Scoping review: risicofactoren en interventies voor daderschap omtrent online criminaliteit

[CONCEPTVERSIE]

Thijs van Beek[1], Elmira Land[1], Remco Spithoven[1] Joeri Loggen[23], en Rutger Leukfeldt[234]

[1] Saxion Hogeschool, Lectoraat Online Weerbaarheid, Wapenrustlaan 11, 7321 DL Apeldoorn

[2] De Haagse Hogeschool, Centre of Expertise Cyber Security, Johanna Westerdijkplein 75, 2521 EN Den Haag

[3] Universiteit Leiden

[4] Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving, De Boelelaan 1077, 1081 HV Amsterdam

Samenvatting

Doel: Het doel van deze studie is het maken van een (compact) overzicht uit wetenschappelijke bronnen, bekende risicofactoren voor daderschap van online criminaliteit - ofwel delicten waarbij ICT het middel en/of het doelwit is - en daarmee verbonden interventies. Hierdoor kunnen professionals van de Nationale Politie en partnerorganisaties in korte tijd de *ins* en *outs* van dit onderwerp te weten komen en effectieve benaderingen voor in de praktijk kunnen ontwikkelen en bijstellen.

Methode: Bovenstaande is gedaan aan de hand van een scoping review. Het doel van een scoping review is om de breedte van de beschikbare kennis over een bepaald onderwerp te identificeren en op een narratieve wijze in kaart te brengen. De scoping review is uitgevoerd op basis van het (PRISMA-Scr) protocol van Leukfeldt en collega's (2022). Om de meest recente literatuur in kaart te brengen, heeft dit onderzoek zich gericht op de studies gepubliceerd van 2021 t/m 2024. Dit resulteerde in 52 relevante studies in de bestaande literatuur.

Resultaten. Uit de resultaten blijkt dat de aangehaalde studies vooral aandacht besteden aan de modus operandi in online criminaliteit. Deze daders opereren vaak binnen netwerken die variëren in mate van organisatie, van hiërarchische structuren tot losse verbanden. Binnen deze netwerken nemen criminelen met verschillende achtergronden en expertises uiteenlopende posities in om criminele activiteiten zo efficiënt en effectief mogelijk te laten verlopen. Het internet speelt hierin een cruciale faciliterende rol, vooral via ondergrondse fora en darknet-marktplaatsen. Op deze platformen kunnen criminelen met elkaar communiceren, informatie delen en kant-en-klare tools verkrijgen om criminaliteit mee te plegen. Hierdoor is het voor criminelen zonder specialistische kennis relatief eenvoudig om (op een grote schaal) hun criminele activiteiten toe te passen. Om slachtoffers te misleiden, maken criminelen gebruik van misleidingstechnieken (zoals autoriteit, tijdsdruk en schaarste) en hanteren zij neutralisatietechnieken (bijvoorbeeld ontkenning van slachtoffer, schade en verantwoordelijkheid) om hun daden te rechtvaardigen. Financieel gewin is een belangrijke motivatie om online criminaliteit te plegen, hoewel sommige daders ook handelen uit wraak, hebzucht of ideologische bevlogenheid. Daarnaast lijken met name economische (zoals welvaart) en sociale factoren (bijvoorbeeld het hebben van deviante vrienden) mensen ertoe aan te zetten om een criminele carrière te bewandelen. Hoewel de literatuur over demografische kenmerken schaars is, lijkt er in de literatuur het beeld te zijn dat met name mannen betrokken zijn bij verschillende vormen van online criminaliteit. Tenslotte benadrukken de aangehaalde studies het nut van voorlichting over de negatieve gevolgen die online criminaliteit kan veroorzaken bij zowel slachtoffers als daders als een effectieve manier om individuen van het criminele pad af te houden.

Discussie. Er is bij vrijwel alle vormen van online criminaliteit relatief weinig onderzoek gedaan naar risicofactoren, zoals demografische kenmerken, intrinsieke eigenschappen en persoonlijkheidskenmerken, in relatie tot daderschap. De meeste studies richten zich voornamelijk op motieven, modus operandi of interventies, terwijl neutralisatietechnieken in mindere mate aan bod komen. Tegelijkertijd benadrukt de literatuur de noodzaak om niet alleen *evidence-based* interventies te ontwikkelen, maar deze ook regelmatig te evalueren en herzien, zodat ze effectief blijven in het licht van de voortdurend veranderde en evoluerende aard van online criminaliteit.

Inhoudsopgave

1. Inleiding

1.1. Introductie

Tegenwoordig is *online criminaliteit*[1] – alle handelingen waarbij ICT van wezenlijk belang is voor de uitvoering van criminaliteit (Yar, 2006) – niet meer weg te denken uit onze sterk gedigitaliseerde samenleving. De politie merkt jaarlijks een toename van ongeveer 25 procent in cybercriminaliteit en gedigitaliseerde criminaliteit (Politie, 2021). Uit de bevindingen van de Cybersecuritybeeld Nederland 2024 komt naar voren dat de digitale dreiging voor Nederland omvangrijk en veelzijdig is, waarbij cyberaanvallen vooral worden uitgevoerd door statelijke en criminele actoren (NCTV, 2024). Statelijke aanvallen maken deel uit van een breder strategisch instrumentarium om nationale belangen te dienen, terwijl criminele groepen op grote schaal en opportunistisch opereren (NCTV, 2024). Daarnaast vormt de verstoring van digitale processen een aanzienlijke dreiging (NCTV, 2024).

De veiligheidsmonitor van 2024 illustreert een beeld dat in 2023 16 procent van de Nederlandse bevolking – dat komt neer op 2,3 miljoen slachtoffers – te maken heeft gehad met één of meer online misdrijven of incidenten (Akkermans et al., 2024). Online fraude en oplichting kwamen het vaakst voor (9 procent), gevolgd door hacken (6 procent), online bedreiging (3 procent) en intimidatie (3 procent) (Akkermans et al., 2024).

In het CBS-rapport wordt verder benoemd dat wat betreft de impact van online criminaliteit 21 procent van de slachtoffers aangeeft dat het incident heeft geleid tot emotionele, psychische en/of financiële problemen (Akkermans et al., 2024; Borwell et al., 2022). Slachtoffers ervaren in de meeste gevallen emotionele of psychische schade (17 procent) en in mindere mate financiële problemen (8 procent) (Akkermans et al., 2024). Daar komt bij dat slachtoffers vaak worden geconfronteerd met 'victim blaming', waardoor ze als het ware dubbel slachtoffer worden (Politie, 2021).

Online criminaliteit is zodoende een omvangrijk maatschappelijk probleem met een aanzienlijke impact en vormt één van de grootste uitdagingen van deze tijd. Het bestrijden ervan brengt dan ook nieuwe uitdagingen met zich mee voor opsporingsdiensten en beleidsmakers. Online criminaliteit komt in vele vormen voor en blijft zich ontwikkelen, waardoor een standaard aanpak niet mogelijk is (NCTV, 2024). De bestrijding vereist een integrale en systematische benadering, waarbij zowel de OM, politie als publieke en private partners een cruciale rol vervullen (NCTV, 2024). Hierbij is het noodzakelijk dat basisteams over de juiste kennis, vaardigheden en middelen beschikken om cybercriminaliteit (op lokaal niveau) aan te pakken (Politie, 2021).

Kennis over daderschap - dat wil zeggen risicofactoren, gehanteerde modus operandi, motivaties, neutralisatietechnieken en effectieve interventies en trainingen - is van essentieel belang om online criminaliteit effectief te kunnen bestrijden. Als bekend is welke individuen een verhoogd risico lopen om online criminaliteit plegen, dan kunnen gerichte en effectieve maatregelen worden genomen om dit te voorkomen. Zo kunnen preventieprogramma's beter worden afgestemd op risicogroepen, maar ook gerichtere voorlichtingscampagnes worden ontwikkeld

[1] Onder online criminaliteit vallen delicten die betrekking hebben op zowel cybercriminaliteit (Engels: *cyber-dependent crime*) als gedigitaliseerde criminaliteit (Engels: *cyber-enabled crime*). Cybercriminaliteit wordt gedefinieerd als delicten waarbij ICT zowel het middel als doel is (McGuire & Dowling, 2013a). Voorbeelden zijn Distributed Denial of Service (DDoS) aanvallen, hacking, en het maken en/of verspreiden van malware. Gedigitaliseerde criminaliteit refereert aan traditionele delicten die gepleegd worden met behulp van ICT (McGuire & Dowling, 2013b). Voorbeelden zijn phishing, cyberstalking en online bankpasfraude. Kortom, online criminaliteit betreft delicten waarbij ICT het middel en/of het doelwit is.

om potentiële daders af te schrikken en hen bewust te maken van de (financiële psychologische) gevolgen van hun daden. Ook inzicht in de werkwijze van criminelen is essentieel voor een effectieve bestrijding van online criminaliteit. Het helpt bij gerichte preventie, snellere opsporing, betere beveiligingsmaatregelen en het verstoren van criminele netwerken. Essentieel is om wetenschappelijke onderbouwde interventies en trainingen te gebruiken, omdat deze aantoonbaar effectief zijn en bedragen aan een gerichte en efficiënte aanpak.

Hoewel er recent een aantal studies zijn verschenen over daderschap (zie bijvoorbeeld de systematische narratieve review van Loggen en collega's (2024a, 2024b), zijn de meeste studies beperkt in hun reikwijdte: studies richten zich alleen op de risicofactoren of de werkwijze van cybercriminelen met daarbij de focus op een specifiek delict. Veel vormen van online criminaliteit hangen met elkaar samen en fluctueren, omdat criminelen vaak zich niet beperken tot één type delict en cyberdelicten steeds vaker een mengvorm zijn cybercriminaliteit en gedigitaliseerde criminaliteit. Om beter inzicht te krijgen van online criminaliteit is het belangrijk dat dit fenomeen vanuit een breed perspectief wordt benaderd, zodat verbanden tussen verschillende aspecten kunnen worden gelegd. Een overkoepelend overzicht van de meeste recente kennis over daderschap ontbreekt, terwijl online criminaliteit snel evolueert en criminelen voortdurend nieuwe methoden en technieken gebruiken.

Er bestaat zodoende bij de Nationale Politie en haar partnerorganisaties de behoefte aan een (compact) overzicht van relevante informatie over daderschap van online criminaliteit, zodat professionals binnen de Nederlandse politiefunctie in korte tijd de ins en outs van dit onderwerp te weten kunnen komen. Op basis van een **scoping review**[2], waarbij op gestructureerde wijze bestaande studies zijn samengevat en geanalyseerd, is de huidige stand van zaken in kaart gebracht.

De onderzoeksvragen van deze scoping review van de beschikbare, wetenschappelijke literatuur over daders van online criminaliteit zijn als volgt:

1. Welke risicofactoren voor daderschap van verschillende vormen van online criminaliteit worden beschreven in de literatuur?
2. Welke interventies voor het voorkomen en/of verminderen van daderschap van online criminaliteit worden beschreven in de literatuur?

1.2. Leeswijzer

Dit rapport is als volgt ingedeeld. In hoofdstuk 2 zal er verder worden ingegaan op de gehanteerde methode van dit onderzoek. Vervolgens wordt in hoofdstuk 3 de resultaten van daderschap besproken. Tenslotte volgt in hoofdstuk 4 de discussie en conclusie.

[2] Het doel van een scoping review is om de breedte van de beschikbare kennis over een bepaald onderwerp te identificeren en op een narratieve wijze in kaart te brengen (Pollock et al., 2024).

2. Methode

2.1. Inleiding

In dit onderzoek is een *scoping review* uitgevoerd om een zo breed mogelijk overzicht te krijgen van de literatuur over daderschap. Het doel van een scoping review is namelijk om de breedte van de beschikbare kennis over een bepaald onderwerp te identificeren en op een narratieve wijze in kaart te brengen (Pollock et al., 2024). De methode die voor de scoping is review is gebruikt is gebaseerd op het protocol van Loggen en collega's (2022). Dit protocol is op haar beurt gestoeld op de Preferred Reporting Items for Systematic Review and Meta-analysis Protocols-extensie voor Scoping Reviews (PRISMA-ScR), een wetenschappelijk ontwikkelde en gevalideerde methode om op een transparante, betrouwbare en systematische wijze een scoping review uit te voeren (Tricco et al., 2018). In dit hoofdstuk zullen we verder ingaan op de gebruikte methode. Vervolgens wordt de gebruikte zoekstrategie beschreven om potentieel relevante papers te identificeren. Daarna wordt er dieper ingegaan op het screenen van de documenten en het extraheren van de relevante data. In het laatste deel van dit hoofdstuk zullen de kenmerken van de in deze studie geïncludeerde papers worden beschreven.

2.2. Inclusiecriteria

Het hoofddoel van deze scoping review was het in kaart brengen van een actueel overzicht van de wetenschappelijke literatuur over risicofactoren en interventies/trainingen voor verschillende vormen van online criminaliteit. Om daarbij een zo breed en volledig beeld te krijgen van de literatuur, zijn studies gericht op onderwerpen als modus operandi (MO), neutralisatietechnieken, motieven en trends ook meegenomen in deze scoping review. Voor wat betreft de geschreven taal zijn alleen de studies in het Engels geselecteerd, omdat de Engelse taal de *lingua franca* van de wetenschappelijke wereld is. Daarnaast worden er alleen de studies meegenomen die zijn gepubliceerd tussen 2022 en 2024 om zo een overzicht te krijgen van de meest recente bevindingen, aangezien Loggen en collega's in hun twee systematische narratieve reviews de literatuur bespreken van vóór 2022 (Loggen et al., 2024a, 2024b).

Zodoende nemen we in deze studie alleen de studies mee wanneer ze voldoen aan de volgende voorwaarden:

1. open access gepubliceerd of toegankelijk via de universiteitsaccounts van de onderzoekers;
2. geschreven in Engels;
3. Gepubliceerd tussen 2021 en 2024
4. Een empirische studie, een (systematische) review of een meta-analyse;
5. gerelateerd aan online criminaliteit (dit omvat cybercriminaliteit en gedigitaliseerde criminaliteit);
6. Is een tijdschriftartikel, boek, hoofdstuk in een boek, congres-/proceedingpaper, technisch rapport, dissertatie/thesis of een overheidsdocument;
7. gericht op risicofactoren voor daderschap, interventies/trainingen gericht op het voorkomen van daderschap en/of aanverwanten onderwerpen (zoals modus operandi, overtuigingstechnieken en trends).
8. en geen correctie, erratum of teruggetrokken paper.

2.3. Query en informatiebronnen

Bij de uitvoering van deze studie hebben de onderzoekers zich gehouden aan de richtlijnen voor gestructureerde literatuurstudies die zijn opgesteld door Loggen en collega's (2022) en PRISMA-ScR (Tricco et al., 2018). Om relevante studies te identificeren, zijn er twee methodes toegepast. Allereerst is er een systematisch zoekopdracht uitgevoerd in zes databases (ACM Digital Library, EbscoHost, ProQuest, Scopus, Web of Science, and Wiley Online Library) op 04-11-2024. Vervolgens is er gekeken naar zoektermen in relevante literatuur. De zoektermen zijn gebaseerd op die van Leukfeldt en collega's (2022). Doordat vanuit de opdrachtgever de wens bestond om meer inzicht te krijgen in investeringsfraude, is deze categorie extra toegevoegd aan de query.

Dit leidde tot een query met in totaal drie categorieën: (1) zoektermen gerelateerd aan financieel gedigitaliseerde criminaliteit (2) zoektermen gerelateerd aan hetzij daderschap (3) uitgesloten categorieën. De derde categorie wordt gebruikt om onderzoeken uit te sluiten die voornamelijk verband houden met medische en milieustudies en onderzoeken gelieerd aan *articifical intelligence* (AI), zoals een machine learning-methode voor het automatische detecteren van malware.

(1) Financieel-economische gedigitaliseerde criminaliteit:
((("cyber-enabled" OR "cyber enabled" OR "computer-enabled" OR "computer enabled") AND (crim*)) OR ((financial OR "financially motivated") AND (cybercrim* OR "cyber crim*" OR "cyber-crim*")) OR (((online OR internet OR cyber OR computer) OR ((online OR internet OR cyber OR computer) AND (romance OR dating OR auction OR retail OR identity OR banking)) OR ("e-commerce" OR "advance-fee" OR "advance fee" OR 419 OR Microsoft OR Whatsapp OR "mass marketing" OR "mass marketing")) AND (fraud* OR scam* OR swindl*)) OR internetfraud* OR "internet-fraud*" OR cyberfraud* OR "cyber-fraud*" OR internetscam* OR cyberscam* OR computerscam* OR phish* OR smish* OR "sms phish*" OR "voice phish*" OR vishing OR skimming* OR "investment fraud"))

(2) Subject
AND ((perpetrat* OR offend* OR crimin*) OR (intervent*))

(3) Excluding category:
AND NOT (medic* OR cell* OR forensic* OR chemical* OR fracture* OR pollution* OR nuclear* OR blockchain* OR "deep learning" OR API* OR "machine learning" OR windows OR APT* OR TCP* OR SIP*)

2.4. Selecteren van documenten

Het beoordelen van potentieel relevante studies is eveneens op systematische wijze uitgevoerd. Na het draaien het van de zoektermen in de verschillende databases zijn alle documenten verzameld en opgeslagen in softwareprogramma Zotero, een open-source referentie management tool. Vervolgens zijn alle titels en abstracts geüpload in ASReview LAB (Van De Schoot et al., 2021). Dit is een state-of-the-art machine learning tool, waarbij (potentieel) relevante papers bovenaan de screeningslijst worden gerangschikt op basis van eerdere beslissingen van de onderzoeker of een abstract al dan niet relevant is. Vervolgens is er een abstract screening tool ontwikkeld (zie Bijlage A). Deze screening tool is gebaseerd op degene die Leukfeldt en collega's (2022)

in hun eigen protocol hanteren. Indien alle vragen uit de abstract screening tool met ‘ja’ of ‘onduidelijk’ worden beantwoord, wordt deze als potentieel relevant aangemerkt. Een ‘nee’ op ten minste een vraag uit de abstract screening tool betekende dat deze niet relevant was voor onze studie.

Hierna zijn alle studies die tijdens het screenen van de abstracts als potentieel relevant waren aangemerkt doorgelezen met een specifieke aandacht voor (1) introductie-, (2) methode- en (3) discussie/conclusie-sectie om de relevantie voor de scoping review te kunnen bepalen. Het doornemen van de studies is in het kwalitatieve analyseprogramma Atlas.ti uitgevoerd aan de hand van een zogenoemde full tekst screening tool (zie Bijlage B). Deze tool is eveneens gebaseerd op degene die Leukfeldt en collega's (2022) in hun eigen protocol hanteren, en werkt op dezelfde manier als de abstract screening tool: worden alle vragen met ‘ja’ beantwoord, dan wordt de studie als relevant bestempeld. Een ‘nee’ op één vraag betekende dat de studie niet werd meegenomen in de uiteindelijke analyse. Studies die niet online toegankelijk waren, werden indien mogelijk, via ResearchGate opgevraagd bij de betreffende auteur(s) via een gestandaardiseerde e-mail.

