds actiever om jongeren te benaderen, zoals blijkt uit uitspraken in de media door het Team Kinderporno van de politie (WNL.tv, 2023).

Wat zijn kenmerken van slachtoffers?

In vergelijking met de andere cybercrimevormen is veel bekend over slachtoffers en daders van sextortion. Uit het Cyberintelligencejaarbeeld blijkt dat de leeftijd van de meeste slachtoffers, mannen en vrouwen, tussen de 18 en 25 jaar ligt (Inteltafel Cyber, 2023). De grootste groep slachtoffers bestaat uit mannen. In het Book of Crime van de Eenheid Amsterdam wordt als verklaring gegeven dat jongeren vaker actief zijn op sociale media (Eenheid Amsterdam, 2021), zoals hiervoor ook beschreven. Door hun jeugdige leeftijd zijn ze volop in ontwikkeling en nieuwsgierig naar seksualiteit en dit maakt hen gevoelig voor seksueel online contact, waarbij ze zich vaak niet bewust zijn van de risico's.

Er zijn verschillende groepen jongeren en volwassenen die meer risico lopen op sextortion. De eerste groep bestaat uit thuiswonenden tussen de 14 en 18 jaar, die vrijwillig naaktfoto's sturen naar een vriendje of vriendinnetje. De tweede groep bestaat uit jongeren van 18 jaar en ouder, die bekend zijn met sexting. Zij denken daar verstandig mee om te gaan, maar komen soms toch in de problemen. De derde groep wordt gevormd door jongeren met een licht verstandelijke beperking. Zij zijn gevoelig voor complimenten en te snel van vertrouwen. De vierde groep bestaat uit niet-westerse jongeren die een alternatief zoeken voor fysiek seksueel contact en gevoeliger zijn voor chantage door hun schaamtecultuur. De vijfde groep bestaat uit jongeren met een diverse seksuele geaardheid[40] die aan het experimenteren zijn en zich veilig wanen in hun digitale omgeving. In deze groep zijn bijvoorbeeld jongeren met gelovige ouders mogelijk extra kwetsbaar voor chantage. De laatste groep bestaat uit volwassen mannen (25 jaar en ouder) die zoeken naar seksuele contacten waarbij ze denken anoniem te zijn en met een zekere naïviteit chatcontacten hebben. Uit een onderzoek naar zedendelicten blijkt dat vrouwen een hoger risico lopen om slachtoffer te worden van wraakporno, (poging tot) seksuele sextortion en (poging tot) seksuele uitbuiting dan mannen na contact via een datingsite of datingapp. Mannen lopen meer risico op financiële sextortion (Wolsink, Kuppens, Brouwer & Ferwerda, 2023).

Melding en minder vaak aangifte

De politie ziet dat de meeste slachtoffers geen aangifte doen. Een expert meldt dat in Oost-Nederland meerdere malen bij verdachten afdreigingen in telefoons zijn aangetroffen, waarbij de slachtoffers geen aangifte hadden gedaan. De verhouding was vaak meer dan tien niet geregistreerde zaken tegen één geregistreerde zaak (aangifte).
Uit het onderzoek van Wolsink et al. (2023) komt ook naar voren dat de meeste slachtoffers wel melding doen bij de politie maar in veel mindere mate aangifte. Voor ongewenste sexting, financiële sextortion, seksuele sextortion, grooming, seksuele uitbuiting, aanranding en verkrachting geldt dat de meeste slachtoffers melding maken. Ook als het gaat om pogingen of dreigen met deze delicten. Er is aarzeling voor het doen van aangifte uit angst dat door de politiebemoeienis de dader contact gaat zoeken met het slachtoffer. Slachtoffers zijn wel voornemens om aangifte te doen wanneer de dader het seksueel beeldmateriaal alsnog verspreidt, de dader het slachtoffer lastig blijft vallen of wanneer er meerdere meldingen over dezelfde dader binnenkomen. Een andere motivatie om het slechts bij een melding te laten, is het idee dat het doen van aangifte geen zin heeft. Tot slot aarzelen slachtoffers die getrouwd zijn of een bepaalde geloofsovertuiging hebben. Zij willen geen aangifte doen, omdat het gevolg hiervan zou zijn dat bijvoorbeeld hun partner of ouders erachter komen wat er is gebeurd.

Wat zijn de verwachtingen in relatie tot de aanpak?

Met betrekking tot de aanpak van sextortion zijn verschillende initiatieven ontwikkeld, die hierna worden beschreven. Allereerst een aanpak die is ontwikkeld in de politie-eenheid Amsterdam[41], een aanpak ontwikkeld door verschillende externe partijen en de introductie van nieuwe wetgeving die als doel heeft om de strafbaarstelling en wettelijke structuur van verschillende vormen van seksueel grensoverschrijdend gedrag te moderniseren. Tot slot wordt kort ingegaan op de ontwikkelingen op het gebied van kunstmatige intelligentie en de invloed hiervan op sextortion. De verwachting bestaat dat sextortion zeker zal stijgen.

40 LHBTIQ+: Lesbisch, homoseksueel, biseksueel, transgender, intersekse en queer. De + staat voor anderen die binnen de samenleving niet als standaard worden gezien zoals aseksuelen.

41 De politie-eenheid Amsterdam is inmiddels niet meer verantwoordelijk voor dit thema. De aanpak is toch opgenomen omdat het nog steeds relevante punten bevat waarmee sextortion kan worden teruggedrongen.

Aanpak door de Eenheid Amsterdam

De Eenheid Amsterdam (2021) stelde in 2020 een multidisciplinair projectteam samen, waarin naast de politie en het Openbaar Ministerie ook een aantal publieke en private partners deelnamen, namelijk de gemeente Amsterdam, het ministerie van Justitie en Veiligheid, KPN Security, en de (nonprofit) slachtofferhulporganisaties Spirit/Qpido en Expertisebureau Online Kindermisbruik/Helpwanted.nl. Het projectteam is inmiddels opgeheven, maar werd ingedeeld in zes werkgroepen en ontplooide verschillende initiatieven:

- Preventie & voorlichting: door het maken van profielen van de slachtoffers en daaruit interventies te formuleren (verschillende games, voorlichting op scholen, aandacht in televisieprogramma's gericht op de jeugd en een Escaperoombus die bij basisscholen langsgaat en waarin door middel van puzzels en interactieve opdrachten leerlingen gewezen worden op de gevaren van internet).
- Intake, screening & opvolging: aangifteproces zo inrichten dat het slachtoffer van begin tot eind serieus genomen wordt (empathie, kennis, naar het juiste team en terugkoppeling naar aangever, behoefte beter in beeld).
- Opsporing & dashboard: opsporing van daders en groeperingen, daarnaast de ontwikkeling van een dashboard om registraties beter te analyseren en van een barrièremodel met voorstellen voor interventies en maatregelen voor iedere stap van het delict.
- Publiek-private samenwerking met een telecomprovider om expose-groepen beter in beeld te krijgen op de chatdienst Telegram.
- Politie & Wetenschap: een app om activiteiten vast te leggen waarbij slachtoffers lastiggevallen worden op Snapchat en wat kan dienen als bewijs voor opsporing in deze zaken.
- Een expert bevestigde dat meerdere zaken zijn gedraaid, waaronder één grote zaak.

Aanpak door externe organisaties

Bij de aanpak van online seksueel geweld zijn ten minste 18 verschillende partijen betrokken. Ze houden zich bezig met preventie, voorlichting, opsporing, vervolging of de bestraffing van online seksueel geweld (soms algemeen, soms specifiek zoals sextortion). Alle partijen zijn door de onderzoekers (Gorissen et al., 2020) benaderd over hun doelen en werkwijzen, en de uiteenlopende taken zijn hierin samengevat. Hierna worden vooral de organisaties opgesomd die betrokken zijn bij de aanpak van sextortion. Doel van de opsomming is om te laten zien dat er veel initiatieven bestaan. Deze organisaties zijn niet altijd van elkaars bestaan op de hoogte. Voordat nieuwe initiatieven in het leven worden geroepen, is het aan te bevelen om eerst naar de bestaande te kijken. Voor een uitgebreide beschrijving volstaat een verwijzing naar het betreffende rapport:

- Opsporing, samenwerken en voorlichting (politie), opsporing en vervolging is een taak van het Openbaar Ministerie, waarbij HALT interventies ontwikkelt om jeugdcriminaliteit te voorkomen.
- Het rapporteren van de aard en omvang en monitoren is een taak van de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen).
- Slachtofferhulp Nederland ondersteunt slachtoffers en verstrekt informatie.
- Onder het Expertisebureau Online Kindermisbruik (EOKM) vallen het Meldpunt kinderporno op internet (gaat om strafbare feiten), Helpwanted.nl (behandelt meldingen van jongeren en biedt informatie over het verwijderen van foto's; deze instantie krijgt vooral meldingen over sextortion) en Stop it Now (hulplijn voor daders). Het EOKM beschikt over een kennisbank met artikelen en rapporten over (online) seksueel kindermisbruik en gerelateerde thema's en factsheets en jaarverslagen van de verschillende programma's van EOKM.
- Meldknop.nl is een initiatief van Veilig Internetten en wordt ondersteund door de politie. Het is een website met informatie en hulp bij internetproblemen (sexting, sextortion, grooming, loverboys etc).
- Het kenniscentrum seksualiteit Rutgers ontwikkelt interventies gericht op preventie en weerbaarheid op scholen en samen met HALT interventies tegen sexting).
- De organisatie Art4respect richt zich specifiek op gendergerelateerd geweld. Atria is het kenniscentrum emancipatie voor gelijke behandeling en gelijke rechten, en vrouwengeschiedenis.
- Qpido doet aan voorlichting, training en hulp bij seksueel grensoverschrijdend gedrag bijvoorbeeld bij sexting en grooming en geeft voorlichting over de gevaren van sociale media.
- Terre des Hommes strijdt tegen kinderarbeid, kinderhandel, kindermisbruik en seksuele uitbuiting van kinderen. WATCH Nederland is een programma van Terre des Hommes en verzamelt onder meer bewijs tegen loverboys en ondersteunt slachtoffers.
- Fier is het expertise– en behandelcentrum van geweld in afhankelijkheidsrelaties, doet ook opvang en voorlichting en is tevens gericht op sextortion, sexting en grooming.
- Pretty Woman is specifiek in Utrecht gericht op hulpverlening aan meisjes tussen 11 en 23 jaar bij risico op misbruik in hun seksuele ontwikkeling, ook heeft de organisatie aandacht voor sociale media, webcamgebruik en sexting.
- De Kindertelefoon is een hulplijn voor kinderen tussen 8 en 18 jaar, voert 1000 gesprekken per dag, heeft een forum en geeft voorlichting op scholen.
- Stichting school & veiligheid i.o. van het ministerie van Onderwijs, Cultuur en Wetenschap geeft voorlichting aan en training op scholen op het gebied van sexting, sextortion, wraakporno en grooming.
- Kwetsbaar Online deelt kennis op haar online platform over mediawijsheid voor jongeren, ouders, hulpverleners en leerkrachten door gastlessen en training op scholen te geven over sexting, sextortion, wraakporno en exposen.
- Bureau Jeugd en Media gaat over mediaopvoeding, mediawijsheid en digitale geletterdheid, en biedt gastlessen, coaching, advies, en workshops op scholen, en aan ouders, over cyberpesten, sexting, veilig internetten, privacy en de invloed van smartphones.

Er zijn talloze interventies bedacht en uitgevoerd die samengevat kunnen worden in vier categorieën: de eerste categorie omvat de initiatieven die gerelateerd zijn aan het vergroten van de seksuele (en relationele) weerbaarheid en het bevorderen van de gezonde seksuele ontwikkeling van de deelnemers. De tweede categorie is een samenstelling van interventies op het gebied van mediawijsheid en (veilig) internetgebruik. De derde categorie is gericht op het voorkomen van recidive van seksueel grensoverschrijdend gedrag. Hierbij ligt de focus dus voornamelijk op daders. De vierde categorie interventies is bedoeld voor slachtoffers van seksueel misbruik of lichamelijk geweld of meisjes die kwetsbaar zijn en het risico lopen slachtoffer te worden van seksueel grensoverschrijdend gedrag. De laatste categorie bestaat uit interventies waarbij expliciet aandacht is voor online seksueel geweld.

Wetgeving

In 2024 loopt er een wetswijzigingsprocedure om de strafbaarstelling en wettelijke structuur van verschillende vormen van seksueel grensoverschrijdend gedrag te moderniseren,

met als doel slachtoffers van seksuele en seksueel getinte misdrijven beter te beschermen. Een van de wetsaanpassingen is dat een persoon strafbaar is wanneer hij of zij seksueel contact heeft met iemand die dit eigenlijk niet wil en hij of zij dit weet of had moeten weten. Seksuele intimidatie wordt zowel offline als online strafbaar gesteld, evenals het als volwassene sturen van seksueel getinte berichten naar kinderen onder de 16 jaar. Het op vrijwillige basis uitwisselen van seksueel beeldmateriaal (sexting) is echter niet langer strafbaar, aangezien dit in het wetsvoorstel wordt beschouwd als normaal seksueel experimenteergedrag. De strafrechtelijke normen gaan daarmee ook gelden in de online wereld. Misbruik van seksueel beeldmateriaal, zoals het ongewenst openbaar maken van seksfilmpjes en naaktfoto's, wordt een seksueel misdrijf in de nieuwe wet. Dit geldt ook voor wraakporno (dat tot voor kort onder Openbare Orde viel), shame-sexting, sextortion en grooming. Het is nog niet duidelijk wie bij de politie sextortion naar aanleiding van de nieuwe wetgeving zal oppakken, de cyberteams of zeden.

Kunstmatige intelligentie

In het geval van sextortion wordt kunstmatige intelligentie (AI) al vaak toegepast, biedt ongekende mogelijkheden en is het meer realiteit dan een toekomstige ontwikkeling. Omdat AI op meer fraudevormen van invloed zal zijn, is een uitvoerigere beschrijving van de mogelijkheden terug te vinden in het hoofdstuk 7 Toekomstige ontwikkelingen.

Andere trends

Dichter bij huis constateerde de Eenheid Limburg in een wekelijks cybercrimeoverzicht (week 38 & 39, 2023) dat in Nederlandse Telegram-chatgroepen op grote schaal contactgegevens en naaktfoto's van vrouwen gedeeld worden (dit bleek, volgens de eenheid, uit onderzoek van NOS Stories naar een online nieuwsvoorziening gericht op jongeren). Van een wettelijk verbod trekken de leden zich weinig aan. In de groepen, met tot wel 85.000 leden, verschenen per dag meer dan 10.000 berichten. De expose-berichten worden in de meeste gevallen voorzien van contactgegevens en gaan vaak gepaard met de oproep om de vrouw of het meisje lastig te vallen. Van 1,5 miljoen verzamelde berichten uit vijftien groepen werden 14.000 mogelijke expose-berichten geanalyseerd. In 7000 gevallen ging het om een expose-bericht en naast een foto of video werden ook iemands naam, contactgegevens van sociale media of telefoonnummer gepost. De beelden gingen bijvoorbeeld vergezeld van iemands profielfoto, en regelmatig ook met sexy foto's, naaktfoto's of zelfs seksfilmpjes. Toegang tot de groepen verkrijgt men meestal via invite-links die mensen met elkaar kunnen delen. Het bedrijf Telegram is niet toegankelijk als het gaat om het verwijderen van beelden, blijkt uit de praktijk. Als beelden al worden verwijderd, richten de beheerders gewoon een nieuwe groep op met dezelfde werkwijzen.

4.8 Beleggingsfraude

Binnen beleggingsfraude kunnen verschillende verschijnings-vormen worden onderscheiden. De drie meest bekende bestaan al heel lang, namelijk boilerroomfraude, ponzi-zwendel en piramidespelen. In essentie is de MO voor alle drie hetzelfde: potentiële slachtoffers worden online of telefonisch overgehaald om hun geld te beleggen waarbij hoge rendementen in het vooruitzicht worden gesteld. Meestal zien slachtoffers niets van hun investeringen terug.

Beleggingsfraude in cijfers

Gemiddeld schadebedrag

€ 27.000

per registratie

1500

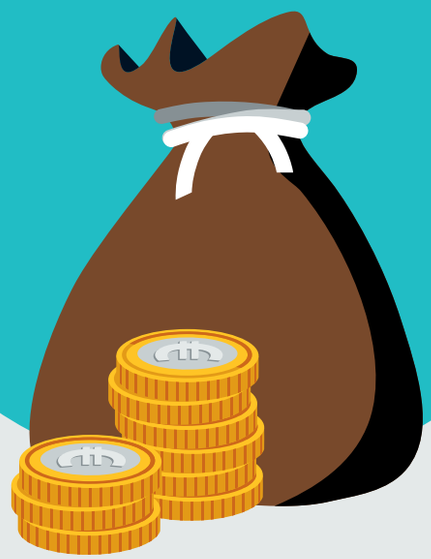
Van 130 registraties in 2020 naar ruim 1500 in 2023.

Ingelegd geld

wordt niet belegd

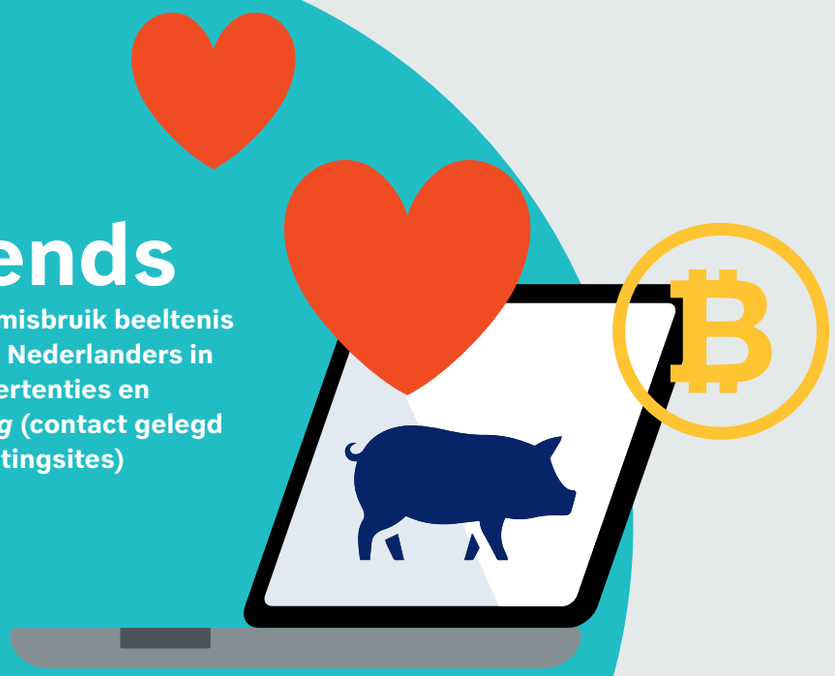
Schadebedragen

lopen sterk uiteen, van 100 tot 1.4 miljoen euro per registratie



Trends

cryptovaluta, misbruik beeltenis van bekende Nederlanders in nepadvertenties en *pig butchering* (contact gelegd via datingsites)



Slachtoffers

worden overgehaald om te investeren in beleggingen

Totale schade in 2023 is

€ 31 miljoen

Beleggingsfraude was tot 2017 in de Veiligheidsagenda ondergebracht in de categorie ‘overig’. De fiscale inlichtingen- en opsporingsdienst (FIOD) is al jaren hoofdverantwoordelijke voor de aanpak. Ondanks dat beleggingsfraude in de vorige dreigingsbeelden als dreiging werd bestempeld, is het niet opnieuw in de Veiligheidsagenda opgenomen. Voor dit fenomeenbeeld zijn de cijfers over de periode 2017 – 2022 bekeken in de politiesystemen. Hiermee kan een inschatting van de omvang van het probleem worden gemaakt.

Hoe heeft het fenomeen zich ontwikkeld?

In de laatste twee deelrapporten Horizontale Fraude (Bloem et al., 2012; 2017) werd beleggingsfraude als een dreiging gekwalificeerd op basis van de gevolgen voor de slachtoffers en de verwachting dat de omvang en impact onverminderd hoog zouden blijven. Beleggingsfraude is daarom al jaren een probleem en blijkt tussen 2019 en 2024 te zijn toegenomen. Beleggingsfraude is een type fraude waarbij het aantal registraties laag is, maar de gemiddelde schadebedragen hoog zijn.

Binnen beleggingsfraude kunnen verschillende verschijningsvormen worden onderscheiden. De drie meest bekende bestaan al heel lang, namelijk boilerroomfraude, ponzi-zwendel en piramidespelen, en worden hieronder besproken. In essentie is de MO voor alle drie hetzelfde: potentiële slachtoffers worden online of telefonisch overgehaald om hun geld te beleggen waarbij hoge rendementen in het vooruitzicht worden gesteld. Meestal zien slachtoffers niets van hun investeringen terug. Aan deze drie vormen zijn drie nieuwe toegevoegd, die gerelateerd zijn aan cryptovaluta, namelijk recovery room fraude, pump en dump en een vorm waarin datingfraude en beleggingen in cryptovaluta worden gecombineerd (pig butchering). Cryptovaluta is een nieuwe trend. Waar slachtoffers voorheen vooral belegden in koophuizen of aandelen in techbedrijven, doen ze dat tegenwoordig in cryptovaluta.

Boilerroomfraude

Een boilerroom is een verzamelnaam voor mensen en organisaties die met agressieve verkoopmethoden potentiële beleggers benaderen om ze waardeloze producten te verkopen. De plek van waaruit dit wordt gedaan, kan een fysiek kantoor zijn, maar steeds vaker ook een goed ogende website. In het verleden was een boilerroom meestal een (relatief) klein kantoor, van waaruit mensen telefonisch benaderd werden om geld te investeren. Doordat de potentiële klanten de telefoongesprekken van de andere medewerkers op de achtergrond kunnen horen, wordt de indruk gewekt dat er een succesvol en betrouwbaar bedrijf actief is. Om potentiële klanten over te halen geld in te leggen, worden hoge rendementen in het vooruitzicht gesteld. In werkelijkheid blijkt het vaak om waardeloze aandelen te gaan. Soms worden ook niet bestaande aandelen verkocht of worden andere financiële producten aangesmeerd, zoals financiële derivaten. In alle gevallen verliezen de slachtoffers het ingelegde vermogen en gaan regelmatig grote sommen geld verloren.

Ponzi-zwendel

Deze vorm van beleggingsfraude is vernoemd naar de oplichter Charles Ponzi. Het is een klassieke vorm van beleggingsfraude. Waarbij niets of slechts een (klein) deel van de inleg wordt belegd. De vooraf afgesproken (hoge) rendementen worden betaald met de inleggelden van latere investeerders.

