Online criminaliteit

2024

DRIO Den Haag
Cluster Cyber Intel
Juni 2024

<Rubricering extern>

Inhoudsopgave

Online criminaliteit

Inleiding

Het internet is niet meer weg te denken uit het dagelijks leven. In 2022 gebruikten bijna alle 12-plussers (94%) in Nederland het internet.[1] De sterk gedigitaliseerde samenleving genereert een gunstige gelegenheidsstructuur voor criminaliteit. Hierdoor is het werkaanbod voor de politie in de afgelopen jaren veranderd en hebben steeds meer delicten een digitale component.

Na de piekjaren in 2020 en 2021 (coronaperiode) is het totaal aantal meldingen en aangiften over online criminaliteit afgenomen. Het aantal meldingen en aangiften bleef in 2023 stabiel (zie voor de cijfers op gemeenteniveau bijlage 1 en 2). De afname is deels het gevolg van een daling van de aangiftebereidheid, deze is voor online delicten gedaald van 19% in 2021 naar 16% in 2023 binnen de Eenheid Den Haag (landelijk is deze trend ook zichtbaar).[2] Echter, er is op basis van de Veiligheidsmonitor 2023 ook een significante daling van het zelfgerapporteerde slachtofferschap van online criminaliteit zichtbaar (van 17,6% in 2021 naar 15,7% in 2023).

Bij de geschetste ontwikkelingen over online criminaliteit dient de kanttekening geplaatst te worden dat door de lage meldings- en aangiftebereidheid er sprake is van een groot dark number. Ook varieert de meldings- en aangiftebereidheid naar het soort delict. Uit de Veiligheidsmonitor blijkt bijvoorbeeld dat van fraude in het betalingsverkeer 25% van de burgers aangifte doet bij de politie terwijl van hacken slechts 9% aangifte doet.[3] Daarbij maakt de wijze waarop online criminaliteit bij de politie wordt geregistreerd het lastig om de precieze omvang in kaart te brengen. Verder is er minder goed zicht op de omvang van online delicten die in de persoonsgerichte sfeer worden gepleegd zoals stalking, bedreiging en smaad/laster/belediging. Politiecijfers geven dus geen volledig beeld van de werkelijke aard en omvang van online criminaliteit.

Online criminaliteit heeft uiteenlopende verschijningsvormen. Bij deze vormen kan zowel sprake zijn van cybercrime (ICT is zowel het doel als het middel) als van gedigitaliseerde criminaliteit (ICT is alleen het middel). Een strikt onderscheid tussen cybercrime en gedigitaliseerde criminaliteit kan niet altijd gemaakt worden, aangezien verschijningsvormen van online criminaliteit vaak mengvormen betreffen. In deze bijdrage wordt dieper ingegaan op de belangrijkste ontwikkelingen in relatie tot de meest voorkomende verschijningsvormen van online criminaliteit.

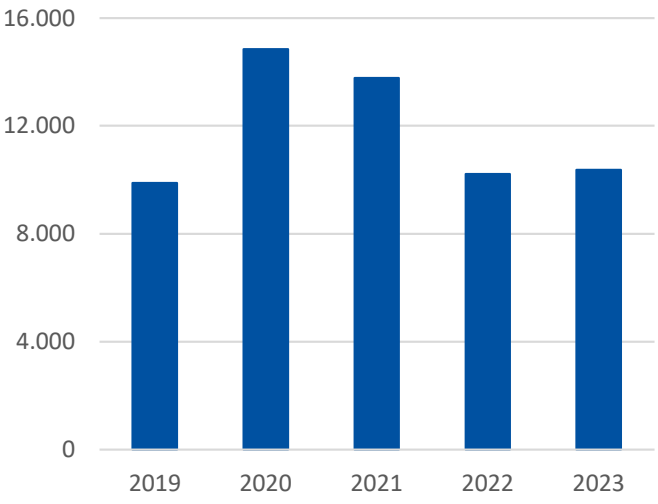
Online fraude

Online criminaliteit waarvan burgers melding of aangifte doen bij de politie betreft voornamelijk online fraude. Uit een recentelijk landelijk onderzoek is gebleken dat in de periode oktober 2022 – september 2023 driekwart van de registraties online fraude betreft.[4]

Online fraude hardnekkig veiligheidsprobleem

Al jaren vindt online fraude op grote schaal plaats in Nederland. Na de coronaperiode is het aantal registraties over online fraude zowel landelijk als in de Eenheid Den Haag gedaald in 2022 en vervolgens redelijk gelijk gebleven in 2023 (zie grafiek 1).

Grafiek 1. Ontwikkeling totaal geregistreerde online fraude Eenheid Den Haag[5]



Online criminaliteit

Online fraude blijft een omvangrijk probleem. Dit is vanwege het verdienmodel dat ondanks continue ontwikkelingen op het gebied van preventie lucratief blijft. Zo is het relatief eenvoudig om online fraude te plegen, omdat kennis en benodigdheden te verkrijgen zijn via anonieme markt- en ontmoetingsplaatsen op zowel het dark web als het clear web, maar ook via berichtendiensten als Telegram. Te denken valt aan phishing panels, lijsten met persoonsgegevens (leads), gestolen accountgegevens en handleidingen over modus operandi. De beschikbaarheid van deze kennis en kunde werkt drempelverlagend voor potentiële fraudeurs om toe te treden tot de criminele markt.[6] Ook zijn de opbrengsten van online fraude meestal hoger in vergelijking met delicten als woninginbraken of diefstal. Dit komt onder meer door de schaalbaarheid van online fraude; met weinig inspanningen kan een grote hoeveelheid slachtoffers tegelijkertijd worden gemaakt. Verder biedt het internet een hoge mate van anonimiteit, waardoor de perceptie van de pakkans van daders laag is.[7]

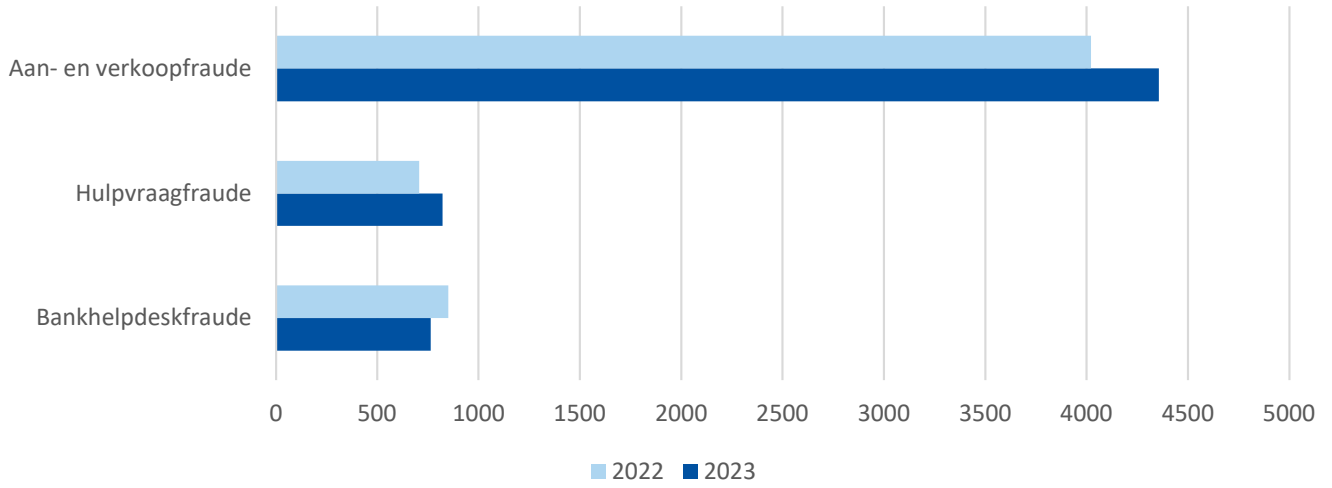
Top drie veelvoorkomende verschijningsvormen wijzigt nauwelijks

Verreweg de meest voorkomende vorm van online fraude is aan- en verkoopfraude; bijna de helft van de aangiftes over online fraude gaan over aan- en verkoopfraude. Andere veelvoorkomende vormen van online fraude betreffen hulpvraagfraude en bankhelpdeskfraude. De top drie van veelvoorkomende verschijningsvormen van online fraude is in 2023 ten opzichte van 2022 nauwelijks gewijzigd (zie grafiek 2).