Zowel het screenen van de abstracts als de tekst is uitgevoerd door één onderzoeker. In het geval er gerede twijfel was over de (ir)relevante van een studie werd er een tweede onderzoeker geraadpleegd. Zie Figuur 1 voor het proces van verzamelen en screenen van potentieel relevante wetenschappelijke studies van daderschap.

2.5. Het in kaart brengen van de data

Van te voren is er een gestructureerd overzicht van relevante thema’s (d.w.z. metadata, methodologie, kwaliteit, resultaten/discussie) opgesteld om systematisch en consistent de data te kunnen extraheren en analyseren. Onder metadata wordt verstaan de bibliografische gegevens: (1) type studie, (2) titel, auteur(s), (3) publicatiedatum, (4) type online criminaliteit, (5) onderzoeksdoel. De methodologie betreft de categorieën (1) soort methode, (2) steekproefgrootte, (2) onderzoekspopulatie, (3) land/continent waar het onderzoek is uitgevoerd. De kwaliteit van de studie refereert aan de betrouwbaarheid en validiteit van een studie dat is gemeten aan de hand van 3-puntsscore: lage kwaliteit, gemiddelde kwaliteit en hoge kwaliteit (zie sectie 2.6).

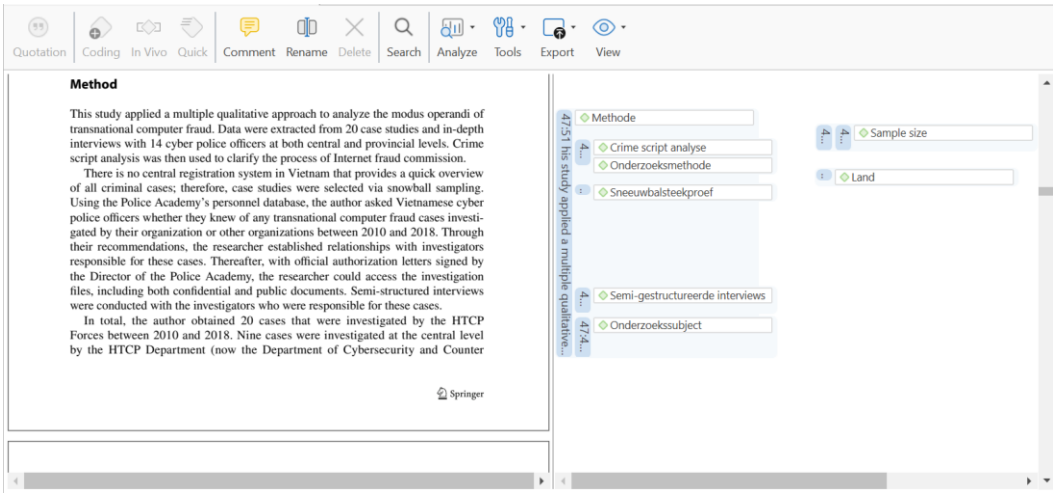
Wat betreft de resultaten/discussie, zijn voor de data extractie de volgende categorieën meegenomen om een zo volledig en diepgaande analyse mogelijk te kunnen maken.

1. **Demografische kenmerken:** verwijst naar de basiskenmerken van een individu, zoals geslacht, leeftijd en opleidingsniveau;
2. **Intrinsieke en persoonlijkheidskenmerken:** verwijzen naar verschillende aspecten van een persoon die invloed hebben op hun gedrag, overtuigingen en interacties met de wereld, bijvoorbeeld IT-kennis, vaardigheden moraliteit;
3. **Criminaliteit:** omvat initiële misdrijven die iemand pleegt en de patronen van crimineel gedrag die zich in de tijd kunnen herhalen of uitbreiden, bijvoorbeeld recidive en meervoudige criminaliteit;
4. **Mentaal:** kan worden omschreven als de mentale en psychologische eigenschappen die invloed hebben op hoe een individu denkt, handelt en reageert in verschillende situaties. (bijv. zelfcontrole, empathisch vermogen en risicogedrag);

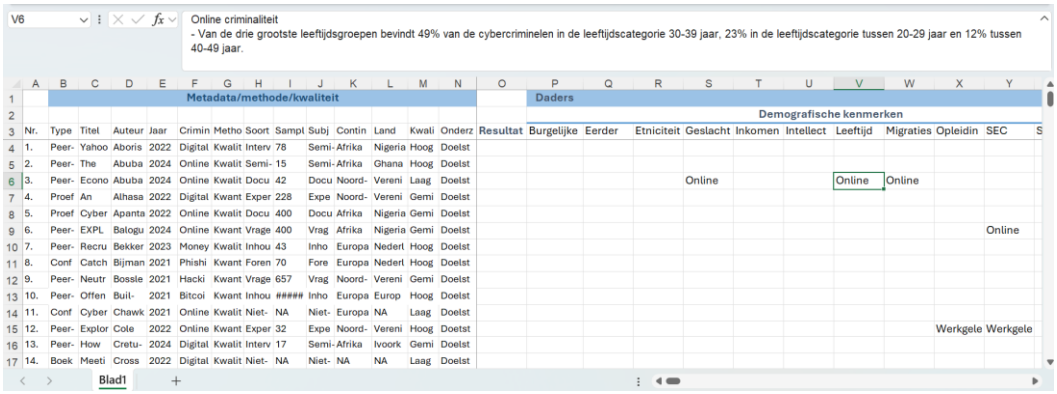
5. **Routine activiteiten:** verwijzen naar het dagelijks gedrag en de activiteiten van criminelen in bepaalde situaties en omgevingen (bijv. computergebruik, internetgebruik en gaming).
6. **Sociale relaties:** verwijzen naar de invloeden uit de sociale omgeving die het gedrag, de keuzes en de ontwikkeling van een individu beïnvloeden (bijv. ouders, peers en sociale banden).
7. **Macrofactoren:** betreffen sociale, economische, politieke, en culturele invloeden die het gedrag van individuen binnen een samenleving beïnvloeden (bijv. werkeloosheid, welvaart en ongelijkheid).
8. **Neutralisatietechnieken:** omvatten strategieën of rechtvaardigingen die individuen hanteren om crimineel of immoreel gedrag te rationaliseren of goed te praten, zodat ze zich minder verantwoordelijk voelen voor hun daden (bijv. verantwoordelijkheid, slachtofferschap en schade ontkennen.
9. **Motieven:** redenen waarom individuen criminaliteit plegen (bijv. financieel gewin, hebzucht en wraak)
10. **Modus operandi:** de werkwijze van criminelen (bijv. het gebruik van online platforms, imitatie en netwerk).
11. **Misleidingstechnieken:** verwijzen naar strategieën of tactieken die worden gebruikt om iemand bewust te misleiden, te manipuleren of te bedriegen (bijv. het gebruik van autoriteit, urgentie en druk).
12. **Trends:** refereert aan opkomende patronen, veranderingen en ontwikkelingen van online criminaliteit (bijv. frequentie, concentratie en groeiende dreiging).
13. **Toekomstig onderzoek:** omvatten de aanbevelingen van auteurs over de richting waarin toekomstig onderzoek nodig op basis van hun eigen bevindingen (bijv. contextuele, methodologische en populatiegericht aspecten).
14. **Interventies/trainingen:** zijn benaderingen die worden ingezet om bepaalde gedragingen te beïnvloeden of te veranderen. Hierbij is er onderscheid gemaakt tussen *slachtoffergerichte* (zoals ondersteuning, monitoren en detecteren) en *dadergerichte* (afschrikking, voorlichting en bewustwording) interventies/trainingen.

De analyse van de overgebleven studies is uitgevoerd in Atlas.ti, waarbij van iedere studie alle relevante data werden gecodeerd en werd geëxtraheerd in (sub)categorieën naar een Excel-bestand (zie screenshots van de codering in Atlas.ti en het Excel-bestand).

Screenshot van een voorbeeld van codering in Atlas.ti.



Screenshot van een gedeelte van het Excel-bestand.



.

2.6. Kritische beoordeling van de individuele studies

Na de dataextractie werden alle relevante wetenschappelijke onderzoeken beoordeeld met behulp van een kwaliteitschecklist. Het is immers belangrijk om de kwaliteit van een studie te kennen, omdat dit de interpretatie van de resultaten kan beïnvloeden. Zo kan er *grosso modo* worden gesteld dat hoe lager de kwaliteitsscore, hoe meer beperkingen een studie kent en hoe voorzichtiger de resultaten daarvan geïnterpreteerd dienen te worden. Met andere woorden: de kwaliteit van een studie zegt iets over de kwaliteit van de resultaten. De kwaliteitsbeoordeling is uitgevoerd door één onderzoeker. In geval van twijfel over de kwaliteitsscore van een studie, is een tweede onderzoeker geraadpleegd.

Met betrekking tot de empirische studies is er een kwaliteitschecklist gebruikt, bestaande uit 9 items, die is ontwikkeld door Hawker en collega's (2002). Ieder item is gemeten via een 1 t/m 4 schaal (1 = Zeer slecht; 2 = slecht; 3 = redelijk; 4 = goed) die per item nader is gedefinieerd. De totale score kan daarmee variëren van de 9 t/m 36 punten (Hawker et al., 2002). De items variëren van 'Abstract en titel' tot aan 'Implicaties en bruikbaarheid' (Hawker et al., 2002). Studies met een score tussen de 9 t/m 23 punten worden beschouwd als 'lage kwaliteit', een score van 24 t/m 29 punten wordt gezien als 'gemiddelde kwaliteit' en tussen 30 t/m 36 punten geeft een 'hoge kwaliteit' aan (Braithwaite et al., 2017). In lijn met Loggen en collega's (2024a, 2024b) is er voor

deze kwaliteitschecklist gekozen vanwege de veelzijdigheid ervan, aangezien deze kan worden toegepast op verschillende soorten empirische studies (Loggen et al., 2024a).

Voor wat betreft de relevante reviews zijn deze op hun kwaliteit beoordeeld aan de hand van de Scale for the Assessment of Narrative Review Articles (SANRA). Dit is een 6-item checklist voor de narratieve beoordeling van reviews welke is opgesteld door Baethge en collega's (2019) en kan worden toegepast op zowel systematische reviews als niet-systematische reviews. De SANRA-items variëren van het 'rechtvaardigen van de relevantie van de gebruikte artikelen' tot aan 'passende presentatie van de data' (Baethge et al., 2019). SANDRA werkt min of meer via dezelfde systematiek als de kwaliteitschecklist van Hawker en collega's (2002). Ieder item is gemeten via een 0 t/m 2 schaal die per item nader is gedefinieerd. De totale score kan daarmee variëren van de 0 t/m 12 punten. Hierbij geeft een score tussen de 0 t/m 6 een lage kwaliteitsscore aan, 7 t/m 9 een gemiddelde kwaliteitsscore en 10 t/m 12 een hoge kwaliteitsscore (Loggen et al., 2024a).

2.7. Synthetiseren van de resultaten

De uitgevoerde datasynthese bestond uit drie stappen, zoals voorgesteld door Petticrew en Roberts (2006). Ten eerste hebben zijn alle studies opgedeeld in één inhoudelijke hoofd categorie: (1) studies met een focus op daderschap. Ten tweede is binnen deze categorie alle studies onderverdeeld naar typen online criminaliteit. Ten derde zijn binnen deze overkoepelende thema's de studies naar subcategorieën zoals risicofactoren, modus operandi en interventies/trainingen. Vervolgens is alle data binnen deze categorieën geanalyseerd en samengevoegd.

2.8. Beschrijving van de geïncludeerde studies

In totaal zijn er op basis van onze zoektermen **624** unieke titels en abstracts geïdentificeerd in de databases. Op basis van het screenen van de titels en abstracts bleven er in totaal **81** mogelijk relevante studies over. Hierbij voldeed elke review aan het inclusiecriterium. Het volledig doorlezen van deze documenten resulteerde vervolgens in **52** daadwerkelijk relevante reviews (zie Figuur 1 voor een volledig overzicht).

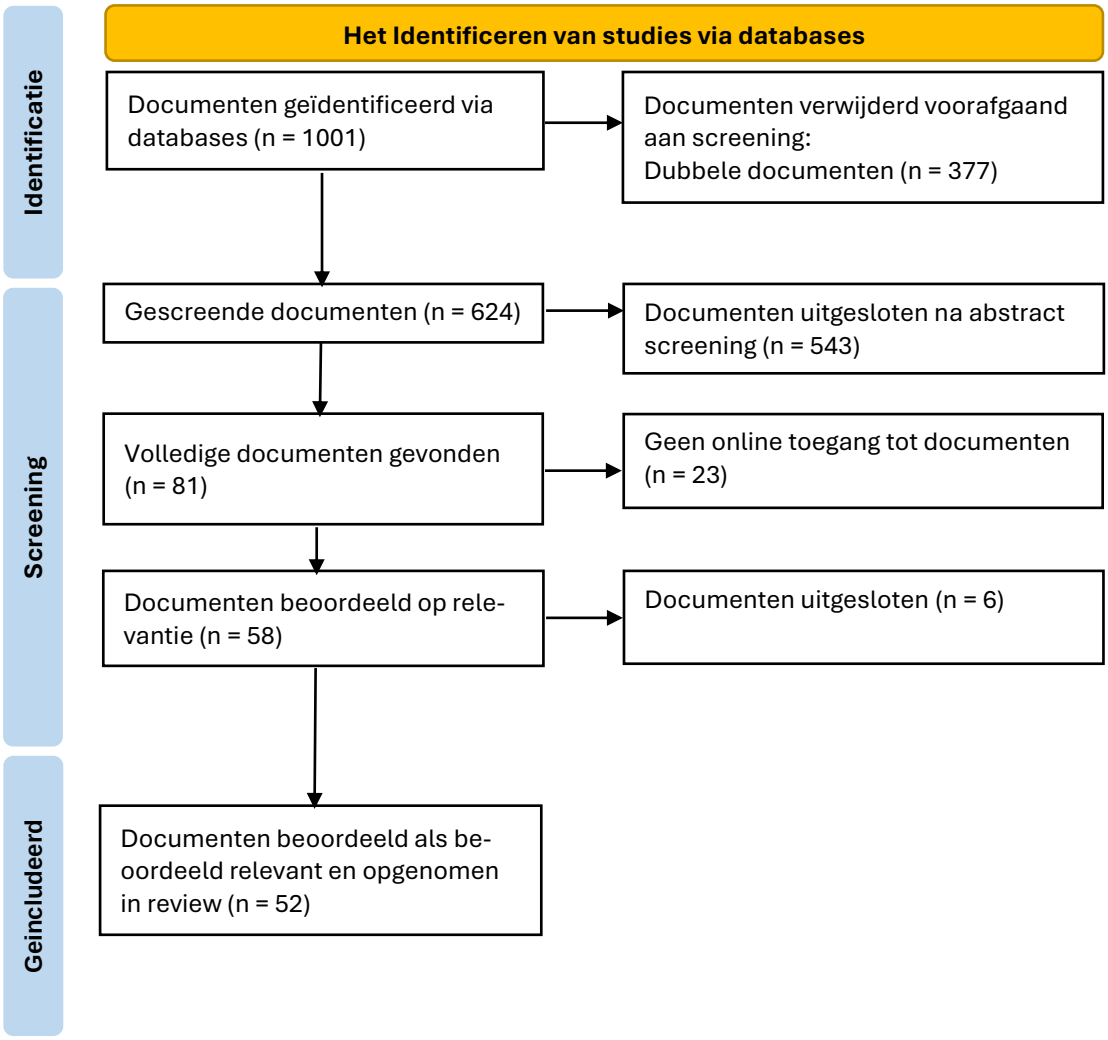
2.9. Kenmerken geïncludeerde studies

In totaal zijn **52** relevante studies meegenomen in dit deze scoping review. De meeste studies hadden betrekking tot online criminaliteit (n = 17), online fraude (n = 11) en datingfraude(n = 10) (zie Tabel 1 voor een overzicht). Daarnaast zijn de meeste studies uitgevoerd in Afrika (n = 11), Noord-Amerika (n = 11) en Azië (n = 10). De meest gebruikte onderzoeksmethoden waren interviews (n = 13), niet-systematische review (n = 10) en experiment (n = 8). Gekeken naar kwaliteit, zijn 22 studies beoordeeld met een hoge kwaliteit, 16 met een gemiddelde kwaliteit, en 14 met een lage kwaliteit.

Tabel 1. Aantal studies die betrekking hebben tot daderschap

Delict	Frequentie
Online criminaliteit (algemeen)	17
Online fraude	11
Datingfraude	10
Phishing	5
Hacking	4
Advance fee fraud (AFF)	3
Malware	3
Online werkgelegenheidsfraude	3
Vishing	3
Business E-mail Compromise (BEC)-fraude	2
Online bankpasfraude	2
Bitcoin gerelateerde online criminaliteit	1
Concession-Abuse-as-a-Service ()-fraude	1
Computer gerelateerde cybercriminaliteit	1
Content gerelateerde cybercriminaliteit	1
E-commerce fraude	1
Goudhandelfraude (GPF)	1
Money mules	1
Online werknemersfraude	1
Pig-butchering scam	1
Social engineering	1
Witwassen	1

Noot. Een aantal studies richtten zich op meerdere vormen van online criminaliteit



Figuur 1. Het proces van verzamelen en screenen van potentieel relevante wetenschappelijke studies van daderschap.

2.10. Inclusiecriterium resultatensectie

Het hoofddoel van deze studie was het in kaart brengen van risicofactoren en interventies/trainingen over de literatuur van daderschap. Sommige reviews gaven ook of uitsluitend inzicht in onder andere de gehanteerde modus operandi, misleidingsstrategieën en neutralisatietechnieken. Aangezien dergelijke informatie mogelijk relevant is voor de Nationale Politie en haar partners, hebben wij zogezegd deze aspecten in de scoping review vermeld.

Verder is ieder onderdeel onderverdeeld in overkoepelende categorieën en aangemerkt met een kleur om een helder overzicht te creëren van de relatie tussen risicofactoren/interventies en delicten. Hierbij geeft **groen** aan dat er sprake is van een positief verband/effect ten aanzien van het type online delict, **blauw** representeert een ambigue of géén verband/effect, **rood** weerspiegelt een negatief verband/effect en **blauw** geeft een beschrijvende/neutrale factor aan.