Piramidespelen

Verschillen weinig van de hierboven genoemde vormen van beleggingsfraude. Het voornaamste verschil is dat de deelnemers geacht worden zelf nieuwe deelnemers aan te brengen. De ‘voet’ van de piramide betaalt het rendement van de top (Bloem et al., 2012; 2017).

Online beleggingsfraude en cryptovaluta

In de loop van de jaren vindt ook beleggingsfraude steeds vaker online plaats. ‘Aantrekkelijke’ beleggingen werden in eerste instantie in bulk mailing rondgestuurd. Later werden deze potentieel aantrekkelijke beleggingsopties steeds vaker verspreid via advertenties, online handelsplatforms, websites en sociale media. Er vond een verschuiving plaats van investeringen in gewone valuta naar cryptovaluta (die lucratief kunnen zijn door koersschommelingen). Via een fictieve beleggingswebsite maakt een potentieel slachtoffer een ‘wallet’ aan (vaak via iDeal). Daarin geld wordt gestort vanaf zijn of haar bankrekening en hiermee kunnen cryptovaluta worden aangeschaft. De oplichter neemt contact op met het slachtoffer en vraagt om een RAT, zoals Anydesk, te installeren, zodat hij mee kan kijken en een handje kan helpen met de ‘beleggingen’. De uitvoering van de oplichting lijkt op andere fraudevormen, zoals helpdeskfraude en bankhelpdeskfraude, omdat de crimineel met deze toegang tot de bankomgeving grote bedragen van de rekening van het slachtoffer haalt en stort op door de criminele organisatie gecontroleerde wallets (Hupkes c.s. Advocaten, z.d.) Het is in het algemeen lastig om deze cryptovaluta terug te halen, omdat de handel in cryptovaluta een grotendeels ongereguleerde markt is en nog weinig toezicht kent.

Voorbeeld van verschillende werkwijzen in één oplichtingszaak

Deze casus betreft een nieuwe vorm van beleggingsfraude, namelijk winsten op dag-handel in cryptovaluta. Beleggers kregen een stop-loss-regeling en een inlegverzekering, dus konden geen geld kwijtraken. Er kon op elk moment worden uitgekeerd. Met een deel van de inleg keerde de oplichter rendementen uit en hield zo klanten tevreden. In werkelijkheid was het een boilerroom: de dader leidde zijn klanten rond in zijn kantoor om vertrouwen te wekken. Hij had ook een website en sociale media waar reclame werd gemaakt met gelikte filmpjes. Het ging ook om Ponzi-zwendel: de dader gebruikte de ingelegde gelden om ‘rendementen’ aan beleggers uit te betalen en om bedragen uit te keren aan klanten die geld wilden opnemen. In totaal werd 5,6 miljoen euro buitgemaakt bij 140 gedupeerden, veelal mensen zonder ervaring met cryptovaluta. Hij besteedde het geld vooral aan een luxe levensstijl (horloges, dure hotels en privéjets) en aan het aflossen van schulden. In 2021 kreeg deze 27-jarige man 15 maanden cel opgelegd voor oplichting met cryptovaluta en witwassen. De opsporing is gedaan door de FIOD en belastingdienst.

(Bron: Smith, z.d.)

Drie vormen van fraude zijn tegenwoordig aan cryptovaluta gerelateerd:

1. Recovery room-fraude
Dit is een vorm waarbij zogenaamde 'sucker lists' worden gebruikt voor beleggingsfraude. Het fenomeen bestaat al lang en vindt tegenwoordig onder andere plaats met cryptobeleggingen. Personen die al eens opgelicht waren, komen op zo'n lijst terecht, met het doel om ze nog een keer op te lichten. Slachtoffers van beleggingsfraude krijgen het voorstel om hun verliezen te compenseren of verloren tegoeden terug te krijgen. Dit kan bijvoorbeeld door (waardeloze) cryptomunten te kopen van of via de 'redder in de nood' of een juridische procedure te starten met diens hulp. Voor de aangeboden hulp wordt een flinke vergoeding gevraagd, die vooraf betaald moet worden. In de paniek waarin de slachtoffers verkeren, gaan ze hier graag op in. De hulp wordt niet verleend en de slachtoffers blijven dubbel berooid achter.

2. Pump en dump
Pump en dump is een vorm van koersmanipulatie waarbij iemand een eigen cryptomunt aanmaakt of veel cryptovaluta van een onbekende (en goedkope) muntsoort aankoopt. Als hij een grote hoeveelheid munten in handen heeft, probeert hij meer mensen deze cryptovaluta te laten kopen. Bijvoorbeeld door reclame voor die muntsoort te maken op sociale media of op internetfora, waarbij grote winsten worden voorgespiegeld. Consumenten worden zo verleid om de desbetreffende cryptovaluta aan te schaffen, en als veel mensen dat doen, stijgt de waarde van de munt. Dit wordt de 'pump' genoemd. Op het moment dat de munt veel waard is, verkoopt (dumpt) de oplichter veel van zijn cryptovaluta. Hierdoor behaalt de oplichter een hoge winst (rendement), maar keldert de waarde van de munt. Mensen die dachten een goede aankoop te hebben gedaan, blijven zitten met een waardeloze cryptomunt (Langenburg, 2022).

3. Datingfraude en beleggingen in cryptovaluta
In 2022 zag de Fraudehelpdesk een nieuwe vorm van beleggingsfraude met cryptovaluta. Op datingapps zoeken oplichters contact met vooral 40-plussers die gescheiden zijn en vermogend. Ze besteden veel aandacht en tijd aan het wekken van vertrouwen, zoals het benadrukken van gezamenlijke financiële interesses. Vervolgens bieden de oplichters dan aan om te helpen investeren in cryptovaluta. In het begin wordt nog de indruk gewekt dat er flinke winsten kunnen worden gemaakt, mensen geloven dit en maken steeds meer geld over. Maar als de investeringen eenmaal groot genoeg zijn, verdwijnt het contact met de date en daarmee al het geld. De slachtoffers raken aanzienlijke bedragen kwijt. Wereldwijd is dit een toenemend probleem, dat bekend staat als *pig butchering*.

In het deelrapport *Horizontale fraude* 2017 (Bloem et al., 2017) werd geconstateerd dat *social engineering* een belangrijke rol speelt bij online fraude. De oplichter gebruikt de zwakste schakel, de mens, om vertrouwen te wekken met het doel allerlei informatie en medewerking te krijgen voor criminele doeleinden. In deze gecombineerde vorm van dating- en beleggingsfraude nemen ze heel veel tijd om vertrouwen te wekken, omdat het veel geld oplevert. De daders opereren internationaal en het internet biedt ruim voldoende mogelijkheden om locaties te verhullen. Een onderzoek in de Verenigde Staten zag een verband met een internationaal mensensmokkelsyndicaat dat wereldwijd slachtoffers maakt vanuit Zuid-oost-Azië. De geldstromen gaan zo snel dat het moeilijk is om grip op de daders te krijgen (Koning, 2024).

Bekende Nederlanders en finfluencers

Omdat de wereld van cryptovaluta ondoorzichtig kan zijn voor onervaren beleggers, laten zij zich graag verleiden door 'ervaren beleggers'. Zoals bekende Nederlanders bepaalde beleggingen lijken aan te prijzen, terwijl feitelijk de beeltenis van de BN'ers is misbruikt. Een andere recente ontwikkeling is dat zogenoemde finfluencers, die in dienst zijn van frauduleuze platforms, tegen een flinke vergoeding klanten werven voor beleggingsfraude. Finfluencers werken op dezelfde manier als influencers op sociale media, waarbij ze proberen het koopgedrag van mensen te beïnvloeden. Velen werken tegen beloning voor bekende merken en hebben een enorm bereik, omdat ze zeer actief zijn en vele volgers (wereldwijd) hebben, op wie ze invloed uitoefenen. Ze maken filmpjes, doen zich voor als experts en verspreiden misleidende informatie. De toename van het aantal finfluencers in korte tijd is door de AFM zorgwekkend genoemd. Een voorbeeld is Grinta Invest[42], dat aan het eind van dit hoofdstuk wordt besproken.

Hoe heeft de omvang zich ontwikkeld?

Zoals eerder omschreven is beleggingsfraude al geruime tijd een probleem. In het deelrapport *Horizontale fraude* 2012 (Bloem & Harteveld, 2012) werd gemeld dat beleggingsfraude slechts veertien keer voorkwam en tot een van de minst voorkomende vormen van fraude behoorde, maar wel met de hoogste schadebedragen. Uit het deelrapport van 2017 (Bloem et al., 2017) bleek dat het aantal registraties van beleggingsfraude nog steeds beperkt was. Tussen 2011 en 2014 nam het aantal toe van 171 naar 223, maar wel met enorme financiële schade per persoon (variërend van 6500 euro tot 200.000 euro).

De omvang van beleggingsfraude werd in dit deelrapport van 2012 op 500 miljoen euro per jaar geschat. In 2017 werd de financiële omvang van de totale schade voor de tien onderzochte vormen van horizontale fraude geschat op 3 miljard euro per jaar. Beleggingsfraude stond op een tweede plaats met een geschatte omvang van 300 miljoen euro per jaar (Bloem et al., 2017). Ook de Autoriteit Financiële Markten (AFM) schatte de omvang op enkele honderden miljoenen euro's per jaar. Dit bedrag was afgeleid uit signalen, maar werd ondersteund door de bedragen die genoemd werden in opsporingsonderzoeken van winsten die groeperingen hadden gemaakt. Vanwege het internationale karakter van deze vorm van fraude kon niet een precies beeld worden gegeven. Beleggingsfraude werd wederom als een dreiging bestempeld, omdat de inschatting was dat de omvang onverminderd groot zou blijven.

42 Op het beleggingsplatform Grinta Invest zijn honderden beleggers voor zeker vijf miljoen euro het schip ingegaan, na promotie van de investeringen door verschillende finfluencers. Deze groep finfluencers bestond uit auteurs van beleggingsboeken en ondernemers met een achtergrond in de auto-en kunsthandel, zij gaven beleggingsadviezen zonder hiervoor de benodigde vergunning te hebben.

De afgelopen jaren is het aantal registraties van fraude met beleggingen flink toegenomen (de precieze aantallen zijn niet bekend):

- ruim 130 in 2020
- ruim 330 in 2021
- ruim 800 in 2022
- ruim 1500 in 2023 met een gemelde schade van bijna 31 miljoen euro.

De precieze omvang van de schade is niet voor ieder jaar bekend. Het Cyberintelligence-jaarbeeld van de Inteltafel Cyber (2023) komt op 27.000 euro per slachtoffer in 2022. In dit rapport zijn alle registraties over dat jaar gecontroleerd; over de andere jaren kan niet met zekerheid een uitspraak worden gedaan. Het hoogste schadebedrag bedroeg 1,4 miljoen euro, het laagste bedrag was onder de 100 euro. In 60 procent van de registraties ging het over beleggingen in cryptovaluta, de overige 40 procent betrof reguliere aandelen. Beleggingsfraude en BEC-fraude zijn de vormen met de hoogste (gemiddelde) schadebedragen.

Externe bronnen

Van de externe bronnen meldt alleen de Fraudehelpdesk aantallen beleggingsfraudezaken, en die lopen steeds verder op, evenals de schade:

- In 2020 bedroeg de totale schade meer dan 13 miljoen euro, verdeeld over bijna 400 slachtoffers, met een gemiddeld verlies van 32.500 euro per persoon.
- In 2021 steeg de schade met 46 procent naar 19 miljoen euro, waarbij ruim 500 slachtoffers gemiddeld 38.000 euro verloren.
- In 2022 betaalden ruim 600 slachtoffers voor niet-bestaande beleggingen. In totaal werd bijna 15 miljoen euro buitgemaakt en het gemiddelde verlies was 25.000 euro per persoon.
- In 2023 waren er in totaal 1000 meldingen, waarin 900 gedupeerden samen meer dan 20 miljoen euro verloren. Hoewel het gemiddelde schadebedrag per persoon iets daalde naar 22.000 euro, varieerden de individuele schadebedragen bij de FHD sterk, van enkele duizenden euro's tot enkele honderdduizenden euro's per persoon.

De aantallen en gemiddelde schadebedragen komen overeen met de aantallen en bedragen in de politiesystemen. Verder meldt ook de FHD dat sinds 2022 pig butchering in opkomst is. In 2022 betaalden 103 van de 130 melders gemiddeld 47.000 euro. De totale schade was bijna 5 miljoen euro. In 2023 ging het om 108 meldingen van deze gecombineerde vorm met een schade van ruim 2 miljoen euro. Voor de 68 gedupeerden was dit gemiddeld bijna 30.000 euro per persoon.

Wat zijn de verwachtingen in relatie tot de aanpak?

De financiële schade en de gemiddelde schadebedragen van beleggingsfraude zijn hoog, ook afgezet tegen het totaal belegd vermogen van particulieren. Particulieren zijn steeds vaker gaan beleggen. In 2014 belegden ongeveer 770.000 huishoudens, in 2022 zijn dat er 1,9 miljoen met een totaal vermogen van 157 miljard euro (De Nederlandsche Bank, 2022) in beleggingsfondsen, aandelen en obligaties. In 2018 was dat nog 58 miljard euro.

In het *Nationaal dreigingsbeeld 2017* werd de volgende verwachting uitgesproken, die nog onverminderd overeind staat:

Op basis van de geschetste ontwikkelingen, zijn er geen aanwijzingen dat de omvang van beleggingsfraude in de komende vier jaar veel zal dalen ten opzichte van het huidige niveau. De verwachting is dat het aantal particuliere beleggers zal toenemen in de komende jaren, evenals het aantal producten waarin zij vooral via het internet kunnen beleggen. Zelfs als deze ontwikkeling niet leidt tot een (flink) groter aantal slachtoffers, dan blijft het probleem hoogstwaarschijnlijk onverminderd omvangrijk. De aanpak van beleggingsfraude is lastig gebleken als gevolg van het grensoverschrijdende karakter. Dit noodzaakt tot internationale samenwerking en een lange adem voor de opsporing, maar leidt regelmatig tot moeizame en langdurige trajecten of frustreert een onderzoek. Hierin is op korte termijn geen grote verbetering te verwachten. Preventie en het zo goed mogelijke informeren en waarschuwen van consumenten lijkt daarom de meest effectieve benadering'. Deze verwachting is uitgekomen en geldt voor de komende jaren nog steeds. Zeker zolang de omstandigheden om te investeren gunstig blijven, zoals een lage rente op spaargeld in verhouding tot inflatie (Bloem et al., 2017, p113).

Aanpak FIOD

In het laatste half jaar van 2023 heeft de FIOD verschillende opsporingsonderzoeken naar beleggingsfraude afgerond. In augustus 2023 hield de FIOD drie verdachten aan die hun slachtoffers met de belofte van hoge rendementen hadden verleid tot investeringen in de Amerikaanse dollar en goud. De verdachten hadden geen vergunning. Het ging om 800 gedupeerden die 56 miljoen euro investeerden, gemiddeld 70.000 euro per persoon (FIOD, 2023).

In een zaak uit juli 2023 ging het om twee verdachten, mannen van ongeveer 26 jaar, die twintig gedupeerden oplichtten voor ongeveer vier miljoen euro (gemiddeld 200.000 euro per persoon). Ze zeiden te investeren in Amerikaanse techbedrijven. De verdachten probeerden te vluchten waarna een internationaal aanhoudingsbevel werd uitgevaardigd en zij konden worden aangehouden (Het Financieele Dagblad, 2023).

In april 2023 arresteerde de FIOD een man (26 jaar) en een vrouw (29 jaar) voor beleggingsfraude; zij hadden zonder vergunning producten aangeboden, en een ponzifraude en een piramidespel opgezet. De minimale inleg was 100.000 euro met een beloofd rendement van 25 procent. In vier jaar tijd werden tachtig beleggers de dupe voor in totaal 26 miljoen euro (gemiddeld 325.000 euro per persoon) (FIOD, 2023b).

Aanpak politie

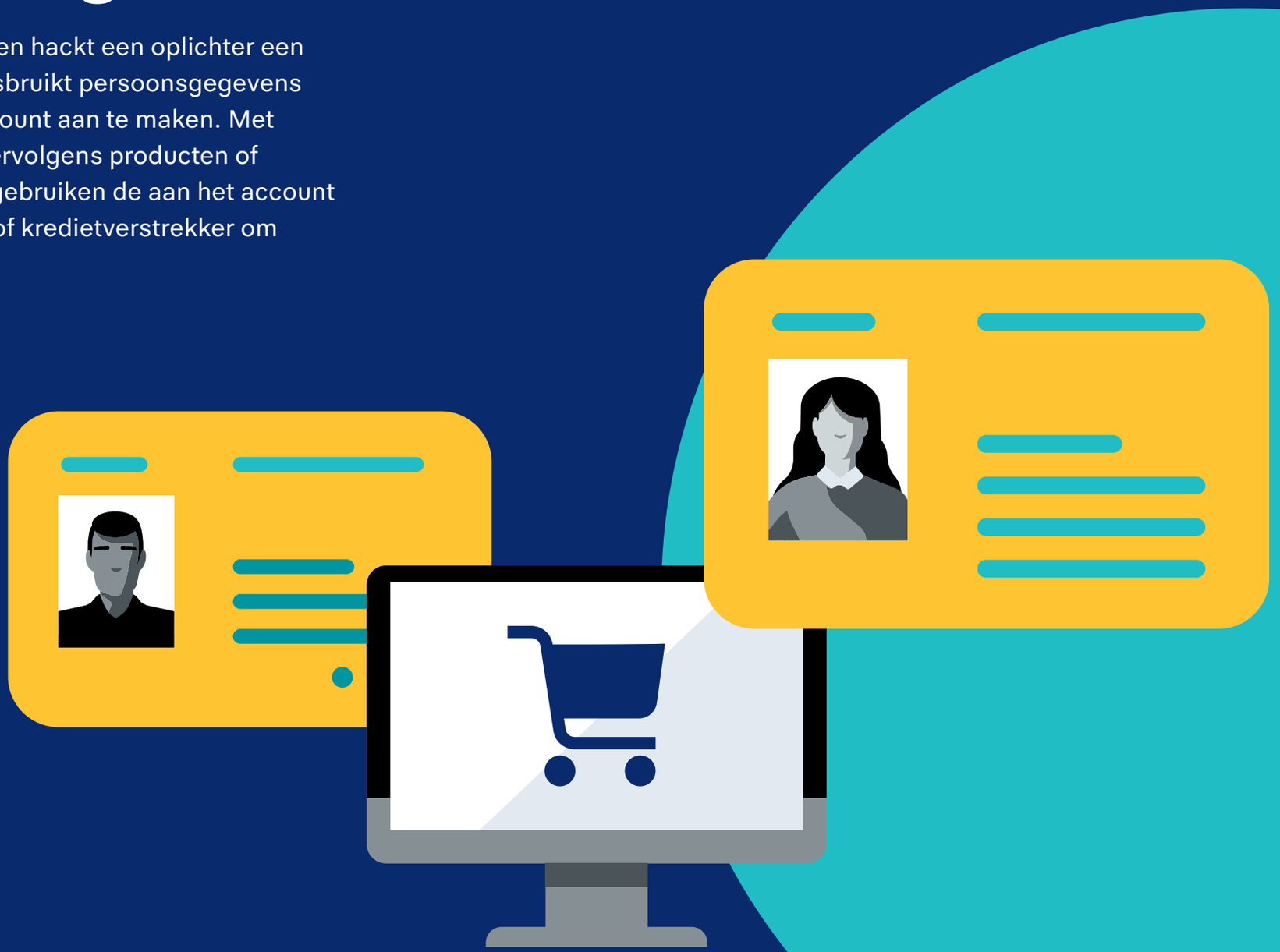
Voorjaar 2023 besteedden de media ruim aandacht aan het beleggingsplatform Grinta Invest (Motké et al., 2023, 23 mei). Honderden beleggers zouden voor zeker vijf miljoen euro het schip zijn ingegaan, na promotie van de investeringen door verschillende finfluencers. Deze groep finfluencers bestond uit auteurs van beleggingsboeken en ondernemers met een achtergrond in de auto-en kunsthandel. Zij gaven beleggingsadviezen zonder hiervoor de benodigde vergunning te hebben. De AFM is naar de finfluencers een onderzoek gestart. De eigenaren van Grinta claimden in valuta te handelen en flinke rendementen te behalen door te handelen met een zelfbedacht algoritme. Ook maakten ze gebruik van een piramideconstructie. In een beleggingsclub werden de leden uitgenodigd vijf deelnemers te vinden om te investeren en van deze investering zouden de aandragers dan 10 procent per persoon commissie opstrijken. Grinta had geen vergunning in Nederland en was gevestigd op de

Marshalleilanden. Enige tijd ging het goed en werden rendementen uitgekeerd, tot het platform ineens sloot en niet meer bereikbaar was. Hierna verdwenen alle investeringen als sneeuw voor de zon. Gedupeerden waren er niet alleen in Nederland, maar ook in België en Slowakije. Een zoekslag leerde dat in Nederland 234 aangiften zijn gedaan. Deze zaak is niet opgepakt, omdat beleggingsfraude de afgelopen jaren beperkte aandacht had van de politie. Hierin komt de komende jaren waarschijnlijk verandering, omdat beleggingsfraude een van de fraudevormen is die wordt besproken binnen de Integrale aanpak online fraude. Deze aanpak is beschreven in het hoofdstuk 7 Toekomstige ontwikkelingen.

Een zoekslag op beleggingsfraude in de politiesystemen leverde over de periode 2017 – 2023 in totaal 23 incidenten op die als opsporingsonderzoek geregistreerd zijn, waarvan vijf bij de FIOD. Wanneer beleggingsfraude meer prioriteit krijgt, zouden in een vervolgonderzoek de aantallen en inhoud beter in kaart gebracht moeten worden. Voor dit fenomeenbeeld bleek de tijdsinvestering te groot om alle lopende onderzoeken in beeld te krijgen.

4.9 Misbruik accounts voor bestellingen

Bij misbruik accounts voor bestellingen hackt een oplichter een webshopaccount van een klant of misbruikt persoonsgegevens van slachtoffers om een webshopaccount aan te maken. Met dit account bestellen de oplichters vervolgens producten of diensten uit naam van deze klant en gebruiken de aan het account gekoppelde creditcard, tegoedkaart of kredietverstrekker om achteraf te betalen.