Aan- en verkoopfraude betreft fraude bij het online (ver)kopen van goederen en diensten, bijvoorbeeld via Marktplaats, webwinkels of social media. Het aantal gevallen van aan- en verkoopfraude ligt in 2023 iets hoger dan in 2022, maar bereikt niet meer het hoge niveau van de coronaperiode. Uit het dashboard van het Landelijk Meldpunt Internetoplichting blijkt dat slachtoffers in laatste helft van 2023 steeds vaker via malafide webshops worden opgelicht.

Bij hulpvraagfraude (ook wel vriend-in-noodfraude of Whatsapp-fraude genoemd) doet de oplichter zich meestal via WhatsApp voor als een bekende die beweert dringend financiële hulp nodig te hebben. Het aantal meldingen en aangiften over hulpvraagfraude was in 2022 enorm teruggelopen, mogelijk als gevolg van verschillende bewustwordingscampagnes. Echter, begin 2023 is weer sprake van een opleving van het aantal gevallen van hulpvraagfraude (+13%). Mogelijk heeft dit te maken met subtiele aanpassingen in de MO, zoals het slachtoffer eerst per sms benaderen in plaats van direct via WhatsApp (zie bovenstaand voorbeeld).

Grafiek 2. Ontwikkeling totaal geregistreerde online fraude Eenheid Den Haag[8]



Verder zijn er signalen dat Nederlandse verdachten van hulpvraagfraude hun focus deels verleggen naar buitenlandse slachtoffers in bijvoorbeeld België en Duitsland. Uit een landelijke verkenning naar criminele netwerken achter geldezels[9] blijkt dat hiervoor aanwijzingen zijn gevonden in in beslag genomen telefoons. Ook zijn bij huiszoekingen buitenlandse simkaarten aangetroffen en is in een opsporingsonderzoek gebleken dat Nederlandse dadergroepen Belgische geldezels ronselen. Bij de Eenheid Den Haag zijn er in 2023 bijna 30 Europese Onderzoeksbevelen (EOB's) binnengekomen over personen die wonen in de Eenheid Den Haag en verdacht worden van hulpvraagfraude in het buitenland (met name in Duitsland).

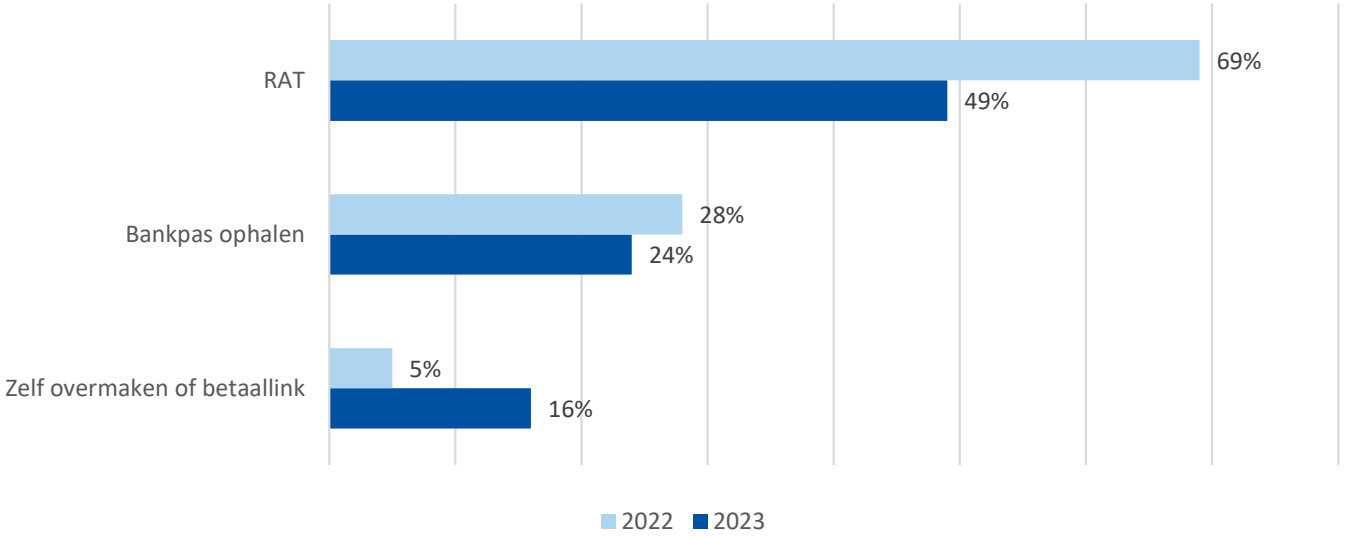
Het aantal meldingen/aangiften over bankhelpdeskfraude zagen we in 2022 sterk toenemen en dat aantal is in 2023 op hetzelfde hoge niveau gebleven. Bankhelpdeskfraude is een vorm van oplichting waarbij het slachtoffer gebeld wordt door een zogenaamde bankmedewerker die hem/haar probeert te overtuigen dat het geld niet veilig is op zijn/haar bankrekening. Vaak "helpt" de oplichter bij het veiligstellen van het geld door gebruik te maken van een Remote Acces Tool (RAT). Hiermee kan de computerbesturing worden overgenomen en kan de dader zichzelf toegang verschaffen tot de bankrekening van het slachtoffer. In 2023 is in bijna de helft van de gevallen van bankhelpdeskfraude gebruik gemaakt van een RAT. Dat aantal is lager dan in 2022 toen ruim twee derde van de bankhelpdeskfraudes plaatsvond met een RAT (zie grafiek 3).

De variant waarbij het slachtoffer zelf het geld overmaakt of een vals betaalverzoek betaalt, is daarentegen toegenomen in 2023. Bij een andere vorm van bankhelpdeskfraude komt de dader thuis langs bij het slachtoffer om de bankpas op te halen. Zowel in 2022 als in 2023 is in ongeveer een kwart van de gevallen sprake van deze variant (zie grafiek 3). In sommige gevallen nemen de daders hierbij ook kostbaarheden zoals sieraden mee. Verder is in 2023 een verandering in de benaderingswijze van slachtoffers geconstateerd. In plaats van gebeld te worden door de bank, ontvangen slachtoffers steeds vaker een sms waarin wordt verzocht de bank te bellen naar aanleiding van bijvoorbeeld een nieuwe aanvraag voor een bankpas.

Verschuivingen in verschijningsvormen en modus operandi

Online fraudeurs zijn flexibel en passen hun werkwijze en gebruik van infrastructuur voortdurend aan. De frequentie van deze aanpassingen is afhankelijk van de effectiviteit van de gebruikte modus operandi. Een werkwijze kan minder effectief worden als deze wordt verstoord door maatregelen van publieke en private instanties of wordt herkend door potentiële slachtoffers.[11] Daarnaast houden online fraudeurs rekening met de actualiteiten en de jaargetijden. Zo zijn mensen rond de feestdagen en Black Friday vatbaarder voor oplichting bij online winkelen.

Grafiek 3. Verhouding verschillende varianten bankhelpdeskfraude[10]



Online criminaliteit

Net zoals in de voorgaande jaren zijn ook in 2023 subtiele wijzigingen in werkwijzen waargenomen (zie hiervoor bij hulpvraagfraude en bankhelpdeskfraude). Een voorbeeld is dat phishinglinks in 2023 in toenemende mate via QR-codes verspreid worden. Ook zien we in 2023 bepaalde verschijningsvormen toenemen en andere juist afnemen. Drie verschijningsvormen die zijn afgenomen zijn betaalverzoekfraude, misbruik van accounts voor bestellingen en helpdeskfraude (zie grafiek 4).

Betaalverzoekfraude is een vorm van cybercrime waarbij het slachtoffer een betaalverzoek ontvangt dat een phishinglink bevat om inloggegevens van de bankomgeving van het slachtoffer te ontfutselen. Het betaalverzoek wordt meestal gedaan in de context van tweedehands handelsplatformen zoals Marktplaats. Betaalverzoekfraude is in 2022 al sterk afgenomen onder andere door maatregelen van Marktplaats en verbeterde detectiesystemen van banken. Deze daling heeft zich doorgezet in 2023.

