Online fraude in beeld

Fenomeenbeeld 2024

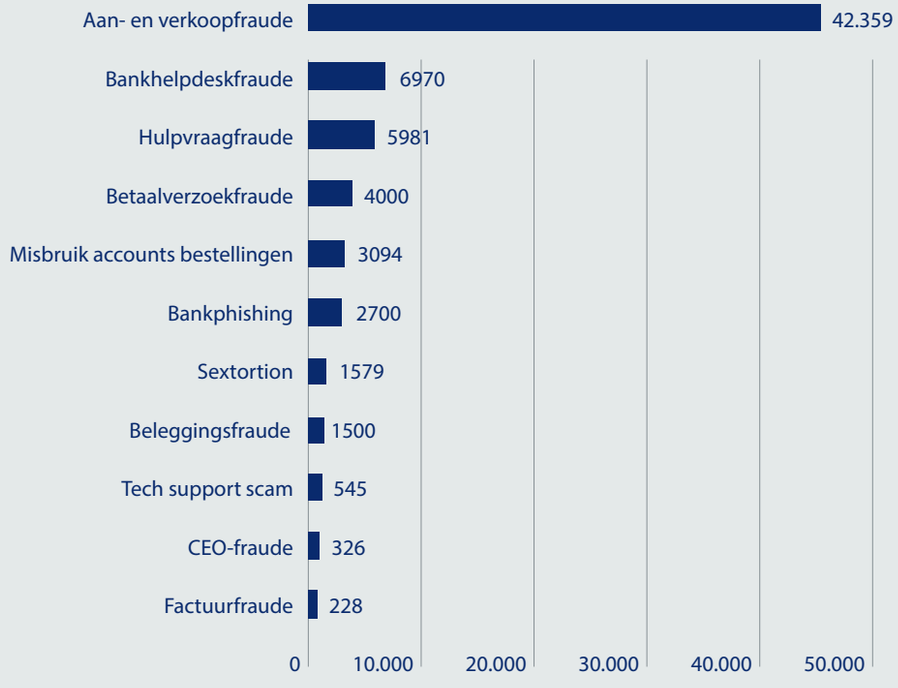
Samenvatting

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 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.

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

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

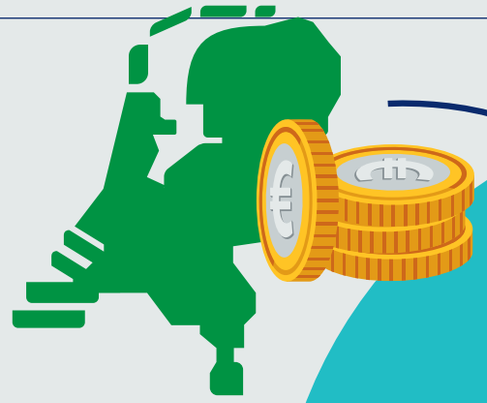
€ €

€ 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

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

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

Een zogenaamde helpdesk

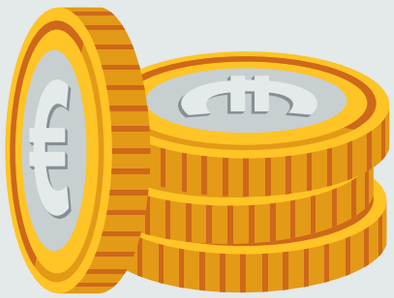
van een softwarebedrijf belt dat er
iets mis is met de computer