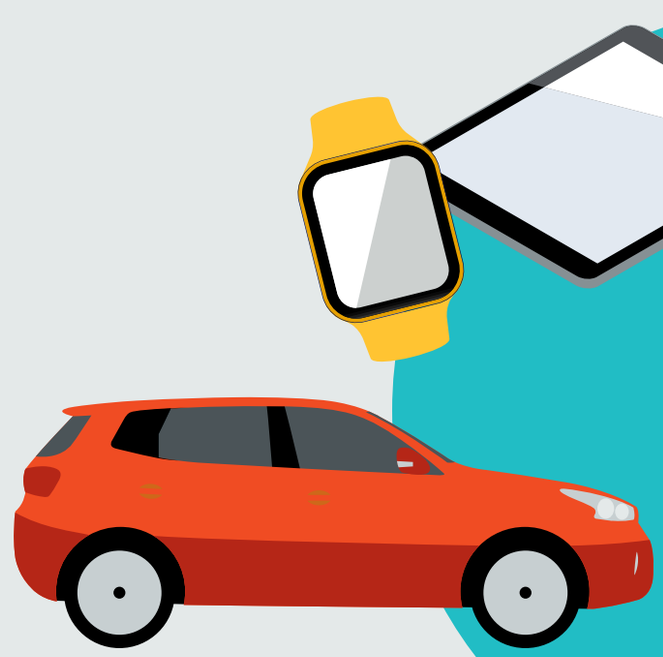
Misbruik accounts voor bestellingen in cijfers

3100

Van 4800 registraties in 2020 naar 3100 in 2023

Goederen

doorgaans voor eigen gebruik of doorverkocht. Ook sprake van heling



Bestellen van

luxe producten

bij grote webshops op naam en rekening van het slachtoffer

Hacken

bestaand account of openen account op naam van een slachtoffer

Stijging

Er is vooral een stijging te zien bij de grootste online warenhuizen en bij fysieke winkelketens die online zijn gaan verkopen.

Totale schade gemiddeld per jaar

€ 1,6 miljoen

Bij misbruik accounts voor bestellingen hackt een oplichter een webshopaccount van een klant van die webshop of misbruikt persoonsgegevens van slachtoffers om een webshopaccount aan te maken. Met dit account bestellen de oplichters vervolgens producten of diensten uit naam van deze klant en gebruiken de aan het account gekoppelde creditcard, tegoedkaart of kredietverstrekker om achteraf te betalen. Het adres wordt in de meeste gevallen aangepast door de dader. De pakketjes worden opgehaald op een afhaalpunt, afgevangen door een katvanger of afgeleverd door een chauffeur van een bezorgdienst die hierbij betrokken is. De goederen worden zelf gehouden, cadeau gegeven aan familie of vrienden of doorverkocht op handelsplaatsen of tweedehandswinkels. Wanneer er sprake is van doorverkopen gaat het om heling en witwassen, maar op deze stappen bestaat weinig zicht. Deze fraudevorm is niet opgenomen in de Veiligheidsagenda.

Hoe heeft het fenomeen zich ontwikkeld?

De werkwijze van misbruik voor bestellingen is onder andere beschreven in het NCB (Bloem & Harteveld, 2019). In de jaren daarna is de werkwijze van deze online fraudevorm weinig veranderd. Bij de grote postorderbedrijven worden de accounts en vaak ook de e-mailaccounts gehackt. Het hacken van het e-mailaccount kan een tussenstap zijn om toegang te krijgen tot de webshopaccounts, maar het komt ook voor dat e-mailaccounts en webshopaccounts tegelijk lijken te zijn gehackt. De accounts zijn waarschijnlijk verkregen uit grote datalekken. Met behulp van *credential stuffing* is met de bemachtigde inloggegevens toegang verkregen tot andere accounts, waarna de inloggegevens te koop worden aangeboden. Daarnaast is geconstateerd dat inloggegevens van e-mailaccounts en/of webshopaccounts worden verkregen door phishing van inloggegevens uit andere accounts, zoals die van Marktplaats, waarna gegevens worden afgevangen. Tot slot worden accounts op het *dark* web aangeboden.

In een oudere analyse (Schuppers, 2018) wordt een bijzondere werkwijze omschreven om aan inloggegevens te komen. Een dader had webshops gebouwd met een ‘achterdeurtje’ waarbij lange tijd inloggegevens van klanten werden afgevangen voor bestellingen bij de grote postorderbedrijven. In een ander opsporingsonderzoek had de dader inloggegevens verkregen door installatie van *keyloggers* op openbare computers. Bij telecombedrijven worden inloggegevens voornamelijk via phishing verkregen. Klanten worden via de mail of sms benaderd door de zogenaamde telecomprovider en worden doorgelinkt naar een namaaksite van die provider. Daar worden de inloggegevens afgevangen.

Bij zowel de postorderbedrijven als de telecombedrijven worden na het hacken van de accounts de accountgegevens aangepast. Het gaat dan primair om het afleveradres, maar het kan ook gaan om aanpassing van het e-mailadres en het wachtwoord om de notificatie aan de slachtoffers te bemoeilijken. Vervolgens bestelt de dader bij de postorderbedrijven, met de optie achteraf betalen, voornamelijk dure elektronica of merkkleding. De bestelde producten zijn voor eigen gebruik of worden doorverkocht. Bij de telecombedrijven vraagt de dader binnen het account van het slachtoffer verlenging van het abonnement aan met een nieuwe telefoon. Vaak is dat de nieuwste versie van een dure telefoon. Goederen die besteld zijn bij postorderbedrijven, worden meestal afgeleverd bij afhaalpunten, terwijl het bij de telecombedrijven vaker gaat om huisadressen. In dat laatste geval worden de pakketten mogelijk onderweg onderschept door de daders. Uit de analyse van Schuppers (2018) bleek dat destijds de afleveringen geconcentreerd waren in de omgeving van Amsterdam, Almere, Rotterdam en Arnhem. Heling gaf een divers beeld te zien: vaak op Marktplaats, Used Products en de Zwarte Markt.

Hoe heeft de omvang zich ontwikkeld?

Misbruik accounts voor bestellingen is in de periode 2016 tot 2020 sterk toegenomen. Er is vooral een stijging te zien bij de grootste online warenhuizen en bij fysieke winkelketens die online zijn gaan verkopen, bijvoorbeeld op het gebied van consumentenelektronica, schoenen, kleding en maaltijden die aan huis bezorgd worden. Verschillende online betaaldiensten worden daarbij genoemd, meer specifiek bedrijven die consumenten in staat stellen om achteraf te betalen. Deze bedrijven nemen als het ware de schuld over (evenals het innen van die schuld), waarbij het achteraf betalen gezien kan worden als een kortlopende kredietverstrekking (project VAK, 2023).

Het fenomeen staat al jaren hoog genoteerd in de lijst van fenomenen die vaak voorkomen binnen de politiesystemen. Ten tijde van het NCB (Bloem & Harteveld, 2019) stond het op de derde plaats en ten tijde van het Cyberintelligencejaarbeeld) van de Inteltafel Cyber (2023) is dat nog niet veranderd.

In 2018 werd ruim duizend keer aangifte of melding gedaan van misbruik accounts voor bestellingen, in 2019 steeg dat naar 2438 en dit verdubbelde in 2020 naar 4811 registraties. In latere jaren trad een geringe daling op, maar de aantallen registraties bleven op een hoger niveau dan de periode 2018-2020 (figuur 12). De cijfers zijn afkomstig uit zowel de Landelijke Cyber Query als de internetaangiften die de politie binnenkrijgt.

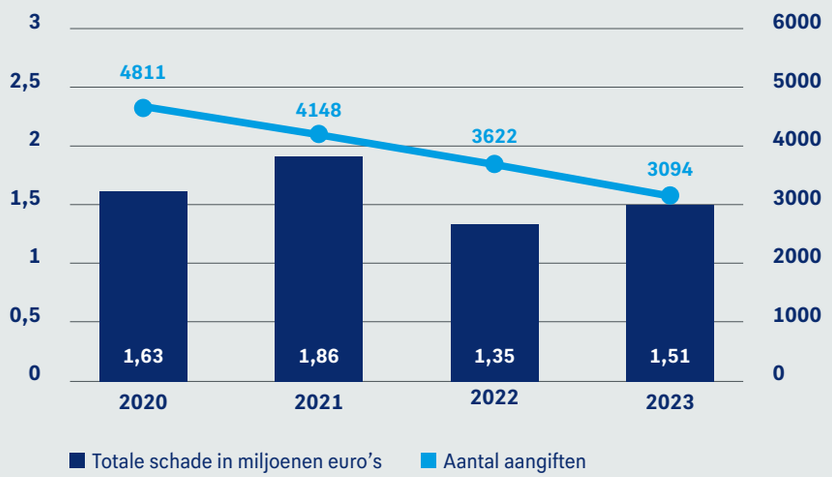
Het misbruiken van accounts beperkt zich echter niet alleen tot het maken van bestellingen op andermans naam of rekening. In het Cyberintelligencejaarbeeld 2022 (Inteltafel Cyber, 2023) wordt bijvoorbeeld ook misbruik van sociale media-accounts geconstateerd. Om in brede zin beter zicht te krijgen op de aantallen en de wijzen waarop accounts worden misbruikt, is vervolgonderzoek noodzakelijk.

De werkelijke aantallen liggen hoger om verschillende redenen. Er wordt in de registratie vaak niet expliciet gesproken over hacking of computervredebreuk, terwijl hier feitelijk wel sprake van is. Uit de registraties blijkt dan dat het account bijvoorbeeld niet meer toegankelijk is voor het slachtoffer: het account is overgenomen en het wachtwoord is veranderd. Of er zijn bestellingen gedaan met iemands account. Verder komt een groot deel van deze delicten niet bij de politie terecht. Deels komt dit door de lage meldingsbereidheid en deels doordat de bedrijven zelf veel tegenhouden.

Tijdens het opstellen van het NCB 2019 (Bloem & Harteveld, 2019) werd dit onder meer bevestigd in informatie van een van de grote postorderbedrijven. Terwijl de politie in 2018 ongeveer 400 registraties had, telde het postorderbedrijf er 4000 in een half jaar tijd. Een groot deel van de meldingen wordt door gedupeerde klanten bij de webshops zelf gedaan, waardoor er vaak geen noodzaak bestaat om ook nog melding te doen bij de politie (voor een schadevergoeding). In het algemeen zijn private partijen vanwege mogelijke imagoschade terughoudend in het doen van uitspraken over de omvang. Daardoor is de totale directe financiële schade lastig te bepalen. Op basis van grove schattingen zou het in 2018 om enkele miljoenen euro’s gaan afgezet tegen de omzet van de miljarden die grote webshops maken.

Figuur 12. Ontwikkeling aantal registraties en totale financiële schade misbruik accounts voor bestellingen

Bron: BVH, BlueIntel



Getroffen bedrijven zien misbruik van accounts als een serieus probleem, waartegen ze continu maatregelen moeten nemen op het gebied van fraudedetectie. In een casus is beschreven dat er op geautomatiseerde wijze miljoenen inlogpogingen werden gedaan, waarvan er 1100 lukten. Deze leidden overigens niet tot frauduleuze bestellingen. Later in het proces werd de fraude toch gedetecteerd en werd voorkomen dat bestellingen konden worden geplaatst. Maar soms zijn de webshops wel tijdelijk hun grip kwijt op het probleem en ontdekken cybercriminelen zwakke plekken in systemen waardoor het aantal account takeovers weer toeneemt (Schuppers, 2018).

In 2020 piekte het aantal registraties van misbruik accounts voor bestellingen en liep het dus in de jaren daarna terug, maar toen nam het aantal gevallen van fraude met bankgegevens/internetbankieren (vooral betaalverzoekfraude en bankhelpdeskfraude) en hulpvraagfraude juist sterk toe. Mogelijk houden dezelfde dadergroepen zich hiermee bezig, en hebben sommige daders de overstap gemaakt naar die andere cybercrimevormen omdat deze (nog) lucratiever zijn. In een van de opsporingsonderzoeken is daadwerkelijk te zien dat daders zich met beide bezighouden en uiteindelijk vooral nog fraude met bankgegevens/internetbankieren plegen. Veelal is hier sprake van het rechtstreeks overmaken van geld van bankrekeningen van slachtoffers, en hoeven hiervoor niet eerst producten te worden verkocht. Bovendien is het plegen laagdrempeliger geworden door Cybercrime-as-a-Service (CaaS) en onderling contact tussen daders over de werkwijzen op platforms als Telegram (project VAK, 2023).

Wat zijn kenmerken van criminele groeperingen?

Jonge daders beginnen vaak met 'uitproberen' van het misbruiken van accounts voor bestellingen en gaan daarin steeds verder. Veelal mislukken bepaalde werkwijzen of worden deze als te riskant gezien, waarna een andere werkwijze wordt geprobeerd. Ook zijn tussen daders veel 'losse verbanden' en ondersteunen ze elkaar vaak tijdelijk bij bijvoorbeeld het uitvoeren van een bepaalde werkwijze of het witwassen van geld, terwijl ze elkaar niet altijd persoonlijk lijken te kennen. Contact vindt dan veelal plaats op een platform als Telegram (Schuppers, 2018; CCT Noord-Nederland, 2020).

Hoewel het in principe mogelijk is om als eenling te opereren, doen maar weinig criminelen dit zonder (technische) ondersteuning of in samenwerking met anderen. De benodigde inloggegevens worden aangekocht op criminele fora op het dark web of via Telegram (CaaS). Daarnaast kunnen daders op Telegram geïnstrueerd worden over het gebruik van methoden – bijvoorbeeld *credential stuffing* - om inloggegevens te stelen. Ook wordt er in sommige gevallen samengewerkt tussen criminelen met verschillende rollen: hackers, oplichters, geldezels, afhalers, ronselaars en facilitators (Schuppers, 2018; CCT Noord-Nederland, 2020). Door deze mogelijkheden is weinig technische kennis vereist om dit delict te kunnen plegen.

Wat zijn de verwachtingen in relatie tot de aanpak?

Tussen 2019 tot 2024 zijn jaarlijks enkele duizenden aangiften bij de politie gedaan, terwijl het werkelijk aantal incidenten waarschijnlijk een tienvoud hoger ligt. Deze blijven echter buiten het zicht omdat ze worden afgewikkeld door de postorderbedrijven en telecomsector zelf.

In 2018 voerde de Eenheid Den Haag in het kader van een thematische aanpak een strategisch onderzoek naar misbruik accounts voor bestellingen uit (Schuppers, 2018)[43], vanwege de aantallen registraties die binnenkwamen. Ten eerste kwam uit dit onderzoek naar voren dat veel incidenten zijn terug te voeren op datalekken, accounts die worden verhandeld op darkweb, phishingmails waar mensen onbedoeld op klikken en het gebruik van zwakke wachtwoorden. Om misbruik van accounts terug te dringen, proberen de getroffen bedrijven allerlei technische oplossingen te bedenken en in te voeren, zoals meer factor-authenticatie, doorlichten van de systemen op zwakheden en training van medewerkers om alert te zijn op phishingmails. Ten tweede bleek dat het structureel doornemen van registraties waarin misbruik accounts voor bestellingen wordt gemeld zowel opsporingsindicaties als inzicht in verdachten opleverde (zoals ook hiervoor beschreven). Op basis van dit onderzoek is een barrièremodel ontwikkeld, dat verder niet geëffectueerd is, omdat de thematische werkwijze werd losgelaten en daarmee ook de thematische aanpak op deze fraudevorm. Hierin lijkt op korte termijn geen verandering te komen. Mocht de belangstelling voor deze fraudevorm op basis van dit hoofdstuk toenemen, komen, dan is het noodzakelijk eerst de actuele stand van zaken in kaart te brengen. Wereldwijd en ook in Nederland lijden bedrijven aanzienlijke schade en de verwachting is dat dit een groot probleem zal blijven.

43 Toen account takeover (ATO) genoemd.

4.10 BEC–fraude (Business E-mail Compromise)

Bij CEO-fraude doet een oplichter zich voor als een hooggeplaatste functionaris, veelal CEO of CFO, van een bedrijf of als voorzitter van een vereniging of stichting. Uit naam van deze functionaris stuurt de oplichter betaalopdrachten naar de afdeling die de financiën afhandelt binnen de organisatie. Bij digitale factuurfraude verschaft de oplichter zich toegang tot een bestaande digitale factuur van een bedrijf, past het bankrekeningnummer aan en stuurt de factuur nogmaals naar de ontvanger vanuit een nagenoeg lijkend e-mailadres (vaak één letter verschil).

BEC – fraude (Business E-mail Compromise) in cijfers

Gemiddeld schadebedrag
per registratie in 2020

€ 63.000

Digitale factuurfraude

9 miljoen

bedrijf wordt gehackt en rekeningnummer op digitale factuur aangepast.

326

Van 120 registraties
in 2020 naar
326 in 2023

CEO-fraude 13 miljoen

oplichter doet zich voor als CEO of voorzitter vereniging en stuurt mail aan financiële afdeling of penningmeester om met spoed (hoog) bedrag over te maken

Gaat om facturen van
partnerbedrijven vaak
gevestigd in het (verre)

buitenland

220

registraties in 2020 en
onveranderd in 2023

De tekst hierna is grotendeels ontleend aan het *Book of Crime* van het Cyberteam van Den Haag (2019) en recentere cijfers die door deze eenheid zijn geleverd. Daarmee zijn de cijfers geüpdatet naar 2023. CEO-fraude en digitale factuurfraude staan bekend onder de naam Business E-mail Compromise (BEC) fraude. In het NCB 2019 (Bloem & Harteveld, 2019) stond dit gecombineerde fenomeen (CEO - en factuurfraude) als één categorie op de vierde plaats in een top 10 van meest voorkomende online fraudevormen. Omdat BEC-fraude tot de fenomenen met de hoogste schadebedragen behoort, wordt in dit hoofdstuk aandacht gevraagd voor CEO-fraude en digitale factuurfraude. BEC-fraude is niet opgenomen in de Veiligheidsagenda.

Hoe heeft het fenomeen zich ontwikkeld?

BEC-fraude is lucratief, omdat de opbrengsten hoog zijn en de kosten minimaal (CCT, Den Haag, 2019). Bij CEO-fraude doet een oplichter zich voor als een hooggeplaatste functionaris, veelal CEO of CFO, van een bedrijf of als voorzitter van een vereniging of stichting. Uit naam van deze functionaris stuurt de oplichter betaalopdrachten naar de afdeling die de financiën afhandelt binnen de organisatie. Of de oplichter vraagt om met spoed iets te halen, zoals cadeaukaarten, waarvan de nummers dan later doorgegeven moeten worden, zodat ze door de oplichters geïncasseerd kunnen worden.

Bij digitale factuurfraude verschaft de oplichter zich toegang tot een bestaande digitale factuur van een bedrijf, past het bankrekeningnummer aan en stuurt de factuur nogmaals naar de ontvanger vanuit een nagenoeg lijkend e-mailadres (vaak één letter verschil). Of de oplichter verzoekt per e-mail om het bankrekeningnummer aan te passen. Het gaat veelal om facturen met grote bedragen die uitgewisseld worden met partnerbedrijven die zijn gevestigd in het buitenland (vaak Azië).

Een variant hierop, die voornamelijk in Nederland speelt, is dat een oplichter zich voordoet als werknemer van een bedrijf en een mail stuurt naar de financiële afdeling met het verzoek om het salaris naar een ander rekeningnummer over te maken (variant salarisdiefstal).

Bioscoopketen opgelicht met CEO-fraude

Casus[44]: Bioscoopketen Pathé is in 2018 slachtoffer geworden van CEO-fraude, waarbij meer dan 19 miljoen euro is buitgemaakt. Criminelen deden zich voor als directeuren van het Franse hoofdkantoor en stuurden e-mails naar de Nederlandse directie met het verzoek om geld over te maken. Zo werd aan de tweekoppige directie gevraagd om 800.000 euro over te maken om een overname in het buitenland te bekostigen, met het dringende verzoek niemand op de hoogte te stellen van de transacties om concurrenten de wind uit de zeilen te nemen. In de mail werd ook verzocht om het contact strikt via de e-mail te laten lopen. De Nederlandse directie van Pathé had twijfels, maar werkte toch mee.

Na de eerste transactie vroegen de oplichters om steeds grotere bedragen. Zo werd er in de tweede transactie bijna 2,5 miljoen euro overgemaakt, in de twee transacties die volgden nog eens 11 miljoen. In een kleine drie weken tijd is bij elkaar een geldbedrag overgemaakt van 19,2 miljoen euro. Omdat er te weinig geld was om over te maken, moest de Nederlandse directie een aanvraag indienen bij een zogeheten cash-pool van het Franse moederbedrijf. Als het echte hoofdkantoor in Frankrijk contact opneemt om te vragen waarom er geld is opgevraagd, wordt duidelijk dat er CEO-fraude is gepleegd.

Beide topfunctionarissen, onder wie de financieel directeur, zijn na de ontdekking van de misser ontslagen. De laatste heeft zijn ontslag aangevochten bij de kantonrechter. Die oordeelde later dat de fraude geraffineerd was en dat de financieel directeur nog enige tijd moest worden doorbetaald. Uit het vonnis kwam naar voren hoe grootschalig de fraude was.

Hoe heeft de omvang zich ontwikkeld?

De aantallen registraties die hierna beschreven worden, zijn afkomstig uit de politiesystemen, maar door verschillende organisatieonderdelen opgesteld. Ofschoon niet bekend is of ze op dezelfde wijze zijn geanalyseerd, kan wel worden afgeleid dat de omvang is gestegen.

Het is lastig om zicht te krijgen op BEC-fraude, omdat de aangifte- en meldingsbereidheid van bedrijven laag is, de incidenten verspreid zijn over de hele wereld en cybersecurity-bedrijven vooral inzicht hebben in de situatie van hun klanten (CCT Den Haag, 2019). Hoewel het beeld over de aard en omvang van BEC-fraude onvolledig is, hebben verschillende instanties en cybersecurity bedrijven gerapporteerd over de omvang van BEC-fraude. Ze spreken over een groeiend probleem. De FBI rapporteerde BEC-fraude in 177 landen (FBI, 2023) en de criminele opbrengsten gingen vooral naar banken in Hong Kong en China, vaak met een tussenstop in Groot-Brittannië. Volgens de FBI werden in 2023 in totaal 21.500 aanvallen in de Verenigde Staten gemeld met een schade van 2.9 miljard dollar (Federal Bureau of Investigation, z.d.). In dit rapport wordt omschreven dat de criminele opbrengsten steeds vaker worden doorgesluisd naar cryptocurrency-rekeningen (waarschijnlijk omdat dit de opsporing bemoeilijkt). Vanwege de omvang heeft de VS dit fenomeen tot prioriteit bestempeld. Het cybersecurity bedrijf Palo Alto Networks meldt op basis van zijn cliëntenbestand dat in 2019 wereldwijd sprake was van bijna 93.000 aanvallen per maand (CCT Den Haag, 2019). In oktober 2020 rapporteert Europol (2020) dat BEC-fraude in een jaar tijd is toegenomen in de EU-lidstaten. Volgens Europol heeft de coronacrisis deze stijging een extra impuls gegeven. Het Economic Crime Survey Nederland (PWC, 2021) meldt cijfers van de financieel-economische criminaliteit waar bedrijven mee te maken hadden. Een groep van 875 respondenten, die binnen bedrijven en andere organisaties in Nederland belast zijn met het in kaart brengen, voorkomen of aanpakken van financieel-economische criminaliteit, gaf gehoor aan de survey. Hiervan gaf 6 procent aan te maken hebben gehad met BEC-fraude.