Van misbruik van accounts voor bestellingen is sprake als de oplichter een webaccount van een slachtoffer hackt en deze vervolgens gebruikt voor het doen van bestellingen van producten en diensten. Ook komt het voor dat de oplichter de identiteits- en adresgegevens van het slachtoffer gebruikt om een nieuw webaccount aan te maken. In de registraties komt naar voren dat de fraude vooral plaatsvindt bij webshops als Zalando en Bol.com. In 2022 steeg het aantal registraties over misbruik van bestellingen met 20%, maar in 2023 is het aantal weer met een kwart gedaald.[12]

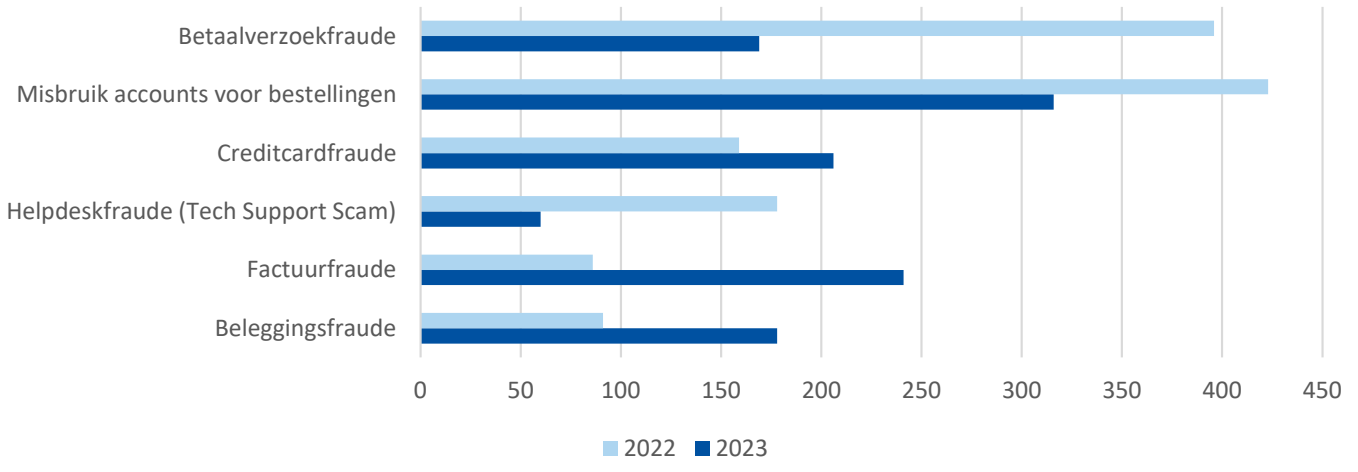
Mogelijk hebben maatregelen van de webshops en bedrijven die een achteraf-betaalservice bieden, invloed gehad op deze afname.

Een andere opvallende daler is helpdeskfraude (Tech Support Scam). Bij deze vorm van helpdeskfraude heeft een slachtoffer telefonisch contact met een zogenaamde medewerker van Microsoft of een ander softwarebedrijf. De oplichter overtuigt het slachtoffer van problemen met diens computer en maakt het slachtoffer geld afhandig. Het is onduidelijk waarom deze verschijningsvorm zo sterk gedaald is. Mogelijk door maatregelen van Microsoft en/of door een toegenomen bewustwording bij burgers.

De verschijningsvormen digitale factuurfraude, creditcardfraude en beleggingsfraude zijn in 2023 juist toegenomen. De stijging bij digitale factuurfraude is terug te voeren op valse betaalverzoeken namens de Belastingdienst waarin bijvoorbeeld wordt verzocht een openstaande schuld te voldoen. In bijna 60% van de gevallen van factuurfraude betreft het een dergelijk vals betaalverzoek van de Belastingdienst.

Bij beleggingsfraude worden slachtoffers meestal overgehaald om geld te investeren in cryptovaluta (zoals Bitcoins). Vervolgens lijken de winsten flink toe te nemen en worden de slachtoffers ertoe bewogen om meer geld te investeren. Slachtoffers zien uiteindelijk niets terug van hun inleg en de zogenaamde rendementen. Het werven van de slachtoffers gebeurt veelal via sociale media platformen zoals Facebook en YouTube.

Grafiek 4. Dalers en stijgers online fraude binnen de Eenheid Den Haag[13]



Schade neemt op sommige vlakken af

Het totale gemelde schadebedrag van online fraude is in 2023 veel hoger dan in 2022. Zo bedroeg de totale schade van online fraude in 2022 in de Eenheid Den Haag bijna €23 miljoen en in 2023 bijna €70 miljoen.[14] Echter, het schadebedrag in 2023 wordt vertekend door een uitschieter van één aangifte van diefstal van cryptomunten waarbij sprake was van een schade van €55 miljoen. Zonder dit gigantische schadebedrag komt de totale schade voor 2023 uit op bijna €15 miljoen; een stuk lager dan in 2022. Dit komt onder andere door een daling van de schade van bankhelpdeskfraude (gedaald van ruim €6 miljoen in 2022 naar ruim €4 miljoen in 2023). Ook uit landelijke cijfers blijkt dat de financiële schade van bankhelpdeskfraude flink is afgenomen. Het gemiddelde schadebedrag van bankhelpdeskfraude is gezakt van gemiddeld €13.770 euro in 2020 naar €6.771 euro in 2023.[15] Mogelijk hebben verschillende interventies, zoals het verlagen van de daglimieten door de banken voor het overmaken van grote sommen geld, geresulteerd in lagere schadebedragen door bankhelpdeskfraude. Aan de andere kant zien we dat het totale schadebedrag van beleggingsfraude in de Eenheid Den Haag toegenomen is van ruim €2 miljoen in 2022 naar ruim €3,5 miljoen in 2023. De schade is omvangrijk bij beleggingsfraude door een hoog gemiddeld schadebedrag (ruim €20.000).

Impact op slachtoffers kan groot zijn

Online fraude kan een enorme impact hebben op slachtoffers. Naast de financiële schade (die overigens niet altijd vergoed wordt), kunnen gevoelens van schaamte en angst optreden.

Uit verschillende studies komt naar voren dat de impact van online criminaliteit vaak onderschat wordt en grotendeels overeenkomt met die van traditionele criminaliteit.[16] Recent onderzoek[17] laat zelfs zien dat slachtoffers van bijvoorbeeld een gehackte bankomgeving significant meer peritraumatische stress en aantasting van het zelfbeeld ervaren dan slachtoffers van een traditionele inbraak.

Ouderen blijven kwetsbaar voor online fraude

Het slachtofferprofiel van slachtoffers van online fraude wijzigt nauwelijks ten opzichte van 2022. Ook in 2023 blijkt dat vooral personen in de oudere leeftijdscategorieën worden getroffen door bankhelpdeskfraude en hulpvraagfraude (zie tabel 1). Uit landelijke cijfers blijkt eveneens dat 80% van de slachtoffers van bankhelpdeskfraude ouder is dan 60.[18]

Bij aan- en verkoopfraude zijn het juist personen in de jongere leeftijdscategorieën die vaker slachtoffer worden. De meeste slachtoffers van fraude met online handel zijn tussen de 35 en 54 jaar. Jongere mensen zijn waarschijnlijk actiever in het doen van online aankopen in vergelijking tot ouderen.

Slachtoffers van de overige vormen van online fraude en oplichting zijn redelijk evenredig verdeeld over de leeftijdscategorieën. Het gaat hierbij om online fraudevormen als betaalverzoekfraude, beleggingsfraude, misbruik van accounts voor bestellingen, creditcardfraude en factuurfraude.

Bij slachtoffers van online fraude is vaak sprake van herhaald slachtofferschap van verschillende varianten van online fraude. Gegevens van slachtoffers worden namelijk regelmatig doorverkocht met als gevolg dat een slachtoffer opnieuw risico loopt een doelwit te worden.[19]

Tabel 1: Aantal slachtoffers per 1.000 inwoners naar leeftijd in 2023[20]

Leeftijdscategorie	Bankhelpdeskfraude	Fraude met online handel	Hulpvraagfraude	Overige Fraude/oplichting
0 t/m 17	0,00	0,43	0,01	0,04
18 t/m 24	0,04	3,03	0,15	0,78
25 t/m 34	0,05	3,22	0,22	0,93
35 t/m 44	0,17	4,28	0,31	0,99
45 t/m 54	0,25	3,35	0,42	1,02
55 t/m 64	0,52	2,05	0,81	0,93
65 jaar of ouder	1,26	0,80	0,91	0,78

De gemiddelde verdachte is jong en vervult de rol van geldezel

In 2023 zijn er ten opzichte van de jaren ervoor meer verdachten van online criminaliteit uit de Eenheid Den Haag in beeld gekomen (zie grafiek 5). De stijging is terug te voeren op de toename van verdachten voor fraude met online handel (van 139 in 2022 naar 483 verdachten in 2023). De stijging kan in verband gebracht worden met de nieuwe werkwijze van het Landelijk Meldpunt Internetoplichting (LMIO) die 1 juli 2023 is ingegaan. Internetaangiftes worden volgens deze werkwijze automatisch gerouteerd op basis van de woonplaats van de verdachte.[22]