Tegen vergoeding is
dit te verhelpen

Eerste online fraudevorm
met gebruik
Remote Access Tool

€ 350

Gemiddeld schadebedrag
van 1600 naar 350 euro
per registratie



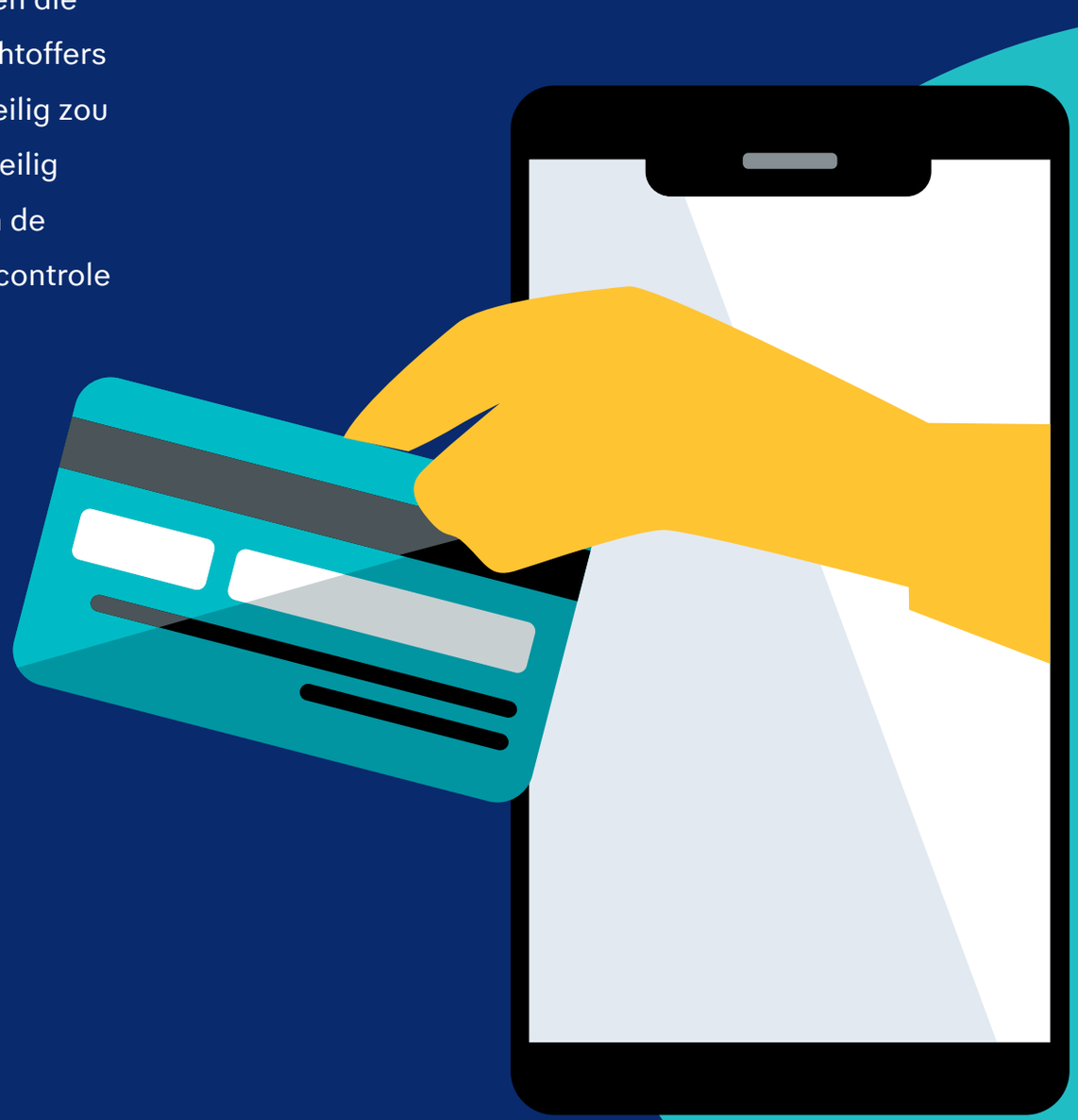
TSS afgenomen dankzij
internationale aanpak door
publiek-private partijen)

€ 200.000

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

Bankhelpdeskfraude

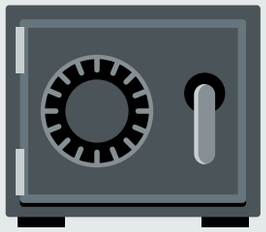
Bankhelpdeskfraude is een vorm van oplichting waarbij slachtoffers telefonisch worden benaderd door personen die zich voordoen als bankmedewerkers. Ze wijzen de slachtoffers erop dat het geld op hun bankrekening(en) niet meer veilig zou zijn en zetten hen vervolgens onder druk om hun geld veilig te stellen (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

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

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

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

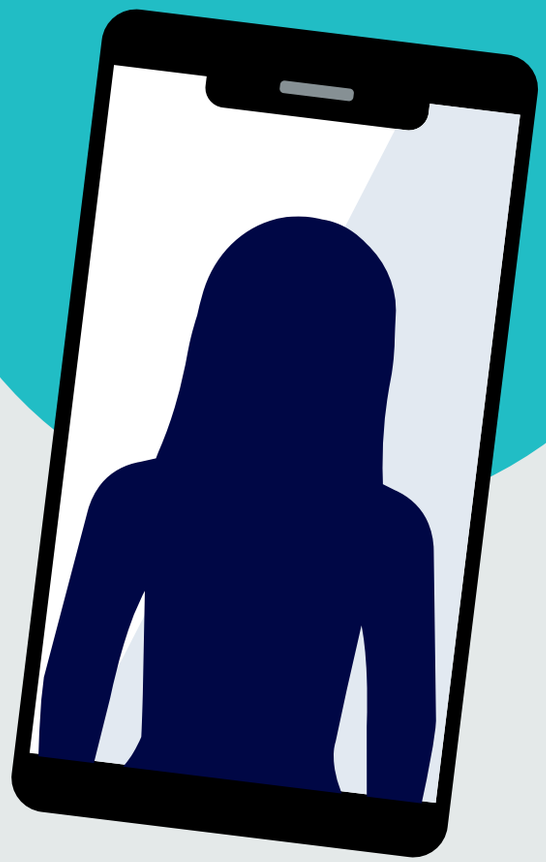
meer foto's, geld,
handelingen
of wraak (relationeel)