In de Nederlandse politiecijfers is in de periode 2016-2020 een verdubbeling van het aantal registraties over BEC-fraude te zien. De precieze aantallen zijn niet vermeld. Globaal steeg CEO-fraude van 50 registraties in 2016 naar ongeveer 120 in 2020. Digitale factuurfraude steeg van 160 naar ongeveer 220 registraties. De schade van BEC-fraude bedroeg in totaal

44 Zie: https://nos.nl/artikel/2258662-pathe-voor-19-miljoen-euro-opgelicht-door-nepmails-hoofdkantoor

ruim 17 miljoen euro en het gemiddelde schadebedrag was ruim 63.000 euro (inclusief flinke uitschieters; de mediaan was 15.600 euro) (CCT Den Haag, 2022).

Het Cyberintelligencejaarbeeld (Inteltafel Cyber, 2023) meldt 483 registraties van BEC-fraude in 2022 en dat is een stijging tegen 375 registraties in 2021. De verhouding in 2022 was 51 procent voor CEO-fraude en 49 procent voor digitale factuurfraude. De schade bedroeg in totaal ruim 23 miljoen euro. De stijging in 2022 was deels te herleiden naar de variant 'verzoek aankoop gift cards', welke opkwam in 2021. Het gaat hier om CEO-fraude: de baas verzoekt een werknemer met spoed gift cards (bijvoorbeeld iTunes kaarten) aan te schaffen en de codes van de cadeaukaarten door te geven. In 2020 en 2021 bleek dat stichtingen en verenigingen in toenemende mate slachtoffer waren van CEO-fraude (vooral sportverenigingen). In bijna de helft van de gevallen betrof het doelwit een stichting of vereniging, in 2022 lijkt dit iets terug te lopen. De focus lijkt te zijn verlegd naar (lokale) overheden. In de voorgaande jaren werden (lokale) overheden nauwelijks slachtoffer van CEO-fraude, maar in 2022 was ongeveer 8 procent van de slachtoffers een overheidsinstantie.

BEC-fraude steeg door in 2023 naar in totaal 605 registraties[45], 228 registraties voor factuurfraude en 326 voor CEO-fraude (51 registraties salarisdiefstal). De schade bedroeg ruim 23 miljoen euro: 9 miljoen voor CEO-fraude en 13 miljoen voor factuurfraude. Hoewel de aantallen stijgen ten opzichte van 2022 blijft het schadebedrag op hetzelfde niveau. Het vastleggen en scoren van de schadebedragen is met mitsen en maren omgeven, zoals eerder beschreven. Om uitspraken over de trend te doen, is controle van de verschillende bronnen noodzakelijk. Onder de categorie factuurfraude vallen in BlueIntel namelijk ook valse facturen (zogenaamde spooknota's), die zogenaamd door de belastingdienst en het CJIB zijn verzonden.

Wat zijn kenmerken van criminele groeperingen?

BEC-fraude wordt vooral geassocieerd met Nigeriaanse actoren en groepen. Nigeria wordt al langer geassocieerd met diverse frauduleuze activiteiten, zoals de bekende 419-fraude. Eerder leek het erop dat 90 procent van de criminele groepen vanuit Nigeria opereerde, maar uit recenter onderzoek blijkt dat BEC-actoren zich bevinden in vijftig verschillende landen en nog maar 50 procent van de oplichters Nigeria als basis heeft (ACID, 2020d). Dit heeft mogelijk te maken met het optreden van de Nigeriaanse autoriteiten tegen BEC-fraude en het toetreden tot deze markt van criminele groepen buiten Afrika, zoals de Russische Cosmic Lynx groep. Daarnaast wordt het steeds makkelijker voor nieuwe actoren om zich toe leggen op BEC-fraude, omdat diensten en tools in toenemende mate te koop zijn op ondergrondse markten (Accenture, 2021). Zes procent van de oplichters heeft Europa als basis, waarvan de meesten zich in het Verenigd Koninkrijk bevinden (61%), maar ook een aantal in Nederland (4%). De informatie hierover verschilt. Volgens Europol (2020) opereren criminele groepen die zich bezighouden met BEC-fraude hoofdzakelijk vanuit Oost-Europa, Nigeria en andere Afrikaanse landen. De meer geavanceerde aanvallen komen vooral uit Israël. Accenture (2021) stelt dat daders steeds vaker afkomstig zijn uit Azië, voornamelijk Vietnam en Indonesië (Vemde & van Dam, 2020).

45 Gecontroleerde registraties door Eenheid Oost-Nederland en auteur van dit rapport afkomstig uit BlueIntel.

Wat zijn kenmerken van slachtoffers?

Voor het NCB 2019 (Bloem & Harteveld, 2019) stelde de DRIO van Noord-Holland als themahouder van BEC-fraude een strategische analyse op van het fenomeen (Vemde & van Dam, 2020). Dit leverde het volgende beeld op: criminelen hebben met factuurfraude vooral succes bij kleine en heel kleine bedrijven met respectievelijk minder dan vijftig en minder dan tien werknemers. Bij het MKB is een toename van BEC-fraude te zien, vooral in 2023 en vooral bij garagehouders (project VAK, 2023). CEO-fraude is vooral gericht op de categorie kleinbedrijf, met minder dan 15 werknemers. Slechts 12 procent van de CEO-fraude vindt plaats bij grote bedrijven (met meer dan 250 werknemers). Verhoudingsgewijs lopen grote bedrijven echter meer risico om slachtoffer te worden van CEO-fraude, omdat minder dan 1 procent van de bedrijven in Nederland binnen deze categorie valt. Het gaat in alle gevallen om grote internationale handelsbedrijven. Daarnaast zijn vooral non-profitorganisaties het slachtoffer, zoals stichtingen, verenigingen en kerken. In 2020 was 40 procent van de slachtoffers van CEO-fraude een non-profitorganisatie, waarna het in 2022 weer afnam en lokale overheden vaker slachtoffer leken te zijn (project VAK, 2023).

Wat zijn kenmerken van daders?

De werkwijzen van CEO-fraude en digitale factuurfraude lijken hetzelfde maar verschillen van elkaar. Daardoor kunnen ook daders en dadergroepen per werkwijze verschillen. Het aantal incidenten dat bij de politie bekend is en naar een (mede)dader heeft geleid, is zeer gering. De zaken die zijn opgepakt, hebben in een aantal gevallen geleid naar een katvanger. Om tot de groeperingen achter deze fraudes te komen, moeten vaak sporen bij internationale partijen worden opgevraagd, zoals bankrekeningen bij banken buiten Nederland, IP-adressen in het buitenland en maildiensten in het buitenland. Door de hoeveelheid rechtshulpverzoeken is het lastig voor een opsporingsteam dergelijke zaken op te pakken. Dit is echter niet onmogelijk, mits het opsporingsteam zich richt op (mede)daders en internationaal voldoende partners heeft.

Wat zijn de verwachtingen in relatie tot de aanpak?

De voorgestelde aanpak, overgenomen uit het BOC van het CCT Den Haag (2019), biedt mogelijkheden om BEC-fraude effectief te bestrijden. Deze aanpak is echter tot op heden niet doorgevoerd, omdat het thema niet meer geprioriteerd is binnen de politie.

Preventie en verstoren

Op basis van het crime script is een barrièremodel ontwikkeld. Door het opwerpen van barrières kan het criminele verdienmodel van BEC-fraude worden verstoord. De opzet van het barrièremodel is gebaseerd op de werkwijze van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Per activiteit in het crime script wordt ingegaan op: de indicatoren (de waar te nemen signalen), de gelegenheden (de gelegenheden die het delict mogelijk maken), de barrières (de drempels die partijen kunnen opwerpen) en de partners (de partijen die bij de aanpak nodig zijn). Het gaat niet alleen over een aanpak door de politie, maar ook over de maatregelen die bedrijven kunnen nemen om dit soort incidenten te voorkomen.

Opsporen
Op basis van het crime script zijn de opsporingsmogelijkheden in kaart gebracht[46]. Globaal kunnen de opsporingsmogelijkheden onderverdeeld worden in tactisch onderzoek, analyse, OSINT-onderzoek, digitaal onderzoek en financieel onderzoek. Buiten deze specifieke opsporingsmogelijkheden zijn er algemene kansen om de opsporing te verbeteren. Ten eerste draagt een completer beeld van BEC-fraude bij aan de opsporing. Het zicht op BEC-fraude kan toenemen door de meldings- en aangiftebereidheid te vergroten. Dit kan bevorderd worden door het online melden of aangifte doen mogelijk te maken. Ten tweede is het van belang om BEC-fraude op nationaal en internationaal niveau continu te monitoren en kennis over nieuwe modus operandi voortdurend uit te wisselen met internationale politiepartners. Ten derde is het voor analysedoeleinden van belang om informatie gecategoriseerd weg te zetten, inclusief informatie uit digitaal forensisch onderzoek. Daarmee kunnen incidenten geclusterd worden en kan vergelijkende zaaksanalyse plaatsvinden, zodat duidelijk wordt of een bepaalde dader of –groep in aanmerking komt voor een cluster incidenten. De registratiewijze zou moeten aansluiten bij de gegevens van andere partners, zodat deze gecombineerd kunnen worden. Tot slot is het van belang om internationaal te gaan opsporen om dadergroepen te identificeren en aan te pakken. Te denken valt aan het opzetten van een joint investigation team waarmee het tijdrovende proces van rechtshulpverzoeken om informatie te delen omzeild kan worden.

Uitvoering
Bij het uitvoeren van de interventies zijn er grofweg drie richtingen mogelijk:
- Bewustwording en preventie;
- Het creëren van meer inzicht in het fenomeen BEC-fraude (aard en omvang);
- Opsporing naar (internationale) criminele groepen die zich bezighouden met BEC-fraude.

Er is voor gekozen om vooral in te zetten op bewustwording en preventie en het creëren van meer inzicht in het fenomeen. Opsporing naar (internationale) criminele groepen is complex onder andere door de verschillende internationale uitdagingen. De verwachting is dat met bewustwording en preventie en het verbeteren van inzicht in het fenomeen sneller winst te behalen valt. Indirect is ook de opsporing hierbij gebaat. Door een completer beeld van het fenomeen BEC-fraude zullen zich zeer waarschijnlijk meer kansen voordoen in het opsporingsproces.

46 Deze gelden in grote lijnen voor alle online fraudevormen.

Overeenkomsten in werkwijzen

In dit gedeelte worden een aantal kenmerken besproken die in vrijwel alle vormen van online fraude terugkomen. Er is gekozen om deze niet afzonderlijk per fraudevorm te bespreken maar gezamenlijk over de verschillende vormen heen. De volgende kenmerken komen aan bod: georganiseerdheid en criminele groeperingen, social engineering, de inzet van geldezels en het witwassen van criminele opbrengsten.

Overeenkomsten in werkwijzen

Social engineering

speelt in alle
fraudevormen een rol

Weinig zicht

op witwassen
criminele opbrengst

Vaste kern

van enkele leden met een
flexibele schil (fluïde structuur)

Wel een hiërarchie,
rolverdeling en
onderlinge afspraken

Criminele groeperingen opereren landelijk

Gaat om lokale groepen
waarvan de leden elkaar
al jaren kennen

Geldezels

zijn essentieel bij
het verplaatsen van
de criminele opbrengst

Geldezelnetwerken

kennen verschillende rollen,
zoals ronselaar of prepper

Criminele opbrengst

vooral besteed aan leefgeld,
meestal statusverhogende
goederen

Georganiseerdheid en criminele groeperingen

Op basis van opsporingsonderzoeken en dossiers wordt een beeld geschetst van de werkwijzen die in verschillende online fraudevormen terugkomen. Het gaat specifiek om de samenwerking, structuur en samenstelling van de criminele groeperingen die deze delicten plegen. Deze kenmerken zijn gevonden in opsporingsonderzoeken naar groepen die actief zijn met (bank-) helpdeskfraude, hulpvraagfraude en phishing, maar ze gelden ook breder. Zo komen in de crimescripts die door project VAK zijn opgeleverd, dezelfde kenmerken terug in andere online fraudevormen, zoals aan- en verkoopfraude, misbruik accounts voor bestellingen en BEC-fraude.

Het ging in de opsporingsonderzoeken om georganiseerde groeperingen en ze pleegden gedurende een langere periode online fraude. Deze groepen bestonden meestal uit minstens drie leden, wat ook nodig is om deze fraudevormen grootschalig en effectief te kunnen plegen. De personen binnen die groepen kenden elkaar vaak al jaren. Ze beperkten zich niet tot het plegen van een enkele fraudevorm, maar waren naast bijvoorbeeld bankhelpdeskfraude ook actief met hulpvraagfraude of betaalverzoekfraude. Ze pleegden in verschillende samenstellingen deze verschillende (fraude)delicten. Voor uitbreiding van de groep of het vervangen van leden, zoeken de kernleden vooral binnen de eigen (vertrouwde) kring van vrienden en bekenden. De meeste groepen die in beeld komen, hebben over een periode van enkele maanden tientallen tot (enkele) honderden slachtoffers gemaakt.

De structuur van de groeperingen is vaak als fluïde te typeren. Dit houdt in dat er een vaste kern is van enkele leden met daaromheen een losse groep van faciliteerders en uitvoerders, zoals bellers, phishers, ophalers of geldezels. Binnen de criminele groepen bestaat een duidelijke rolverdeling waarbij verschillende groepsleden een te onderscheiden bijdrage leveren aan het plegen van het delict. Tussen de verschillende rollen bestaan duidelijke hiërarchische verhoudingen, waarbij uitvoerende rollen worden aangestuurd door rollen die vooral coördineren (kernleden). Deze coördinatoren zorgen dat de samenwerking binnen de groep goed verloopt door de noodzakelijke voorbereidingen te treffen en duidelijke afspraken te maken over de uitvoering.

Onder dergelijke voorbereidingen kunnen verschillende zaken worden geschaard. Een voorbeeld is het tijdig regelen van leads. Leads zijn lijsten met persoonlijke gegevens van potentiële slachtoffers die bijvoorbeeld op Telegram worden verkocht voor criminele doeleinden. Het vermoeden bestaat dat dergelijke (bel)lijsten met persoonlijke gegevens illegaal verkregen zijn uit de callcenterwereld (project VAK, 2022) of afkomstig uit hacks van computers en bedrijven, bijvoorbeeld van de klantenadministratie. Binnen de opsporingsonderzoeken varieert
de hoeveelheid gegevens in deze leadslijsten van enkel naam en telefoonnummer tot lijsten met veel meer persoonlijke informatie, zoals geslacht, naam, adres, woonplaats, telefoonnummer (vast en 06), e-mailadres, geboortedatum en bankgegevens. Afhankelijk van de online fraudevorm worden slachtoffers meer of minder gericht benaderd en zijn meer of minder gegevens nodig. Zo is voor het versturen van een phishingmail of -sms alleen een naam en e-mailadres of telefoonnummer al voldoende, maar hebben groeperingen bij het plegen van bankhelpdeskfraude behoefte aan meer persoonlijke gegevens.

De leden van de groeperingen maken onderlinge afspraken met elkaar. Deze afspraken zijn nodig om duidelijkheid te verschaffen over de uitvoering van het delict en om de criminele activiteiten af te schermen. In de onderlinge communicatie vermijden groepsleden zoveel mogelijk telefoongesprekken en communiceren vooral via sociale media-apps, zoals Telegram en Snapchat, of via nog veiliger geachte chat apps als Wickr en Signal. Communicatie met slachtoffers verloopt vaak via Voice over IP (VOIP)[47] met encryptie en nummer-spoofing, of via simkaarten die regelmatig gewisseld en vernieuwd worden, soms met gebruik van buitenlandse simkaarten en oudere telefoons die gegevens alleen op de simkaart opslaan. Alle *devices* (laptops, telefoons) worden uitsluitend voor criminele activiteiten gebruikt.

Tot slot is er binnen de criminele groeperingen, ondanks de fluïde samenstelling, vaak sprake van hiërarchische verhoudingen, zoals hiervoor ook geschetst is. Dit is af te leiden uit de aansturing van de diverse rollen binnen de uitvoering (instructies coördinator), en een deel te herleiden uit sancties die opgelegd kunnen worden. Zo zijn er indicaties dat de ‘lagere rangen’ (rollen) bij misstappen verantwoording moeten afleggen aan de ‘hogere rangen’, bijvoorbeeld door het inleveren van paspoorten, autosleutels en geld.

Social engineering

Social engineering is een techniek waarbij oplichters psychologische manipulatie gebruiken om potentiële slachtoffers te misleiden, om zodoende vertrouwelijke informatie afhandig te maken of toegang tot systemen te krijgen. Deze misleiding vindt zowel online als offline plaats en kan zeer geraffineerd zijn. Verschillende overtuigingsprincipes worden ingezet, waarmee de oplichters inspelen op menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. *Social engineering* is gangbaar binnen tal van vormen van online fraude met het doel om slachtoffers actief te laten meewerken aan acties die nadelig voor hen uitpakken. Hierbij is aan het volgende te denken.

Bij verschillende telefonische helpdeskfraudes spelen de oplichters in op angst en onwetendheid door te suggereren dat er verdachte activiteiten op de rekening of computer zijn geconstateerd. Degene die belt doet zich daarbij voor als een fraude- of IT-expert, wat de beller autoriteit verschaft, en biedt aan om de problemen te verhelpen (sympathie). Hierdoor is het slachtoffer eerder geneigd mee te werken. Bij aan- en verkoopfraude plaatsen de oplichters veel nepgetuigenissen en valse positieve recensies op valse webshops om potentiële slachtoffers te overtuigen dat ze te maken hebben met een betrouwbare website (conformiteit). Bij aankoop van vooral luxeproducten houdt de oplichter nog een poosje contact met het slachtoffer om tijd te rekken om (nog) geen argwaan te veroorzaken. Bij beleggingsfraude spelen de oplichters in op angst om hoge rendementen mis te lopen (*fear of missing out*), bijvoorbeeld op beleggingen in aandelen, *non-fungible tokens* (NFT’s), bitcoins of andere cryptomunten. Naast (zelfbenoemde) experts die hoge winsten garanderen, plaatsen ze op sociale media ook vaak advertenties met beroemdheden om mensen over te halen snel rijk te worden (autoriteit). Bij bankphishing of smishing[48] komt er vaak een kort bericht van een vertrouwde partij (bank, overheid) om met behulp van een link snel ergens actie op

47 Bijlage 4, woordenlijst

48 Bijlage 4, woordenlijst

te ondernemen, zoals het aanvragen van een nieuwe pas of het bevestigen van de identiteit (autoriteit, schaarste). Tot slot is de truc bij sextortion vooral wederkerigheid. De oplichter stuurt eerst zelf (zogenaamd eigen) beelden om het slachtoffer over te halen om ook beeldmateriaal te delen. Het slachtoffer is dan eerder geneigd dit te doen.

Inzet geldezels

Een geldezel of crypto-ezel is een persoon die (al dan niet bewust) zijn of haar bankrekening, pinpas of crypto-wallet laat gebruiken voor criminele doeleinden. Geldezels spelen een cruciale rol in verschillende soorten online fraude door als tussenschakel te dienen voor het verplaatsen van gestolen of frauduleus verkregen geld. Hierdoor verhullen ze de sporen naar de daadwerkelijke criminelen en de herkomst van het geld. Uit Nederlands onderzoek blijkt dat geldezels kunnen verschillen in achtergrond, maar een gemeenschappelijk kenmerk is dat ze allemaal gemakkelijk te beïnvloeden zijn. Dit zijn bijvoorbeeld jongeren, nieuwkomers in het land, werklozen, mensen met schulden, een drugsverslaving of een licht verstandelijke beperking. Soms worden ze onder druk gezet, gemanipuleerd of bedreigd met geweld (Leukfeldt, 2020).

Rondom de inzet van geldezels en hun rekeningen zijn meestal meerdere personen betrokken. Dit kunnen bijvoorbeeld personen zijn die aspirant-geldezels benaderen in de buurt of online via Snapchat of Instagram (rol ronselaar). Wanneer iemand wordt geronseld als geldezel, dan kan er sprake zijn van criminele uitbuiting. Daarnaast komen personen naar voren die het buitgemaakte geld van de ene geldezelrekening overmaken naar de andere (rol gooier). Voorafgaand aan deze transacties zijn de rekeningen al zo geprepareerd dat de oplichters beveiligings- en detectiemaatregelen bij de betreffende banken en betaalplatformen gemakkelijk omzeilen (rol prepper). Door betrokkenheid van deze en andere rollen wordt ook wel gesproken van geldezelnetwerken (project VAK, 2023). In vrijwel alle vormen van online fraude die in dit rapport zijn besproken is de inzet van geldezels te zien (en geldezelnetwerken) om direct luxe goederen te kopen, geld te cashen, te verplaatsen of wit te wassen.

Witwassen van criminele opbrengst

Dit deel gaat uitgebreid in op het witwassen van de criminele opbrengsten van online fraude en geeft een beeld over de manieren waarop deze winst wordt besteed, weggesluisd of geïnvesteerd. Daarnaast wordt besproken welke witwascategorieën - en vormen het meest worden ingezet. Het beeld is vooral gebaseerd op een analyse op bankhelpdeskfraude, maar is representatief voor (veel) andere online fraudevormen waarin dezelfde methoden worden toegepast. In de analyse wordt zoveel mogelijk het National Risk Assessment Witwassen van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) gehanteerd als onderliggende methodiek (van der Veen & Heuts, 2024). Hierin wordt rekening gehouden met de verschillende redenen (doelen) die achter het witwassen van de criminele opbrengst kunnen zitten. Deze doelen kunnen grofweg worden onderverdeeld in drie categorieën: leefgeld, bedrijfskosten en investeringen. Voor de resultaten uit de analyse is informatie gebruikt uit zowel opsporingsonderzoeken, dossieranalyse als verdachte transacties bij de Financial Intelligence Unit Nederland (FIU-Nederland). Meer details van de analyse zijn in bijlage 3 terug te vinden.