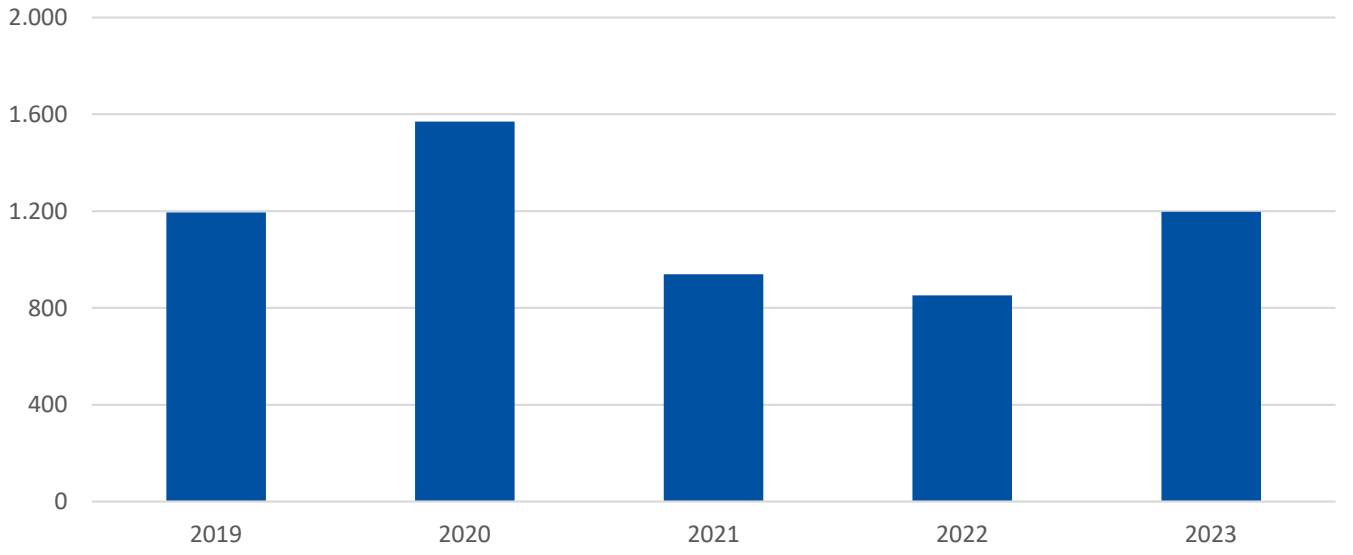
Net zoals voorgaande jaren zijn de verdachten die in beeld komen voor (de meeste vormen van) online fraude voor een substantieel deel jongvolwassen mannen tussen de 18 en 24 jaar. Bij fraude met online handel valt wel op dat de verdachten in 2023 minder vaak minderjarigen betreffen. Zo was in 2022 ongeveer 40% van de verdachten minderjarig. In 2023 is dit aandeel gezakt naar 12%.

Uit het verdachtenbeeld[23] blijkt dat in de periode juni 2023 – januari 2024 vooral laaghangend fruit in beeld is gekomen bij de politie. Ruim 60% van de verdachten vervult de rol van geldezel (iemand die al dan niet bewust zijn of haar bankrekening laat gebruiken voor criminele doeleinden). Geldezels lopen het meeste risico om tegen de lamp te lopen, omdat ze eenvoudig te traceren zijn. Vaak zijn geldezels personen die makkelijk te beïnvloeden zijn zoals immigranten of mensen met schulden of een licht verstandelijke beperking.[24]

Andere rollen die regelmatig voorkomen zijn die van casher en ophaler. Een casher haalt het geld dat is gestort op de rekening van een geldezel, bij een geldautomaat uit de muur. De ophaler haalt onder andere bankpassen op bij slachtoffers. Een enkele keer komen verdachten in beeld die relevantere rollen vervullen zoals die van een ronselaar of een hacker.

In de afgelopen jaren is verwevenheid tussen traditionele en digitale criminaliteit geconstateerd.[25] (Leden van) criminele jeugdgroepen hebben hun criminele activiteiten uitgebreid naar het digitale domein. Dit komt bijvoorbeeld tot uiting in bepaalde Telegram-groepen waarin jongeren informatie en diensten uitwisselen voor het plegen van online fraude en in (drill)rapmuziek waarin gepocht wordt over hun succes in wat zij de F-game (fraudegame) noemen.[26] Hierdoor bestaan er zorgen dat onder verdachten van online fraude in toenemende mate sprake is van geweldstoepassing. In een landelijk onderzoek[27] signaleren experts uit de politiepraktijk in toenemende mate gebruik van geweld en wapenbezit. Te denken valt aan cybercriminelen die elkaar rippen. Toch zijn er - voor zover bekend - binnen de Eenheid Den Haag in 2023 weinig raakvlakken tussen verdachten van online fraude en kernleden binnen de rivaliserende jeugdgroepen. Ook blijkt uit het landelijke onderzoek dat geweldsincidenten onder cybercriminelen vooralsnog weinig voorkomen. Hierbij dient opgemerkt te worden dat goed zicht hierop bij de politie wellicht ontbreekt.

Grafiek 5. In beeld gekomen verdachten online criminaliteit woonplaats Eenheid Den Haag[21]



Ransomware

Ransomware is malware die data- en systeembestanden versleutelt. Vaak moet het slachtoffer een losgeldbedrag betalen om de bestanden en systemen weer toegankelijk te maken of om te voorkomen dat de data gepubliceerd wordt.

Ransomware wordt in Nederland nog steeds gezien als de grootste bedreiging voor de digitale veiligheid.[28] Het maakt een prominent deel uit van de verstorende cyberaanvallen in Nederland. Ransomware kan tot gevolg hebben dat de bedrijfscontinuïteit van (vitale) organisaties verstoord wordt of dat gevoelige informatie op straat komt te liggen. Ook kan buitgemaakte informatie worden verhandeld en gebruikt worden om andere misdrijven mee te plegen.

Stijging ransomware-aanvallen wereldwijd en in Nederland

In 2022 was sprake van een dalling van het aantal ransomware-aanvallen. Deze daling hield waarschijnlijk verband met het uitbreken van de oorlog in Oekraïne.[29] Vanaf het voorjaar van 2023 lijkt het aantal ransomware-aanvallen zowel wereldwijd[30] als in Nederland[31] weer toe te nemen. Een groeiend aantal nieuwe spelers lijkt actief te zijn.[32] Ook maakt de verdere verspreiding van 'Ransomware-as-a-Service' (RaaS)-programma's in combinatie met de hoge winsten het eenvoudig en aantrekkelijk voor kleinere spelers om tot de ransomware-markt toe te treden.[33]

De aangiften bij de politie laten deze stijging daarentegen niet zien. Echter, van ransomware wordt zelden melding gedaan bij de autoriteiten.[34] In 2023 zouden volgens de politiecijfers iets meer dan 100 incidenten bij organisaties in Nederland hebben plaatsgevonden. Door cybersecuritybedrijven konden nog eens 40 unieke incidenten[35] aan deze aantallen toe worden gevoegd.[36]

Toename schade ondanks afname betalingsbereidheid

De bereidheid van slachtoffers om losgeld te betalen lijkt wereldwijd af te nemen.[37] Waar deze in 2022 nog rond de 40% lag, is deze in 2023 gedaald naar rond de 30%. In Nederland was de bereidheid om losgeld te betalen in 2023 slechts 18%.[38] Een verklaring hiervoor is de toegenomen weerbaarheid van organisaties. Organisaties investeren in een goed back-up beleid, het beveiligen van netwerken en voorlichting van personeel. Uit de praktijk blijkt dat organisaties minder snel geneigd zijn losgeld te betalen indien ze goed kunnen herstellen.[39]

Hoewel de betalingsbereidheid van losgeld is gedaald, is het wereldwijde totale schadebedrag[40] dat is betaald flink toegenomen (van $567 miljoen naar $1,1 miljard).[41] Hierin zijn de kosten door verlies aan bedrijfscontinuïteit, herstelkosten en reputatieschade nog niet meegenomen. Bovendien wordt veel losgeld betaald in de vorm van cryptocurrency, wat lastig te traceren is. Dit maakt dat het daadwerkelijke schadebedrag waarschijnlijk nog hoger ligt.