2.11. Definities van de delicten

In Tabel 2 is een overzicht gegeven van alle vormen van online criminaliteit met bijbehorende definitie die in deze scoping review aan bod komen.

Tabel 2.
Alle vormen van online criminaliteit beschreven in deze review, inclusief definitie.

Type	**Omschrijving**
Online criminaliteit	Betreft alle delicten waarbij ICT het middel en/of het doelwit is.
Cybercrime in enge zin	Delicten waarbij ICT zowel het middel als doel is (McGuire & Dowling, 2013a). Voorbeelden zijn hacking en het maken en/of verspreiden van malware.
Hacking	Betreft het ongeautoriseerd toegang verkrijgen tot apparaten zoals mobiele telefoons en computers (Lee et al., 2023, p. 1). Cybercriminelen krijgen hierbij toegang tot de online informatie van gebruikers, wat schade kan veroorzaken (Lee et al., 2023). Een crimineel kan bijvoorbeeld proberen toegang te krijgen tot iemands online account door gebruik te maken van persoonlijke gegevens van het slachtoffer, zoals inlog-ID en wachtwoord (Lee et al., 2023, p. 2)
Malware	Is kwaadaardige software die wordt gemaakt om zonder toestemming informatie van een gebruiker te wijzigen, verwijderen of te bespioneren (Chawki, 2021). Het kan zich verspreiden via internet of externe apparaten zoals USB-sticks (Chawki, 2021). Voorbeelden van malware zijn virussen, ransomware, bots en Trojaanse paarden (Chawki, 2021).
Gedigitaliseerde criminaliteit	Gedigitaliseerde criminaliteit refereert aan traditionele delicten die gepleegd worden met behulp van ICT (McGuire & Dowling, 2013b). Voorbeelden zijn phishing, vishing en online bankpasfraude.
Online fraude	Onder online fraude vallen traditionele criminele activiteiten gericht op het verkrijgen van geld door middel van bedrog of misleiding met behulp van netwerkcommunicatietechnologie, het verstrekken van frauduleuze uitnodigingen aan potentiële slachtoffers of het uitvoeren van frauduleuze transacties via internet (Burton et al., 2022; McGuire & Dowling, 2013b; Shang et al., 2022). Meestal leiden phishing-e-mails of sms-berichten gebruikers naar illegale websites die virussen downloaden of wachtwoorden, bankgegevens of andere gevoelige informatie stelen (Burton et al., 2022).
Phishing	Is een wijdverbreide vorm van *social engineering* die gebruikersreferenties verzamelt door doelwitten ertoe te verleiden persoonlijke of financiële informatie vrij te geven, zoals creditcardgegevens, op een frauduleuze website (Bijmans et al., 2021, p. 3757)
Vishing	Is een vorm van digitaliseerde fraude waarbij slachtoffers via telefoongesprekken, vaak uitgevoerd met behulp van Voice over Internet Protocol (VoIP), worden misleid om persoonlijke informatie of geld af te staan (Van Nguyen, 2022).

Datingfraude	Is een vorm van online fraude waarbij oplichters op digitale platforms romantische interesses wekken met als doel hun slachtoffers (grote sommen) geld afhandig te maken (Abubakari, 2024, p. 710).
Pig-butchering scam	In het Nederlands betekent het letterlijk 'varkensslachtingsfraude', is een nieuwe vorm van datingfraude waarbij criminelen vooropgezette romantische misleidingsstrategieën gebruiken om vertrouwen te winnen bij hun slachtoffers (Wang, 2024). Uiteindelijk maken ze gebruik van valse investeringsplatformen en cryptovalutakanalen om de fraude uit te voeren (Wang, 2024). Het is daarbij een vorm van mensenhandel waarbij slachtoffers niet alleen moeten werken, maar ook criminele activiteiten moeten uitvoeren (Wang, 2024). Het verschil met andere vormen van mensenhandel is dat slachtoffers worden behandeld als verhandelbare goederen, totdat ze geen waarde meer hebben (Wang, 2024).
Advance fee fraude	Is een vorm van oplichting waarbij fraudeurs gebruikmaken van digitale communicatiemiddelen om slachtoffers te misleiden (Tambe Ebot, 2023, p. 1). Criminelen proberen slachtoffers te overtuigen om vooraf een bedrag te betalen voor beloofde goederen of diensten die in werkelijkheid niet bestaan (Tambe Ebot, 2023, p. 1). Zodra fraudeurs een eerste betaling ontvangen, verzinnen ze nieuwe of herhalen ze eerdere leugens om maar extra betalingen van het slachtoffer te ontvangen (Tambe Ebot, 2023, p. 1). Ze blijven dit doen totdat het slachtoffer de fraude ontdekt en stopt met betalen (Tambe Ebot, 2023, p. 1).
Business Email Compromise (BEC)-fraude	Omvat het imiteren van e-mailadressen van leidinggevenden, medewerkers of zakenpartners, door middel van hacking of e-mailspoofing (Abubakari & Amponsah, 2024). Met deze vervalste e-mails worden financiële overboekingen aangevraagd, vaak met vervalste machtigingsbrieven en handtekeningen (Abubakari & Amponsah, 2024).
Goudhandelfraude (GPF)	Is een vorm van online criminaliteit waarbij slachtoffers worden misleid met investeringen in goudprojecten (Abubakari & Amponsah, 2024).
E-commerce fraude	Ook wel bekend als *customer-to-customer* (C2C) *fraude*, is een vorm van online fraude dat plaatsvindt via online platformen voor handel en transacties (Lee, 2022, p. 2530). Hierbij worden internet en sociale media vaak ingezet om vertrouwen en een goede relatie tussen verkopers en kopers op te bouwen (Lee, 2022, p. 2530). E-commercefraude kan verschillende vormen aannemen, waaronder fraude met leveringen, betalingen, retouren en restituties, en wordt zowel door verkopers als kopers gepleegd (Lee, 2022, p. 2530).
Concession-Abuse-as-a-Service (CAaaS)	Is een vorm van online fraude waarbij frauduleuze klanten proberen een gratis vervangingsproduct of terugbetaling van online winkels te

	krijgen door klantenservicemedewerkers te manipuleren en het retourproces uit te buiten (Sun et al., 2021, p. 4170).
Online werkgelegenheids-fraude	Is een vorm van online fraude waarbij niet-bestaande vacatures worden aangeboden met als doel om persoonlijke, gevoelige en/of financiële informatie van het slachtoffer te verkrijgen (Cole, 2022).
Online werknemers-fraude	Is een vorm van online fraude wordt aan de hand van online computertoegang gepleegd tegen het bedrijf of organisatie waar iemand voor werkt met als doel financiële voordelen te behalen (Othman & Ameer, 2022).
Online bankpas-fraude	Is een vorm van identiteitsdiefstal waarbij de creditcardgegevens van een ander zonder toestemming worden overgenomen om aankopen op de rekening te boeken of er geld van af te halen (Nguyen & Luong, 2021, p. 422).
Witwassen	Is het proces waarbij bezittingen afkomstig uit criminele activiteiten worden omgezet of overgeboekt om de illegale herkomst te verbergen of om criminelen te faciliteren (Abubakari & Amponsah, 2024).
Social engineering	Refereert aan het manipuleren van mensen door middel van bedrog om toegang te krijgen tot gevoelige informatie of beveiligde systemen (Steinmetz et al., 2021, p. 1). Dit kan verschillende vormen aannemen, zoals phishing (e-mailfraude), smishing (sms-fraude), spear-phishing (gerichte e-mailfraude), vishing (telefonische fraude) en bedrog in persoon (Steinmetz et al., 2021, p. 1).
Money mules	Ofwel geldezels of katvangers worden door cybercriminelen gebruikt om het spoor tussen slachtoffers en criminelen te verdoezelen, waardoor het voor wetshandhavingsinstanties moeilijker wordt om mensen achter de criminele netwerken op te sporen (Bekkers & Leukfeldt, 2023).
Bitcoin-gerelateerde online criminaliteit	Betreffen onder andere blackmail, sextortion en ramsomware waarbij betalingen via Bitcoin plaatsvinden (Buil-Gil et al., 2021).
Computer-gerelateerde cybercriminaliteit	De belangrijkste vormen van *computer-gerelateerde cybercriminaliteit* zijn cybertransacties en cyberfinanciering (Lee et al., 2023, p. 2). Bij een cybertransactie kan een crimineel proberen winst te maken uit nepverkopen (Lee et al., 2023, p. 2). Wat betreft cyberfinanciering kan een crimineel proberen een microbetaling te doen door de mobiele telefoongegevens van het slachtoffer te gebruiken zonder toestemming (Lee et al., 2023, p. 2).

3. Resultaten

3.1. Inleiding

In dit hoofdstuk zullen we stilstaan bij de resultaten van dit onderzoek. Eerst zal er in sectie 3.2 verder worden ingaan op de literatuur gerelateerd aan daderschap van online criminaliteit. De (risico)factoren zijn onderverdeeld in verschillende categorieën, namelijk: (1) demografische kenmerken; (2) intrinsieke en persoonlijkheidskenmerken; (3) mentaal; (4) routine activiteiten; (5) sociale relaties; (6) macrofactoren; (7) neutralisatietechnieken; (8) motieven; (9) Modus operandi; (10) misleidingstechnieken; (11) trends; (12) toekomstig onderzoek; (13) Interventies/trainingen.

Er zal stil worden gestaan bij de volgende online delicten, namelijk online criminaliteit (algemeen) (3.1.1), hacking (3.1.2), malware (3.1.3), online fraude (3.1.4), phishing (3.1.5), vishing (3.1.6), online romantisch fraude (3.1.7), pig-butchering scam (3.1.8), advance fee fraud (3.1.9), e-commerce fraude (3.1.10), concession-Abuse-as-a-Service (CAaaS)-fraude (3.1.11), online werkgelegenheidsfraude (3.1.12), online werknemersfraude (3.1.13), online bankpasfraude (3.1.14), social engineering (3.1.15), money mules (3.1.16), bitcoin-gerelateerde criminaliteit (3.1.17), overige vormen van online criminaliteit (3.1.18).

3.1.1. Online criminaliteit

Introductie

Wetenschappelijke literatuur

Onder online criminaliteit vallen delicten die betrekking hebben op zowel cybercriminaliteit (Engels: cyber-dependent crime) als gedigitaliseerde criminaliteit (Engels: cyber-enabled crime). Cybercrimee in enge zin wordt gedefinieerd als delicten waarbij ICT zowel het middel als doel is (McGuire & Dowling, 2013a). Voorbeelden zijn hacking en het maken en/of verspreiden van malware. Gedigitaliseerde criminaliteit refereert naar traditionele delicten die gepleegd worden met behulp van ICT (McGuire & Dowling, 2013b). Voorbeelden zijn phishing, cyberstalking en online bankpasfraude. Kortom, online criminaliteit betreft alle delicten waarbij ICT het middel en/of het doelwit is. In totaal zijn er zeventien studies geïdentificeerd die betrekking hebben op online criminaliteit. Dit betreffen de onderzoeken van Abubakari en Amponsah (2024), Apantaku (2021), Balogun en collega's (2024), Chawki (2021), Dearden en Gottschalk (2024), Faqir en Arfaoui (2024), Johnson (2024), Johnson en Nikolovska (2024), Khweiled en collega's (2021), Lakhani (2021), Leong en collega's (2024), Leukfeldt en Holt (2022), Lusthaus en collega's (2024), Orjiakor en collega's (2022), Puchkov (2021), Rachh (2024) en Zhou en collega's (2024).

De studie van Abubakari en Amponsah (2024) onderzocht op basis van een documentenanalyse gehanteerde misleidingsstrategieën en rollen die Ghanese diasporagroepen in de VS innemen bij verschillende vormen van online criminaliteit. Dit onderzoek kent een lage kwaliteitsscore.

Apantaku (2021) heeft middels een *mixed method benadering* (d.w.z. documentanalyse, focusgroups en interviews) onderzoek gedaan naar de motivatie, werkwijze en opkomende trends van online criminaliteit in Nigeria. De studie is met een gemiddelde kwaliteitsscore beoordeeld.

Balogun en collega's (2024) hebben aan de hand van vragenlijsten de prevalentie van online criminaliteit onder bachelorstudenten aan de Universiteit van Ilorin (Nigeria) onderzocht. De kwaliteit van deze studie is als gemiddeld beoordeeld.

Chawki (2021) heeft op zijn beurt middels een niet-systematische review onderzocht welke technieken door cybercriminelen in de Europese Unie en VS werden gebruikt tijdens de COVID-19 pandemie en welke preventieve methodes er tegen cyberaanvallen zijn. De kwaliteit van deze studie is als laag beoordeeld.

In het surveyonderzoek van Dearden en Gottschalk (2024) werd aan de hand van de *gemakstheorie*[3] geprobeerd om online criminaliteit in de VS te verklaren en werd er bestudeerd hoe cryptocurrency nieuwe kansen biedt voor anonieme financiële transacties. De studie is met een gemiddeld kwaliteitsscore beoordeeld.

Faqir en Arfaoui (2024) hebben een niet-systematische review uitgevoerd naar de psychologische motivaties die cybercrimineel gedrag aansturen. Dit onderzoek kent een lage kwaliteitsscore.

In de niet-systematische review van Johnson (2024) bespreekt de auteur de toekomstige misdaadagenda met daarbij een specifieke focus op opkomende technologieën. De studie is met een lage kwaliteitsscore beoordeeld.

[3] De gemakstheorie stelt dat (1) gelegenheid, (2) bereidheid en (3) motief crimineel gedrag stimuleren (Dearden & Gottschalk, 2024).

Johnson en Nikolovska (2024) hebben experimenteel onderzoek uitgevoerd naar de impact van (vrijheidsbeperkende) maatregelen op de toe- of afname van verschillende vormen van online criminaliteit tijdens de COVID-19 pandemie in het VK. De kwaliteit van deze studie is als hoog beoordeeld.

Khweiled en collega's (2021) hebben middels een trend- en patroonanalyse onderzocht hoe tijdens de COVID-19 pandemie verschillende soorten cyberaanvallen wereldwijd in de eerste helft van 2020 zijn veranderd ten opzichte van dezelfde periode in 2019. Daarbij bestudeerden de auteurs hoe criminelen de crisis benutten om verschillende vormen van online criminaliteit te plegen en onderzochten ze in hoeverre het gebrek aan bewustzijn bij gebruikers heeft bijgedragen aan de toename van deze aanvallen (Khweiled et al., 2021). De kwaliteit van deze studie is als laag beoordeeld.

Lakhani (2021) heeft een niet-systemantische review uitgevoerd naar het profiel van de cybercrimineel en de sociaal-psychologische factoren die hieraan bijdragen. Het onderzoek is met een lage kwaliteitsscore beoordeeld.

De studie van Leong en collega's (2024) zich op hoe cybercriminelen AI-technologie gebruiken voor online fraude en hoe AI kan worden ingezet om dit tegen te gaan. De studie is met een lage kwaliteitsscore beoordeeld.

Het doel van Leukfeldt en Holt (2022) was om aan de hand van Nederlandse politiedossiers en interviews in de VS, het VK en Duitsland te onderzoeken of cybercriminelen specialistisch zijn in het uitvoeren van bepaalde vormen van cybercriminaliteit of verschillende soorten criminaliteit plegen. De kwaliteit van deze studie is als hoog beoordeeld.

Lusthaus en collega's (2024) onderzochten middels een casestudy in het VK de netwerkstructuur, samenwerking en externe interacties van cybercriminele netwerken. De kwaliteit van dit onderzoek is als hoog beoordeeld.

Orjiakor en collega's (2022) hebben via het interviewen van Nigeriaanse jonge mannen uit met een criminele achtergrond onderzoek gedaan naar de criminele attitudes en denkpatronen die online criminaliteit ondersteunen. De studie is met een hoge kwaliteitsscore beoordeeld.

In de niet-systematische review van Puchkov (2021) wordt de opkomst van het internet en de rol die het heeft bij cybercriminaliteit behandeld. Het onderzoek is met een lage kwaliteitsscore beoordeeld.

De studie van Rachh (2024) onderzoekt aan de hand van criminaliteitscijfers de ruimtelijke en temporele patronen van online criminaliteit in India om te begrijpen waar deze misdaden zich het vaakst voordoen en wat de achterliggende oorzaken zijn. De studie is met een lage kwaliteitsscore beoordeeld.

Zhou en collega's (2024) tenslotte hebben survey-onderzoek gedaan naar de relatie tussen traditioneel en online sociaal leren gericht op online criminaliteit in China. De kwaliteit van dit onderzoek is als hoog beoordeeld. Zie Tabel 3 voor een overzicht van de relevante studies, en zie Tabel 4 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met online criminaliteit.

Tabel 3.
De referenties en kwaliteitsboordeling van de relevante studies voor online criminaliteit.

Referentie	Kwaliteit
(Abubakari & Amponsah, 2024)	Laag
(Apantaku, 2021)	Gemiddeld
(Balogun et al., 2024)	Gemiddeld
(Chawki, 2021)	Laag
(Dearden & Gottschalk, 2024)	Gemiddeld
(Faqir & Arfaoui, 2024)	Laag
(Johnson, 2024)	Laag
(Johnson & Nikolovska, 2024)	Hoog
(Khweiled et al., 2021)	Laag
(Lakhani, 2021)	Laag
(Leong et al., 2024)	Laag
(Leukfeldt & Holt, 2022)	Hoog
(Lusthaus et al., 2024)	Hoog
(Orjiakor et al., 2022)	Hoog
(Puchkov, 2021)	Laag
(Rachh, 2024)	Laag
(Zhou et al., 2024)	Hoog

Demografische factoren

Geslacht. Het lijkt erop dat mannen een grotere betrokkenheid hebben bij online criminaliteit dan vrouwen (Abubakari & Amponsah, 2024; Zhou et al., 2024). Zo blijkt uit een analyse van het Amerikaanse ministerie van Justitie dat van de 67 onderzochte cybercriminelen binnen de diasporagroepen 91% mannen en 9% vrouwen waren (Abubakari & Amponsah, 2024).

Inkomen. Het onderzoek van Dearden en Gottschalk (2024) toont aan dat een hoger inkomen positief lijkt samen te hangen met online criminaliteit. Volgens de auteurs kan dit mogelijk komen door het ervan van financiële druk (Dearden & Gottschalk, 2024). Deze druk ontstaat niet om te kunnen voorzien in de basisbehoeftes, maar door uitdagingen om een hogere levensstandaard te behouden (Dearden & Gottschalk, 2024).