Besteding criminele opbrengst

Uit de politiegegevens komen drie soorten bestedingen naar voren, te weten statusverhogende uitgaven, crypto en crimineel startkapitaal.

De eerste categorie uitgaven betreft de aanschaf van statusverhogende producten. Een groot deel van de criminele opbrengst wordt uitgegeven aan luxe of statusverhogende goederen, zoals horloges, sieraden, (designer)kleding, reizen, hotels, casinobezoek, telefoons en laptops. Een belangrijk deel van deze aankopen is bestemd om door te verkopen of om te zetten in spullen die geld opleveren. Zo blijken aangeschafte telefoons na doorverkoop te worden aangeboden via een reguliere verkoper op grote online warenhuizen (Inteltafel cyber, 2023).

Naast het hebben van luxe goederen geeft het bezitten van contant geld ook status aan deze groep(en), zo is gebleken uit opsporingsdossiers. Bij de aankoop van luxe items in fysieke of online (elektronica) winkels, wordt de criminele herkomst van het geld altijd verhuld door hetzij een pinbetaling of overschrijving te koppelen aan de rekening van een geldezel of slachtoffer, hetzij met cash of anonieme prepaid betaalkaarten (zoals cadeaukaarten of prepaid creditcards) af te rekenen. Een deel van de criminele opbrengsten wordt weggesluisd naar anonieme prepaidkaarten om tegoeden te krijgen. Het ophogen van tegoeden of aankoop van tegoedkaarten gebeurt meestal direct vanuit de rekeningen van slachtoffers of geldezels. Met deze kaarten worden betalingen gedaan, maar ze kunnen ook worden doorverkocht via Telegram of fora op het darkweb (project VAK 2023).

De tweede categorie uitgaven betreft de aanschaf van verschillende cryptovaluta. Veel groeperingen besteden hieraan een deel van de criminele opbrengsten.[49] Meestal betreft het bitcoins, maar in mindere mate ook andere cryptomunten zoals ethereum, dogecoins, binance coins of cardano. De aanschaf gebeurt vaak via bekende handelsplatforms, waar onder andere cryptovaluta worden aangeboden, verkocht en opgeslagen. Op de (online) wallets waar de aangeschafte cryptomunten in eerste instantie terechtkomen (vaak op naam van een slachtoffer)[50], blijven deze bedragen over het algemeen niet lang staan. De oplichters sluizen de cryptovaluta door naar verschillende andere wallets (bijvoorbeeld van crypto-ezels) of op rekeningen van de criminelen. Ze maken soms ook gebruik van een mixerdienst, ook wel cryptocurrency-tumblers genoemd (project VAK, 2024)[51].

Het is niet helemaal duidelijk wat de belangrijkste drijfveren zijn achter de aankoop van cryptovaluta. Voor een deel vinden criminelen dit mogelijk een interessante investering. De aankoop hiervan en het meermaals overboeken en omzetten kan ook bedoeld zijn om de herkomst en de bestemming van het geld achter de cryptovaluta te verhullen. Dit verklaart waarschijnlijk ook de vele financiële dienstverleners met buitenlandse rekeningen (IBAN) die op de telefoons van de criminelen worden aangetroffen.

49 Bij bijna 35 procent van alle verdachte transacties gekoppeld aan verdachten van bankhelpdeskfraude, komen betalingen naar handelsplatforms voor waarmee cryptovaluta wordt aangekocht (Zie bijlage 3.5).

50 Bij verschillende aangiften van online fraude (bijvoorbeeld bij bankhelpdeskfraude) blijken de criminelen met behulp van informatie (IDs en selfies) van nietsvermoedende slachtoffers wallets (accounts) op hun naam te hebben geopend.

51 Bijlage 4, woordenlijst.

Tot slot zien zijn er signalen dat de criminele opbrengst wordt gebruikt als startkapitaal om andere delicten te kunnen financieren of om onroerend goed aan te kopen in het buitenland. Zo zijn er zaken bekend waarbij daders zich inkochten in de cocaïnehandel (project VAK, 2024).

Verdachte transacties

Het bovenstaande overzicht naar bestedingsvormen is afkomstig uit de opsporingsdossiers. Hierna wordt een beeld gegeven van de witwasvormen die we het meest zien gebaseerd op een analyse van FIU-gegevens, waarin alle betreffende verdachte transacties (VT's) zijn gekoppeld aan verdachten van voornamelijk bankhelpdeskfraude (periode 2019 - 2023) (zie voor uitgebreide uitleg bijlage 3).

Uit deze analyse blijkt dat witwassen het meest frequent voorkomt via de volgende methoden:
1. Girale transacties bij vergunde banken
2. Stromannen, geldezels of geldezel
3. Contante transacties/stortingen bij vergunde banken
4. Payment Service Providers (PSP's)
5. Aanbieders van financiële cryptodiensten

Deze uitkomst kan deels worden verklaard aan de hand van de modus operandi van de criminele groepen en de wijze waarop verdachten buiten het zicht van opsporingsinstanties of de monitoring van banken proberen te blijven. Zo zijn bijvoorbeeld het overboeken of pinnen van geld via verschillende rekeningen op naam van geldezels (of slachtoffers) onlosmakelijk verbonden met de uitvoering (methode 1, 3 en 2). Daarnaast zien we dat verdachten een deel van de criminele opbrengsten investeren in cryptovaluta of gebruiken om spullen te kopen bij webwinkels (zoals giftcards en telefoons), wat vaak via PSP's verloopt (methode 5 en 4).

Samenvattend is er binnen online fraudevormen beperkt zicht op de wijze waarop geld wordt witgewassen. Over het algemeen zijn de meeste incidenten van witwassen onder het doel leefgeld te scharen. Dit gebeurt in de vorm van aankopen van luxe spullen (telefoons, merkkleding), die voor een deel onder de meldgrens[52] of volledig buiten zicht blijven. Bedrijfskosten om online fraude te kunnen (blijven) plegen, komen nauwelijks naar voren in de verdachte transacties, en de bedragen die hierin omgaan zijn ook beperkt in vergelijking met andere delicten (zoals grootschalige drugshandel of productie). Ze beperken zich vooral tot het 'salaris' van criminele medewerkers, het inhuren van facilitators (ophalers, geldezels) en de aankoop van phishingkits, leads en belscripts. Tot slot zijn er enkele indicaties dat de oplichters de criminele opbrengsten investeren, bijvoorbeeld in onroerend goed of als startkapitaal voor andere criminele activiteiten (project VAK, 2024).

52 In Nederland moeten financiële instellingen en andere meldingsplichtige organisaties ongebruikelijke transacties melden aan de Financial Intelligence Unit (FIU-Nederland) volgens de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Enkele objectieve meldgrenzen hiervoor zijn bijvoorbeeld contante betalingen boven de 10.000 euro of transacties met een creditcard of prepaid betaalkaart van meer dan 15.000 euro. Zie: https://www.fiu-nederland.nl/home/meldergroepen/

6

Niet-financiële gevolgen voor slachtoffers

Online fraude veroorzaakt niet alleen financiële schade, ook de niet-financiële gevolgen zijn aanzienlijk. Slachtoffers ontwikkelen vaak psychische en emotionele klachten, die behalve op henzelf ook vaak een grote impact hebben op hun directe omgeving.[53] De persoonlijke gevolgen van dergelijke online delicten worden nog vaak onderschat en daardoor kan niet goed worden ingespeeld op de behoeften die deze slachtoffers aan nazorg of begeleiding hebben. Hierna worden de niet financiële gevolgen voor slachtoffers in algemene lijnen uitgewerkt en niet specifiek beschreven voor de verschillende fraudevormen.

Emotionele en psychische gevolgen

Volgens de Veiligheidsmonitor (CBS, 2024) en het rapport online veiligheid en criminaliteit 2022 (CBS, 2023) ervaart een vijfde tot een kwart (24%) van de slachtoffers van online criminaliteit emotionele, psychische of financiële problemen. Online bedreiging en intimidatie (zoals sextortion) veroorzaken de meeste problemen (33%). Slachtoffers van online oplichting en fraude geven in bijna een op de vier gevallen (23%) aan problemen te hebben ervaren.

Wanneer financiële en emotionele of psychische gevolgen afzonderlijk worden bekeken, valt op dat slachtofferschap van online criminaliteit vaker leidt tot emotionele of psychische problemen dan tot financiële problemen. Vooral bij online bedreiging en intimidatie is dit verschil relatief groot (30% tegen 7%). Dit is niet verwonderlijk aangezien hier niet altijd een financieel motief aan ten grondslag ligt. Opvallender is dat ook binnen de categorie online oplichting en fraude meer slachtoffers emotionele of psychische problemen rapporteren (17% tegen 11%).

Veel slachtoffers melden een verminderd vertrouwen in mensen (37%) en een verminderd gevoel van veiligheid (30%). Slaapproblemen, depressieve klachten, angstklachten en herbelevingen van het incident komen voor bij 7 tot 8 procent van de slachtoffers. Vooral deze laatste emotionele of psychische problemen worden door slachtoffers van online bedreiging en intimidatie vaker gerapporteerd (rond de 16%).

Vergelijking tussen traditionele en online criminaliteit

In verschillende onderzoeken is de impact van online fraude vergeleken met vormen van traditionele criminaliteit, bijvoorbeeld vormen die qua impact vergelijkbaar zouden moeten zijn, zoals de babbeltruc en bankhelpdeskfraude, en woninginbraak en het online hacken van een account voor internetbankieren. (Borwell et al., 2023; Bluhm et al., 2022). De impact omvat de psychische gevolgen zoals angst, depressie, boosheid, financiële problemen en aantasting van het zelfbeeld. De resultaten laten zien dat verschillende vormen van online criminaliteit, zoals bankhelpdeskfraude, phishing of sextortion, qua impact niet onderdoen voor traditionele criminaliteit, zoals babbeltruc en inbraak.

De gevolgen van sommige online fraudevormen en traditionele criminaliteit zijn vergelijkbaar, zeker wanneer er financiële consequenties zijn. Slachtoffers ervaren tijdsverlies, het verlies van werk en het niet kunnen nakomen van contractuele afspraken. Vergelijkbare emo-

53 Bredere maatschappelijke gevolgen zoals het verlies van vertrouwen in het betalingssysteem of in de medemens worden in dit deel buiten beschouwing gelaten.

“

‘Kleindochter kwam binnen,
oh oma u bent opgelicht’

‘daarna ging het zo slecht,
ik werd iedere nacht wakker,
hoorde steeds die stem
‘nu mevrouw, nu actie ondernemen’,
dat zelfverwijt knaagt zo verschrikkelijk’

tionele en psychische gevolgen omvatten verminderd vertrouwen in anderen en gevoelens van machteloosheid, maar ook schaamte, verdriet, stress, eenzaamheid en woede (Leukfeldt, Notté & Malsch, 2018).

In sommige opzichten is de impact van online delicten zelfs groter. Een belangrijke verklaring hiervoor is dat slachtoffers vaak niet precies begrijpen wat hen is overkomen. Ze blijven zitten met het gevoel dat ze actief hebben meegewerkt aan het delict, wat leidt tot zelfverwijt (*self blame*) of het gevoel dat hun omgeving hen verwijten maakt (*victim blaming*). Slachtoffers van online fraude en andere online delicten hebben daarom behoefte aan duidelijkheid over hoe het delict heeft kunnen plaatsvinden, zowel om het beter te kunnen verwerken als om herhaling in de toekomst te voorkomen (Borwell et al., 2021).

Een bijkomend gevolg en verschil met traditionele criminaliteit kan zijn dat slachtoffers zich niet altijd serieus genomen voelen door de politie. Ook kan de impact langer duren bijvoorbeeld door het gemak van het verspreiden van seksueel beeldmateriaal, moet het slachtoffer leven met de gedachte dat de beelden blijven rondzwerven en later weer opduiken. Deze angsten blijven lang bestaan en gaan gepaard met depressie, een verlaagd zelfvertrouwen en verlies van vertrouwen in anderen. Daarnaast is reputatieschade een belangrijk gevolg. Ook voor andere delicten geldt dat de gevolgen kunnen aanhouden, zoals een frauduleuze webshop die blijft bestaan. Of de stalker die maar doorgaat met online activiteiten, waardoor gevoelens van paranoia en angst kunnen ontstaan. Een belangrijk verschil tussen online fraude en traditionele delicten is dat de gevolgen van online criminaliteit grenzeloos in tijd, ruimte en publiek kunnen zijn (Leukfeldt et al., 2018).

Gezinsimpact en veiligheidsgevoelens

De impact van online fraude beperkt zich niet alleen tot de directe slachtoffers, maar heeft vaak ook een grote invloed op gezinnen en families. Dit is afhankelijk van de hoeveelheid buitgemaakt geld, of er vergoeding van het verloren geld heeft plaatsgevonden, en wat het overgebleven vermogen is. Vaak is er sprake van dubbele impact, niet alleen verwijten de slachtoffers zichzelf dat ze hebben meegewerkt aan de oplichting, ook de sociale omgeving begrijpt het niet altijd en kan zodoende het slachtoffer medeverantwoordelijk houden voor de gevolgen (Leukfeldt et al., 2018).

Verder kan door een nieuwe werkwijze de impact van een delict veranderen. Zo is bijvoorbeeld in 2022 de pas-ophaalvariant binnen bankhelpdeskfraude sterk opgekomen. Hierbij komen daders ook fysiek langs op het thuisadres van de slachtoffers om de betaalpassen op te halen. Het is goed voor te stellen dat deze hybride variant met zowel online als fysieke elementen een andere (extra) impact heeft op de veiligheidsgevoelens van burgers en hun psychisch welbevinden.

7

Toekomstige ontwikkelingen

In dit deel wordt ingegaan ontwikkelingen die de komende jaren van invloed zijn op online fraudevormen. Hierbij moet worden aangetekend dat de toekomst lastig is te voorspellen, evenals precies bepalen welke technologische, economische of politieke ontwikkelingen (veel) impact gaan hebben. Dit gezegd hebbende worden hieronder twee ontwikkelingen beschreven waarvan wordt verwacht dat deze van invloed zullen zijn, namelijk generatieve artificiële intelligentie (AI) en de intensivering van de aanpak van online fraude. We hebben ervoor gekozen om deze ontwikkelingen in een overkoepelend hoofdstuk op te nemen, omdat de impact ervan niet beperkt is tot één fraudevorm. Ze zullen daarom eerst algemeen worden beschreven en waar mogelijk worden aangevuld met voorbeelden van de impact op een specifieke fraudevorm.

Generatieve AI

Op 19 april 2024 overleed Daniel Dennett, Amerikaans hoogleraar filosofie gespecialiseerd in vraagstukken over het bewustzijn, de filosofie van de geest en de laatste jaren ook in kunstmatige intelligentie. Hij waarschuwde de laatste jaren van zijn leven aanhoudend en dringend voor de gevolgen van kunstmatige intelligentie, omdat het bewustzijn voor de gevaren ervan ontbreekt en daardoor de noodzaak om er iets aan te doen. Als gevolg van kunstmatige intelligentie wordt het vertrouwen in onze maatschappij ondermijnt, omdat het mogelijk is om mensen te vervalsen, die voor echt kunnen doorgaan in de door ons gecreeerde digitale omgevingen. Omdat, zegt hij, en dat is de kern van het succes van fraude in het algemeen, mensen geloven in alles wat in redelijke en geloofwaardige taal tegen ons aan praat en dit kunnen zij dus niet weerstaan. Spoedig zal het niet meer mogelijk zijn te zeggen of je familie of vrienden echt zijn als ze je online benaderen. Dennett stelt niet alleen dat hoogwaardige technologie moet worden ontwikkeld om dit te voorkomen of op te sporen, maar ook zware bestraffingen en het verantwoordelijk stellen van de techbedrijven die dit faciliteren (Dennett, 2023).

Generatieve AI is een vorm van kunstmatige intelligentie (AI) die op basis van een (menselijke) vraag of opdracht met behulp van algoritmen nieuwe, originele inhoud creëert, zoals een tekst, afbeelding of video. Dergelijke door de computer gegenereerde afbeeldingen of andere inhoud wordt ook wel synthetische media genoemd (project VAK, 2023). Hoewel de manipulatie van beelden of andere media niet nieuw is, denk aan programma's zoals Photoshop, worden door AI de mogelijkheden om beeldmateriaal te manipuleren steeds beter, gebruiksvriendelijker en toegankelijker. Voorbeelden van breed beschikbare, (deels) gratis of populaire generatieve AI-toepassingen zijn chat GPT of Gemini (voor tekst), DALL-E of Midjourney (voor afbeeldingen) en Vidnoz (voor video). De technieken achter deze en andere toepassingen ontwikkelen zich snel, wat onder meer blijkt uit de steeds betere kwaliteit van de gegenereerde media. Het gebruik van deze toepassingen zal daarom de komende jaren alleen maar toenemen en experts verwachten dat in 2025 90 procent van de digitale content synthetisch is. Ze spreken dan ook van een 'post truth' tijdperk, omdat echte inhoud niet meer te onderscheiden is van synthetische (van der Sloot & Wagensveld, 2022).

Op dit moment worden de genoemde voorbeelden (en soortgelijke) AI-toepassingen breed gebruikt voor verschillende (legale) doeleindes. De techniek biedt een heleboel nieuwe creatieve mogelijkheden. Aan de ene kant biedt het voor criminelen ook gelegenheid tot misbruik, bijvoorbeeld om mensen te misleiden. Aan de andere kant kan de opsporing van criminaliteit ook profijt hebben van AI-toepassingen (project VAK, 2023). Aangezien geen hoog kennisniveau nodig is, zullen deze tools de komende jaren vermoedelijk veelvuldig worden ingezet om nieuwe of meer effectieve criminele plannen te bedenken en uit te voeren (DRIO Eenheid Limburg, 2023; Schuilenburg & Soudijn, 2023).

Vooral *deep fakes* (een samentrekking van de woorden *deep learning* en *fakes*) lijken zorgen te baren en worden gezien als de grootste dreiging voor de veiligheid. Met behulp van *deepfaketechnologie* kunnen bestaande afbeeldingen en bewegende beelden gecombineerd worden en over elkaar heen gezet. Met behulp van AI kunnen zo compleet nieuwe beelden worden gegenereerd die met het blote oog niet of nauwelijks van echt zijn te onderscheiden. Hierdoor lijkt het alsof iemand iets zegt of doet, wat in werkelijkheid nooit is gebeurd (Schuilenburg & Soudijn, 2023). Voor het ontwikkelen en gebruiken van overtuigende *deepfakes* is over het algemeen wel wat meer expertise nodig, al wordt ook hier de drempel snel lager. Niet elke (cyber)crimineel heeft hier voldoende affiniteit mee, en tegelijkertijd zijn er veel criminelen die interesse hebben in de mogelijkheden ervan. Bij een deel van de criminelen zal daarom een behoefte bestaan voor Deepfake-as-a-Service diensten, zoals ook voor andere cybercrimevormen bestaan (Cybercrime-as-a-service, Ransomeware-as-a-service). Deze diensten zijn al te vinden. Zo meldt Europol dat er speciale online handelsplaatsen zijn waar klanten een verzoek kunnen doen voor onder andere *deepfake* video's en daarnaast zijn er ook steeds meer bronnen beschikbaar die op maat gemaakte diensten en tutorials aanbieden voor synthetische visuele en audio technologie om beveiligingsmaatregelen te omzeilen (project VAK, 2023).

De inzet van verschillende synthetische media zullen het voor criminelen mogelijk maken om hun succesfactor aangaande online fraude te vergroten, tezamen met toepassingen op het gebied van *social engineering* (project VAK, 2023). Dit kan op verschillende manieren plaatsvinden. Zo kunnen in verschillende deepfakes (foto's, video's of voiceberichten) stemmen of afbeeldingen van een familielid, collega of leidinggevende worden verwerkt om potentiële slachtoffers over te halen. De oplichters zoeken internet af op zoek naar eerder gedeelde foto's of video's uit openbare profielen op sociale media. Daarmee kunnen ze een zoon, dochter of vader een verhaal laten vertellen, waarin hij of zij in (financiële) nood verkeert, of een leidinggevende een voicebericht laten sturen aan zijn werknemer met de boodschap dat een belangrijke betaling nog even snel gedaan moet worden. Dit kan leiden tot veel meer slachtoffers van hulpvraagfraude of CEO-fraude.

Het ligt ook in de lijn der verwachting dat met AI nog betere phishingmails en -sms'jes kunnen worden gegenereerd. Op termijn kan hierdoor een opleving van bijvoorbeeld betaalverzoekfraude of smishing ontstaan. Het gebruik van deepfakes verbreedt ook de mogelijkheden om sextortion te plegen. Hiervoor hoeft een dader (in theorie) geen echte naaktbeelden meer te bemachtigen om het slachtoffer mee af te persen. De oplichters maken synthetische beelden en plaatsen bijvoorbeeld het hoofd van een slachtoffer op een willekeurig seksueel getinte foto of video. Deze zijn realistisch genoeg voor slachtoffers om verspreiding te willen voorkomen. Dit maakt het relatief eenvoudig om meer slachtoffers op deze wijze af te persen[54]. Tot slot ligt het binnen helpdeskfraude voor de hand dat nieuwe overtuigende belscripts worden ontwikkeld.

Bovenstaande voorbeelden gaan vooral in op de vormen van online fraude die in dit rapport centraal staan. De komende jaren zal generatieve AI niet alleen van invloed zijn op al bestaande vormen, maar zal ook leiden tot nieuwe (online) fraudevormen die nu nog niet of nauwelijks voorkomen. Wat AI in de toekomst gaat betekenen voor de aard en omvang van online fraude blijft dan ook lastig te voorspellen. Hoe dan ook kan het gebruik van AI door criminelen worden gezien als een volgende stap in de digitalisering van criminaliteit (Schuilenburg & Soudijn, 2023).

54 Dit lijkt in opkomst in de Verenigde Staten. De FBI waarschuwde al eerder voor deze vorm van afpersing, en meldde een sterke stijging in het aantal deepfake sextortion gevallen in de VS sinds medio 2023. Zie: https://www.ic3.gov/Media/Y2023/PSA230605

AI & online fraude

De komende jaren zullen criminelen generatieve AI toepassen om bestaande vormen van online fraude verder te ontwikkelen. Het gebruik van AI zal waarschijnlijk ook leiden tot nieuwe fraudevormen.