De stijging in het totaal betaalde schadebedrag, ondanks de gedaalde betalingsbereidheid, kan te maken hebben met de toename van het aantal ransomware-aanvallen. Daarnaast is steeds vaker sprake van losgeldbedragen die minstens één miljoen dollar bedragen waardoor het gemiddelde losgeldbedrag hoger is komen te liggen.[42]

Grote vermogende (vitale) organisaties vaker doelwit

Ransomwaregroepen blijven hun werkwijze en afpersingstechnieken verfijnen om efficiënter te werken en de betalingsbereidheid van slachtoffers te vergroten. Zo is het in het afgelopen jaar opgevallen dat ransomwaregroepen steeds vaker de "big game hunting' strategie toepassen. Hierbij worden gericht grote, vermogende organisaties aangevallen.[43] Hieronder vallen ook organisaties in de vitale sectoren zoals de zorg- en publieke sector. Dit soort organisaties zijn eerder bereid om losgeld te betalen om hun bedrijfsproces te kunnen hervatten en te voorkomen dat gevoelige gegevens uitlekken. Op basis van leakpages wordt een wereldwijde toename van aanvallen in de zorgsector gesignaleerd.[44] In Nederland is hier vooralsnog geen sprake van. Toch kan niet worden uitgesloten dat ook de Nederlandse publieke sector de komende tijd vaker doelwit zal zijn van ransomware-aanvallen.

Meer hybride vormen van ransomware-aanvallen

Verder is vanaf 2019 de trend zichtbaar dat gegevens geëxfiltreerd worden. Dit kan een tactiek op zichzelf zijn of wordt in combinatie met het versleutelen van gegevens uitgevoerd.[45] Ransomware-groepen persen hun slachtoffers af met publicatie van de gegevens op speciale leaksites op het dark web. Daarnaast kunnen de gegevens aangevuld worden met andere buitgemaakte informatie en worden doorverkocht aan andere criminelen.[46] De bibliotheek van Gouda werd in juni 2023 slachtoffer van ransomware. De aanvallers claimden 30 gigabyte aan data buit te hebben gemaakt en persoonlijke gegevens van personeel en klanten werden op het darkweb gelekt.[47]

Het komt ook in toenemende mate voor dat criminelen enkel inbreken op systemen zonder ransomware te gebruiken. Vervolgens wordt er losgeld geëist om bijvoorbeeld een ransomware-aanval of publicatie van de inbraak te voorkomen. Vanaf december 2023 gelden aangescherpte vereisten voor het melden van cyberincidenten. Organisaties die zich hier niet aanhouden riskeren hoge boetes, waardoor openbaring van een inbraak niet enkel reputatieschade met zich mee kan brengen.[48]

De verwachting is dat in de toekomst vaker hybride vormen van ransomware-aanvallen uitgevoerd worden waarbij geschakeld wordt tussen exfiltratie, versleuteling of vernietiging van data of inbraak zonder het gebruik van ransomware. De keuze van de toegepaste techniek is voornamelijk afhankelijk van de waarde van de gegevens.[49]

Ook vindt er veel zogenaamde ‘rebranding’ plaats onder ransomware-aanvallers om beter onder de radar te blijven. Ransomware-groepen gaan verder onder een nieuwe naam of delen van de groep splitsen zich af.[50] Hierdoor kunnen slachtoffers ook tweemaal door dezelfde aanvallers worden geraakt. Voor de opsporingsinstanties is het daardoor lastig om te achterhalen wie er achter een aanval zit.

Sextortion

Sextortion is een vorm van afpersing waarbij wordt gedreigd om seksueel getint beeld(materiaal) openbaar te maken of te verspreiden.

Toegenomen aantal meldingen en aangiften

In 2023 is het aantal registraties over sextortion gestegen ten opzichte van 2022. Een kanttekening hierbij is dat er in 2023 een wijziging heeft plaatsgevonden in de LCQ waardoor de stijging mogelijk deels een registratie-effect is. Toch is de stijging van het aantal registraties over sextortion een trend die al langer zichtbaar is.

Veel slachtoffers komen waarschijnlijk niet in beeld bij de politie, omdat zij vaak geen melding of aangifte doen uit schaamte of angst voor ‘victim blaming’.[51] De daadwerkelijke omvang van sextortion ligt waarschijnlijk dus een stuk hoger.

Meestal is sprake van een financieel motief

Bij de meeste gevallen van sextortion ligt er een financieel motief aan ten grondslag (86% in 2023). Vaak gebruikt de dader een nepprofiel van een sociaal digitaal platform om het slachtoffer te benaderen. Het eerste contact verloopt meestal via sociale media kanalen zoals Instagram (62%), maar ook via datingapplicaties of -websites (12%) of online chatwebsites (9%). Vaak wordt het slachtoffer via social engineering overtuigd om vrijwillig seksueel getint materiaal af te geven. Vervolgens wordt het slachtoffer met dit materiaal afgeperst.

In ongeveer 12% van de gevallen is sprake van sextortion met een seksueel motief. Hierbij wordt het slachtoffer ertoe gedwongen om meer seksueel getint materiaal aan te leveren, seksuele handelingen met de dader te verrichten of zelfs een (seksuele) relatie aan te gaan met de dader. Een derde van de slachtoffers van sextortion met een seksueel motief kent de dader persoonlijk (vaak een ex-partner). In de gevallen dat het slachtoffer de dader niet kent wordt het eerste contact vooral via Snapchat gelegd.

In enkele gevallen gaat het om overige sextortion. Hierbij dreigt de dader met het openbaren van het beeldmateriaal uit jaloezie of om een (criminele) wederdienst van het slachtoffer te ontvangen.[52]

Grote impact op slachtoffers

Sextortion heeft veel impact op het slachtoffer.[53] De psychische en emotionele schade die het online delict kan aanrichten, valt te vergelijken met fysiek seksueel geweld. Vooral jongvolwassen mannen worden slachtoffer van sextortion. Toch worden ook relatief veel minderjarige jongens en meisjes slachtoffer van sextortion (20% van de slachtoffers). Uit onderzoek blijkt dat vrouwen een hoger risico lopen om slachtoffer te worden van seksuele sextortion en mannen van financiële sextortion.[54]

Verschillende soorten daders

Bij sextortion is sprake van verschillende soorten daders. Het kan gaan om individueel opererende daders[55] of om groepen die sextortion als een lucratief verdienmodel zien en meerdere slachtoffers maken. Bij individuele daders gaat het soms ook om ex-partners die handelen vanuit een emotioneel motief. In januari verschenen vier verdachten uit Den Haag, Delft en Zoetermeer voor de rechter in verband met sextortion.[56] Deze criminele groep heeft minstens 45 slachtoffers gemaakt die onder druk bedragen variërend tussen enkele honderden tot duizenden euro's moesten betalen. Het wederrechtelijke verkregen voordeel van de verdachten lag tussen de €2.250 en €15.000 per persoon.

Digitale veiligheid

De digitale veiligheid is verbonden met de geopolitiek

In het afgelopen jaar zijn de geopolitieke spanningen tussen landen verder verhard. Cyberaanvallen zijn een belangrijk instrument van statelijke actoren om hun geopolitieke belangen te behartigen.[57] Deze digitale aanvallen kunnen bedoeld of onbedoeld organisaties en burgers in Nederland raken en derhalve maatschappij-ontwrichtende gevolgen hebben.

Het conflict tussen Rusland en Oekraïne is een bekend voorbeeld van de geopolitieke verharding. Logischerwijs richten de cyberaanvallen van Rusland zich voornamelijk op Oekraïne, maar Nederlandse organisaties kunnen wel indirect geraakt worden als zij afhankelijk zijn van een Oekraïense organisatie of haar infrastructuur.[58] Tot dusver hebben zich in Nederland geen ontwrichtende cyberaanvallen in de context van dit conflict voorgedaan.

Ook criminele groepen en hacktivisten[59] mengen zich, al dan niet in samenwerking met of gedoogd door statelijke actoren, in het conflict. Zo zijn enkele Nederlandse ziekenhuizen begin 2023 getroffen door diverse DDoS-aanvallen door pro-Russische hacktivisten vanwege de steun die Nederland aan Oekraïne biedt.[60] Daarnaast zijn diverse overheidswebsites in maart 2023 verminderd bereikbaar geweest door een DDoS-aanval. Deze werd vermoedelijk uitgevoerd door een pro-Russische hacktivistische groep en hield verband met het uitvaardigen van het arrestatiebevel tegen de Russische president Poetin door het Internationaal Strafhof in Den Haag.