Leeftijd. De literatuur is niet consistent met betrekking tot leeftijd en de kans om online criminaliteit te plegen. Zo laat de studie van Dearden en Gottschalk (2024) zien dat online criminaliteit afneemt naarmate de leeftijd toeneemt. Abubakari en Amponsah (2024) constateren daarentegen dat van de drie grootste leeftijdsgroepen 49% van de cybercriminelen in de leeftijdscategorie 30-39 jaar bevindt, 23% in de leeftijdscategorie tussen 20-29 jaar en 12% tussen 40-49 jaar.

Migratiestatus. In de studie van Abubakari en Amponsah (2024) komt naar voren dat wat betreft migratiestatus de meerderheid (76,9%) van de Ghanese cybercriminelen een verblijfsvergunning had (Abubakari & Amponsah, 2024).

Opleidingsniveau. Het lijkt erop dat opleidingsniveau negatief is gecorreleerd met online criminaliteit (Dearden & Gottschalk, 2024). Dit betekent dat cybercriminaliteit afneemt naarmate het opleidingsniveau toeneemt (Dearden & Gottschalk, 2024).

Intrinsieke en persoonlijkheidskenmerken

IT-kennis. Het lijkt erop dat over het algemeen cybercriminelen technisch vaardige mensen zijn (Faqir & Arfaoui, 2024). Wel is het zo dat dit kan afhangen van het type online criminaliteit (Zhou et al., 2024). Het plegen van gedigitaliseerde criminaliteit, zoals seksuele intimidatie en cyberpesten, vereist minder technologische expertise dan het plegen van cybercrime in enge zin, zoals hacken (Zhou et al., 2024). Er is als het ware een onderscheid te maken tussen criminelen die gebruik maken van kant-en-klare algoritmen/tools en echte criminele cyberexperts die deze diensten zelf ontwikkelen (Puchkov, 2021).

Morele ontwikkeling. Morele ontwikkeling lijkt een rol te spelen bij de vatbaarheid voor het plegen van cybercriminaliteit. Volgens Kohlbergs theorie van morele ontwikkeling groeit het morele oordeel van individuen mee met hun intellectuele ontwikkeling (Lakhani, 2021). Personen met een lagere ethische predispositie blijken vatbaarder te zijn voor online criminaliteit, zoals cyberpesten of financiële fraude (Lakhani, 2021). Voor deze individuen hebben persoonlijke belangen vaak prioriteit boven morele overwegingen (Lakhani, 2021).

Mentaal

Cognitieve bias. Psychologische vooroordelen, zoals overmoed of de illusie van controle, kunnen ertoe leiden dat mensen het risico onderschatten hoeveel risico ze lopen bij het plegen van online criminaliteit, maar ook de kans dat ze uiteindelijk tegen de lamp lopen (Faqir & Arfaoui, 2024).

Cognitieve Gedragstheorie. De *Cognitieve Gedragstheorie* van Aaron Beck benadrukt dat schadelijke denkpatronen, zoals onrealistische gedachten over de voordelen van online criminaliteit, bijdragen aan crimineel gedrag (Faqir & Arfaoui, 2024).

Empathie. Het lijkt erop dat mensen die een gebrek aan empathie hebben vatbaarder zijn voor het plegen van online criminaliteit (Faqir & Arfaoui, 2024).

Psychoanalytische Theorie. De *Psychoanalytische Theorie* van Freud suggereert dat online criminaliteit voortkomt uit onbewuste verlangens en conflicten, zoals de behoefte aan controle of de uiting van onderdrukte emoties, die mede mogelijk worden gemaakt door de anonimiteit van het internet (Faqir & Arfaoui, 2024).

Risicogedrag. Het lijkt erop dat sommige mensen een hoge tolerantie voor risico hebben, waardoor ze online criminaliteit plegen zonder de mogelijke gevolgen in ogenschouw te nemen (Faqir & Arfaoui, 2024).

Space Transition Theorie. De *Space Transition Theorie* stelt dat de cyberspace en echte criminaliteit elkaar beïnvloeden. Mensen die zich niet passen in de maatschappij kunnen eerder afdwalen in online criminaliteit. Online anonimiteit en gebrek aan controle kunnen online criminaliteit in de hand werken (Faqir & Arfaoui, 2024).

Stress. Stressfactoren zoals financiële problemen, relatieproblemen of werkontevredenheid kunnen mensen aanzetten tot het plegen van online criminaliteit als een manier om met de stress om te kunnen gaan (Faqir & Arfaoui, 2024).

Zelfcontrole. Onderzoek wijst uit dat mensen met een lagere zelfcontrole meer kans hebben om online criminaliteit te plegen (Faqir & Arfaoui, 2024; Zhou et al., 2024).

Criminaliteit

Meervoudige dader. Het lijkt erop dat sommige cybercriminelen zich specialiseren in een bepaalde vorm van online criminaliteit, terwijl andere zich of richten op meerdere vormen van online criminaliteit (Leukfeldt & Holt, 2022). Deze balans tussen specialisatie en veelzijdigheid

suggereert dat financieel gemotiveerde cybercriminelen mogelijk niet als een aparte dadergroep hoeven te worden gezien (Leukfeldt & Holt, 2022). Volgens Abubakari en Amponsah (2024) zijn cybercriminelen vaak betrokken bij verschillende vormen van cybercriminaliteit vanwege de onderlinge verbondenheid van deze misdrijven. Het plegen van online liefdesfraude bijvoorbeeld kan leiden tot andere criminele activiteiten, zoals witwassen, identiteitsdiefstal en beleggingsfraude (Abubakari & Amponsah, 2024). Analyse van persberichten en aanklachten toont eveneens aan dat Ghanese cybercriminelen, die zich zowel in Ghana als in de VS begeven, zich bezighouden met meerdere vormen van online criminaliteit, zoals datingfraude, witwassen en identiteitsdiefstal (Abubakari & Amponsah, 2024).

Sociale relaties

Gemeenschap. Het lijkt erop dat de gemeenschap een belangrijke rol speelt waarom mensen online criminaliteit gaan plegen (Balogun & collega's, 2024; Faqir & Arfaoui, 2024; Orjiakor en collega's (2022). De wens om geaccepteerd te worden binnen online gemeenschappen kunnen mensen ook aanzetten tot online criminaliteit (Faqir & Arfaoui, 2024). Dit is met name het geval als de persoon denkt dat het gedrag sociaal acceptabel is (Faqir & Arfaoui, 2024). De resultaten uit het onderzoek Balogun en collega's (2024) laten zien respondenten denken dat de toename van online criminaliteit onder studenten wordt veroorzaakt vanwege angst om aan academische behoeften te voldoen.

Groepsdruk. Groepsdruk lijkt in de meeste gevallen een belangrijke oorzaak te zijn van online pesten (Lakhani, 2021).

Imitatie. Imitatie lijkt een belangrijk proces te zijn bij het overnemen van crimineel gedrag. Personen die zich omringen met mensen die crimineel gedrag vertonen vaak gaan dit gedrag imiteren (Lakhani, 2021). Dit imitatiegedrag wordt versterkt door omgevingen die crimineel gedrag aanmoedigen (Lakhani, 2021).

Intimidatie. Mogelijk speelt intimidatie een rol om online criminaliteit te plegen (Balogun et al., 2024).

Online media. In het onderzoek van Lakhani (2021) wordt er gesteld dat afwijkend gedrag wordt beïnvloed onder andere online media.

Ouderschap. Mogelijk draagt slecht ouderschap bij aan de toename van online criminaliteit (Balogun et al., 2024).

Peers. Het lijkt erop dat peers een belangrijke rol spelen waarom mensen online criminaliteit gaan plegen (Faqir & Arfaoui, 2024; Lakhani, 2021; Orjiakor et al., 2022; Zhou & et al., 2024). De beïnvloeding door leeftijdsgenoten kan zowel in de offline als online wereld plaatsvinden (Lakhani, 2021). Orjiakor en collega's (2022) constateren bijvoorbeeld dat daders voornamelijk via vrienden of naaste collega's in de online criminaliteit terecht zijn gekomen.

Sociale banden. Het lijkt erop dat sterkere sociale banden de kans verkleinen om online criminaliteit te plegen (Zhou et al., 2024).

Traditioneel en online sociaal leren. Zhou en collega's (2024) dat *traditioneel sociaal leren* (d.w.z. interactie met peers in de fysieke wereld) een persoon vatbaarder maakt voor het plegen van verschillende vormen online criminaliteit (Zhou & collega's, 2024). *Online sociaal leren* (d.w.z. interactie met peers in de online wereld) leidt daarbij tot een meer gespecialiseerde cybercrimineel die specifieke criminele vaardigheden en ervaringen ontwikkelt in bepaalde vormen van online criminaliteit (Zhou & collega's, 2024). Verder lijkt het erop dat traditioneel sociaal leren een betere voorspeller is van gedigitaliseerde criminaliteit (bijvoorbeeld cyberpesten) dan voor

cybercrime in enge zin (zoals hacken) (Zhou & collega's, 2024). Dit kan ermee te maken dat de cyberwereld veel kansen biedt voor gedigitaliseerde criminaliteit door de aanwezigheid van kwetsbare slachtoffers en afwezigheid van toezicht (Zhou & collega's, 2024). Mensen die door traditionele criminaliteit negatieve opvattingen tegenover wetsovertredingen hebben ontwikkeld, zullen eerder geneigd zijn om gelegenheidsmisdaden (bijvoorbeeld seksuele intimidatie of pesten) te plegen dan misdaden die technische expertise vereisten (zoals hacken) (Zhou & collega's, 2024).

Macrofactoren

Armoede. Het lijkt erop dat armoede mogelijk bijdraagt aan een toename van online criminaliteit (Apantaku, 2021; Balogun en collega's, 2024; Faqir & Arfaoui, 2024).

Cultuur. Het lijkt erop dat culturele overtuigingen een belangrijke rol spelen in online criminaliteit. Uit de studie van Lakhani (2021) komt naar voren dat in met name collectivistische samenlevingen groepsloyaliteit en groepsdruk vaak het gedrag van mensen beïnvloeden. Culturele variabelen, zoals machtsafstand, individualisme, masculiniteit en onzekerheidsvermijding, kunnen een rol spelen waarom mensen online criminaliteit plegen (Lakhani, 2021).

Maatschappelijke eisen. Mogelijk speelt het gevoel te moeten voldoen aan maatschappelijke eisen waarom mensen overgaan tot het plegen van online criminaliteit (Balogun & collega's, 2024).

Migratie. Migratie lijkt in met name ontwikkelingslanden een belangrijke rol te spelen in online criminaliteit (Apantaku, 2021). Jonge mensen migreren door economische druk van rurale naar stedelijke gebieden waar ze vaak werkloos blijven vanwege een gebrek aan passende vaardigheden (Apantaku, 2021). Om toch in de eigen (basis)behoeften te kunnen voorzien en te kunnen stijgen op de maatschappelijk ladder, wenden velen zich tot de online criminaliteit (Apantaku, 2021). Deze situatie is zichtbaar in landen met hoge niveaus van rurale-urbane migratie en online criminaliteit, zoals China, Mexico en Rusland (Apantaku, 2021).

Ongelijkheid. Hoge ongelijkheid lijkt een rol te spelen bij het plegen van online criminaliteit (Apantaku, 2021).

Religieuze overtuigingen. Het lijkt erop dat religieuze overtuigingen mogelijk een rol spelen in online criminaliteit. De studie van Lakhani (2021) toont aan dat bewustwording van religieuze verboden op digitale piraterij binnen religieuze groepen leidt tot een significante afname van digitale piraterij.

Wetgeving en wetshandhaving. Effectieve wetten en adequate wetshandhaving kan van positieve invloed zijn op de prevalentie van online criminaliteit (Faqir & Arfaoui, 2024).

Neutralisatietechnieken

Dehumanisering. Uit de studie van Orjiakor en collega's (2022) blijkt dat deelnemers termen als ‘werk’, ‘klant’ of ‘pionnen’ gebruiken om hun slachtoffers te objectificeren. Dit wijst volgens de auteurs op het dehumaniseren van slachtoffers en een gebrek aan empathie jegens slachtoffers (Orjiakor et al., 2022).

Digitale ruimte (ethische filter). Het lijkt erop dat de digitale wereld een ‘ethisch’ filter biedt tussen de crimineel en de samenleving, waardoor er een psychologische afstand ontstaat tussen dader en slachtoffer (Lakhani, 2021), wat weer kan leiden tot minder berouw en empathie bij een crimineel (Faqir & Arfaoui, 2024).

Economische rechtvaardiging. Veel daders in de studie van Orjiakor en collega's (2022) beschouwden online criminaliteit als een rechtmatige manier om geld te verkrijgen, omdat ze ervan overtuigd zijn dat ze hun 'eerlijk aandeel' terughalen van buitenlandse landen die volgens hen rijkdom uit het land onttrekken (Orjiakor et al., 2022).

Hogere loyaliteiten. Mogelijk neutraliseren cybercriminelen door een beroep te doen op hogere loyaliteiten, zoals de criminele activiteiten worden gepleegd ten bate van een hoger en groter doel (Lakhani, 2021).

Koloniaal verleden. Sommige fraudeurs, opererend vanuit Nigeria, neutraliseren hun daden als een vorm van gerechtigheid en vergelding, vooral ten opzichte van westerse slachtoffers, omwille van de historische onrechtvaardigheid en uitbuiting tijdens de koloniale periode (Orjiakor et al., 2022).

Ontkennen van schade. Het lijkt erop dat criminelen hun daden neutraliseren door het ontkennen van schade door bijvoorbeeld te stellen dat er geen schade is ontstaan door criminele activiteit (Lakhani, 2021).

Ontkennen van slachtofferschap. Het lijkt erop dat cybercriminelen hun daden neutraliseren door het ontkennen van slachtofferschap (Lakhani, 2021; Orjiakor et al., 2022) door bijvoorbeeld te stellen dat hun slachtoffers toch rijk zijn en daardoor weinig last ervan zou hebben of dat hun verliezen op de een of andere manier zouden zijn gedekt (Orjiakor et al., 2022).

Ontkennen van verantwoordelijkheid. Het lijkt erop dat criminelen hun daden neutraliseren door het ontkennen van verantwoordelijkheid, zoals 'Het is niet mijn schuld' (Lakhani, 2021, p. 147).

Veroordelen van de veroordelaars. Het lijkt erop dat cybercriminelen mogelijk hun daden neutraliseren door het oordeel van anderen in twijfel te trekken door bijvoorbeeld te stellen: 'hoe durven ze mij te veroordelen, alsof ze het zelf nog nooit eerder hebben gedaan'(Lakhani, 2021, p.147).

Motieven

Afpersing. Uit het onderzoek van Rachh (2024) komt naar voren slachtoffer te zijn geweest van afpersing een belangrijke rol speelt in India waarom mensen betrokken raken bij online criminaliteit.

Altruïsme. Het is niet geheel duidelijk of altruïsme een motief is voor het plegen van online criminaliteit. Onderzoeken zijn niet eenduidig over de rol van altruïsme als motivatie voor online criminaliteit (Apantaku, 2021). De studie van Apantaku (2021) laat zien dat sommige cybercriminelen beweren dat hun acties zijn gericht ten behoeve van de samenleving. Ze leggen bijvoorbeeld kwetsbaarheden in de beveiliging van grote organisaties bloot om verbeteringen aan te kunnen dragen (Apantaku, 2021).

Avengers. Zogenoemde 'Avengers' plegen digitale misdrijven uit persoonlijke wrok, onrecht en de wens om macht of emotionele bevrediging te verkrijgen (Faqir & Arfaoui, 2024). Ze richten zich op specifieke mensen, groepen of organisaties en hun motieven kunnen variëren van financiële winst tot wraak (Faqir & Arfaoui, 2024).

Disrespect. De studie van Rachh (2024) laat zien dat iemand online criminaliteit pleegt als reactie op het ervaren van disrespect.

Financieel gewin. Het lijkt erop dat geld verdienen een belangrijke drijfveer is om online criminaliteit te plegen (Abubakari & Amponsah, 2024; Apantaku, 2021; Faqir & Arfaoui, 2024; Orjiakor et al., 2022; Puchkov, 2021). Redenen hiervoor kunnen variëren van het dekken van de eigen

levensbehoeften tot aan het onderhouden van een gezin (Orjiakor et al., 2022). Verder lijkt het erop dat cybercriminelen zich vooral richten op het maken van snelle (financiële) winsten (Puchkov, 2021).

Financiële problemen. Het lijkt erop dat financiële problemen leiden tot een verhoogde kans om online criminaliteit te plegen (Dearden & Gottschalk, 2024).

Hebzucht. Mogelijk speelt hebzucht ook een rol waarom mensen online criminaliteit plegen. Uit het onderzoek van Balogun en collega's (2024) komt naar voren de meerderheid van de respondenten gelooft dat de hoge mate van online criminaliteit onder studenten van de Universiteit van Ilorin onder andere het gevolg is van hebzucht.

Seksuele uitbuiting. De studie van Rachh (2024) laat zien dat slachtoffer zijn van seksuele uitbuiting een belangrijk motief was om over te gaan tot het plegen van online criminaliteit.

Wraak. Wraak lijkt ook een belangrijk motief te zijn waarom mensen overgaan tot het plegen online criminaliteit (Apantaku, 2021; Faqir & Arfaoui, 2024; Rachh, 2024).

Modus operandi

AI-technologie. AI lijkt steeds vaker door fraudeurs te worden gebruikt om frauduleuze activiteiten, zoals online identiteitsfraude, te plegen (Leong et al., 2024). Zo worden geautomatiseerde technieken, zoals het generen van valse inhoud (zoals tekst, afbeeldingen en video's), het klonen van stemmen voor impersonatie en AI-gedreven chatbots, gebruikt door cybercriminelen om online criminaliteit te plegen (Leong et al., 2024).