Ruim 23 miljoen euro buitgemaakt met deepfake

Het gebruik van generatieve AI in de uitvoering van gedigitaliseerde criminaliteit is niet alleen toekomstmuziek. Vooral internationaal zijn al verschillende incidenten naar voren gekomen. Een voorbeeld is een CEO-fraude uit begin 2024 waarin het Britse ingenieurs- en ontwerpbureau Arup, bekend van het Sydney Opera House, via een deepfake is opgelicht. Ze betaalden omgerekend maar liefst 23,5 miljoen euro[55].

De medewerker in kwestie werd uitgenodigd voor een videogesprek met verschillende stafleden waaronder de CFO. In werkelijkheid waren alle aanwezigen in de meeting deepfake creaties, die leken op en klonken als de collega's die hij herkende. Had de betrokken medewerker in eerste instantie nog twijfels bij de uitnodigingsmail van het vergaderverzoek (phishingmail), deze waren als sneeuw voor de zon verdwenen tijdens het overleg. Hierin gaf de 'fake' senior manager uiteindelijk opdracht voor een aantal financiële transacties.

Intensivering aanpak online fraude

Om online fraude te bestrijden is in de afgelopen jaren al veel gebeurd. Zo hebben in dit verband al veel opsporingsonderzoeken gelopen om daders op te sporen. Daarnaast zijn ook technische barrières opgeworpen om het moelijker te maken om bijvoorbeeld tech support scam, aan en verkoopfraude, phishing of bankhelpdeskfraude te plegen en hebben tal van preventieve informatiecampagnes gelopen om mensen te informeren over deze praktijken.

Het is voor de opsporing niet mogelijk om alle zaken op te pakken en ondanks alle gedane inspanningen worden nog steeds veel mensen slachtoffer. Vanwege de grote emotionele en financiële gevolgen blijft de aanpak van gedigitaliseerde criminaliteit of specifieker online fraudes[56], van groot belang. Voor het terugdringen van online fraudes wordt daarom ingezet op een integrale aanpak, bovenop de al lopende en ingezette activiteiten. Met een dergelijke integrale aanpak is een grotere impact te bereiken dan met losstaande initiatieven en op termijn biedt dit ook aangrijpingspunten om eventuele nieuwe opkomende fraudevormen effectief te bestrijden[57].

De integrale aanpak online fraude is in 2022 opgestart door het ministerie van Justitie en Veiligheid en publieke en private partijen. De aanpak heeft als doel om meerjarig gezamenlijk de krachten te bundelen, de onderlinge informatiepositie te verstevigen, het kennisniveau te verhogen, te weten en te doen wat werkt om sneller, flexibeler en effectiever op te kunnen treden tegen online fraude teneinde het aantal slachtoffers te verminderen. Hierbinnen is de inzet van de politie en het Openbaar Ministerie (OM) gericht op het realiseren van een brede, schaalbare en innovatieve aanpak, waarmee zowel de plegers als dienstverleners van online criminaliteit, waaronder online fraude, worden aangepakt. Naast opsporing en strafrechtelijke vervolging wordt ingezet op alternatieve interventies in samenwerking met publieke en private partners. Met deze brede bestrijding worden criminele activiteiten en netwerken verstoord, wordt strafbaar gedrag voorkomen, worden criminele winsten afgepakt en wordt opgetreden tegen strafbare feiten (Ministerie van Justitie en Veiligheid, 2023)[58].

In 2024 en navolgende jaren wordt de integrale aanpak uitgewerkt voor een aantal grote en veel voorkomende online fraudevormen, namelijk aankoopfraude en verkoopfraude, beleggingsfraude, phishing met betaalgegevens, hulpvraagfraude en identiteitsfraude. Bankhelpdeskfraude is de eerste online fraudevorm waarvoor in 2024 interventies zijn uitgewerkt binnen de integrale aanpak online fraude. Dergelijke interventies of (technische) barrières hebben als doel om burgers en bedrijven te beschermen tegen fraude en proberen tegelijkertijd in te grijpen op het verdienmodel van criminele netwerken. In het kader hiervan hebben in 2023 de eerste bijeenkomsten plaatsgevonden om gezamenlijk met de ketenpartners tot effectieve en haalbare interventies te komen. In de loop van 2024 wordt een aantal van deze interventies getest en geïmplementeerd. Hoewel dit mogelijk niet meteen tot een het ei van Columbus leidt, zal het voor criminele netwerken op termijn waarschijnlijk wel steeds moeilijker worden om grote hoeveelheden slachtoffers te maken of inkomsten te genereren.

Verder uitgewerkt en geïmplementeerd op alle benoemde fraudevormen zal de integrale aanpak de komende jaren vermoedelijk een remmende en beperkende invloed hebben op de ontwikkeling van online fraude en daarmee ook op een groot deel van de gedigitaliseerde criminaliteit.

55 Zie o.a.: https://www.ft.com/content/b977e8d4-664c-4ae4-8a8e-eb93bdf785ea

56 De meldingen van gedigitaliseerde criminaliteit die bij de politie binnen komen betreffen in grote mate online fraude. De schatting is dat ongeveer 74 procent van de criminaliteit met een substantiële digitale component, betrekking heeft op (online) fraude (Willekers et al., 2024).

57 Zie: https://open.overheid.nl/documenten/ronl-4b6df7b6-bdda-4e50-9c28-cd106409a997/pdf

58 Zie: https://www.eerstekamer.nl/behandeling/20230224/brief_regering_integrale_aanpak/info

8

Bijlagen

Bijlage 1
Onderzoeksvragen

Het doel is een verdiepende analyse op de thema's en de volgende vragen zijn richting-gevend:

Hoe heeft het fenomeen zich ontwikkeld?
- Wat wordt verstaan onder het fenomeen? Definitie en afbakening.
- Hoe heeft de aard (werkwijze) zich ontwikkeld met betrekking tot de wijze waarop de criminaliteit wordt gepleegd (over de afgelopen jaren)? Dit kan per thema verschillen.
- Hoe heeft de omvang zich ontwikkeld in termen van hoeveelheid (onder andere gemiddelde schadebedragen, hoeveel registraties, totale omvang schade)?
- Wat zeggen externe bronnen over de omvang en schade?
- Wie zijn de (voornaamste) slachtoffers en wat zijn kenmerken van deze slachtoffers? Burgers, bedrijven, organisaties, overheid, scholen et cetera.
- Zijn er wereldwijde ontwikkelingen in relatie tot Nederland?

Kenmerken criminele groeperingen:
- Is er zicht op criminele groeperingen?
- Zijn er verdachten?
- Zijn er geografische zwaartepunten te onderkennen als het gaat om daderschap of verdachtenstatus en zo ja, is dat verklaarbaar?
- Werken ze multidisciplinair? Verschillende soorten criminaliteit en vormen van fraude/oplichting?
- Wat zijn kenmerken van criminele groeperingen? Maken ze gebruik van andermans kennis (op gebied van ict of geldstromen: dienstverleners, notarissen, advocaten)? Gebruiken ze afscherming? Hoe ontstaan contacten (bijvoorbeeld via forums)? Gebruiken ze geweld?
- Bestaat zicht op het wegsluizen van criminele gelden (bijvoorbeeld via money transfers, geldezels, bankrekeningen, aanschaf van dure/luxe dingen)? Via bancair systeem onderwereld? Naar buitenland?

Gevolgen samenleving:
- Wat zijn de gevolgen voor de samenleving?
- Wat zijn de verwachtingen voor de komende vijf jaren? Disclaimer: vergissingen liggen voor de hand.

Aanpak:
- Welke factoren bevorderen het plegen van dit verschijnsel of houden het in stand? Denk aan verouderde wetgeving, internationaal karakter, gebruik infrastructuur Internet of Things, cloud computing, attributie (wie is dader, wat is intentie), complexiteit (wie is verantwoordelijk voor (on)veiligheid)?
- Welke factoren voorkomen het plegen van dit verschijnsel? (vijf punten PIAC (preventie, verstoring, attributie, notificatie en schadebeperking), welke interventiemethoden kunnen worden toegepast?
- Welke aanpak is succesvol gebleken?

Wat is al aangepakt? Opsporingsonderzoeken:
- Hoeveel en welke zaken zijn op het thema opgepakt en geregistreerd door het OM?
- Hoeveel en welke zaken zijn op het thema opgepakt door de cyberteams of DR?
- Aantallen en soorten zaken die door LMIO en Centurion gerouteerd worden naar eenheden?
- Is er samenwerking met andere organisaties met betrekking tot het thema, welke zijn dat en hoe verloopt dat (knelpunten, ervaringen)?

Voor de verdieping zullen verschillende bronnen worden geraadpleegd, binnen en buiten de politie en nationaal en internationaal.

Bijlage 2 Methode

Bronnen

De gebruikte bronnen zijn vooral afkomstig uit de politiesystemen, zoals Basisvoorziening Handhaving (BVH), BlueView, BlueIntel (hierna beschreven), SummIT, Financial Intelligence Unit, Rechtshulpverzoeken en Cognosrapportages. Verder zijn er opsporingsonderzoeken[59] gebruikt en zijn diverse interne politierapporten geraadpleegd. Wat dat laatste betreft valt te denken aan het Book of Crimes dat diverse eenheden hebben gemaakt en naar crimescripts die opgesteld zijn door het project VAK. Externe publicaties zijn afkomstig onder andere van het Centraal Bureau voor de Statistiek, WODC en Europol. Ook is gebruik gemaakt van feedback van inhoudsdeskundigen. Interne feedback werd verzorgd door de Electronic Crimes Taskforce (ECTF), Landelijk Meldpunt Internetoplichting en collega's van diverse eenheden. Externe feedback was afkomstig van verschillende partijen, zoals de Fraudehelpdesk.

De beschrijving over de Landelijke Cybercrime Query (LCQ) hierna is afkomstig uit de *Monitor Jeugdcriminaliteit 2020* (*Hesseling et al*., 2021). De data over de verschillende fenomenen zijn gebaseerd op registraties van meldingen en aangiften uit de Landelijke Cybercrime Query (LCQ). Alleen voor Bankhelpdeskfraude zijn aan de LCQ registraties verdachten gekoppeld om te komen tot een verdachtenbeeld. Voor een goed begrip van de gegevens uit de LCQ, en daarmee ook de validiteit en betrouwbaarheid van deze gegevens, is een vergelijking met een indeling in de standaardclassificatie van misdrijven bij de politie noodzakelijk.

Cijfers over de door de politie geregistreerde criminaliteit zijn gebaseerd op een indeling in maatschappelijke klassen in de Basisvoorziening Handhaving (BVH) uitgaande van het Informatiemodel Nederlandse Politie (INP). Een maatschappelijke klasse is een code waarmee een incident (zoals een delict) wordt gedefinieerd en vastgelegd in een registratie in de BVH van de Nederlandse politie. Er wordt hierbij geen koppeling gelegd tussen een maatschappelijke klasse en artikelen uit het Wetboek van Stafrecht of andere relevante wetgeving (zoals de Opiumwet). Al naar gelang de aard van het incident kan een maatschappelijke klasse betrekking hebben op één of meer artikelen uit het wetboek van strafrecht.

De enige maatschappelijke klasse die bij de politie mogelijk is voor cybercriminaliteit is F90. De definitie van F90 'cybercrime' in de BVH is: 'alle vormen van bezitsaantasting waarbij de computer zowel het middel als het doel is.' Juridisch gesproken valt deze maatschappelijke klasse onder dertien artikelen uit het Wetboek van Strafrecht

59 Het aantal opsporingsonderzoeken dat is bekeken, verschilt sterk per online fraudevorm. Zo zijn er bij bankhelpdeskfraude enkele tientallen grote onderzoeken doorgenomen met veel informatie over de verdachten, criminele samenwerkingsverbanden en werkwijze. Bij veel andere onderwerpen ligt dit een stuk lager en zijn soms meer enkele opsporingsonderzoeken teruggevonden.

Uit onderzoek van de politie blijkt dat cybercriminaliteit niet alleen terugkomt in F90 maar ook in verschillende andere maatschappelijk klassen (Borwell et al., 2020). Een belangrijke reden is dat in de praktijk diverse vormen van cybercriminaliteit vaak verweven zijn met andere vormen van criminaliteit. Zo is computer-vredebreuk meestal een middel om ICT binnen te dringen voor het plegen van fraude met internetbankieren met behulp van banking malware (bijvoorbeeld artikel 138ab Sr; artikel 138c Sr; artikel 139d Sr; oplichting artikel 326 Sr of witwassen artikel 420bis Sr). Daarnaast speelt cybercriminaliteit een rol bij de uitvoering (modus operandi) van traditionele delicten, zoals misdrijven in de persoonlijke sfeer (denk aan smaad of bedreiging). Er is sprake van een opeenvolging van verschillende strafbare feiten (Campman et al., 2012; Wagen et al., 2020) en de strafbare feiten die vallen onder cybercriminaliteit zijn dan één van de delicten die worden gepleegd. Het toekennen van een maatschappelijk klasse aan een incident naar aanleiding van een melding of (een aangifte) van een misdrijf blijft in de praktijk lastig.

Soms worden in de loop van de tijd maatschappelijke klassen toegevoegd. In maart 2023 kwam het voorstel voor drie nieuwe maatschappelijke klassen (mk's), waaronder een nieuwe voor sextortion, omdat alleen een mk sexting bestond die de lading van de delicten niet dekte. Deze nieuwe mk is inmiddels ingevoerd en de naam is veranderd in Misbruik seksueel beeldmateriaal (MSB; F5295) met de volgende beschrijving: Alle feiten waarbij wederrechtelijk seksueel beeldmateriaal van een ander wordt vervaardigd, verspreid openbaar gemaakt of anderszins wordt gebruikt, bijvoorbeeld met de bedoeling om te beledigen of af te persen. Met andere woorden, alle gevallen van ongewenste sexting, wraakporno, sextortion, exposen en heimelijk filmen. Vanuit het team zeden is een overzicht gemaakt met o.a. gekoppelde wetsartikelen. Op voorstel van team zeden van de politie is de mk grooming ongewijzigd gebleven tot de implementatie van de nieuwe Wet Seksuele Misdrijven, omdat grooming uit andere gedragingen bestaat dan Misbruik seksueel beeldmateriaal dat een typisch zedendelict is. De wetgeving rond dit artikel gaat grondig wijzigen en het wetgevingstraject is nog gaande (in de paragraaf over aanpak volgt een uitgebreidere beschrijving).

Naast een maatschappelijke klasse worden aan een registratie in de BVH ook diverse documenten gekoppeld zoals een verklaring van een melder, een toelichting van de verbalisant, het proces-verbaal van aangifte van een misdrijf, een ambtshalve opgemaakt proces-verbaal van een misdrijf of een bevinding naar aanleiding van een actie van de politie. Deze documenten bevatten termen en zinnen die veel informatie geven over wat er feitelijk is gebeurd. Het gaat dan niet alleen om termen en zinnen die kunnen aangeven welke strafbare feiten mogelijk zijn gepleegd, maar ook op welke wijze (modus operandi) en of er sprake is van eventuele dader- en/of opsporingsindicaties.
Voor het zoeken van relevante registraties in de BVH is ten eerste een tekstquery ontwikkeld voor het vinden van registraties die duiden op mogelijke cybercriminaliteit: de Landelijke Cybercrime Query. Ten tweede is een classificatiesysteem ontwikkeld samen met een codeerinstructie voor het handmatig controleren van de gevonden BVH-registraties op basis van de LCQ (is er inderdaad sprake van cybercriminaliteit?) en het toevoegen van nieuwe variabelen zoals de verschijningsvorm van cybercriminaliteit.

De Landelijke Cybercrime Query

De LCQ is door de Dienst Landelijke Informatieorganisatie (DLIO) van de Nederlandse politie samen met diverse andere eenheden ontwikkeld. In de LCQ staan een groot aantal zoek-

termen die op zichzelf of in combinatie kunnen duiden op cybercriminaliteit. Omdat er geen koppeling bestaat tussen de artikelen uit het Wetboek van Strafrecht en de maatschappelijke klasse, termen en zinnen in de BVH-documenten van een registratie van een incident is voor het vinden van de juiste woorden uitgegaan van verschijningsvormen van cybercriminaliteit die al in breed verband gehanteerd worden en te vinden zijn in de literatuur. Bijvoorbeeld door het Nationaal Cyber Security Centrum (NCSC), het WODC en door de politie in het *Nationaal dreigingsbeeld* (NDB). Het ging om bekende verschijningsvormen zoals hacken (computervredebreuk), malware, websiteaanvallen (DDoS), botnets, ransomware (afpersing, dreigen met computercriminaliteit) en phishing met malware. Voor ieder van deze verschijningsvormen is een tekstquery gemaakt. Voor deze opzet is gekozen zodat experts en andere geïnteresseerden per verschijningsvorm input konden leveren. Door het raadplegen van de literatuur en deskundigen, het onderzoeken van de intersubjectiviteit door de uitkomsten van verschillende codeurs onderling te vergelijken en te bespreken, is getracht de validiteit (meten we wat we willen meten) van het instrument zo goed als mogelijk te waarborgen in termen van 'inhoudsvaliditeit' (Swanborn, 1987; Scheepers et al., 2016).

Gegeven de verwevenheid is het strakke onderscheid tussen cybercriminaliteit en gedigitaliseerde criminaliteit losgelaten. Het gaat niet alleen om de op zichzelf staande vormen van cybercriminaliteit, zoals ransomware of DDoS, maar de zoektermen geven daarnaast zicht op gedigitaliseerde criminaliteit die verweven is met cybercriminaliteit. Voorbeelden van dit laatste zijn het hacken van accounts om deze te misbruiken voor bestellingen (fraude), het gebruik van phishinglinks om persoonlijke gegevens te verkrijgen, het inzetten van Remote Access Tools om toegang tot de computer te krijgen of het verkrijgen van wachtwoorden. In de modus operandi van verschillende vormen van criminaliteit komen deze toepassingen van cybercriminaliteit (meestal computervredebreuk) terug, zoals bij misbruik accounts voor bestellingen, betaalverzoekfraude of helpdeskfraude.
Uitgangspunt was een eerste query die uitging van F90. De ervaring leerde dat deze voor verbetering vatbaar was omdat er sprake was van vals-positieve en vals-negatieve registraties die meekwamen in het resultaatbestand. In een aantal stappen is in de periode februari 2017 tot september 2017 toegewerkt naar een nieuwe query. Dit is gebeurd door middel van een proces van testen, evalueren, vervangen van termen en operatoren (zoals 'and' of 'or'). Hierbij zijn ook twee alternatieve query's gebruikt om de uitkomsten te vergelijken en door feedback van deskundigen in diverse eenheden (intersubjectiviteit). De verbeterde versie van de Landelijke Cybercrime Query is in september 2017 in gebruik is genomen, waarbij in ieder geval de maatschappelijke klasse F90 registraties worden opgevraagd en alle andere relevante registraties op basis van de zoektermen.

In de periode december 2018 tot april 2019 is de LCQ opnieuw aangepast. De belangrijkste reden was dat als gevolg van de digitalisering van de samenleving de politie met enige regelmaat nieuwe of aangepaste modus operandi constateert bij het plegen van misdrijven met een digitale component. Een voorbeeld is helpdesk-fraude of tech support scam. Aanvankelijk werden deze misdrijven hoofdzakelijk gepleegd uit naam van Microsoft, maar in de loop van de tijd was er ook steeds meer sprake van andere helpdesks. Dergelijke aanpassingen zijn niet alleen noodzakelijk maar ook gebruikelijk bij het zoeken naar registraties op basis van teksten. In dit verband wordt ook verwezen naar de kanttekeningen bij de bruikbaarheid van machine-learning-achtige technieken, concept-drift en wat dit betekent voor trend-onderzoek (Tollenaar et al., 2019, pagina 102-103). De consequentie van het voorgaande is wel dat de LCQ vooral valide resultaten genereert voor de periode dat de tekstquery ongewijzigd blijft (begin 2019 tot heden). Bij trendonderzoek dient rekening gehouden te worden met registratie-effecten als de tekstquery tussentijds wordt aangepast als er sprake is van nieuwe ontwikkelingen op het terrein van cybercriminaliteit.
Een andere vraag is in hoeverre er sprake is van een valide meting in termen van de daadwerkelijke (hoeveelheid) cybercriminaliteit die plaatsvindt in Nederland en de daarbij betrokken verdachten, de zogenoemde 'externe validiteit' (Swanborn, 1987). Dat is niet mogelijk omdat de meldingen, aangiften en verdachten van cybercriminaliteit bij de politie geen a-selecte steekproef vormen uit de onbekende populatie gepleegde misdrijven of verdachten in Nederland. Het darknumber bij de politie van cybercriminaliteit blijft aanzienlijk en selectief. Zo is de aangiftebereidheid van burgers en rechtspersonen beperkt en verschilt dit per verschijningsvorm (CBS, 2018; Weijer et al., 2020). Zo werd bijvoorbeeld in 2019 in ruim één op de twaalf gevallen (8%) van cybercriminaliteit of gedigitaliseerde criminaliteit aangifte gedaan bij de politie door burgers (CBS, 2020). Voor bedrijven ligt het percentage tussen de 6 procent en 14 procent (CBS, 2018; Weijer et al., 2019).
De lage aangiftebereidheid van burgers en bedrijven verklaart deels het verschil tussen de uitkomsten van het aantal jongeren dat zelf opgeeft cyberdelicten te plegen (zie hoofdstuk 2 over zelfrapportage in dit rapport) en het aantal bij de politie bekende verdachten.

Classificatie registraties uit de LCQ

De resultaten van de LCQ met de gevonden registraties uit de BVH vormen het startpunt voor een handmatige classificatie van de registraties in termen van de verschijningsvormen van cybercriminaliteit. Deze classificatie gebeurt door medewerkers van de informatieorganisatie van de tien politie-eenheden en vindt vanaf 1 januari 2019 plaats in een specifieke en gestandaardiseerde database (BlueIntel). Om ervoor te zorgen dat het coderen zo betrouwbaar mogelijk plaatsvindt, is een specifieke codeerinstructie geschreven op welke wijze het coderen plaats dient te vinden.
Ten eerste wordt door de codeur nagegaan of er daadwerkelijk sprake is van een registratie cybercriminaliteit. Ten tweede worden de valide registraties qua verschijningsvorm ingedeeld in hoofd- en subcategorieën op basis van het veronderstelde motief bij het plegen van het misdrijf en de gebruikte werkwijze. De delictscategorieën zijn geldelijk gewin (fraude/oplichting en afpersing/chantage), de beschadiging van een persoon of rechtspersoon door smaad/laster/belediging) (persoonsgericht), politieke of ideologisch motieven (hacktivisme) en delicten met motieven als verveling, spel, grensverkenning, prestige en uiting van frustraties (vandalisme/baldadigheid; Borwell et al., 2020). Naast de hoofdcategorieën worden de registraties ook ingedeeld in meer gedetailleerde subcategorieën. De hoofdcategorieën (en ter illustratie enkele voorbeelden van de subcategorieën) zijn hierna uiteengezet (Hesseling, Harteveld, & Bloem (2021).