Een ander conflict dat zijn weerslag heeft op het wereldwijde digitale domein is het conflict tussen Israël en Palestina. Vrijwel direct na de eerste aanval werden er DDoS-aanvallen op Israëlische media- en overheidswebsites uitgevoerd. Ook werden er diverse aanvallen op de infrastructuur van Israël geconstateerd, zoals op wereldwijde GPS-ontvangers en industriële besturingssystemen. Daarnaast zijn ook in dit conflict hacktivistische groepen actief en is er gedreigd met ransomware-aanvallen richting landen die Israël steunen. Tot nu toe blijven cyberaanvallen beperkt tot de regio rondom Israël en Palestina, maar het is niet uitgesloten dat deze zich verder verspreiden en een effect kunnen hebben op Nederland.[61]

Cybercriminelen profiteren van technologische ontwikkelingen

De snelle ontwikkeling op het gebied van kunstmatige intelligentie (AI) vormt een risico voor het digitale domein.[62] Door de huidige ontwikkelingen in AI wordt het plegen van online criminaliteit toegankelijker voor de niet-technische crimineel. Ook kunnen criminelen door de automatisering die AI biedt, efficiënter te werk gaan.

Het taalmodel ChatGPT[63] was begin 2023 de snelst groeiende app in de geschiedenis. Na twee maanden had de chatbot al 100 miljoen actieve gebruikers.[64] Al snel verscheen er een verbeterde versie die in staat is nog complexere taken uit te voeren.[65] Op dit moment is het gebruik van generatieve AI, zoals ChatGPT, bij cyberaanvallen nog beperkt. Wel zijn er intussen verschillende criminele versies verschenen waarmee een gebruiker geavanceerde BEC-fraude en phishing-aanvallen kan plegen.[66] Voorbeelden van dergelijke tools zijn WormGPT[67] en FraudGPT.[68] Generatieve AI kan tevens gebruikt worden om malware te ontwikkelen, kwetsbare websites bloot te leggen en biedt handleidingen voor hacken. Ook kan generatieve AI onbedoeld onwaarheden verspreiden of doelbewust ingezet worden voor de verspreiding van desinformatie.[69]

De ontwikkeling van deepfakes[70] is, onder andere door de opkomst van generative AI, in een stroomversnelling geraakt. Er is steeds meer data beschikbaar waarmee de modellen kunnen werken en de technieken zijn steeds geavanceerder. Hierdoor wordt de technologie voor criminelen toegankelijker.[71] Onlangs is bijvoorbeeld gewaarschuwd voor een nieuwe methode om deepfakes te maken. Criminelen gebruiken malware om toegang te verkrijgen tot de gezichtsscans die mensen op hun telefoon gebruiken. Vervolgens worden hiervan, met behulp van kunstmatig intelligentie, deepfakes gemaakt die gebruikt worden om bijvoorbeeld toegang tot een bankrekening te verkrijgen.[72]

Hoewel al enige tijd wordt gevreesd dat deepfakes in toenemende mate gebruikt zullen worden voor criminele doeleinden, wordt dit in de politieregistraties tot op heden weinig teruggezien. Dit komt waarschijnlijk omdat er op dit moment nog vrij veel beeldmateriaal van iemand nodig is om realistische deepfakes te kunnen maken. Daarnaast is de Nederlandstalige kunstmatige intelligentie nog niet zo ver als de Engelstalige alternatieven en vormt het verwerken van emotie een extra moeilijkheidsgraad. Afgelopen jaar werd bijvoorbeeld een Engelstalige deepfake gemaakt van de topman van de Bunq-bank om hiermee CEO-fraude te plegen.[73]

Wel zijn er in de politieregistraties al voorbeelden van de inzet van deepfakes bij sextortion; hierbij zijn op (amateuristische wijze) naaktbeelden gecreëerd door het hoofd van een slachtoffer op een afbeelding van een naakt lichaam(sdeel) te fotoshoppen. Door de snelle ontwikkelingen op het gebied AI wordt het steeds makkelijker om dergelijke 'deepnudes' realistischer te maken. De verwachting is dan ook dat deepnudes vaker ingezet zullen worden bij bijvoorbeeld sextortion.[74]

De metaverse is een virtuele wereld waarin online en offline lastig te onderscheiden zijn. Allerlei aspecten uit de fysieke wereld, zoals wonen en werken, zijn geïntegreerd in deze virtuele wereld. Helaas biedt deze virtuele wereld ook mogelijkheden voor criminelen.[75] Zo is er op dit moment al sprake van de 'Darkverse'; een dark web variant binnen de metaverse waarbinnen criminele communicatie en illegale activiteiten, zoals verboden handel, plaatsvindt.[76] Daarnaast kan de metaverse gebruikt worden voor witwassen, diefstal van cryptovaluta en verspreiding van ideologische en extremistische ideeën en desinformatie.

Tevens vervagen de grenzen ten aanzien van gedrag door het anonieme karakter van deze online wereld. Hierdoor kunnen belediging, intimidatie, bedreiging en seksueel gerelateerde misdaden zich in de metaverse voordoen.[77] Dit kan zijn weerslag hebben in de fysieke wereld. Zo kan een virtuele aanranding net als een fysieke aanranding leiden tot trauma's en psychologische problemen.[78]

Toelichting en bronnen

Inleiding

1. Akkermans, M., Arends, J., Derksen, E. en Reep, C. (2023). *Online Veiligheid en Criminaliteit 2022*. Centraal Bureau voor de Statistiek: Den Haag/Heerlen/Bonaire.
2. CBS (2024). *Veiligheidsmonitor 2023*. Den Haag: Centraal Bureau voor de Statistiek.
3. CBS (2024). *Veiligheidsmonitor 2023*. Den Haag: Centraal Bureau voor de Statistiek.

Online fraude

4. Merk, A., Schuppers, K. en Willekers, M. (2024). *Online Blauw – Kwantitatief onderzoek naar digitale criminaliteit op basis van politiedata*.
5. Bronnen: BVH – Stuurkubus Cognos, de Landelijke Cybercrime Query. Het gaat om de combinatie van fraudedelicten uit de zogenoemde Landelijke Cybercrimequery + een aantal maatschappelijke klassen in de BVH met betrekking tot fraude die vaak/vrijwel altijd online fraude betreffen. Hierbij is er een beperkt deel false positives (registraties die eigenlijk offline fraude betreffen).
6. TNO (2023). *Online fraude*. Den Haag: TNO.
7. TNO (2023). *Online fraude*. Den Haag: TNO.
8. Bronnen: BVH – Stuurkubus Cognos en de Landelijke Cybercrime Query.
9. Bekkers L., Van Leuken, M. & Leukfeldt, R. (2024). *Criminele netwerken achter geldezels*. Rapportage deel 1: verkenning. Den Haag: De Haagse Hogeschool.
10. Bron: BVH – de Landelijke Cybercrime Query. Voor een klein deel overlappen de verschillende varianten van bankhelpdeskfraude elkaar. Zo komt het voor dat de dader het slachtoffer belt en gebruik maakt van een RAT of geld laat overmaken en later de bankpas komt ophalen.
11. TNO (2023). *Online fraude*. Den Haag: TNO.
12. Hierbij dient opgemerkt te worden dat de variant waarbij enkel misbruik wordt gemaakt van de identiteits- en adresgegevens van het slachtoffer niet goed meekomt in de LCQ. De aantallen betreffen dus een onderschatting van de werkelijk omvang.
13. Bron: Landelijke Cybercrime Query.
14. Het betreft een optelling van de totale schade van aan- en verkoopfraude (bron: dashboard LMIO), registraties in de categorie fraude en oplichting (bron: BVH-registraties opgehaald met de LCQ) en vriend-in-noodfraude (bron: dashboard ViN-fraude in Kibana).
15. Korpsmedia. (2024, 11 maart). *Minder bankhelpdeskfraude in 2023*. https://blue.politie.local/nieuws/64b407f0-3d84-4833-808f-e262be3f7c6f
16. Weulen Kranenbarg, M. & van 't Hoff-de Goede, S., (2023). *Online criminaliteit in criminologisch perspectief: Recente ontwikkelingen in het onderzoek naar daders en slachtoffers van online criminaliteit*. In: Tijdschrift voor Criminologie. 65, 4, p. 400-419 20 p.
17. Promotieonderzoek Jildau Borwell.
18. Korpsmedia. (2024, 11 maart). *Minder bankhelpdeskfraude in 2023*. https://blue.politie.local/nieuws/64b407f0-3d84-4833-808f-e262be3f7c6f
19. Europol (2023). *Online fraud schemes: a web of deceit. Europol Spotlight Report series*. Publications Office of the European Union, Luxembourg.
20. Bronnen: Landelijke Cybercrime Query (categorie fraude/oplichting), BVH F636 (categorie Fraude met online handel), tekstquery hulpvraagfraude, CBS.
21. Bronnen: BVH – Verdachtenkubus Cognos. MK's: F614 Fraude met betaalproducten, F620 Overige horizontale fraude, F636 Fraude met online handel, F651 Telefonische helpdeskfraude, F652 Online identiteitsfraude, F650 Hulpvraagfraude, F90 Cybercrime.
22. LMIO (2023). *Werkinstructie uitgestelde screening en alternatieve interventies bij fraude met onlinehandel (F636)*. Landelijk Meldpunt Internetoplichting.