75%

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

Totale schade per jaar
€ 500.000

Seksueel getint
beeldmateriaal als
chantagemiddel



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

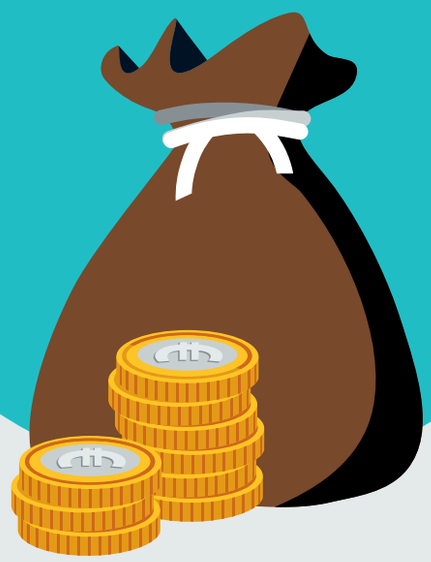
Van 130 registraties in 2020 naar ruim 1500 in 2023.

Ingelegd geld

wordt niet belegd

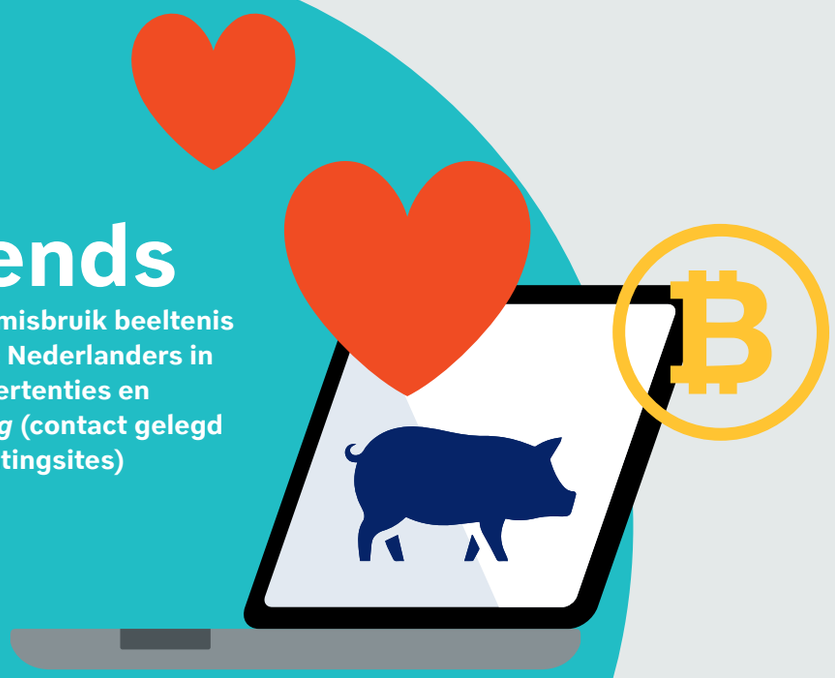
Schadebedragen

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

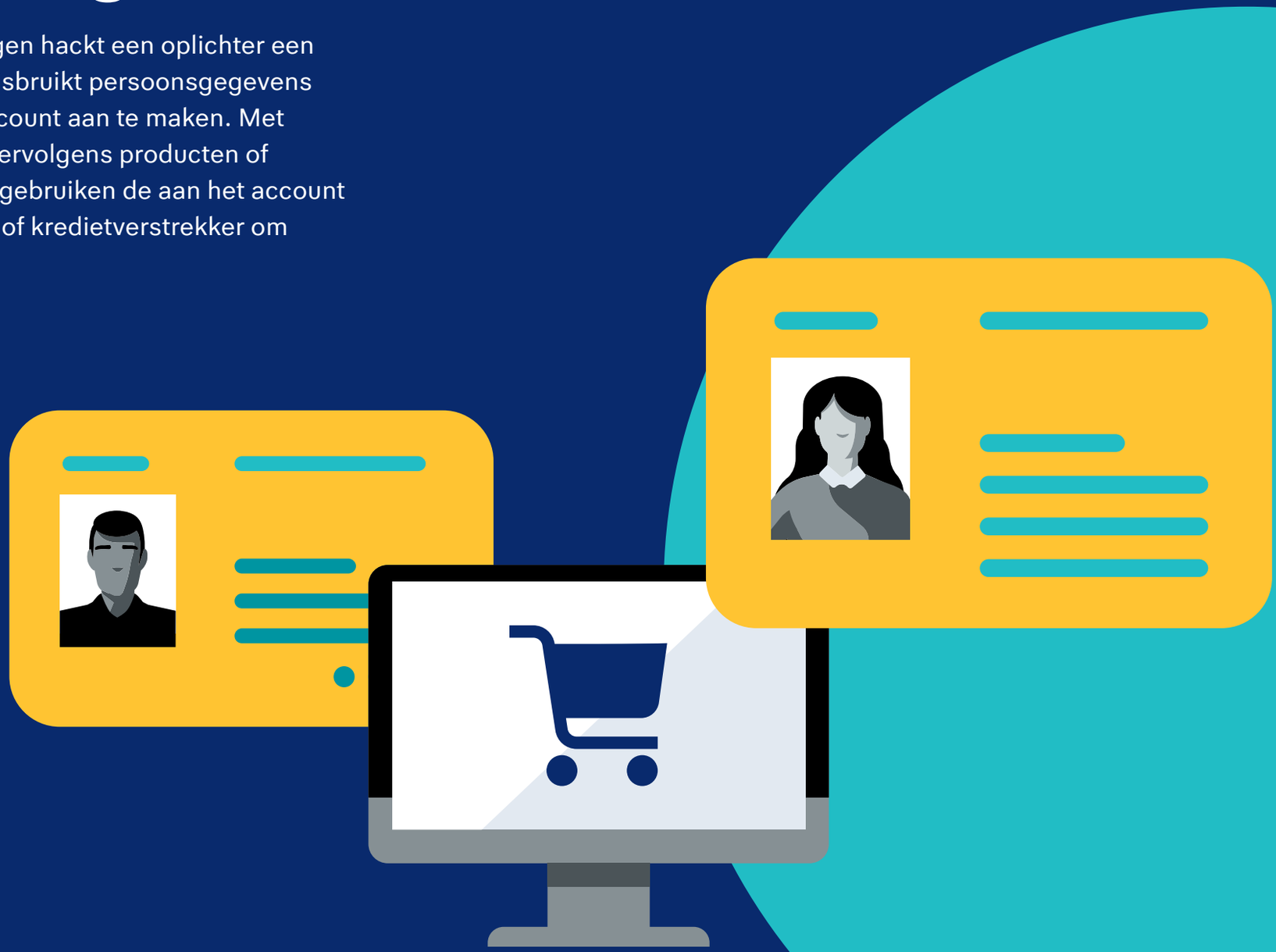
worden overgehaald om te investeren in beleggingen

Totale schade in 2023 is

€ 31 miljoen

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.



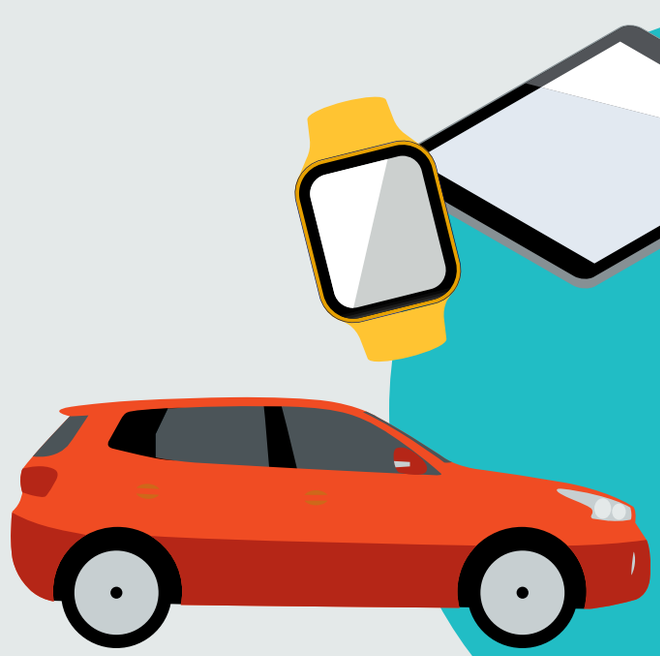
Misbruik accounts voor bestellingen in cijfers

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

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

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

Niet-financiële gevolgen voor slachtoffers

In verschillende onderzoeken is de impact van online fraude vergeleken met traditionele criminaliteit. 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.

“

‘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’

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 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.

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.

Bron: https://integraleaanpakonlinefraude.nl/

Fenomeenbeeld Online fraude

https://www.politie.nl/nieuws/2024/november/21/00-ruim-100-miljoen-euro-schade-door-online-fraude-in-2023.html