Gebruik van persoonsgegevens. Het lijkt erop dat online criminelen zich veelal richten op de persoonsgegevens van slachtoffers. De opkomt van sociale netwerksites en smartphones heeft tot een overvloed aan persoonlijke informatie geleid die door cybercriminelen worden verzameld en gedeeld (Chawki, 2021). Hierbij richten ze zich vooral op de volgende persoonsgegevens: (1) sociale zekerheidsnummers, (2) geboortedatum, (3) adressen en contactnummers, (4) informatie over huidige en vorige werkplekken, (5) financiële accountinformatie, (6) achternaam van de moeder en (7) en andere persoonlijke informatie, zoals e-mailwachtwoorden (Chawki, 2021). *Sociale zekerheidsnummers* worden gebruikt voor identiteitsdiefstal, aangezien ze toegang bieden tot overheidsinformatie, belastinggegevens en financiële diensten (Chawki, 2021, p. 992). De *geboortedatum* van het slachtoffer kan worden gebruikt voor identiteitsdiefstal of als onderdeel van beveiligingsvragen voor wachtwoordherstel (Chawki, 2021, p. 992). *Adressen en contactnummers* worden gebruikt voor verificaties van online transacties of om slachtoffers verder te misleiden in phishing aanvallen (Chawki, 2021, p. 992). *Informatie over huidige en vorige werkplekken* helpt cybercriminelen om een profiel van het slachtoffer op te kunnen bouwen (Chawki, 2021, p. 992). *Financiële accountinformatie* zijn essentieel voor diefstal van geld via bankrekeningen of voor het verkrijgen van toegang tot online betalingssystemen (Chawki, 2021, p. 992). De *achternaam van de moeder* wordt vaak gebruikt als een beveiligingsvraag voor wachtwoordherstel; cybercriminelen kunnen hiermee wachtwoorden resetten en toegang krijgen tot accounts (Chawki, 2021, p. 992). Als laatste *andere persoonlijke informatie*, zoals e-mailwachtwoorden, die cruciaal zijn voor toegang tot een breed scala aan persoonlijke gegevens en accounts (Chawki, 2021, p. 922). Het verzamelen van deze informatie kan leiden tot identiteitsdiefstal en ernstige beveiligingsproblemen voor slachtoffers (Chawki, 2021, p. 992).

Netwerk. Het lijkt erop dat cybercriminelen vaak opereren in criminele netwerken (Apantaku, 2021; Abubakari & Amponsah, 2024; Leukfeldt & Holt, 2022). Het onderzoek van Leukfeldt en Holt (2022) laat zien dat betrokkenen bij cybercriminaliteit, zowel specialisten als

generalisten, vaak onderdeel waren van grotere online criminele netwerken. Deze netwerken helpen criminelen bij het herkennen en benutten van kansen om verschillende vormen van online criminaliteit te plegen (Leukfeldt & Holt, 2022). Cybernetwerken variëren sterk, van losser georganiseerde groepen tot striktere clusters, met veel voorkomende typen zoals cyberfraude- en malware-netwerken (Lusthaus et al., 2024). Daarbij is er een onderscheid te maken tussen tussen goepen die de cyberaanvallen organiseren en groepen die de opbrengsten verwerken (Lusthaus et al., 2024). Daarnaast bevatten veel netwerken offline elementen en zijn niet volledig online georganiseerd. Dit laat volgens Lusthaus en collega's (2024) zien dat cybercriminelen lokaal zijn ingebed, wat in lijn is met eerder onderzoek (Lusthaus et al., 2024). Ook constateren de auteurs dat veel cybercriminelen dezelfde taal, nationaliteit of regionale achtergrond delen (Lusthaus et al., 2024). Gemeenschappelijke kenmerken bevorderen het vertrouwen en de samenwerking tussen criminelen (Lusthaus et al., 2024).

Online platforms. Het lijkt erop dat online platforms een belangrijk rol spelen in het faciliteren van online criminaliteit (Apantaku, 2021; Lusthaus et al, 2024; Puchkov, 2021). Via ondergrondse platforms als Deep Web en Dark Web wisselen criminelen tools, methoden, informatie en opbrengsten uit, wat leidt tot een professioneel ecosysteem (Apantaku, 2021). Puchkov (2021) constateert bijvoorbeeld dat cybercriminelen op online fora gestolen creditcard- en persoonsgegevens verhandelen. Lusthaus en collega's (2024) constateren in hun onderzoek dat online platforms worden gebruikt om expertise of contacten te vinden die niet binnen het eigen netwerk beschikbaar zijn, waarna verdere samenwerking meestal via privé communicatieplatforms verloopt.

Wisselende MO. Het lijkt erop dat cybercriminelen constant hun technieken aanpassen om steeds effectiever te kunnen opereren (Puchkov, 2021). Dit maakt het voor wetshandhavers en beveiligingsexperts lastig om snel en adequaat in te kunnen grijpen (Puchkov, 2021).

Trends

Anonimiteit. Technologische vooruitgangen en de globalisering van netwerken maken het voor cybercriminelen makkelijker om hun doelen te bereiken (Faqir & Arfaoui, 2024). Een belangrijke component hiervan is dat de virtuele anonimiteit die aanzienlijk heeft bijgedragen aan crimineel actieve ervaringen in de online wereld (Lakhani, 2021).

Corporate crimes. Puchkov (2021) constateert een groeiende trend van bedrijfsmisdrijven, met name in de financiële sector, waar online criminaliteit vaak hand in hand gaat met corruptie en social engineering.

Cryptocurrency. Meerderde onderzoeken tonen aan dat cryptocurrencies nieuwe mogelijkheden biedt voor online criminaliteit (Dearden & Gottschalk, 2024; Johnson, 2024). Deze digitale valuta kan verschillende vormen van online criminaliteit, zoals witwassen, ponzifraude en beursfraude, gemakkelijker maken (Johnson, 2024). Zo kan het worden gebruikt als hulpmiddel voor aankoop van illegale goederen (Dearden & Gottschalk, 2024). Bij ramsomware-aanvallen wordt cryptocurrency door criminelen gebruikt vanwege de anonimiteit en gemakkelijke wereldwijde verhandelen ervan (Johnson, 2024). Het risico op criminaliteit kan mogelijk groter worden op het moment dat overheden de digitale munt omarmen of als die wordt geïntegreerd in virtuele omgevingen als metaverse (Johnson, 2024).

DarkNet. De snelle vooruitgang in hardware- en softwaretechnologie draagt bij aan een voortdurende groei van het aantal DarkNet-gebruikers (Puchkov, 2021).

Digitaal bewijs. Puchkov (2021) stelt dat een belangrijk aspect van het bestrijden van cybercriminaliteit is het verzamelen en verwerken van digitale bewijs. Dit brengt de politie tot nieuwe uitdagingen op het gebied van procedurele en digitale forensische vaardigheden, aangezien het identificeren en veiligstellen van digitale bewijs complex en technisch is (Puchkov, 2021).

Extravagante levensstijl. Het onderzoek Leukfeldt en Holt (2022) ondersteunt het idee dat cybercriminelen hun inkomsten uit criminele activiteiten vaak uitgeven aan een extravagante levensstijl, zoals dure kleding en auto's.

Frequentie. Traditionele vormen van cybercriminaliteit, zoals ransomware en banking-Trojans, blijven wijdverspreid (Puchkov, 2021). Er was bijvoorbeeld tussen 2015 en 2018 een aanzienlijke toename van cyberaanvallen wereldwijd, waarbij cybercriminelen gebruik maakten van bekende tools zoals ransomware, spyware en software die betalingsprotocollen compromitteerde (Puchkov, 2021). Eenvoudige vormen van online criminaliteit, waar dus niet veel technische kennis voor nodig is, blijft vooral onder jonge daders toenemen en vertoont op de korte termijn geen tekenen van afname (Puchkov, 2021). Daarnaast wordt de toename van georganiseerde cybercriminaliteit wordt gekenmerkt door een groeiend aantal individuen en criminele groepen die profiteren van de (online) zwarte markt, zoals ontwikkeling van malware en virussen, het beheer van botnets en het behalen van financiële winst uit vertrouwelijke informatie (Puchkov, 2021). Puchkov (2021) constateert ook dat er een stijging lijkt te in misdaden tegen kinderen is, vooral op het gebied van seksuele uitbuiting. Zo is er steeds meer videomateriaal over kindermisbruik en andere vormen van pedofilie (Puchkov, 2021). Criminelen zoeken, bewerken en verspreiden seksueel getinte inhoud die veelal door kinderen zelf is gemaakt (Puchkov, 2021).

Groeiende dreiging. De dreiging van cybercriminaliteit groeit doordat cybercriminelen steeds geavanceerdere vaardigheden ontwikkelen en georganiseerde aanvallen uitvoeren (Puchkov, 2021). Voor financiële instellingen neemt het risico toe door gerichte aanvallen op persoonlijke accounts, waarbij gestolen gegevens worden gebruikt voor identiteitsfraude en manipulatie van bankkaartnummers (Puchkov, 2021). Ransomware vormt, vooral in combinatie met spyware, één van de grootste wereldwijde cyberdreigingen, waarbij betalingen worden onderschept en doorgestuurd (Puchkov, 2021). Er zijn twee typen ransomware te onderscheiden: (1) zelfstandige ransomware en (2) combinatie ramsomware. *Zelfstandige ramsomware* wordt gebruikt door jonge cybercriminelen en *combinatie ransomware* wordt ingezet door kleine hackersgroepen die ransomware combineren met andere software om betalingen te herleiden of accounts te compromitteren (Puchkov, 2021).

Internet. Het internet wordt steeds vaker ingezet voor desinformatie, reputatieschade en manipulatie van meningen, waardoor het een slagveld is geworden voor waardevolle informatie (Puchkov, 2021). Kwaadwillende organisaties gebruiken informatietechnologieën om nieuwe vormen van oorlogen te voeren, waaronder informatieoorlogvoering (Puchkov, 2021).

Kant- en-klare tools. De beschikbaarheid van kant-en-klare criminele tools heeft ertoe geleid dat individuen, zonder geavanceerde technische kennis, kunnen deelnemen aan online criminaliteit (Apantaku, 2021; Puchkov, 2021).

Ontwikkelingslanden. De studie van Lusthaus en collega's (2024) laat zien dat online criminaliteit in ontwikkelingslanden, zoals Nigeria en Rusland en Argentinië, groeit door hoge technologische expertise en beperkte regelgeving. Daardoor worden deze landen ideale uitvalbasissen voor complexe criminele technologieën en diensten (Lusthaus et al., 2024). Strengere

regelgeving en handhaving in landen als de VS, Canada en Australië beperken daarentegen de activiteiten van cybercriminelen (Lusthaus et al., 2024).

Ontwikkelingslanden. In onwikkelingslanden, zoals Nigeria, Roemenië en Argentinië, groeit door hoge technologische expertise en beperkte regelgeving, waardoor ze bronnen worden van complexe criminele tools en diensten (Apantaku, 2021). In tegenstelling hiermee beperken strengere regelgeving en handhaving in landen als de VS, Canada, het VK en Australië de activiteiten van cybercriminelen (Apantaku, 2021).

Risico's van AI-technologie. Hoewel AI mogelijkheden biedt, zoals verbeteringen in geneesmiddelenonderzoek, brengt het ook risico's met zich mee (Johnson, 2024). Voorbeelden zijn het creëren van deepfakes, AI-gecoördineerde aanvallen en geavanceerde cyberfraude (Johnson, 2024). Verder stellen Leong en collega's (2024) dat door AI-technologie aangedreven oplichtingspraktijken zowel voor individuen als bedrijven aanzienlijke risico's kunnen vormen. Individuen lopen het risico op financiële verliezen, identiteitsdiefstal en privacy-schendingen. Bedrijven kunnen financiële schade en reputatieverlies ervaren door scams die gericht zijn op hun medewerkers en klanten (Leong et al., 2024). Nepinhoud die door AI wordt gecreëerd, kan de reputatie van bedrijven schaden en het consumentenvertrouwen ondermijnen (Leong et al., 2024). Verder stellen de auteurs dat de groei van dergelijke scams het vertrouwen in digitale interacties en platforms verlaagt (Leong et al., 2024). Dit kan leiden tot minder gebruikers en economische schade (Leong et al., 2024). Ook wordt er in de tekst betoogt dat AI-gedreven manipulatie op sociale media verdeeldheid kan zaaien en de publieke opinie kan beïnvloeden, wat een bedreiging kan vormen voor democratische samenlevingen (Leong et al., 2024). De toegankelijkheid van AI stelt kwaadwillende actoren in staat om grootschalige scams te organiseren, waardoor de maatschappelijke impact van AI-fraude toeneemt (Leong et al., 2024).

Rol van staten. In sommige landen, zoals Rusland en China, wordt online criminaliteit steeds meer geaccepteerd als onderdeel van het dagelijks leven (Apantaku, 2021). Overheden legitimeren online criminaliteit door steun aan cyberoorlogsvoering, omdat deelname aan cyberaanvallen wordt gezien als patriottisch en een manier om de nationale economie te versterken (Apantaku, 2021). Daarnaast voeren staten zelf ook cyberaanvallen uit (Puchkov, 2021). Hierbij is te zien dat staten hun cyberaanval activiteiten intensiveren, met name cyberspionage, waarbij internet verbonden systemen en gesloten netwerken worden gehackt om informatie over nationale veiligheid en economische gegevens te verzamelen (Puchkov, 2021).

Versmelting van online criminaliteit. Cybercriminaliteit en gedigitaliseerde criminaliteit misdaden lijken steeds meer te vervagen (Lusthaus et al., 2024). Zo zijn veel aanvallen op systemen meest meestal niet winstgevend zijn zonder extra elementen zoals slachtoffer-manipulatie of witwasnetwerken (Lusthaus et al., 2024). Veel moderne malware-aanvallen zijn vormen van cyber-gefaciliteerde bankfraude of afpersing (Lusthaus et al., 2024).

Toekomstig onderzoek

Context en landen. Meerdere studies suggereren dat om online criminaliteit beter te kunnen begrijpen toekomstig onderzoek zich moet richten op zoveel mogelijk verschillende contexten (Apantaku, 2021; Leukfeldt & Holt, 2022; Orjiakor & et al., 2022; Zhou & collega's, 2024). Toekomstig onderzoek zou volgens Orjiakor en collega's (2022) de drijfveren, motivaties en denkpatronen van online criminaliteit wereldwijd moeten onderzoeken om verschillen en overeenkomsten in verschillende landen/continenten te kunnen begrijpen. De studie van Leukfeldt en Holt

(2022) bevatte een steekproef daders die werden onderzocht doorgrote Europese en Noord-Amerikaanse politieagentschappen. Hun gedrag en uitgavenpatronen weerspiegelen mogelijk niet die van cybercriminelen in andere delen van de wereld (Leukfeldt & Holt, 2022). Toekomstig zou daarom de steekproef moeten uitbreiden naar andere delen van de wereld (Leukfeldt & Holt, 2022). De studie van Apantaku (2021) richtte zich op Nigeria, maar de omstandigheden verschillen per land door unieke socioculturele, economische, regelgevende en technologische factoren. Het herhalen van het onderzoek in andere landen kan volgens de auteur zowel overeenkomsten als verschillen in de ontwikkeling van online criminaliteit laten zien (Apantaku, 2021).

Cyberoorlog en normalisatie. Cyberoorlogsvoering kan een rol spelen bij het normaliseren van online crimineel gedrag (Apantaku, 2021). Gericht onderzoek kan volgens Apantaku (2021) meer duidelijkheid verschaffen over de betrokkenheid van cyberlegers en hun bijdrage aan het normaliseren ervan.

Daderperspectief. Toekomstig zou zich moeten richten op het perspectief van cybercriminelen (Apantaku, 2021). Dit kan helpen om effectievere strategieën te ontwikkelen om de impact van deze misdaden te voorkomen of te verminderen (Apantaku, 2021).

Evaluatie. Er is behoefte aan het aan het evalueren van preventiestrategieën zodat beter inzicht wordt verkregen in welke maatregelen effectief zijn in het bestrijden van online criminaliteit (Apantaku, 2021; Johnson, 2024; Johnson & Nikolovska, 2024). Apantaku (2021) stelt dat cybersecuritystrategieën wereldwijd zijn niet altijd effectief gebleken. Toekomstig onderzoek zou volgens de auteur hierop moeten focussen (Apantaku, 2021). Dit kan worden gedaan door de standpunten van belanghebbenden te analyseren en factoren te identificeren die de implementatie ervan belemmeren (Apantaku, 2021). Verder laten Johnson (2024) en Johnson en Nikolovska (2024) zien dat er nagenoeg geen onderzoek is gedaan naar de effectiviteit van preventiemaatregelen tegen online criminaliteit. Dit wordt volgens Johnson (2024) versterkt doordat (politie) data vaak te laat wordt geanalyseerd, waardoor er onvoldoende kan worden ingespeeld op nieuwe vormen van online criminaliteit (Johnson, 2024).

Faciliterende factoren. Er lijkt behoefte te zijn aan meer onderzoek naar faciliterende factoren van online criminaliteit (Balogun & collega's, 2024; Leukfeldt & Holt, 2022; Orjiakor en collega's, 2022). Leukfeldt en Holt (2022) hebben in hun studie niet de oorzaken van crimineel gedrag onderzocht, waardoor het onduidelijk blijft waarom sommige daders zowel online als offline misdrijven plegen. Meer studies zijn er volgens de auteurs nodig om te begrijpen welke factoren de criminele loopbaan van cybercriminelen beïnvloeden (Leukfeldt & Holt, 2022). Hierdoor kunnen er effectievere interventies worden ontwikkeld ter voorkoming van recidive (Leukfeldt & Holt, 2022). Aansluitend geven Balogun en collega's (2024) aan dat er voortdurend onderzoek moet worden gedaan naar onderliggende factoren van online criminaliteit, zodat controle- en preventiemaatregelen effectief kunnen worden aangepast.

Methode en data-analyse. Meerdere onderzoeken benadrukken het belang van het gebruik van verschillende onderzoeksmethodes bij het analyseren van online criminaliteit (Abubakari & Amponsah, 2024; Dearden en Gottschalk, 2024; Johnson, 2024; Leukfeldt & Holt, 2022; Zhou & et al., 2024). Abubakari en Amponsah (2024) benadrukken het belang van demografische factoren bij het begrijpen van crimineel gedrag in diasporagemeenschappen. Hun studie is gebaseerd op persberichten en officiële aanklachten, wat de toepasbaarheid volgens de auteurs op andere criminele gemeenschappen mogelijk beperkt, en daarom zouden interviews met daders meer inzicht geven in hun motivaties (Abubakari & Amponsah, 2024). Overeenkomstig geven Leukfeldt en Holt (2022) aan dat het beperkte bewijs in hun onderzoek van uitgaven en verdiensten van

daders te wijten is aan het type politiedata dat gebruikt werd. Wetshandhavingsonderzoeken richten zich namelijk vooral richten op bewijs dat verdachten verbindt met specifieke criminele activiteiten (Leukfeldt & Holt, 2022). Toekomstig onderzoek, zoals interviews met daders en politie, is daarom nodig om het verdienpotentieel van cybercriminelen beter te kunnen begrijpen (Leukfeldt & Holt, 2022). Verder stellen de auteurs dat gestructureerde interviews ook kunnen bijdragen in het beter begrijpen van hoe online criminaliteit de levensstijl van daders beïnvloedt (Leukfeldt & Holt, 2022). Daarnaast suggereren Zhou en collega's (2024) om de rol van de causale mechanismen van sociaal leren op dadergedrag beter te kunnen begrijpen, dat er longitudinale data – in plaats van cross-sectionele – gebruikt moet worden. In het onderzoek van Johnson (2024) wordt er aangegeven dat er verschillende technieken gebruikt moeten worden, zoals horizon scanning, literatuuronderzoek en Delphi-methodes met experts, om dreigingen van nieuwe vormen van online criminaliteit te identificeren. Dit zou volgens de auteur moeten leiden tot een lijst van potentiële dreigingen die kunnen worden beoordeeld op waarschijnlijkheid en impact (Johnson, 2024).