Toelichting en bronnen

23. Sinds juli 2023 legt het Cluster Cyber Intel informatie over verdachten van online criminaliteit vast in Summ-IT.
24. Bekkers L., Van Leuken, M. & Leukfeldt, R. (2024). *Criminele netwerken achter geldezels*. Rapportage deel 1: verkenning. Den Haag: De Haagse Hogeschool.
25. Bekkers L., Van Leuken, M. & Leukfeldt, R. (2024). *Criminele netwerken achter geldezels*. Rapportage deel 1: verkenning. Den Haag: De Haagse Hogeschool.
26. NOS. (2022, 14 december). *Mensen OPLICHTEN voor F-GAME. De waarheid over online fraude*. https://www.youtube.com/watch?v=9kquffZBgLo
27. Bekkers L., Van Leuken, M. & Leukfeldt, R. (2024). Criminele netwerken achter geldezels. Rapportage deel 1: verkenning. Den Haag: De Haagse Hogeschool.

Ransomware

28. NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid; Sophos. (2024, 13 maart). *The 2024 Sophos Threat Report*. https://news.sophos.com/en-us/2024/03/12/2024-sophos-threat-report/
29. Rusland en Oekraïne zijn belangrijke bronlanden van georganiseerde cybercriminaliteit. Door het uitbreken van de oorlog kozen criminelen een kant en kwamen bestaande samenwerkingsverbanden onder druk te staan.
30. ENISA (2023). *Enisa Threat Landscape 2023*. Athene: The European Union Agency for Cybersecurity; Sentsova, A. (2024, 19 januari). *Ransomware goes political and other extortion activity of 2023*. Analyst1. https://analyst1.com/ransomware-goes-political-and-other-extortion-activity-of-2023/
31. NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
32. Politie (2023). *Ransomware Intelbeeld nr. 11 Juni, Juli & Augustus 2023*.
33. Chainalysis (2024, 7 februari). *Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline*. https://www.chainalysis.com/blog/ransomware-2024/
34. ENISA (2023). *Enisa Threat Landscape 2023*. Athene: The European Union Agency for Cybersecurity.
35. Het gaat bij deze cijfers om organisaties groter dan 100 fte.
36. NCSC. (2024, 22 februari). *Jaarbeeld Ransomware 2023*. Publicatie | Nationaal Cyber Security Centrum. https://www.ncsc.nl/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023
37. Coveware (2024, 26 januari). *New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying*. https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying;

    ENISA (2023). *Enisa Threat Landscape 2023*. Athene: The European Union Agency for Cybersecurity;

    Politie (2023) *Monthly Cyber Threat Report July 2023*;

    Toulas, B. (2024, 29 januari). *Ransomware payments drop to record low as victims refuse to pay*. BleepingComputer. https://www.bleepingcomputer.com/news/security/ransomware-payments-drop-to-record-low-as-victims-refuse-to-pay/
38. Coveware (2024, 26 januari). *New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying*. https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying;

    NCSC. (2024, 22 februari). *Jaarbeeld Ransomware 2023*. Publicatie | Nationaal Cyber Security Centrum. https://www.ncsc.nl/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023
39. Politie (2023) *Ransomware Intelbeeld nr. 14 November 2023*.
40. Hoe hoog het totale losgeldbedrag in Nederland ligt is niet bekend.

Toelichting en bronnen

41. Chainalysis (2024, 7 februari). Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline. https://www.chainalysis.com/blog/ransomware-2024/
42. Chainalysis (2024, 7 februari). *Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline*. https://www.chainalysis.com/blog/ransomware-2024/;
    Sophos. (2023). *The State of Ransomware 2023*. https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
43. Boyd, C. (2023, 14 juli). *Ransomware making big money through "big game hunting"*. https://www.malwarebytes.com/blog/news/2023/07/ransomware-making-big-money-through-big-game-hunting
44. Z-CERT. (2023). *Cybersecurity Dreigingsbeeld voor de zorg 2023*. https://z-cert.nl/wp-content/uploads/DEF-Z-CERT_RapportDreigingsbeeld2023.pdf
45. Politie (2023c) Monthly Cyber Threat Report July 2023.
46. ASD. (2023). *Annual Cyber Threat Report 2022–23*. https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023
    Milenkoski, A., & Rijnders, G. (2022, 20 oktober). *Ransoms without ransomware, data corruption and other new tactics in cyber extortion.* SentinelOne. https://www.sentinelone.com/blog/ransoms-without-ransomware-data-corruption-and-other-new-tactics-in-cyber-extortion/
47. Omroep West. (2023, 6 juni). *Hackers vallen bibliotheek in Gouda aan*. Omroep West. https://www.omroepwest.nl/nieuws/4724013/hackers-vallen-bibliotheek-in-gouda-aan
48. SentinelOne. (2024, 15 januari). *SentinelLabs onderzoekt nieuwe afpersingstactiek van cybercriminelen.* Emerce. https://www.emerce.nl/wire/sentinellabs-onderzoekt-nieuwe-afpersingstactiek-cybercriminelen
49. Milenkoski, A., & Rijnders, G. (2022, 20 oktober). *Ransoms without ransomware, data corruption and other new tactics in cyber extortion*. SentinelOne. https://www.sentinelone.com/blog/ransoms-without-ransomware-data-corruption-and-other-new-tactics-in-cyber-extortion/
50. Chainalysis (2024, 7 februari). *Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline*. https://www.chainalysis.com/blog/ransomware-2024/

Sextortion

51. Bracquez, J. (2022). *Slachtoffer of eigen schuld? Een vignetstudie naar de percepties ten aanzien van slachtoffers van sextortion.* Universiteit Gent.
52. Politie. (2023b). Crime script sextortion.
53. Cense, M., & Redert, A. (2022). *Wat bepaalt de impact van online seksueel geweld?* Rutgers. https://rutgers.nl/wp-content/uploads/2022/06/Rapport-Wat-bepaalt-de-impact-van-online-seksueel-geweld.pdf
54. Wolsink, J., Kuppens, J., Brouwer, N., & Ferwerda, H. (2022). *Mismatch. Een verkennend fenomeenonderzoek naar het plegen van zedendelicten na contact via een datingsite of datingapp*. Arnhem/Den Haag: Bureau Beke/Politie & Wetenschap.
55. NOS. (2023a, 20 januari). *Slachtoffer van seksuele afpersing: "Stap naar de politie".* NOS. https://nos.nl/artikel/2460628-slachtoffer-van-seksuele-afpersing-stap-naar-de-politie
56. Gruijthuijsen, M. (2024, 15 januari). *Tientallen mannen werden met naaktfoto's en -video's afgeperst: 'Hoop dat je je lesje hebt geleerd'.* AD. https://www.ad.nl/den-haag/tientallen-mannen-werden-met-naaktfotos-en-videos-afgeperst-hoop-dat-je-je-lesje-hebt-geleerd~a41c432e/