Overigens blijken de indelingen van de verschijningsvormen van cybercriminaliteit van de politie, het WODC en het CBS op basis van het zoeken van woorden of via machine-learning van elkaar te verschillen (Tollenaar et al., 2019; CBS, 2019; Borwell et al., 2020). Het gebruik van diverse indelingen hangt samen met de verschillende doelen die zijn of worden nagestreefd. Welke indeling te prefereren is, valt niet zonder meer vast te stellen zonder nader onderzoek. De politie hanteert de indeling vanuit haar taakstelling om zo goed als mogelijk (in)zicht te krijgen in concrete maatschappelijke veiligheidsproblemen, voor intelligence doeleinden en het kunnen richten van een integrale aanpak door (bijvoorbeeld) preventie, victim notificatie, verstoren of opsporing.

Hoofdcategorie	Subcategorie en voorbeelden
Fraude/oplichting	Helpdeskfraude (Tech Support Scam), fraude met internetbankieren (phishing), misbruik accounts voor bestellingen
Afpersing/chantage	Ransomware, sextortion, DDoS
Persoonsgericht huiselijke kring	Stalking
Persoonsgericht vrienden of kennissen	Smaad/laster/belediging
Persoonsgericht zakelijke sfeer	Diefstal gegevens
Persoonsgericht onbekende dader	Bedreiging
Vandalisme/baldadigheid	DDoS-aanval, defacement, hacktivisme
Hacktivisme	Hacktivisme
Overige cybercriminaliteit	Hacken onbekend motief

De gekoppelde verdachten

In het resultaatbestand van de LCQ is ook bekend of bij een registratie van een misdrijf er sprake is van een of meer bekend geworden verdachten (inclusief per verdachte diverse identificerende gegevens zoals naam, leeftijd, adres). Deze worden automatisch gekoppeld aan de desbetreffende BVH-registratie.

Bijlage 3
Witwassen van criminele opbrengsten

De onderstaande financiële paragraaf gaat in op het witwassen van de criminele opbrengsten van bankhelpdeskfraude. Als onderliggende methodiek wordt zoveel mogelijk de National Risk Assessment Witwassen van het WODC gehanteerd (Van der Veen et al., 2024). Aan de hand hiervan wordt zo goed mogelijk uitgewerkt op welke manieren het witwassen plaatsvindt en via welke vormen dit het meest gebeurt.

Financiële paragraaf Bankhelpdeskfraude

Bankhelpdeskfraude in georganiseerd verband is gericht op het behalen van winst. Aangezien deze winsten niet legaal zijn, brengt dit voor de crimineel diverse problemen met zich mee. Zo staat op witwassen een strafbedreiging van maximaal zes jaar, die zelfs kan oplopen tot acht jaar in het geval van herhaald plegen (420ter WvSr). Grote criminele winsten zijn ook niet zondermeer in het legale financiële stelsel te besteden. Dat komt omdat publiek-private samenwerking onderdeel is geworden van de algehele witwasbestrijding. Zo wordt van financiële instellingen en diverse private partijen verwacht dat zij in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) iedere transactie tegen het licht houden en bij twijfel melden aan FIU-Nederland. FIU-Nederland kan transacties vervolgens verdacht verklaren wanneer daar aanleiding toe is. Daarmee staan deze transacties direct beschikbaar aan de opsporingsdiensten. Financiële sporen kunnen ook als ondersteunend bewijs in een strafzaak omtrent de fraudevorm dienen. Ook bestaat er het risico dat de overheid de illegale winsten op het spoor komt en deze in beslag neemt of een ontnemingsprocedure start. Voor zulke procedures hoeven de winsten niet eens met specifieke criminele activiteiten in verband gebracht te worden om jaren na dato nog tot een financieel opsporingsonderzoek te leiden. Het is voldoende om aan te tonen dat het geld of de goederen niet uit legale bron gefinancierd kan zijn. Tot slot bestaat er het gevaar dat criminele winsten kapers op de kust aantrekken aangezien de meeste slachtoffers liever geen aangifte bij de politie doen gezien de illegale herkomst van het gestolen geldbedrag.

Maar de ene criminele winst is de andere niet. Nog afgezien van de omvang, kan ook onderscheid gemaakt worden in verschillende doeleinden. Kort samengevat kan de besteding van criminele winsten in drie categorieën worden geplaatst. Het gaat om 1) leefgeld, 2) bedrijfskosten en 3) investeringen (op langere termijn). Daarmee wordt het volgende bedoeld.

Onder leefgeld worden uitgaven verstaan die in het legale financiële stelsel vrijwel onopgemerkt blijven. Bijvoorbeeld omdat het onder de meldgrens blijft of volledig buiten zicht blijft. Te denken valt aan kleinere contante uitgaven voor bijvoorbeeld boodschappen, benzinegeld, of incidenteel grotere contante uitgaven voor bijvoorbeeld de aanschaf van merkkleding of vakanties in het buitenland.

Onder bedrijfskosten worden uitgaven gerekend die in het kader in het geval van bankhelpdeskfraude veelal in de voorbereiding vallen. Zulke uitgaven worden deels in een illegale context, deels in een legale context gedaan. In de illegale categorie vallen uitgaven die te maken hebben met bijvoorbeeld de aankoop van phishingkits, leads en belscripts, het 'salaris' van criminele medewerkers, het inhuren van facilitators (ophalers, geldezels) of het verrichten van witwasdiensten. In de legale categorie vallen uitgaven die te maken hebben met de aankoop benodigde apparatuur, zoals telefoons, headsets of laptops of het huren van locaties (hotels of vakantieparken).

Onder investeringen worden uitgaven of beleggingen in de bovenwereld gerekend die doorgaans betrekking hebben op de langere termijn. Te denken valt aan de aankoop van vastgoed om zelf te wonen of als beleggingsvehikel of het investeren in cryptovaluta of het opzetten van een legale onderneming.

Het opdelen van de criminele winsten in drie categorieën wil niet zeggen dat deze strikt gescheiden zijn. Soms lopen deze in elkaar over. Het punt is dat criminele winsten op verschillende manieren worden gebruikt en verschillende doelen hebben. Hoe hoger het bedrag en hoe meer raakvlakken er zijn met het legale financiële stelsel, hoe meer moeite gedaan zal moeten worden om onder de radar te blijven. Er is dan sprake van economisch witwassen. Dat wil zeggen, het verrichten of laten verrichten van handelingen om de criminele oorsprong van het geld te verhullen zodat het in het legale financieel-economisch stelsel kan worden aangewend.

Economisch witwassen kan op diverse manieren plaatsvinden. Ook bij bankhelpdeskfraude in georganiseerd verband worden verschillende witwasvormen aangetroffen. Om hier enigszins ordening in aan te brengen, wordt gebruik gemaakt van de National Risk Assessment Witwassen (Van der Veen & Heuts, 2024). Dit is een analyse die door het WODC is uitgevoerd in het kader van de vierde Europese anti-witwasrichtlijn. Volgens deze richtlijn is elke EU-lidstaat verplicht een National Risk Assessment (NRA) Witwassen op te stellen. In Nederland hebben de WODC-rapporteurs hiertoe 74 verdiepende interviews met (anti-witwas) experts afgenomen, een enquête uitgevoerd en drie groepsgewijze expertmeetings gehouden. Op basis van een longlist van vijftig dreigingen werden uiteindelijk achttien vormen van witwassen benoemd.

De meeste van deze achttien vormen spelen bij het witwassen van bankhelpdeskfraude (voor zover bekend) niet of nauwelijks een rol[60], zoals witwassen via buitenlandse (offshore) structuren, ondergronds of hawala-bankieren, het opknippen van trustkantoor-dienstverlening of commercieel vastgoed. Op basis van informatie uit opsporingsonderzoeken, maar ook (dossier)analyse op verdachte transacties bij FIU-Nederland[61] zien we enkele witwasvormen wel terugkomen bij (verdachten van) bankhelpdeskfraude. Tabel 1 beperkt zich tot de vijf meest voorkomende witwasvormen die op het gebied van bankhelpdeskfraude in georganiseerd verband voorkomen. Tevens wordt vermeld in welke relatie de genoemde witwasvorm staat tot leefgeld, bedrijfskosten of investeringen.

Tabel 1. Witwasvormen in relatie tot frequentie en aard
Bron: Van der Veen & Heuts, 2024 en eigen bewerking

Witwasvorm	Frequentie	L/B/I
1. Witwassen via girale transacties bij vergunde banken	Zeer Hoog	L/B/I
2. Witwassen via stromannen, katvangers of *money mules*	Zeer Hoog	L/B/I
3. Witwassen via contante transacties/stortingen bij vergunde banken	Hoog	L/B
4. Witwassen via *Payment Service Providers*	Hoog	L/B
5. Witwassen via aanbieders van financiële cryptodiensten	Middel/Hoog	L/I

Hieronder worden de afzonderlijke witwasvormen nader uitgelegd.

1. Witwassen via girale transacties bij vergunde banken
Het gaat hier om overmaken of ontvangen van gelden met betrekking tot particulieren of rechtspersonen. In feite worden de vergunde banken misbruikt en zijn zij zelf niet bewust betrokken. Veelal zijn girale transacties onderdeel van andere witwasmethoden. Girale transacties vinden bij bankhelpdeskfraude in georganiseerd verband niet alleen plaats in het kader van witwassen. Het is een centraal onderdeel van de modus operandi waarbij geld van burgers wordt buitgemaakt via diverse overschrijvingen naar verschillende (inter)nationale rekeningen die de criminelen beheren. We zien deze vorm daarom zeer veel terug bij (verdachten van) bankhelpdeskfraude in georganiseerd verband, maar de relatie van deze witwasvorm tot leefgeld, bedrijfskosten of investering is (dan) nog ongewis. Uit de FIU-gegevens bleek dat girale overboekingen bij ongeveer 90 procent van alle verdachte transacties een rol speelt.[62]

2. Witwassen via stromannen, geldezels of money mules
In deze categorie is sprake van derde personen die relatief makkelijk vervangbaar zijn maar wel belangrijk zijn om de Ultimate Beneficial Owner (UBO) of opdrachtgever buiten beeld te houden. Binnen bankhelpdeskfraude spelen vooral geldezels een zeer belangrijke rol door

60 Bij veel vormen blijft dit onduidelijk omdat de omvang hiervan niet of zeer moeilijk uit de databronnen is op te maken, bijvoorbeeld witwassen via particulier vastgoed.
61 Deze analyse is gebaseerd op de in totaal 7594 verdachte transacties waarbij verdachten van bankhelpdeskfraude betrokken zijn.
62 Elke verdachte transactie krijgt vanuit de FIU maar een soort transactie toegekend. Bij het doornemen van de dossierbeschrijving blijken binnen een transactie vaak meerdere witwasvormen terug te komen. Om hier meer recht aan te doen, is per transactie gescoord welke witwasvormen naar voren komen. Hierdoor kunnen verschillende witwasvormen in een registratie terugkomen en tellen de percentages niet op tot 100 procent.

(hun) betaalrekeningen en/of pinpassen beschikbaar te stellen aan de criminelen. Naast het buiten beeld houden van degenen die uiteindelijk over de buitgemaakte gelden kunnen beschikken, zijn de geldezels daarmee een cruciale schakel in de modus operandi binnen bankhelpdeskfraude (en andere fraudevormen). Bij georganiseerde groepen komt het gebruik van geldezels (vrijwel) altijd terug. In de FIU-gegevens is moeilijk zichtbaar te maken welk deel van de verdachte transacties betrekking heeft op geldezels. Hiervoor moet van de betrokken personen bij een verdachte transactie hun rol (als katvanger) bekend zijn. Een dergelijke analyse op rolniveau valt buiten de scope van dit onderzoek. Verder is ook bij deze witwasvorm de relatie tot leefgeld, bedrijfskosten of investering vaak ongewis en betreft het gebruik van derde personen (geldezels) een onderdeel van andere witwasmethoden die (mogelijk later) plaatsvinden.

3. Witwassen via contante transacties/stortingen bij vergunde banken

Het gaat hier om afstorten of opnemen van contant geld van bankrekeningen. Deze rekeningen kunnen op naam staan van particulieren of rechtspersonen. De vergunde banken hebben zelf geen deel aan het witwasproces. Binnen bankhelpdeskfraude zien we dit vooral terug in de vorm van contante opnames, meer specifiek het cashen van de criminele opbrengst. Dit gebeurt doorgaans direct vanaf de rekeningen van slachtoffers. Alternatief wordt het geld eerst overgemaakt naar verschillende rekening(en) op naam van een geldezel.
Binnen de FIU data heeft ongeveer vier procent van de registraties betrekking op het cash opnemen van geld via geldautomaten of anderszins. Op basis van opsporingsonderzoeken zien we dat deze witwasmethode veelvuldig wordt toegepast en vooral binnen de pasophaalvariant vrijwel altijd plaatsvindt. Dit komt waarschijnlijk binnen de FIU data maar beperkt in beeld, aangezien een groot deel van de cash opnames vanaf rekeningen van slachtoffers worden gepind (en niet als verdachte transacties terugkomen). Het cash geld wat hiermee in handen komt van de verdachten, is voornamelijk te relateren tot leefgeld en bedrijfskosten. Zo worden veel luxe spullen cash aangeschaft en criminele handlangers betaald voor hun diensten.

4. Witwassen via Payment Service Providers (PSP's)

Webwinkeliers kunnen via PSP's klantbetalingen accepteren. Deze betalingen van klanten komen eerst op bankrekeningen van de aan de PSP gelieerde stichting derden-gelden terecht. De PSP's keren vervolgens de betalingen weer uit op de bedrijfsrekening van de webwinkeliers. Dat uitbetalen vindt vaak in batches plaats, dat wil zeggen, afzonderlijke transacties worden gebundeld en het totaalbedrag van alle transacties wordt uitbetaald. Daardoor ontbreekt voor banken het toezicht op individuele transacties. Omdat PSP's vaak in het buitenland zitten, kunnen zij niet goed controleren of de webwinkelier daadwerkelijk producten heeft geleverd.
Veel van de criminele groepen gebruiken de criminele opbrengst om online producten of tegoedkaarten te kopen via verschillende webwinkels. Hierbij spelen PSP's vaak een rol bij de afwikkeling van de betaling, die overigens doorgaans vanuit rekeningen van slachtoffers of geldezels plaatsvindt. Het is echter onbekend of het verminderde toezicht van PSP's daarbij bewust wordt misbruikt om geld wit te wassen of een toevallige bijkomstigheid is.
In totaal komt bij bijna 36 procent van de alle VT's ook betalingen via PSP's terug. De aangeschafte spullen, zoals giftcards, laptops of mobiele telefoons worden, naast eigen (crimineel) gebruik, via verschillende kanalen doorverkocht. Dit geld is daarmee voornamelijk te relateren aan leefgeld en in mindere mate aan bedrijfskosten of investering.

5. Witwassen via aanbieders van financiële cryptodiensten

Volgens de NRA gaat het hier in feite om de handel in virtuele valuta. Maar ook het aanbieden of gebruik maken van zogeheten *crypto mixing* services wordt hieronder geschaard. Dit is een *online dienst* waarbij crypto's tegen betaling van een commissie worden opgesplitst en in andere samenstelling weer worden samengevoegd om de herkomst of bestemming te verhullen. Uit opsporingsonderzoek is op te maken dat bij veel verdachten van bankhelpdeksfraude het aankopen van virtuele valuta populair is. De aankoop gebeurt vaak via bekende handelsplatforms, zoals Binance, Litebit, Coinbase, Bitvavo, Nuri of OKX. Op de (online) wallets waar de aangeschafte de cryptomunten in eerste instantie terechtkomen (vaak op naam van een slachtoffer), blijven deze bedragen over het algemeen niet (lang) staan. Deze worden doorgaans verder doorgesluisd of overgeboekt naar verschillende andere wallets (bijvoorbeeld van crypto-ezels) of rekeningen van de criminelen. Soms wordt hierbij gebruik gemaakt van een mixerdienst, ook wel cryptocurrency-tumblers genoemd (project VAK, 2024).

In totaal komt bij bijna 35 procent van de alle verdachte transacties ook betalingen richting de eerdergenoemde handelsplatforms terug, in de verdachte transacties komen geen crypto mixers naar voren. Het is niet helemaal duidelijk wat de belangrijkste drijfveren zijn achter de aankoop van de cryptovaluta. Voor een deel vinden de criminelen dit mogelijk een interessante investering van hun buitgemaakte geld. Daarnaast is de aankoop hiervan en het meermaals overboeken en omzetten mogelijk vooral bedoeld om de herkomst en de bestemming van het geld achter de cryptovaluta zo veel mogelijk te verhullen. Ook worden er langzamerhand onderling betalingen mee geregeld, zodat het ook onderdeel van het bedrijfsproces is geworden.

Bijlage 4
Woordenlijst

- **BlueIntel:** registraties die dagelijks uit de Landelijke Cyber Query komen, worden door de eenheden gelezen en gecategoriseerd op diverse kenmerken en vastgelegd in een excel-database genaamd BlueIntel. Het doel is om o.a. overzichten en beelden te maken. De categorieën in de database komen overeen met de fenomenen zoals in dit rapport weergegeven en onderzocht. De aantallen uit deze database gebruiken we om een beeld van de omvang te geven (per fenomeen).

- **Bonker:** dit zijn criminelen 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 dan door zogenaamde ‘geldezels’

- **Credential stuffing:** houdt in dat een aanvaller met elders gestolen informatie een bepaald account tracht binnen te komen. Meestal zijn de inloggegevens gestolen bij een datalek van een bepaalde dienst en omdat mensen van dezelfde, kunnen door één hack opeens meerdere accounts gecompromitteerd worden.

- Een **crime script** is een uitvoerige uitwerking van de stappen en acties die doorlopen worden bij het plegen van een misdrijf. Het wordt gebruikt om de verschillende fasen van een criminele activiteit te analyseren, van voorbereiding tot uitvoering en nasleep, en helpt bij het identificeren van kwetsbaarheden voor gerichte interventies.

- **Crypto mixers en cryptocurrency-tumblers** zijn beide diensten die worden gebruikt om de herkomst van cryptocurrencies te verhullen. Dit gebeurt door de digitale munten van verschillende gebruikers te mixen, waarna de gemixte munten weer worden verdeeld. Dergelijke stappen maken het moeilijker om transacties te traceren en de oorspronkelijke eigenaar te identificeren.

- **Cybercrime-as-a-service** wil zeggen dat cybercriminelen illegale diensten, tools en kits op het gebied van hacken en cybercriminaliteit aanbieden op allerlei sociale media platforms. Door deze diensten te verkopen en op de markt te brengen, zijn mensen met weinig technische expertise in staat om zich bezig te houden met cybercriminaliteit. Enkele veelvoorkomende voorbeelden van Cybercrime-as-a-Service zijn bijvoorbeeld Ransomware-as-a-Service (RaaS), Distributed Denial of Service-as-a-Service (DDoSaaS) of Phishing-as-a-Service (PaaS). Maar ook Botnets-for-hire of het aanbieden van diensten voor het stelen van inloggegevens komen vaak voor.

- **Exposen** is het publiekelijk te schande maken door compromitterend beeldmateriaal te verspreiden.

- **Facilitators:** de inmenging in de bovenwereld is in veel gevallen bedoeld om criminele activiteiten te blijven faciliteren of buiten zicht te houden. Hiervoor gebruiken groeperingen ‘facilitators’. Dit zijn (rechts)personen die bewust, onbewust of gedwongen de ondermijnende criminaliteit mogelijk maken. Dit kan gaan om een boer die wordt gedwongen op zijn land een drugslab te faciliteren en geen vragen te stellen. Of om een crimineel die in het bestuur van een sportclub toetreedt en geld witwast via de club. In veel gevallen gaat om geldezels, die hun pas beschikbaar stellen om criminele gelden weg te sluizen via hun bankrekening.

- **Gegevensdragers**: een fysiek voorwerp (telefoon, tablet, laptop, computer, usb-stick, SD-kaart) waarop personen gegevens opslaan.

- **Keyloggers:** is een vorm van spyware die elke toetsaanslag op een computer, smartphone of tablet vastlegt. Met deze software verzamelen cybercriminelen vertrouwelijke gegevens, zoals wachtwoorden en financiële gegevens. De spyware wordt meestal onbewust gedownload door op een link in een bericht te klikken.

- **Leads:** digitale lijst met persoonsgegevens die bijvoorbeeld op Telegram verkocht worden aan cybercriminelen en die als doelwit voor online fraude gebruikt worden.

- **Maatschappelijke klasse:** feitcodes binnen de politiesystemen die gebruikt worden om incidenten in vast te leggen. F900 is de feitcode voor cybercriminaliteit, F620 voor horizontale fraude.

- **Phishing:** met phishing proberen cybercriminelen onrechtmatig persoonlijke gegevens van iemand te verkrijgen en/of binnen te dringen op een apparaat of account van die persoon. Meestal krijgen potentiële slachtoffers een mail of sms of app met een link en als ze deze aanklikken, komen ze in een valse bankomgeving terecht die bedrieglijk echt lijkt. Phishing is vaak de opmaat naar andere online fraudevormen, zoals bankhelpdeskfraude, hulpvraagfraude, telefonische helpdeskfraude en misbruik accounts voor bestellingen.

- Een **phishing kit** is een tool die bedoeld is om namaaksites van bekende merken te genereren en deze vervolgens te verkopen aan oplichters, zoals op sociale mediasites als Telegram. Het is opmerkelijk dat deze kits vaak zo goed in elkaar zitten dat er geen speciale vaardigheden nodig zijn om ze in de praktijk toe te passen.

- **Phishing panel**, ook wel beheerpaneel genoemd, wordt door cybercriminelen gebruikt om phishing websites te monitoren, om live gegevens van phishing slachtoffers te ontvangen en op te slaan, en om tegelijkertijd gegevens en vragen aan slachtoffers aan te bieden voor bijvoorbeeld een verificatie proces. Het vereist veel expertise om deze panels zelf te ontwikkelen en in de meeste gevallen worden zulke phishing panels (en phishing websites) door cybercriminelen aangeschaft of gehuurd in de vorm van kant en klare phishing kits.