Sociaal leertheorie. De sociaal leertheorie stelt dat mensen nieuw gedrag leren door het observeren van sociale effecten van anderen. Er is volgens Faqir en Arfaoui (2024) meer onderzoek nodig om via deze theorie te begrijpen hoe online gemeenschappen bijdragen aan de verspreiding van online criminele kennis en methoden.

Steekproef. Om de generaliseerbaarheid te bevorderen, zou toekomstig onderzoek grotere steekproeven en diverse vormen van online criminaliteit moeten includeren (Lusthaus et al., 2024; Zhou et al., 2024). Zo zijn de resultaten uit de studie van Lusthaus en collega's (2024) gebaseerd op tien strafzaken die niet representatief zijn voor alle vormen van online criminaliteit. Daarom zou toekomstig onderzoek het aantal strafzaken moeten uitbreiden en zich richten op meerdere vormen van online criminaliteit (Lusthaus et al., 2024). Daarnaast stellen Dearden en Gottschalk (2024) dat meer onderzoek nodig is om te bestuderen of de traditionele leeftijd-criminaliteitscurve ook van toepassing is op online criminaliteit. Hoewel uit de resultaten van het onderzoek anders blijkt, kan dit volgens de auteurs variëren tussen verschillende type online criminaliteit (Dearden & Gottschalk, 2024).

Interventie/trainingen

Slachtoffergericht

Bewustzijn. Er zou meer moeten worden ingezet om het bewustzijn bij gebruikers omtrent de risico's en gevolgen van online criminaliteit te vergroten (Balogun et al., 2024; Chawki, 2021; Faqir & Arfaoui, 2024; Khweiled et al., 2021; Johnson, 2024). Educatieve initiatieven kunnen consumenten, professionals en jongeren trainen in cyberveiligheid en verantwoord digitaalgedrag (Faqir & Arfaoui, 2024). Mensen moeten bijvoorbeeld leren hoe ze phishing e-mails kunnen herkennen en melden (Faqir & Arfaoui, 2024).

Detectie. Khweiled en collega's (2021) pleitten voor de ontwikkeling van geavanceerdere detectiesoftware on cyberaanvallen effectief te kunnen identificeren. Aansluitend stellen Leong en collega's (2024) dat AI een cruciale rol kan spelen in het opsporen en voorkomen van online fraude in sectoren als cybersecurity, finance en e-commerce. AI-technieken maken gebruik van geavanceerde algoritmen (zoals gedragsanalyse en real-time monitoring) en machine learning-technieken die het mogelijk maken om efficiënt en effectief afwijkingen, patronen en indicatoren van online fraude te kunnen identificeren (Leong et al., 2024).

Innovatieve methodes. Johnson (2024) stelt dat voor het begrijpen en voorkomen van toekomstige criminaliteit het gebruik van innovatieve methoden, zoals natuurlijke taalverwerking en grote taalmodellen, noodzakelijk is naast traditionele technieken uit de milieucriminologie. Zo kan volgens de auteurs situationele criminaliteitspreventie een kader zijn om na te denken over preventiemogelijkheden (Johnson, 2024).

Monitoren. Khweiled en collega's (2021) pleitten voor striktere ICT-monitoring wanneer zich uitzonderlijke situaties voordoen, zoals een pandemie.

Ondersteuning slachtoffer. Slachtoffers van online criminaliteit zouden uitgebreide ondersteuning, zoals counseling, juridische hulp en financiële compensatie, moeten krijgen om herstel te bevorderen en herhaling op slachtofferschap te voorkomen (Faqir & Arfaoui, 2024).

Risicobeoordeling. Om slachtofferschap van online criminaliteit te verkleinen, zou volgens Puchkov (2021) gebruik gemaakt moeten worden van risicobeoordelingen. Een effectieve risicobeoordeling moet menselijke acties en kwetsbaarheden identificeren, en de impact hiervan op systemen en hulpbronnen analyseren (Puchkov, 2021).

Samenwerking. Meerdere onderzoeken opperen dat er meer samenwerking moeten komen tussen verschillende overheden en private organisaties Faqir & Arfaoui, 2024; Lakhani, 2021). Volgens Faqir en Arfaoui (2024) is samenwerking tussen overheidsinstanties, wetshandhaving, private sector en internationale partners noodzakelijk om online criminaliteit te kunnen bestrijden. Samenwerking met private partijen stelt opsporingsinstanties in staat om criminele trends te analyseren, onderzoekslijnen te bepalen en bewijs te verzamelen (Lakhani, 2021).

Wetgeving. Er is behoefte aan wetgeving die is aangepast aan hedendaagse vormen van online criminaliteit (Faqir & Arfaoui, 2024; Johnson, 2024; Puchkov, 2021). Zo pleitten Faqir en Arfaoui (2024) voor krachtige wetgeving die aangepast is aan technologische ontwikkelingen en samenwerking tussen landen bevordert (Faqir & Arfaoui, 2024). Hierbij is het van belang dat verschillende type online criminaliteit helder worden gedefinieerd, er passende straffen komen, er naast internationale samenwerking ook proactieve samenwerking is tussen publieke en private sectoren en dat bescherming en privacy van slachtoffers wordt gewaarborgd (Faqir & Arfaoui, 2024). Aansluitend stelt Puchkov (2021) dat er grondige analyse nodig is van bestaande wetgeving om juridische leemtes te identificeren, aangezien sommige strafrechtelijke bepalingen voor offline misdrijven niet altijd geschikt zijn voor online misdrijven en daarom moeten worden herzien (Puchkov, 2021). Johnson (2024) geven bovendien aan dat in gedecentraliseerde omgevingen, zoals metaverses, het moeilijker is om verantwoordelijkheid te definiëren (Johnson, 2024). Een mogelijke oplossing die de auteur aandraagt, is het betrekken van zogenoemde *decentralised autonomous organisations* (DAOs), organisaties die zonder centrale autoriteit opereren (Johnson, 2024).

Zelfbeschermingsmaatregelen. Chawki (2021) komt in zijn studie met een aantal aanbevelingen voor gebruikers om hun online veiligheid te vergroten. Zo stelt hij dat er veilige betaalopties, zoals PayPal of Google Wallet, moeten worden gebruikt (Chawki, 2021). Ook wordt er aangeraden om niet op links te klinken of bestanden te downloaden van onbekende websites (Chawki, 2021). Verder zouden URL’s zorgvuldig gecontroleerd moeten worden om zeker te zijn van de authenticiteit (Chawki, 2021). Ook zouden gebruikers niet zomaar onbekende e-mailbijlagen moeten openen, omdat deze vaak virussen bevatten, zoals malware of ransomware - banken en overheidsinstanties sturen zelden links om gegevens te verifiëren (Chawki, 2021). Ook wordt er afgeraden om online financiële of persoonlijke informatie te delen (Chawki, 2021). Als

laatste wordt er geadviseerd om altijd een tweefactor authenticatie te gebruiken om accounts beter te beveiligen (Chawki, 2021).

Dadergericht

Cognitieve bias. De cognitieve gedragstheorie van aan Aaron Beck benadrukt dat schadelijke denkpatronen, zoals onrealistische gedachten over de voordelen van online criminaliteit, bijdragen aan crimineel gedrag (Faqir & Arfaoui, 2024). Door deze negatieve gedachten te vervangen en positieve gedragingen aan te moedigen, kan online criminaliteit worden verminderd (Faqir & Arfaoui, 2024)

Ethisch gedrag. Meerdere onderzoeken stellen dat ethisch gedrag moet worden bevorderd (Balogun et al., 2024; Faqir en Arfaoui, 2024; Lakhani, 2021). Er zouden volgens Balogun en collega's (2024) workshops en trainingen moeten worden gegeven over het ethisch gebruik van ICT-tools. Verder stellen Faqir en Arfaoui (2024) dat morele principes en waarden in onlinegedrag moeten worden bevorderd door verantwoordelijk digitaal gedrag bij het grote publiek aan te moedigen. Omdat dergelijke maatregelen collectieve voordelen bieden, kunnen beleidsinitiatieven, zoals samenwerking of publieke interventie, nodig zijn om implementatie ervan te waarborgen (Lakhani, 2021).

Sociaalgerichte interventies. Apantaku (2021) geeft in zijn studie aan dat online criminaliteit vooral wordt beïnvloed door sociale, culturele en economische motieven. Uitsluitend technologische interventies zijn daardoor volgens de auteur ineffectief en daarom zou de focus moeten komen te liggen op sociale interventies als gezinszorg, onderwijs en ondersteuning bij economische stress (Apantaku, 2021).

Socioculturele en economische gerichte aanpak. Volgens Apantaku (2021) zouden landen zich moeten richten op de socioculturele en economische oorzaken die online crimineel gedrag veroorzaken. Door economische groei en betere kansen te bieden aan mensen, kunnen talenten op een positieve manier worden benut en kan crimineel gedrag worden verminderd (Apantaku, 2021). Aansluitend stellen Orjiakor en collega's (2022) dat het creëren van werkgelegenheid en sociale voorzieningen belangrijk is om jongeren te ontmoedigen om online criminaliteit te plegen.

Verdienmodel. Het lijkt erop dat het verminderen van het verdienmodel van criminelen online criminaliteit kan doen afnemen (Johnson, 2024). Dit kan bijvoorbeeld worden bewerkstelligd door de mogelijkheden voor witwassen via mixer-diensten te beperken (Johnson, 2024).

Tabel 4. Samenvatting resultaten van de literatuur over online criminaliteit

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
Geslacht (man)	IT-kennis	-	Gemeenschap	Armoede	Dehumanisering	AI-technologie	Anonimiteit	Context en landen	Bewustzijn
Leeftijd	Morele ontwikkeling		Groepsdruk	Cultuur	Digitale ruimte (ethische filter)	Gebruik van persoonsgegevens	Corporate crimes	Cyberoorlog en normalisatie	Detectie
Migratiestatus	Cognitieve bias		Intimidatie	Maatschappelijke eisen	Economische rechtvaardiging	Netwerk	Cryptocurrency	Daderperspectief	Innovatieve methodes
Opleidingsniveau	Cognitieve gedragstheorie		Ouderschap	Migratie	Hogere loyaliteiten	Online platforms	DarkNet	Evaluatie	Monitoren
	Empathie		Peers	Ongelijkheid	Koloniaal verleden	Wisselende MO	Digitaal bewijs	Faciliterende factoren	Ondersteuning slachtoffer
	Psychoanalytische Theorie		Sociale banden	Religieuze overtuigingen	Ontkennen van schade		Extravagante levensstijl	Methode en data-analyse	Risicobeoordeling
	Risicogedrag		Traditioneel en online sociaal leren	Wetgeving en wetshandhaving	Ontkennen van slachtofferschap		Frequentie	Sociaal leertheorie	Samenwerking
	Space Transition theorie				Ontkennen van verantwoordelijkheid		Groeiende dreiging	Steekproef	Wetgeving

Stress		Veroordelen van de ver-oordelaars	Internet	Zelfbescher-mingsmaatre-gelen
Zelfcontrole		Afpersing	Kant-en-klare tools	Cognitieve bias
Meervoudige dader		Altruïsme	Ontwikke-lingslanden	Ethisch gedrag
		Avengers	Risico van AI	Sociaalgerichte interventies
				Socio-econo-misch interven-tie
		Disrespect	Rol van sta-ten	Verdienmodel
		Financieel gewin	Versmelting van online criminaliteit	
		Financiële problemen		
		Hebzucht		
		Seksuele uit-buiting		
		Wraak		

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.2. Hacking

Introductie

Wetenschappelijke literatuur

Hacking betreft het ongeautoriseerd toegang verkrijgen tot apparaten zoals mobiele telefoons en computers (Lee et al., 2023, p. 1). Cybercriminelen krijgen hierbij toegang tot de online informatie van gebruikers, wat schade kan veroorzaken (Lee et al., 2023). Een crimineel kan bijvoorbeeld proberen toegang te krijgen tot iemands online account door gebruik te maken van persoonlijke gegevens van het slachtoffer, zoals inlog-ID en wachtwoord (Lee et al., 2023, p. 2). In totaal zijn er vier studies geïdentificeerd die betrekking hebben op hacking. Dit betreffen de onderzoeken van Bossler (2021) Johnson en Nikolovska (2024), Khweiled en collega's (2021) en Lee en collega's (2023).

Bossler (2021) heeft via een vragenlijst onderzocht hoe studenten neutralisatietechnieken gebruiken om hun bereidheid om cyberaanvallen uit te voeren te rechtvaardigen. Dit onderzoek kent een gemiddelde kwaliteitsscore.

Johnson en Nikolovska (2024) hebben experimenteel onderzoek uitgevoerd naar de impact van (vrijheidsbeperkende) maatregelen op de toe- of afname van verschillende vormen van online criminaliteit tijdens de COVID-19 pandemie. De kwaliteit van deze studie is als hoog beoordeeld.

Khweiled en collega's (2021) hebben middels een trend- en patroonanalyse onderzocht hoe tijdens de COVID-19 pandemie verschillende soorten cyberaanvallen wereldwijd in de eerste helft van 2020 zijn veranderd ten opzichte van dezelfde periode in 2019. Daarbij keken de auteurs naar hoe criminelen de crisis benutten om verschillende soorten online criminaliteit te plegen en onderzochten ze in hoeverre het gebrek aan bewustzijn bij gebruikers heeft bijgedragen aan de toename van deze aanvallen (Khweiled et al., 2021). Dit onderzoek kent een lage kwaliteitsscore.

Lee en collega's (2023) hebben middels interviews met politie rechercheurs criminele factoren voor verschillende vormen van online criminaliteit onderzocht om vervolgens met suggesties te komen voor preventieve maatregelen. De kwaliteit van dit onderzoek is als hoog beoordeeld. Zie Tabel 5 voor een overzicht van de relevante studies, en zie Tabel 6 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met hacking.

Tabel 5.
De referenties en kwaliteitsboordeling van de relevante studies voor hacking.

Referentie	Kwaliteit
(Bossler, 2021)	Gemiddeld
(Johnson & Nikolovska, 2024)	Hoog
(Khweiled et al., 2021)	Laag
(Lee et al., 2023)	Hoog

Demografische kenmerken

Geslacht en leeftijd. Het lijkt erop dat hackers voornamelijk mannen zijn van alle leeftijden (Lee et al., 2023). Wat betreft de verdachten van hacking, komt uit het onderzoek van Lee en collega's

(2023) naar voren dat het merendeel man (89,23%) was met uiteenlopende leeftijden - variërend van tieners tot 50-plussers (98,96%).

Criminaliteit

Strafblad en recidive. Het lijkt erop dat de meeste criminelen die hacking plegen *first offenders* zijn en dat een substantieel kleinere groep een eerdere veroordeling op haar naam heeft staan (Lee et al., 2023). Lee en collega's (2023) constateren dat van de verdachten 57,14% geen strafblad had, 21,43% een eerdere veroordeling kent, 0% 2 tot 6 eerdere veroordelingen heeft en 17,86% 6 tot 9 eerdere veroordelingen op hun namen hebben.

Routine activiteiten

Chatrooms. Het is onduidelijk of van het spenderen in chatrooms een voorspellend effect uitgaat op het plegen van hacking. Bossler (2021) constateert dat studenten die meer tijd in chatrooms doorbrachten, bereidwilliger bleken te zijn binnenlandse en buitenlandse overheidsservers te doorzoeken naar informatie, en om websites van een officiële buitenlandse overheidsinstantie te hacken. Dit kan volgens de auteurs worden verklaard doordat meer tijd in chatrooms doorbrengen kan helpen bij het verkrijgen en delen van informatie over hacking (Bossler, 2021). Eerder onderzoek waaraan de auteur refereert laat echter zien dat meer tijd op sociale media doorbrengen correleert met een lagere bereidheid om illegale activiteiten te ondernemen, zoals het aanvallen van overheids- of bankservers (Bossler, 2021). Dit zou te maken kunnen hebben met online sociale controle, waarbij mensen die meer tijd op sociale media doorbrengen, sterke netwerken hebben en bang zijn dat deviant gedrag hun online status zou schaden (Bossler, 2021).

Sociale relaties

Peers. Het hebben van deviante vrienden vergroot mogelijk de kans op betrokkenheid bij hacking verhoogt. De studie van Bossler (2021) laat zien dat vanuit het omgaan met hackende leeftijdsgenoten een voorspelde significante treedt op de bereidheid om te hacken. Mogelijke verklaring is dat hackers zowel online als offline contacten hebben om kennis te delen en elkaar te helpen bij het verbeteren van hun hack-technieken (Bossler, 2021). Daarbij zorgen zulke contacten dat hacking wordt goedgekeurd en reiken ze elkaar manieren aan om hacking te rechtvaardigen (Bossler, 2021).

Neutralisatietechnieken

Neutralisatietechnieken (algemeen). Er lijkt mogelijk sprake te zijn dat neutralisatietechnieken de kans vergroten om betrokken te raken bij hacking. Volgens het onderzoek van Bossler (2021) blijkt dat het gebruik van neutralisatietechnieken de bereidheid vergroot om verschillende vormen van hacking te ondernemen. Dit omvat o.a.: (1) Het *defacen*[4] van websites van belangrijke binnenlandse en buitenlandse overheidsfunctionarissen; (2) het defacen van officiële websites van belangrijke binnenlandse en buitenlandse overheidsinstellingen; (3) het binnendringen in servers van binnenlandse en buitenlandse banken met als doel fondsen te stelen en deze vervolgens aan slachtoffers van overheidsbeleid te schenken; en (4) het doorzoeken van servers van binnenlandse en buitenlandse overheidsinstanties op geheime documenten met de intentie deze openbaar te maken om de overheid in verlegenheid te brengen (Bossler, 2021).

[4] *Defacen* is het zonder toestemming aanpassen van websites.

Hogere morele principes. In tegenstelling tot eerder onderzoek, constateren Bossler (2021) weinig bewijs voor een verband tussen hogere loyaliteiten (Engels: *appeal to higher loyalties*) en de bereidheid om te hacken.