Toelichting en bronnen

Digitale veiligheid

57. NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
58. NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
59. Hacktivisten zijn criminelen die vanuit een politieke of sociale motivatie cybercriminaliteit plegen.
60. NOS. (2023, 30 januari). *Pro-Russische DDoS-aanvallers hebben het gemunt op Nederlandse ziekenhuizen.* NOS. https://nos.nl/artikel/2461833-pro-russische-ddos-aanvallers-hebben-het-gemunt-op-nederlandse-ziekenhuizen
61. Politie. (2023, 11 oktober). *Aansluiting hacktivisten bij oorlog Israël* [Presentatieslides]. LOCO;
    Sharma, S. (2023, 11 oktober). *Israel-Hamas conflict extends to cyberspace*. CSO Online. https://www.csoonline.com/article/655223/israel-palestine-conflict-extends-to-cyberspace.html
62. NCTV. (2023). *Cybersecuritybeeld Nederland 2023*. Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
63. ChatGPT is een taalprogramma dat gebaseerd is op generative artifical intelligence. Het is in staat om menselijke teksten te begrijpen en zelf ook te generen.
64. Hu, K. (2023, 2 februari). *ChatGPT sets record for fastest-growing user base - analyst note*. Reuters. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/
65. Hetler, A. (2023, december). *ChatGPT*. WhatIs. https://www.techtarget.com/whatis/definition/ChatGPT
66. The Hacker News (2023, juli 2023). *WormGPT: New AI Tool Allows Cybercriminals to Launch Sophisticated Cyber Attacks*. https://thehackernews.com/2023/07/wormgpt-new-ai-tool-allows.html
67. Kelley, D. (2023, 13 juli). *WormGPT - the generative AI tool cybercriminals are using to launch BEC attacks.* SlashNext. https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/
68. Mascellino, A. (2023, 26 juli). *Dark web markets offer new FraudGPT AI tool*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/dark-web-markets-fraudgpt-ai-tool/
69. Hetler, A. (2023, december). *ChatGPT.* WhatIs. https://www.techtarget.com/whatis/definition/ChatGPT;
    Irei, A. (2023, 7 april). ChatGPT security risks in the enterprise. Security. https://www.techtarget.com/searchsecurity/tip/ChatGPT-security-risks-in-the-enterprise
70. Deepfakes zijn nepvideo's gemaakt met kunstmatige intelligentie. Je kunt door middel van deepfake bijvoorbeeld het gezicht van een spreker in een video vervangen door dat van iemand anders of iemand iets laten zeggen wat diegene nooit heeft gezegd.
71. Kasteleijn, N. (2023, 8 oktober). *Deepfakes van Tom Hanks en topman Bunq laten risico zien van AI-video's.* NOS. https://nos.nl/artikel/2493308-deepfakes-van-tom-hanks-en-topman-bunq-laten-risico-zien-van-ai-video-s
72. Rietkerk, S. (2024, 7 april). Alarm om nieuwe criminele truc met deepfake: *"Hackers kopiëren je gezicht en plunderen je bankrekening"*. De Telegraaf. https://www.telegraaf.nl/lifestyle/90522879/alarm-om-nieuwe-criminele-truc-met-deepfake-hackers-kopieren-je-gezicht-en-plunderen-je-bankrekening#:~:text=Cybercriminelen%20hebben%20een%20nieuwe%20manier,maatregelen'%20om%20dit%20te%20voorkomen.
73. Hoeffnagel, W. (2023, 4 oktober). *Oplichters bootsen stem en beeld van Bunq-topman Ali Niknam na. Dutch IT Channel.* https://www.dutchitchannel.nl/news/403957/oplichters-bootsen-stem-en-beeld-van-bunq-topman-ali-niknam-na
74. Politie. (2023). Crime script sextortion.

Toelichting en bronnen

75. Gómez, J., Johnson, S. D., Borrion, H., & Lundrigan, S. (2023*). A scoping study of crime facilitated by the Metaverse*. University College London. https://doi.org/10.31235/osf.io/x9vbn
76. Huq, N., Reyes, R., Lin, P., & Swimmer, M. (2022, 8 augustus). *Metaworse? The Trouble with the Metaverse*. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse
77. Huq, N., Reyes, R., Lin, P., & Swimmer, M. (2022, 8 augustus). *Metaworse? The Trouble with the Metaverse.* Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse
78. Smith, A. (2024, 24 januari). *Rape in virtual reality: How to police the metaverse*. Context. https://www.context.news/digital-rights/sex-assault-claims-and-crime-raise-fears-of-new-virtual-wild-west

Bijlage 1

Meldingen en aangiften online fraude per delictscategorie en per gemeente*

	Aan- en verkoopfraude		Bankhelpdesk-fraude		Hulpvraagfraude		Overige fraude en oplichting	
	2022	2023	2022	2023	2022	2023	2022	2023
's-Gravenhage	1.114	1.319	168	163	134	205	528	497
Leidschendam-Voorburg	134	203	28	30	29	34	84	64
Pijnacker-Nootdorp	125	122	15	18	27	20	52	26
Wassenaar	52	49	15	15	6	11	29	24
Zoetermeer	280	287	51	25	46	56	110	117
Delft	216	226	29	29	36	38	117	62
Rijswijk	120	133	27	20	21	38	63	54
Westland	217	182	51	33	42	43	99	87
Midden-Delfland	38	36	8	4	5	15	22	13
Hillegom	47	65	11	19	9	9	19	16
Katwijk	144	127	34	37	22	23	68	47
Leiden	237	333	53	43	49	62	115	104
Leiderdorp	62	86	15	21	20	11	33	23
Lisse	52	41	27	21	8	8	21	19
Noordwijk	90	84	35	27	32	14	58	37
Oegstgeest	51	50	15	19	18	25	23	25
Teylingen	91	75	26	28	17	32	32	29
Voorschoten	50	53	14	21	8	12	29	19
Zoeterwoude	19	12	7	4	4	4	9	9
Alphen aan den Rijn	268	258	56	48	43	48	108	77
Bodegraven-Reeuwijk	68	61	21	18	21	12	29	26
Gouda	168	164	33	29	26	36	70	55
Kaag en Braassem	53	61	19	19	19	11	23	16
Krimpenerwaard	108	120	31	29	19	18	42	42
Nieuwkoop	56	59	23	13	14	11	30	30
Waddinxveen	71	58	17	15	13	11	27	25
Zuidplas	91	90	22	15	19	15	39	35
Eenheid Den Haag	4.022	4.354	851	764	707	822	1.879	1.578

*Disclaimer: Digitale criminaliteit is niet gebonden aan bepaalde gemeentegrenzen, dus cijfers op lokaal niveau zijn niet geschikt om een goed beeld van het veiligheidsprobleem te vormen.

Bron: BVH-registraties opgehaald met de Landelijke Cybercrime Query (LCQ), stuurkubus MK F636 en een tekstquery gericht op hulpvraagfraude.

Toelichting overige fraude en oplichting:
Hieronder vallen delicten als betaalverzoekfraude, misbruik van accounts voor bestellingen, helpdeskfraude (tech support scam), beleggingsfraude, creditcardfraude, diefstal van cryptomunten en overige vormen van online fraude.

Bijlage 2

Meldingen en aangiften cybercrime overige delictscategorieën*

	Afpersing/chantage		Persoonsgericht		Overig	
	2022	2023	2022	2023	2022	2023
's-Gravenhage	55	65	87	73	20	22
Leidschendam-Voorburg	7	14	9	3	2	1
Pijnacker-Nootdorp	8	9	2	5	3	2
Wassenaar	2	4	4	5	-	1
Zoetermeer	13	17	16	13	10	2
Delft	6	9	10	5	3	5
Rijswijk	6	5	11	3	2	1
Westland	8	15	8	18	3	6
Midden-Delfland	1	1	2	1	-	1
Hillegom	3	2	1	1	1	-
Katwijk	8	6	2	2	1	-
Leiden	18	19	15	11	6	6
Leiderdorp	3	3	2	2	1	-
Lisse	-	4	1	4	2	2
Noordwijk	4	5	5	3	1	1
Oegstgeest	2	4	3	3	1	-
Teylingen	4	8	2	1	4	2
Voorschoten	4	1	4	2	1	5
Zoeterwoude	-	1	-	-	-	-
Alphen aan den Rijn	16	11	16	7	2	4
Bodegraven-Reeuwijk	3	4	2	1	1	1
Gouda	4	6	3	4	2	3
Kaag en Braassem	3	2	2	1	-	4
Krimpenerwaard	3	12	-	9	2	5
Nieuwkoop	2	4	2	1	-	2
Waddinxveen	4	7	3	2		2
Zuidplas	5	5	4	5	1	1
Eenheid Den Haag	192	243	216	185	69	79

*Disclaimer: Digitale criminaliteit is niet gebonden aan bepaalde gemeentegrenzen, dus cijfers op lokaal niveau zijn niet geschikt om een goed beeld van het veiligheidsprobleem te vormen.

Bron: registraties uit de BVH opgehaald met de Landelijke Cybercrime Query (LCQ). De LCQ is gericht op cybercrime, waardoor registraties over gedigitaliseerde criminaliteit, vooral in de persoonsgerichte sfeer, niet goed meekomen.

Toelichting delictscategorieën:
Afpersing/chantage: delicten waarbij geld afhandig wordt gemaakt door middel van bedreiging (met geweld of smaad/laster.
Persoonsgericht: delicten die primair zijn gericht op beschadiging van een persoon.
Overige: Delicten met een politiek of ideologisch motief (hacktivisme) of delicten met motieven als verveling, spel, grensverkenning.