- **Prepper:** deze persoon is verantwoordelijk voor het prepareren van (geldezel)rekeningen, crypto wallets en koppelingen tussen betaalplatformen en/of betaalmiddelen. Om dit te doen heeft de prepper uitgebreide kennis nodig over beveiligings- en detectiemaatregelen bij de betreffende platformen.

- **RAT of Remote Access Tool:** is legitieme software waarmee een ICT'er vanaf één basiscomputer kan inloggen op alle geregistreerde computers en deze op afstand kan beheren. Bijvoorbeeld voor probleemoplossing, hulp op afstand en een goede werking van de computers binnen het netwerk. Oplichters gebruiken RAT's om toegang te krijgen tot privénetwerken van slachtoffers om vertrouwelijke informatie te ontvreemden of om handelingen binnen een bankomgeving te verrichten (zoals geld overboeken en/of om limieten te verhogen).

- **Search Engine Optimization** (SEO) zorgt ervoor dat websites zo hoog mogelijk scoren (ranken) in de resultaten van online zoekmachines. In het geval van helpdeskfraude (tss) bij mensen die online hulp zoeken bij computerproblemen.

- **Smishing:** phishing via sms of andere chatdiensten, zoals WhatsApp of Telegram.

- **Spoofing:** binnen de politie en breder binnen organisaties actief in het cyberdomein wordt de term spoofing vooral gebruikt om een techniek te beschrijven waarmee fraudeurs zich kunnen voordoen als iemand anders door valse weergave-informatie mee te geven aan een sms, e-mail of inkomend telefoonnummer. Het is daarbij meer een onderdeel van de werkwijze binnen veel online fraudevormen, dan een overkoepelende categorie.

- **VoIP** is een technologie die het mogelijk maakt om telefoongesprekken via een internetverbinding te voeren in plaats van via traditionele telefoonlijnen. Voorbeelden van VoIP-diensten zijn Skype, WhatsApp en Zoom.

- **Wallet:** een cryptovaluta wallet, of crypto wallet, is een softwareproduct of fysiek apparaat dat de openbare en privésleutels op cryptovaluta-accounts bewaart.

Bijlage 5 Afkortingen

BEC	Business E-mail Compromise
BVH	Basis Voorziening Handhaving
BOSZ	Betere Opsporing door Sturing op Zaken
CEO	Chief Executive Officer
CFO	Chief Financial Officer
DLIO	Dienst Landelijke Informatieorganisatie
DRIO	Dienst Regionale Informatieorganisatie
ECTF	Electronic Crime Task Force
FHD	Fraudehelpdesk
FIOD	Fiscale inlichtingen- en opsporingsdienst
ICT	Informatie- en communicatietechnologie
LCQ	Landelijke Cyberquery
LOCO	Landelijk Operationeel Cybercrime Overleg
MK	Maatschappelijke klasse
NVB	Nederlandse Vereniging van Banken
OM	Openbaar Ministerie
OSINT	Open Source Intelligence
PSP	Payment Service Provider
THTC	Team High Tech Crime
UBO	Ultimate Beneficial Owner

Bijlage 6
Stakeholders

Autoriteit Financiële Markten (AFM)
Coin
Consumentenbond
Electronic Crime Task Force (ECTF)
Fiscale inlichtingen- en opsporingsdienst (FIOD)
Fraudehelpdesk
Functioneel Parket
Interpolis
KPN
Landelijk Meldpunt Internetoplichting
Meta
Ministerie van Economische Zaken
Ministerie van Financiën
Ministerie van Justitie en Veiligheid: Integrale aanpak online fraude
Nederlandse Vereniging van Banken
Openbaar Ministerie
Parket Generaal
Thuiswinkel.org
Vereniging van Nederlandse Gemeenten (VNG)
VNO-NCW/MKB

9

Bronnen

Abraham, J., Junger, M., Koning, L., C. Njoki & S. Rogers (2023). *The state of scams in the Netherlands – 2023* [Powerpoint slides]. Global Anti-Scam Alliance (GASA). Geraadpleegd van https://www.gasa.org/downloads

Banken.nl. (2023, 4 juli). *NVB roept op tot meer samenwerking om online fraude te bestrijden.* Geraadpleegd van https://www.banken.nl/nieuws/24460/nvb-roept-op-tot-meer-samenwerking-om-online-fraude-te-bestrijden

Bekkers, L., M. van Leuken & R. E. Leukfeldt (2024). *Criminele netwerken achter geldezels. Rapportage deel1: verkenning. Een verkennend onderzoek naar de aard van cybercriminele netwerken achter geldezeldelicten en aangrijpingspunten voor de aanpak ervan.* Den Haag / Amsterdam: Lectoraat Cybercrime & Cybersecurity, NSCR & De Haagse Hogeschool.

Betaalvereniging Nederland. (2020, 16 april). *Veel meer phishing en bankpasfraude in 2019.* Geraadpleegd van https://www.betaalvereniging.nl/actueel/nieuws/phishing-bankpasfraude-2019/#:~:text=De%20schade%20door%20phishing%20naar,94%20miljoen%20euro%20in%202019

Bloem, B.A. & A. Harteveld (2019). *Nationaal Cyberbeeld 2016 - 2019*. Zoetermeer: Dienst Landelijke Informatieorganisatie Politie.

Bloem, B.A., A. Harteveld & M. De Heus (2017). *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Politie intern.

Bloem, B.A. & A. Harteveld (2012). *Horizontale fraude. Nationaal dreigingsbeeld 2012.* Politie intern.

Bluhm, K., Borwell, J. & W. Stol (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift voor Veiligheid*, 21, 3-4. doi: 10.5553/TvV/.000045

Borwell, J., J. Jansen & W. Stol (2023). *The psychological impact of cybercrime victimization: The importance of personal and circumstantial factors* [Manuscript under review].

Borwell, J., J. Jansen & W. Stol (2021). Comparing the victimization impact of cybercrime and traditional crime. *Journal of Digital Social Research,* 3(3), 85-110. doi: org/10.33621/jdsr.v3i3.66

Borwell, J., & K. Bos-Riepma (2018). *Tech support scam: Verdiepende analyse.* Groningen: Dienst Regionale Informatieorganisatie, eenheid Noord-Nederland.

Borwell, J. (2017). *Wie wordt de digitale beurs gelicht? De persoonlijkheids-en demografische kenmerken.* Thesis. NHL Hogeschool en Poitieacademie.

Borwell, J., K. Schuppers, J. Rooyakkers & A. Harteveld. (2020). Het cybercrimebeeld van de Nederlandse politie. Van algemeen beeld naar verdiepende analyse en aanpak. In: Poot, C. de, Lievens, E., Stol, W. & Kimpe, L. de (redactie). Politie en Cybercrime. *Cahier Politiestudies,* jaargang 2020, 3(56).

Campman, I., P. Dedert, R. Hesseling & P.J. Huijskens., et al. (2012). *Criminaliteit in een gedigitaliseerde samenleving.* Amsterdam/Den Haag/Rotterdam/Utrecht/ Zoetermeer: Nationale Politie (Politie intern).

Centraal Bureau voor de Statistiek (2023, 11 mei). *Online Veiligheid en Criminaliteit 2022.* CBS. Geraadpleegd van https://www.cbs.nl/nl-nl/longread/rapportages/2023/online-veiligheid-en-criminaliteit-2022

Centraal Bureau voor de Statistiek (2022, 22 september). *Financiële schade van criminaliteit tegen burgers.* CBS. Geraadpleegd van https://www.cbs.nl/nl-nl/longread/statistische-trends/2022/financiele-schade-van-criminaliteit-tegen-burgers

Centraal Bureau voor de Statistiek (2018). *Cybersecuritymonitor 2018: Een verkenning van dreigingen, incidenten en maatregelen.* Den Haag: Centraal Bureau voor de Statistiek.

Centraal Bureau voor de Statistiek (2024). *Veiligheidsmonitor 2023.* Den Haag: CBS.

Centraal Bureau voor de Statistiek (2022). *Veiligheidsmonitor 2021.* Den Haag: CBS.

Centraal Bureau voor de Statistiek (2016). *Veiligheidsmonitor 2015*. Den Haag: CBS.

Centraal Bureau voor de Statistiek (2015, 11 maart). *Tablet verdringt bord van schoot.* Geraadpleegd van https://www.cbs.nl/nl-nl/nieuws/2015/11/tablet-verdringt-bord-van-schoot

CCT Den Haag (2019). *Book of crime BEC-fraude*. Politie intern.

CCT Limburg (2020). *Book of crime: Betaalverzoekfraude*. Politie intern.

CCT Noord-Nederland (2020). *Book of crime: Webshopaccount Takeovers*. Politie intern.

CCT Den Haag (2022). *BEC-fraude: Cijfermatige ontwikkelingen t/m juni 2022.* Politie intern.

De Nederlandsche Bank (2022, 30 november). *Grote verliezen bij huishoudens op beleggingsfondsen*. Geraadpleegd van https://www.dnb.nl/algemeen-nieuws/statistiek/2022/grote-verliezen-bij-huishoudens-op-beleggingsfondsen/#:~:text=Posities%20beleggingsfondsen%20huishoudens%20in%20perspectief&text=De%20totale%20beleggingen%20in%20effecten,%2C7%25%20aangehouden%20beleggingsfondsvermogen%20betreft.

Dennet, D.C. (2023) *The problem with counterfeit people.* Geraadpleegd van https://www.theatlantic.com/technology/archive/2023/05/problem-counterfeit-people/674075/

Dienst Regionale Informatieorganisatie. Eenheid Limburg. (2023). *Strategisch veiligheidsbeeld 2023-2024. Ten aanzien van de geprioriteerde veiligheidsthema's*. Politie intern.

Dienst Landelijke Informatieorganisatie, Analyse & Onderzoek (2022a), *Horizontale fraude: verschuiving naar digitale vormen.* Politie intern.

Dienst Landelijke Informatieorganisatie & Dienst Regionale Informatieorganisatie (2022b). *Cybercrime enge zin & gedigitaliseerde criminaliteit. Overeenkomsten en verschillen: waar ligt het onderscheid?* Politie intern.

Dienst Regionale Informatieorganisatie Rotterdam (2022). *Cybercrime Jaarbeeld 2021*. Politie intern.

Eenheid Amsterdam (2021). *Book of crime: sextortion.* Politie intern.

Eenheid Rotterdam, werkgroep Tech Support Scam (2021). *Book of Crime Tech Support Scam*. Politie intern.

Eenheid Den Haag (2022). *BEC-fraude. Cijfermatige ontwikkelingen 2022.* Politie intern.

Eijndhoven, B. van (2023, 23 mei). *AFM onderzoekt 'finfluencers' na miljoenenverlies beleggers.* Geraadpleegd van https://www.bnr.nl/nieuws/financieel/10513380/afm-onderzoekt-finfluencers-na-miljoenenverlies-beleggers

European Union Agency for Cybersecurity (ENISA, 2022). *ENISA threat landscape for ransomware attacks*. doi: 10.2824/456263.

Europol (2020). *Internet Organised Crime Threat Assessment (IOCTA 2020).* European Union Agency for Law Enforcement Cooperation 2020.

Federal Bureau of Investigation (z.d.). *Internet Crime Report 2023.* Geraadpleegd van https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

Federal Bureau of Investigation (2023, 9 juni). *Public Service Announcement. Business E-mail Compromise: The $50 Billion Scam.* FBI. Geraadpleegd van https://www.ic3.gov/Media/Y2023/PSA230609

Fiscale Inlichtingen en Opsporingsdienst (FIOD)(2023, 23 augustus). *Drie verdachten aangehouden in onderzoek naar omvangrijke beleggingsfraude*. Geraadpleegd van https://www.fiod.nl/drie-verdachten-aangehouden-in-onderzoek-naar-omvangrijke-beleggingsfraude/

Fiscale Inlichtingen en Opsporingsdienst (FIOD)(2023b, 20 april augustus). *Aanhouding vanwege grootschalige beleggingsfraude.* Geraadpleegd van https://www.fiod.nl/aanhouding-vanwege-grootschalige-beleggingsfraude/

Fraudehelpdesk. (2023). *Persbericht jaarcijfers. Fraudehelpdesk: toename telefonische oplichting 2022.* Apeldoorn: Fraudehelpdesk.

Gorissen, M., J. el Akehal, F. Weerman & S. van de Weijer (2020). *Het fenomeen online seksueel geweld. Een literatuuronderzoek naar de kennis over omvang, aard en aanpak.* Den Haag: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

Hesseling, R., A. Harteveld & B.A. Bloem (2021). Jeugdige verdachten van cybercriminaliteit. In A. M. van der Laan, M.G.C.J. Beerthuizen & N.C. Boot (red.). *Monitor Jeugdcriminaliteit 2020. Ontwikkelingen in de jeugdcriminaliteit in de eerste twee decennia van deze eeuw (pp. 143-155)*. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum.

Hesseling, R. (2021). *Horizontale fraude in de eenheid Den Haag - een strategische quickscan.* Politie intern.

Het Financieele Dagblad (23, 11 oktober). *Verdachte Nederlandse 'techinvesteerder' aangehouden in Miami*. Geraadpleegd van https://fd.nl/financiele-markten/1492634/verdachte-nederlandse-techinvesteerder-aangehouden-in-miami#:~:text=De%20van%20beleggingsfraude%20verdachte%20Rutger,gedeponeerd%20bij%20de%20Amerikaanse%20rechtbank

Hupkes c.s. Advocaten (z.d.). *Toename fraude via Anydesk en wallets voor cryptovaluta.* Geraadpleegd van https://www.hupkesadvocaten.nl/toename-fraude-via-anydesk-en-wallets-voor-cryptovaluta/

Inteltafel Cyber (2023). *Cyberintelligencejaarbeeld 2022*. Politie intern.

Junger, M., B. Veldkamp & L. Koning (2022). *Fraudevictimisatie in Nederland. Enschede: Universiteit Twente.* Geraadpleegd van https://www.utwente.nl/nl/bms/fraudvic/fraudevictimisatie-in-nederland.pdf

Kramer, J-A, A. Blokland & M. Soudijn (2020). *Witwassen als bedrijfsmatige activiteit: de verborgen netwerken van witwassers. Tijdschrift voor Criminologie 2020 (62) 4.* doi: 10.5553/TvC/0165182X2020062004001

Koning, M. (2023, 3 februari). *Haar Tinder-date zou haar wel even leren beleggen (reconstructie).* NRC Handelsblad.

Langenburg, V. (2022, 29 augustus). *De strafrechtelijke aanpak van crypto-fraude.* Geraadpleegd van https://www.jaeger.nl/de-strafrechtelijke-aanpak-van-crypto-fraude/

Laumans, W. & P. Vugts (24, 4 augustus). *Hoe twintigers op 'koelbloedige, professionele en stuitende' wijze tientallen ouderen oplichtten.* Geraadpleegd van https://www.ad.nl/binnenland/hoe-twintigers-op-koelbloedige-professionele-en-stuitende-wijze-tientallen-ouderen-oplichtten~a9223030/

Leidse hoofdverdachte sextortion-zaak op vrije voeten (2020, 11 februari). *Omroep West.* Geraadpleegd van https://www.omroepwest.nl

Leukfeldt, E. R., & Holt, T. J. (2022). *Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. Computers in Human Behavior, 126.* https://doi.org/10.1016/j.chb.2021.106979

Leukfeldt, R., Notté, R. & M. Malsch (2018). Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit. Den Haag: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) & Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Marketing Tribune (2022, 27 juni). *Ruim een derde Nederlanders verkoopt tweedehands spullen.* https://www.marketingtribune.nl/algemeen/nieuws/2022/06/ruim-een-derde-nederlanders-verkoopt-tweedehands-spullen/index.xml#:~:text=Uit%20het%20onderzoek%20komt%20naar,te%20komen%20van%20unieke%20stukken

Ministerie van Justitie en Veiligheid (2023). *Actieplan Online Fraude.* Geraadpleegd van https://www.eerstekamer.nl/overig/20230224/actieplan_online_fraude/document

Ministerie van Veiligheid en Justitie (2023). *Veiligheidsagenda 2023 - 2026.* Den Haag: Ministerie van Veiligheid en Justitie.

Ministerie van Justitie en Veiligheid (2019). *Uitwerking Veiligheidsagenda 2019 - 2022*. Den Haag: Ministerie van Justitie en Veiligheid.

Miramirkhani, N., Starov, O. & Nikiforakis, N. (2017). *Dial One for Scam: A Large-Scale Analysis of Technical Support Scams*, published on NDSS 2017 of the Internet Society. https://arxiv.org/pdf/1607.06891

Motké, S., Sewuster, P. & J. Belboer (2023, 23 mei). *Beleggers verliezen 5 miljoen op platform na promotie door finfluencers.* Financieel Dagblad. https://fd.nl/financiele-markten/1473968/beleggers-verliezen-5-mln-op-platform-na-promotie-door-finfluence

NCTV & NCSC (2022): Nationaal Coördinator Terrorismebestrijding en Veiligheid & Nationaal Cyber Security Centrum (2022). *Cybersecuritybeeld Nederland*. CSBN 2022. Den Haag: NCTV.

Nederlandse Vereniging van Banken (2023, 29 maart). *Meer samenwerking essentieel in strijd tegen online fraude.* https://www.nvb.nl/nieuws/meer-samenwerking-essentieel-in-strijd-tegen-online-fraude/

Nederlandse Vereniging van Banken (2022, 8 april). *Online oplichters richten zich steeds meer op de klant*. https://www.nvb.nl/nieuws/online-oplichters-richten-zich-steeds-meer-op-de-klant/

Nederlandse Vereniging van Banken (2021, 4 juni). *Toetsingscriteria voor coulance bij schade door bankhelpdeskfraude*. Geraadpleegd van https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing

Nederlandse Vereniging van Banken, 2019, 27 maart). *3,81 miljoen euro schade door phishing bij internetbankieren in 2018*. Geraadpleegd van https://www.betaalvereniging.nl/actueel/nieuws/381-miljoen-euro-schade-door-phishing-bij-internetbankieren-in-2018/

Openbaar Ministerie & Politie (2024). *Cybercrimebeeld Nederland 2024.* Geraadpleegd van https://fts.politie.nl/cybercrimebeeld/

Plas, T. van der (2021). *Voortgangsrapportage 2021. Programma Cybercrime, Centurion en LMIO*. Politie intern.

Politie maakt zich zorgen over sextortion: bedreigingen worden steeds erger (2023, 25 augustus). WNL.tv. Geraadpleegd van https://wnl.tv

PWC (2021). *Economic Crime Survey 2021.* Geraadpleegd op 17 juni 2024, van https://www.pwc.nl/nl/actueel-publicaties/assets/pdfs/pwc-economic-crime-survey-2021.pdf

Roks, R.A, E.R. Leukfeldt & J.A. Densley (2020). The Hybridization of Street Offending in the Netherlands. *The British Journal of Criminology: an international review of crime and society.* doi:10.1093/bjc/azaa091

Roks, R. & N. Monshouwer (2019). F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiele Verkenningen*, 2(20), 44-58.

Rooyakkers, J. & M. Weulen Kranenbarg (2020). Vissen met een nieuwe hengel: een onderzoek naar betaalverzoekfraude. *Justitiële verkenningen*, 46(2), 19-43.

Schuilenburg, M. & Soudijn , M. (2024). AI-criminaliteit: Een verkenning van actuele verschijningsvormen. *Justitiële verkenningen*, 1(50), 12-29.

Schuppers, K. (2018). Frauduleuze bestellingen door middel van account takeover: Aard, omvang, ontwikkeling en barrières [conceptrapportage]. Den Haag: Dienst Regionale Informatieorganisatie (DRIO).

Sloot, B. van der & Y. Wagensveld (2022). Deepfakes: regulatory challenges for the synthetic society. *Computer Law & Security Review*, 46, doi: https://doi.org/10.1016/j.clsr.2022.105716

Smith, M. (z.d.). *Jonge crypto-oplichter leidde luxeleventje maar moet nu cel in.* Geraadpleegd van https://www.rtl.nl/rtl-nieuws/artikel/5269056/celstraf-oplichter-witwassen-crypto-bitnextfast-pieter-j

Staats, W., C. Meerts E. Kleemans & W. Huisman (2021). *Nieuwe manieren van samenwerken. Een systematische literatuurreview naar de (effectiviteit van) publiek-private samenwerking op het gebied van financieel-economische criminaliteit en cybercrime*. Amsterdam: Vrije Universiteit.

Thuiswinkel.org (2023, 21 maart). *Nederlandse consument geeft online 33,3 miljard uit in 2022.* https://www.thuiswinkel.org/webshops/nieuws/nederlandse-consument-geeft-online-33-3-miljard-uit-in-2022/#:~:text=Nederlanders%20hebben%20in%202022%20voor,is%20daarmee%20toegenomen%20met%2015%2

Veen, H.C.J., van der & L.F. Heuts (2024). *National Risk Assessment Witwassen.* Den Haag: WODC.

Vemde, S. van & N. van Dam (2020). *Digitale factuurfraude en CEO-fraude bij profit en non-profit organisaties*. Politie intern.

Wagen, W. van der, J.J. Oerlemans & M. Weulen Kranenbarg (2020). *Basisboek cybercriminaliteit.* Den Haag: Boom Criminologie.

Weijer, S.G.A. van de, E.R. Leukfeldt & S. van der Zee (2020). *Slachtoffer van onlinecriminaliteit, wat nu? Een onderzoek naar aangiftebereidheid onder burgers en ondernemers.* Den Haag: Sdu Uitgevers.

Willekers, M., K. Schuppers & A. Merk (2024). *Online Blauw – Kwantitatief onderzoek naar digitale criminaliteit op basis van politiedata.* DRIOs. Politie intern.

Wolsink, J., Kuppens, J., N. Brouwer & H. Ferwerda. (2023). Mismatch. *Een verkennend fenomeenonderzoek naar het plegen van zedendelicten na contact via een datingsite of datingapp*. Den Haag: Politie & Wetenschap, Arnhem: Bureau Beke.

Meer fenomeenbeelden

Bekijk alle fenomeenbeelden op:
www.politie.nl/informatie/publicaties-over-georganiseerde-criminaliteit

Colofon
Uitgave:
Eenheid Landelijke Expertise en Operaties (LX)
Postbus 100
3970 AC Driebergen

Zoetermeer, september 2024
Rubricering: niet vertrouwelijk

Projectmanager:
Alexandra van den Heerik, LO & LX

Vormgeving:
Team Productie, Politiedienstencentrum, LO & LX.

Wijze van verwijzen:
Online fraude in beeld: Fenomeenbeeld Online fraude 2024. Politie, Eenheid Landelijke Opsporing en Interventies & Eenheid Landelijke Expertise en Operaties.

P-24-3006-04