Ontkennen van slachtofferschap. Het lijkt erop dat daders die slachtoffer geen slachtofferstatus (Engels: *deny victim status*) toekennen meer bereid zijn om bankservers te compromitteren en buitenlandse overheidsservers te doorzoeken (Bossler, 2021). Een mogelijke verklaring hiervoor is dat studenten die bereid zijn om bedrijven te hacken zichzelf zien als slachtoffers door de acties van diezelfde beschrijven (Bossler, 2021). Ze geloven daarbij verder dat buitenlandse overheden meer gestraft zouden moeten worden dan de overheid van hun eigen land (Bossler, 2021).

Ontkennen van schade. Ontkennen van letsel (Engels: *denying injury*) lijkt geen voorspellende factor te zijn bij het plegen van hacking (Bossler, 2021). Uit het onderzoek van Bossler (2021) blijkt dat hoewel hackers vaak beweren dat hun acties weinig schade veroorzaken, het eigenlijke doel van ideologisch gemotiveerde hackers toch is om schade toe te brengen aan een entiteit die hen eerder schade heeft toegebracht (Bossler, 2021). Daarnaast constateren Lee en collega's (2023) dat hacken, zoals toegang krijgen tot online accounts, vaak niet wordt erkend als even ernstig als fysieke inbraak, hoewel ze juridisch vergelijkbaar zijn (Lee et al., 2023).

Persoonlijke rechtvaardiging. De neutralisatietechniek *the metaphor of the ledger*, wat iemands geloof inhoudt dat hij meer goed dan slecht heeft gedaan in zijn leven, lijkt mogelijk niet de bereidheid van het plegen van verschillende vormen van hacking te vergroten. De studie van Bossler (2021) laat juist zien dat hoe sterker iemand de *metaphor of the ledger* aanhangt, hoe minder bereid die persoon is tot het hacken van een overheidswebsite.

Rechtvaardiging door vergelijking. Het lijkt erop dat rechtvaardiging door vergelijking (Engels: *justifcation by comparison*), waarbij daders verklaren dat ze ergere misdaden zouden kunnen plegen, geen significant effect te hebben op het plegen van hacking (Bossler, 2021).

Rechtvaardiging op basis van noodzaak. Verdediging van noodzaak, oftewel geen andere keuze hebben, lijkt geen significant effect te hebben op de kans op het plegen van hacking (Bossler, 2021).

Rechtvaardigingsclaim. Een rechtvaardigingsclaim (Engels: *claim of entitlement*) verwijst naar de overtuiging dat iemand het recht zou moeten hebben op toegang tot computerinformatie die een overheid, school, bedrijf of individu over hem of haar bezit, zelfs zonder expliciete toestemming (Bossler, 2021). Deze overtuiging blijkt een belangrijke voorspeller te zijn van de bereidheid om websites van persoonlijke overheidsfunctionarissen en overheidsinstellingen te hacken, evenals van het doorzoeken van overheidsservers op zoek naar gênante informatie (Bossler, 2021). Deze neutralisatietechniek kende alleen geen significante relatie met de bereidheid om bankservers te compromitteren (Bossler, 2021).

Verantwoordelijkheid ontkennen. Verantwoordelijkheid ontkennen (Engels: *denying responsibility*) lijkt geen significant effect te hebben op het plegen van hacking (Bossler, 2021).

Veroordelaars veroordelen. Het lijkt erop dat van de neutralisatietechniek veroordelaars veroordelen (Engels: *condemned the condemners*) een voorspellend effect uitgaat op het plegen van hacking. Zo blijkt uit het onderzoek van Bossler (2021) dat respondenten die de veroordelaars veroordeelden bereid waren om alle vier de onderzochte vormen van hacking te plegen. Motieven van (ideologisch gemotiveerde) hackers zijn onder andere om corrupte overheden en wetshandhavingsinstanties te straffen, maar ook doordat over het algemeen de hackerscultuur het strafrechtelijk systeem van de overheid wantrouwen en als vijandig beoordelen (Bossler, 2021).

Verspreiding van schuld. Verspreiding van schuld (Engels: *difussion of guilt*), ofwel als de meeste mensen iets doen kan het niet zo verkeerd zijn, lijkt alleen een voorspellend effect te hebben op de bereid tot het hacken van websites van belangrijke binnenlandse en buitenlandse overheidsfunctionarissen (Bossler, 2021).

Motieven

Game-items. Uit het onderzoek van Lee en collega's (2023) blijkt dat 14.29% van de verdachten betrokken was bij hacking vanwege game-items. Games-items verwijst naar het gebruik maken van andermans ID en wachtwoord om spelitems te bemachtigen, schade aan te richten of deze te verkopen (Lee et al., 2023). Jongere verdachten, zoals tieners, gebruikten vaak accounts van ouders of andere volwassenen om toegang te krijgen tot games (Lee et al., 2023). Anderen hackten persoonlijke informatie om anoniem accounts aan te maken op websites (Lee et al., 2023).

Plezier en impulsiviteit. Een belangrijk motief om te hacken is plezier. Zo blijkt uit het onderzoek van Lee en collega's (2023) dat 35.71% van de verdachten waren betrokken bij hacking uit impulsiviteit, nieuwsgierigheid of amusement, vaak zonder besef van de illegaliteit. Sommigen werden hiertoe aangezet door vrienden of omdat ze toevallig toegang hadden tot persoonlijke informatie, zoals wachtwoorden van een vriend (Lee et al., 2023).

Woede. Uit het onderzoek van Lee en collega's (2023) komt naar voren 7.14% van de verdachten betrokken waren bij hacking om hun woede te uiten over een onderwerp of persoon.

Modus operandi

Gebruikte kanalen. De resultaten uit het onderzoek van Lee en collega's (2023) suggereren dat de belangrijkste kanalen die hackers gebruiken zijn: *online sites* (zoals portals, gamesites en webwinkels) die verantwoordelijk waren voor 75% van de gevallen, *interne systemen van organisaties* (zoals provinciale kantoren) vormden 10,72% van gevallen, *bulletin boards* (zoals een bulletin board van een instelling) waren goed voor 7,14% en tenslotte *mobiele messenger-apps* (zoals KakaoTalk) die ook goed waren voor 7,14% van de gevallen.

Koopbaarheid van persoonsgegevens. Het onderzoek van Lee en collega's (2023) constateert dat in 3,57% de gevallen de verdachten persoonlijke informatie van anderen online konden kopen, met name via de (online) zwarte markt.

Persoonlijke informatie. De studie van Lee en collega's (2023) identificeerden twee hoofdmethoden van hacking: diefstal van persoonlijke informatie (85,71% van de gevallen) en lekken van persoonlijke informatie (14,29%). Bij diefstal van persoonlijke informatie gebruiken verdachten ongeautoriseerd de persoonlijke informatie van anderen om toegang te krijgen tot online platforms om bijvoorbeeld examenvragen te bemachtigen of te het controleren van een partner op ontrouw (Lee et al., 2023). Bij de tweede methode lekken verdachten persoonlijk informatie voor bijvoorbeeld e-mailreclame (Lee et al., 2023). De studie van de auteurs laat zien dat verdachten vaak gebruik maakten van USB-drives of Messenger-diensten om gegevens te kopiëren (Lee et al., 2023). De bevindingen uit de studie benadrukken dat de meeste verdachten persoonlijke informatie inzetten voor hacking-gerelateerde misdaden en wijzen op het belang van beter beheer en beveiliging van persoonlijke gegevens (Lee et al., 2023). Verder geven hackers aan dat ze gemakkelijk toegang konden krijgen tot persoonsgegevens (Lee et al., 2023).

Trends

Frequentie. De bevindingen van Johnson en Nikolovska (2024) suggereren dat hacken tijdens COVID-19 toenam. Het lijkt erop dat de niveaus van online fraude gekoppeld waren aan patronen van mobiliteit en online activiteit, dus het aantal hackingen namen toe naarmate vrijheidsbeperkingen toenamen en namen af naarmate de maatregelen werden versoepeld (Johnson & Nikolovska, 2024).

Relatie tot het slachtoffer. Het lijkt erop dat de meeste hackers geen relatie hebben met het slachtoffer. Zo blijkt uit het onderzoek van Lee en collega's (2023) dat 39,29% van de verdachten het slachtoffer niet persoonlijk kenden, in 17,86% van de gevallen waren de dader en het slachtoffer vrienden van elkaar en bij 14,29% van de verdachten was het slachtoffer een geliefde. In minder gevallen betrof het slachtoffer de werkgever (10,71%), school alumnus (7,14%), de buurman (3,57%) zakelijke relatie (3,57%) of familie (3,57%) (Lee et al., 2023).

Toekomstig onderzoek

Chatrooms en sociale media. Toekomstig onderzoek moet zich volgens Bossler, (2021) richten op hoe het tijd spenderen in chatrooms en op sociale media de bereidheid tot het plegen van online criminaliteit beïnvloedt, zoals het hacken van websites en aanvallen op kritieke infrastructuur (Bossler, 2021).

Steekproef. Vervolgonderzoek naar waarom sommige individuen bereid zijn om zowel kleine als grote cyberaanvallen op binnen- en buitenlandse doelen uit te voeren, is volgens Bossler (2021) belangrijk vanwege de gevolgen voor nationale veiligheid, publieke veiligheid en financiële stabiliteit (Bossler, 2021). Volgens de auteurs zijn huidige inzichten, inclusief die uit de eigen studie, vooral zijn gebaseerd op beperkte steekproeven van studenten van een paar universiteiten (Bossler, 2021). Om beter te begrijpen hoe verschillende politieke en economische structuren deze kwesties contextualiseren, zou volgens de onderzoekers toekomstig onderzoek zich moeten richten meer diverse populaties niet-universitaire studenten van zowel binnen als buiten de Verenigde Staten moeten includeren (Bossler, 2021).

Interventies/trainingen

Slachtoffergericht

Monitoren. Volgens Khweiled en collega's (2021) helpen monitoring en risicobeheer om cyberdreigingen te verminderen en organisaties te beschermen tegen online criminaliteit.

Dadergericht

Afschrikking. Bossler (2021) suggereert dat afschrikkingsgebaseerde strategieën om online criminaliteit te bestrijden ineffectief blijken te zijn. Ideologisch gebaseerde hackers zijn mogelijk zelfs moeilijker af te schrikken dan financieel georiënteerde hackers vanwege hun sterke drang om hun 'ideologische missie' te voltooien (Bossler, 2021). Daarom zouden volgens de auteur landen er sterk rekening mee moeten houden dat het uitbreiden van wetgeving en het verhogen van straffen waarschijnlijk niet het gewenste afschrikwekkende effect hebben.

Bewustzijn schade. Educatieve programma's zouden zich moeten richten op het informeren van individuen dat hacking, zelfs eenvoudigere vormen, aanzienlijke financiële en emotionele gevolgen kan hebben voor individuen, bedrijven en landen (Bossler, 2021). Bossler (2021) stelt dat het doel van zulke interventies niet is om te sturen op lange termijn veranderingen bij mensen, maar eerder zinspeelt op het geweten van potentiële daders te spelen (Bossler, 2021).

Neutralisatietechnieken. Volgens Bossler (2021) zouden preventieprogramma's gericht moeten zijn op het voorlichten van jongeren en jongvolwassenen van gehanteerde neutralisatietechnieken, zoals veroordeling van de veroordelaars en ontkenning van het slachtoffer, die worden gebruikt om online criminaliteit te rechtvaardigen (Bossler, 2021). Deze programma's zouden kunnen helpen om deze technieken te identificeren en te leren hoe ze kunnen voorkomen dat hun besluitvorming wordt beïnvloed door deze overtuigingen (Bossler, 2021).

Tabel 6. Samenvatting resultaten van de literatuur over hacking.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
Geslacht en leeftijd	Strafblad en recidive	Chatrooms	Peers	-	Neutralisatie-technieken (algemeen)	Gebruikte kanalen	Frequentie	Chatrooms en sociale media	Monitoren
					Hogere morele principes	Koopbaarheid van persoonsgegevens	Relatie tot het slachtoffer	Steekproef	Afschrikking
					Ontkennen van slachtofferschap	Persoonlijke informatie			Bewustzijn schade
					Ontkennen van schade				Neutralisatie-technieken
					Persoonlijke rechtvaardiging				
					Rechtvaardiging door vergelijking				
					Rechtvaardiging o.b.v. noodzaak				
					Rechtvaardigingsclaim				
					Verantwoordelijkheid ontkennen				

				Veroordelaars veroordelen Verspreiding van schuld Game-items Plezier en impul-siviteit Woede					
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.3. Malware

Introductie

Wetenschappelijke literatuur

Malware is kwaadaardige software die wordt gemaakt om zonder toestemming informatie van een gebruiker te wijzigen, verwijderen of te bespioneren (Chawki, 2021). Het kan zich verspreiden via internet of externe apparaten zoals USB-sticks (Chawki, 2021). Voorbeelden van malware zijn virussen, ransomware, bots en Trojaanse paarden (Chawki, 2021). In totaal zijn er twee studies geïdentificeerd die betrekking hebben op malware. Dit betreft het onderzoek van Chawki (2021) en Kigerl (2021).

Chawki (2021) heeft middels een niet-systematische review onderzocht welke technieken er door cybercriminelen in de Europese Unie en VS werden gebruikt tijdens de COVID-19 pandemie, en daarbij effectieve methodes belicht om cyberaanvallen aan te pakken. De kwaliteit van deze studie is als laag beoordeeld.

Het onderzoek van Kigerl (2021) analyseerde 871.146 e-mails om de impact van de *routine activiteiten theorie*[5] op onder andere malware in 120 landen in kaart te brengen. De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 7 voor een overzicht, en zie Tabel 8 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met malware.

Tabel 7.
De referentie en kwaliteitsboordeling van de relevante studies voor malware.

Referentie	Kwaliteit
(Chawki, 2021)	Laag
(Kigerl, 2021)	Hoog

Macrofactoren

Internetgebruikers. De studie van Kigerl (2021) wijst uit het aantal internetgebruikers in een land de meest consistente en sterkste voorspeller blijkt te zijn van malware. Hoe meer internetgebruikers een land heeft, hoe meer malware-aanvallen er in een land zijn (Kigerl, 2021).

Welvaart. Het lijkt erop dat BBP geen significante voorspeller van malware als er rekening werd gehouden met het aantal internetgebruikers (Kigerl, 2021). Met andere woorden: rijkere landen kennen meer malware-aanvallen, niet vanwege hun welvaart, maar omdat het aantal internetgebruikers hoger is dan bij armere landen (Kigerl, 2021). Eerder onderzoek waaraan de Kigerl (2021) refereert laat daarentegen zien dat landen met hoge werkloosheid en veel internetgebruikers de meeste cyberaanvallen uitvoeren, terwijl landen met veel werkloosheid en weinig internetgebruikers de minste aanvallen hebben (Kigerl, 2021). Dit kan ermee te maken hebben dat rijkere, technologisch ontwikkelde landen vanwege hun welvaart meer kansen bieden voor online criminaliteit, terwijl economisch zwakkere landen die wel beschikken over hoogwaardige technologie juist vaker cybercriminelen aantrekken (Kigerl, 2021).

[5] De *routine activiteiten theorie* stelt dat criminaliteit ontstaat wanneer er een geschikt doelwit is, een gemotiveerde dader aanwezig is en er een gebrek aan capabele bewakers is.

Modus operandi

Blokkeren van toegang. Ransomware, een type van malware, richt zich op het blokkeren van toegang tot gegevens of systemen van slachtoffers. Aanvallers eisen losgeld, tegenwoordig vaak in ontraceerbare bitcoins, in ruil voor het herstellen van de toegang (Chawki, 2021). Het blokkeren van de toegang gebeurt doordat slachtoffers via HTML-links schadelijke software downloaden (Chawki, 2021). Er lijken drie veelvoorkomende methodes te worden gebruikt: (1) *crypto-ransomware* waarbij bestanden worden versleuteld, (2) *locker-ransomware* waarbij volledige toegang tot het systeem wordt geblokkeerd, (3) en een combinatie van beide (Chawki, 2021).

Social engineering. Uit de studie van Chawki (2021) komt naar voren dat criminelen gebruik van social engineering-technieken om slachtoffers te manipuleren en hen te overtuigen om malware te installeren.

Verspreiding via download of bijlages in e-mails. Het lijkt erop dat malware, zoals Trojaanse paarden en ransomware, vaak wordt verspreid via downloads of bijlagen in e-mails (Chawki, 2021). Een Trojaans paard komt vaak voor in legale software, zoals populaire games, downloadbare bestanden of pop-upvensters (Chawki, 2021). Een Trojaans paard installeert zich automatisch zodra het wordt gedownload en wordt elke keer uitgevoerd wanneer de computer opstart (Chawki, 2021). Na de installatie kan het de beveiligingsmaatregelen van de computer omzeilen en schadelijke handelingen uitvoeren, zoals het uploaden van bestanden, het inzien van wachtwoorden en het monitoren van het scherm (Chawki, 2021). In tegenstelling tot wormen, die zichzelf automatisch dupliceren, heeft een Trojaans paard altijd de interactie van de gebruiker nodig om zich te verspreiden (Chawki, 2021). Een veelvoorkomende schadelijke actie van een Trojan is het uitschakelen van de harde schijf en het overschrijven van opstartprogramma's (Chawki, 2021).

Toekomstig onderzoek

Multilevel model. De studie van Kigerl (2021) onderzocht de routine-activiteiten theorie op nationaal niveau in plaats van op individueel niveau. Volgens het onderzoek zou toekomstig onderzoek beide niveaus moeten combineren in een multilevel model, waarin zowel individuele als macro-economische factoren worden meegenomen, om zo een beter begrip van malware te krijgen (Kigerl, 2021).

Tabel 8. Samenvatting resultaten van de literatuur over malware.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	Internetgebruikers Welvaart	-	Blokkeren van toegang Social engineering Verspreiding via download of bijlages in e-mails	-	Multilevel model	-
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.4. Online fraude

Introductie

Wetenschappelijke literatuur

Onder online fraude vallen traditionele criminele activiteiten gericht op het verkrijgen van geld door middel van bedrog of misleiding met behulp van netwerkcommunicatietechnologie, het verstrekken van frauduleuze uitnodigingen aan potentiële slachtoffers of het uitvoeren van frauduleuze transacties via internet (Burton et al., 2022; McGuire & Dowling, 2013b; Shang et al., 2022). Meestal leiden phishing-e-mails of sms-berichten gebruikers naar illegale websites die virussen downloaden of wachtwoorden, bankgegevens of andere gevoelige informatie stelen (Burton et al., 2022). In totaal zijn er tien studies geïdentificeerd die specifiek betrekking hebben op online fraude. Dit betreffen de studies van Aborisade (2023), Alhasan 2022), Cretu-Adatte en collega's (2024), Cross (2022), Jiang en collega's (2024), Johnson en Nikolovska (2024), Kigerl (2021), Levi en Smith (2022), Nguyen en Luong (2021) en Ojolo en Singh (2023).

De studie van Aborisade (2023) heeft via interviews onderzocht hoe de houding van ouders en gezinsfactoren in Nigeria bijdragen aan de betrokkenheid van kinderen bij online fraude en hoe dit de rol van ouders in de opvoeding beïnvloedt. Dit onderzoek kent een hoge kwaliteitsscore.

Aan de hand van experimenteel onderzoek heeft Alhasan (2022) onderzocht of technologie mensen een gevoel van afstand geeft, waardoor ze mogelijk eerder geneigd zijn om onlinefraude te plegen. Ook is er in de studie onderzocht hoe vertrouwd iemand is met technologie en of dit van invloed is op de relatie tussen het afstandseffect van technologie en onethisch handelen (Alhasan, 2022). De studie is met een gemiddelde kwaliteitsscore beoordeeld.

Cretu-Adatte en collega's (2024) onderzochten in hun studie hoe Ivoriaanse cybercriminelen te werk gaan bij online fraude, hoe ze de wet omzeilen en hoe ze hun criminele winsten beheren. De kwaliteit van deze studie is als gemiddeld beoordeeld

Cross (2022) heeft via een niet-systematische review geschetst wat er momenteel bekend is van digitale fraude omtrent de gehanteerde modus operandi van daders en effectieve interventies om digitale fraude te bestrijden. De studie is met een lage kwaliteitsscore beoordeeld.

Jiang en collega's (2024) hebben een experiment uitgevoerd waarin ze hebben onderzocht hoe winst- of verliesgerichte berichten digitale fraude beïnvloeden en hoe risicoperceptie de reactie op fraude en interventies bepaalt. Het onderzoek is met een hoge kwaliteitsscore beoordeeld.

Johnson en Nikolovska (2024) hebben experimenteel onderzoek uitgevoerd naar de impact van (vrijheidsbeperkende) maatregelen op de toe- of afname van verschillende vormen van online criminaliteit, waaronder digitale fraude, tijdens de COVID-19 pandemie. De kwaliteit van deze studie is als hoge beoordeeld.

Het onderzoek van Kigerl (2021) analyseerde 871.146 e-mails om de impact van de *routine activiteiten theorie*[6] op digitiale fraude in 120 landen in kaart te brengen. De kwaliteit van deze studie is als hoog beoordeeld.

[6] De routine activiteiten theorie stelt dat cybercriminaliteit ontstaat wanneer er een geschikt doelwit is, een gemotiveerde dader aanwezig is en er een gebrek aan capabele bewakers is.

Levi en Smith (2022) hebben in hun artikel gekeken naar de kenmerken van (gedigitaliseerde) fraude tijdens pandemieën en bestudeerden of er unieke risico's aan verbonden zijn. Het onderzoek is met een lage kwaliteitsscore beoordeeld.

Het onderzoek van Nguyen en Luong (2021) heeft op basis van een sociale netwerkanalyse - gecombineerd met data van criminele profielen en interviews met de politie – de structuur van online fraudenetwerken (d.w.z. bankpasfraude en vishing) in Vietnam onderzocht. Het onderzoek is met een gemiddelde kwaliteitsscore beoordeeld.

De studie van Ojolo en Singh (2023) heeft aan de hand van interviews onderzocht hoe Nigeriaanse fraudeurs omtrent online fraude criminele vaardigheden ontwikkelen, samenwerken en kennis delen binnen hun netwerken. De studie is met een gemiddelde kwaliteitsscore beoordeeld. Zie Tabel 9 voor een overzicht, en zie Tabel 10 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met online fraude.

Tabel 9.
De referenties en kwaliteitsboordeling van de relevante studies voor online fraude.

Referentie	**Kwaliteit**
(Aborisade, 2023)	Hoog
(Alhasan, 2022)	Gemiddeld
(Cretu-Adatte et al., 2024)	Gemiddeld
(Cross, 2022)	Laag
(Jiang et al., 2024)	Hoog
(Johnson & Nikolovska, 2024)	Hoog
(Kigerl, 2021)	Hoog
(Levi & Smith, 2022)	Laag
(Nguyen & Luong, 2021)	Gemiddeld
(Ojolo & Singh, 2023)	Gemiddeld

Sociale relaties

Gedeelde banden en gemeenschappelijke affiliaties. Het lijkt erop dat criminele samenwerking niet alleen wordt bepaald door persoonlijke relaties, maar ook door gedeelde banden met een groep en gemeenschappelijke affiliaties met verschillende geografische locaties (Ojolo & Singh, 2023). Dit lijkt te suggereren dat samenwerking tussen criminelen ook afhankelijk is van gemeenschappelijke belangen en netwerken over grenzen heen (Ojolo & Singh, 2023).

Groepsinteractie. Het leerproces voor fraude lijkt als eenvoudig te worden beschreven, omdat informatie en praktijken vooral via groepsinteractie worden gedeeld (Ojolo & Singh, 2023). Jongeren die geïnteresseerd zijn in online fraude kunnen worden gerekruteerd door vrienden, kennissen of anderen met veel kennis van illegale activiteiten (Ojolo & Singh, 2023).

Mentorschap. De studie Ojolo en Singh (2023) toont aan dat jonge mensen investeren in geavanceerde trainingen voor verschillende vormen van cybercriminaliteit, zoals betaalpasfraude, om grotere opbrengsten te behalen. Mentorschap is een cruciaal onderdeel van dit leerproces, waarbij mentoren hun kennis delen in ruil voor een percentage van de opbrengsten van een geslaagde oplichting (Ojolo & Singh, 2023).

Ouders. In de studie van Aborisade (2023) komt naar voren dat de acceptatie, steun en betrokkenheid van ouders invloed hebben op de deelname van jongeren aan online fraude in Nigeria. Ouders gaven in de studie aan dat deze acceptatie met name komt door de slechte

sociaaleconomische condities in het land en daardoor het lastig was voor ouders om het gedrag hun kinderen te veranderen (Aborisade, 2023). De kinderen gebruikten de opbrengsten om financiële controle over hun ouders uit te oefenen, wat invloed had op hun opvoeding (Aborisade, 2023).

Macrofactoren

Internetgebruik. De studie van Kigerl (2021) wijst uit dat het aantal internetgebruikers in een land de meest consistente en sterkste voorspeller blijkt te zijn van online fraude. Met andere woorden: hoe meer internetgebruikers een land heeft, hoe meer online fraude in een land plaatsvinden (Kigerl, 2021).

Welvaart. Welvaart lijkt negatief geassocieerd te zijn met online fraude (Kigerl, 2021; Ojolo en Singh, 2023). Dit betekent dat mensen in armere landen vaker betrokken zijn bij online fraude dan rijkere landen (Kigerl, 2021). Rijkere landen bieden meer kansen voor online fraude, omdat welvaart meer goederen en mogelijkheden voor online fraude bieden (Kigerl, 2021).

Neutralisatietechnieken

Neutralisatie bij ouders van fraudeurs. De studie van Aborisade (2023) toont aan dat daders niet alleen de acceptatie van online fraude bij hun ouders beïnvloeden, maar ook hun betrokkenheid bij online fraude en criminele levensstijl. Volgens de auteur laat dit zien dat zowel ouders als kinderen elkaar beïnvloeden in de opvoeding en de ontwikkeling van de onderlinge relatie (Aborisade, 2023). De economische voordelen die voortvloeien uit online fraude vergroten de autonomie van kinderen en beïnvloeden hun ontwikkelingsproces (Aborisade, 2023). Dit roept vragen op over hoe goed ouders afwijkend gedrag bij hun kinderen kunnen controleren, zoals sociale controletheorieën binnen het gezin suggereren. (Aborisade, 2023). Aborisade (2023) plaatst verder ook vraagtekens bij de sociale bindingstheorie, die stelt dat crimineel gedrag ontstaat door zwakkere of verbroken sociale banden met wetgevende mensen en instellingen.

Motieven

Financieel gewin. Het lijkt erop dat financieel gewin een belangrijke drijfveer is om online fraude te plegen (Levi & Smith, 2022).

Hebzucht. Hebzucht lijkt eveneens een reden te zijn waarom mensen betrokken raken bij online fraude (Levi & Smith, 2022).

Modus operandi

Anticiperen. Het lijkt erop dat online fraudeurs met hun fraudepraktijken inspelen op situaties die zich voordoen. Zo laat het onderzoek van Levi en Smith (2022) zien dat fraudeurs de COVID-19 pandemie gebruikten om hun oplichtingspraktijken aan te passen, zoals het aanbieden van valse beschermingsmiddelen en vaccins. Om slachtoffers succesvol te kunnen bedriegen, moeten daders moeiteloos van de ene techniek of verhaallijn naar de andere kunnen overschakelen (Cross, 2022).

Netwerk (actoren). Het lijkt erop dat fraudeurs opereren binnen een netwerk (Cretu-Adatte & collega's, 2024; Ojolo & Singh, 2023). Een crimineel netwerk bestaat veelal uit verschillende actoren. *Kernleden* die de oplichting initiëren. *Professionele enablers* die bieden diensten aanbieden, zoals het verstrekken van valse documenten of het ontwikkelen van phishingwebsites. *Gerekruteerde enablers* die beschikken over essentiële informatie of middelen voor het

uitvoeren van criminele activiteiten, waarvoor cybercriminelen betalen om er toegang toe te krijgen. Tenslotte geldezels die hun bankrekening ter beschikking stellen om geld tussen verschillende rekeningen te kunnen plaatsten, zodat kernleden minder makkelijk te traceren zijn door opsporingsinstanties (Cretu-Adatte et al., 2024). Binnen een netwerk opereren leden binnen de groep doorgaans autonoom, maar werken samen wanneer dat nodig (Ojolo & Singh, 2023). Samenwerking stelt fraudeurs in staat om sneller en efficiënter geld te verdienen, de opbrengsten te delen en vaardigheden te verbeteren (Ojolo & Singh, 2023). Zo kan iemand die zich bezighoudt met datingfraude samenwerken met een spammer om betalingen via alternatieve kanalen te laten verlopen (Ojolo & Singh, 2023).

Netwerk (structuur). Nguyen en Luong (2021) constateren dat netwerken met een hoge mate van online activiteit zelden strak georganiseerd zijn in vergelijking met netwerken met een lagere mate van online activiteit. Er worden vier verschillende typen netwerken geïdentificeerd op basis van de mate van leiderschap (Nguyen & Luong, 2021). Het eerste type netwerk betreft *zwermnetwerken*, die geen duidelijk leiderschap hebben, zoals net opgerichte hackforums (Nguyen & Luong, 2021). Deze netwerken kunnen snel veel leden aantrekken zonder strikte lidmaatschapsbeperkingen, waardoor ze moeilijk door wetshandhavingsinstanties aan te pakken zijn (Nguyen & Luong, 2021). De tweede type zijn *gedistribueerde netwerken*, die worden gekenmerkt door onduidelijk leiderschap en veel online activiteit (Nguyen & Luong, 2021). Hoewel er meestal één of enkele centrale spelers zijn, ontbreekt een duidelijke leider, waardoor deze netwerken lastig te centraliseren zijn, is er geen duidelijke leider, wat deze netwerken moeilijker te centraliseren maakt (Nguyen & Luong, 2021). Tot het derde type behoort enkelgerichte netwerken, die geleid worden door één leider, zoals online aankoopnetwerken en vervalsingskaarten-netwerken (Nguyen & Luong, 2021). Deze netwerken zijn kleiner en meer gestructureerd (Nguyen & Luong, 2021). Groepsgerichte netwerken vormen de vierde categorie die worden georganiseerd door een kernsubgroep van leiders, zoals telefoon oplichtings-netwerken en volwassen hackforums (Nguyen & Luong, 2021). Deze netwerken zijn groter en vereisen samenwerking binnen de leiderschapsstructuur (Nguyen & Luong, 2021).

Samenwerking corrupte overheidsfunctionarissen. Cretu-Adatte en collega's (2024) constateren online fraudeurs samenwerken met corrupte overheidsfunctionarissen die werkzaam zijn bij banken, de politie, geldtransactiekantoren of andere openbare instellingen. Deze functionarissen krijgen in ruil voor hun diensten een deel van de fraudeopbrengst (Cretu-Adatte et al., 2024).

Smurfen. De studie van Cretu-Adatte en collega's (2024) laat zien dat fraudeurs grote geldbedragen verdelen in kleinere sommen, een techniek die bekend staat ‘smurfen’, om te voorkomen dat financiële tussenpersonen argwaan krijgen.

Technologie. Het onderzoek van Ojolo en Singh (2023) constateert dat technologie criminelen helpt om hun activiteiten uit te breiden, zodat deze niet meer gebonden zijn aan één plek. Zo kunnen fraudeurs zowel online als offline samenwerken (Ojolo & Singh, 2023). Ze delen kennis met elkaar, wat hen helpt om nieuwe strategieën te ontwikkelen om hun fraudeleuze activiteiten te kunnen vergemakkelijken (Ojolo & Singh, 2023). Samenwerking is wel sterk afhankelijk van de mate waarin criminelen informatie vrij met elkaar kunnen delen (Ojolo & Singh, 2023).

Verliesaversie. Het onderzoek van Jiang en collega's (2024) toont aan dat dat fraude vooral werken door het verhogen van de verliesaversie. Oplichtingspraktijken die de nadruk leggen op een mogelijk verlies bij uitblijven van een reactie, maken mensen meer bewust van dat risico, waardoor mensen sneller geneigd zijn te reageren (Jiang et al., 2024).

Misleidingstactieken

Autoriteit. Het lijkt erop dat online fraudeurs autoriteit gebruiken om slachtoffers te misleiden. Zo doen daders zich voor als professionals, zoals bankmedewerkers of overheidsfunctionarissen, om vertrouwen te wekken bij slachtoffers (Cross, 2022).

Schaarste. Een tactiek die fraudeurs ook gebruiken is het presenteren van een aanbod als uniek en tijdelijk, zodat slachtoffers zich onder druk gezet voelen om snel te beslissen zonder de gevolgen goed te overdenken of advies te vragen. (Cross, 2022).

Urgentie. Het lijkt erop dat fraudeurs een gevoel van tijdsdruk creëren om slachtoffers te misleiden door bijvoorbeeld aan te geven dat ze zo snel mogelijk geld nodig hebben voor een noodgeval (Cross, 2022).

Trends

Afwezigheid capabele bewaker. Uit de studie van Levi en Smith (2022) komt naar voren dat de afwezigheid van capabele bewakers, zoals politie en autoriteitsfiguren, tijdens de COVID-19-pandemie een belangrijke factor was die bijdroeg aan online fraude. Omdat de focus verschoof naar het handhaven van sociale afstandsregels en het monitoren van virus-hotspots, kreeg traditionele politiezorg, zoals de bestrijding van economische criminaliteit, minder aandacht (Levi & Smith. 2022).

COVID-19 pandemie. Door de COVID-19 pandemie waren mensen meer afhankelijk van digitale technologieën doordat mensen in lockdown thuis verbleven en afhankelijk waren van online platforms voor werk (Levi & Smith, 2022). Dit leidde tot een toename van online fraude (Levi & Smith, 2022). Daaropvolgend constateren Johnson en Nikolovska (2024) dat online fraude tijdens de pandemie leek te schommelen in lijn met mobiliteit en online activiteit, waarbij het toenam bij strengere beperkingen en afnam na versoepelingen.

Obstakels voor opsporing en vervolging. Uit de studie van Cross (2022) komt naar voren dat er een aantal belangrijke obstakels zijn voor effectieve opsporing en vervolging van online fraude. Ten eerste maakt het de fysieke nabijheid tussen dader en slachtoffer overbodig, wat de opsporing en rechtsvervolging bemoeilijkt (Cross, 2022). Ten tweede is online fraude vaak internationaal van aard, wat samenwerking tussen landen vereist, maar dit kan traag en bureaucratisch verlopen (Cross, 2022). Ten derde maakt online fraude gebruik van geavanceerde technieken zoals identiteitsvervalsing, waarvoor politieagenten vaak niet over de juiste expertise beschikken (Cross, 2022). Als laatste maakt het gebruik van gestolen of valse identiteiten het lastig om fraudeurs te identificeren (Cross, 2022).

Toekomstige studies

Effectiviteit van verlies-geframede waarschuwingen. Toekomstig onderzoek zou zich moeten richten op hoe mensen oplichting herkennen en welke factoren hun motivatie beïnvloeden (Jiang et al., 2024). Het onderzoek van Jiang en collega's (2024) toont aan dat waarschuwingen gericht op verlies effectiever zijn dan die over winst, omdat ze het risico op oplichting beter benadrukken (Jiang et al., 2024).

Externe validiteit. De fraudestimuli in de studie van Jiang en collega's (2024) bestonden alleen uit tekstuele materialen, zonder afbeeldingen of interactie, wat mogelijk niet overeenkomt met echte scams. Toekomstig onderzoek zou een realistischer scenario moeten creëren, met

afbeeldingen en interactieve elementen, zoals het klikken op URL's en reageren op scams, om de authenticiteit te verbeteren (Jiang et al., 2024).

Generaliseerbaarheid en diversiteit. Volgens Ojolo en Singh (2023) zou toekomstig onderzoek zich moeten richten op de aard, drijfveren, motivaties en denkwijzen achter online fraude in andere landen en regio's. Hierdoor kunnen overeenkomsten en verschillen in motivatie, doelwitten en denkpatronen beter worden begepen (Ojolo & Singh, 2023). Jiang et al. (2024) geeft aan dat de steekproef in hun onderzoek voornamelijk bestaat uit studenten en daarmee niet het volledige scala van internetgebruikers, zoals ouderen, vertegenwoordigt. Daarom stellen de auteurs dat toekomstig onderzoek verschillende leeftijdsgroepen moeten betrekken om de bevindingen te generaliseren (Jiang et al., 2024).

Kwetsbaarheid demografische groepen. In het onderzoek van Cross (2022) wordt er benadrukt dat het belangrijk is om de kwetsbaarheid voor online fraude binnen verschillende demografische groepen te erkennen en te begrijpen hoe daders deze zwaktes exploiteren om hun frauduleuze methoden aan te passen (Cross, 2022).

Longitudinaal onderzoek. Volgens Jiang en collega's (2024) zou toekomstig onderzoek zich moeten richten op de verschillende effecten van waarschuwingen vóór en na oplichting met behulp van een uniforme aanpak en consistente methoden.

Meervoudige perspectieven. Toekomstig onderzoek zou de perspectieven van verschillende delen van sociale netwerken, zoals daders, wetshandhavers en cybercriminelen, moeten combineren om online fraude vanuit diverse invalshoeken te begrijpen (Aborisade, 2023). Op die manier kan volgens de auteurs de sociale context achter de groei van online fraude beter worden doorgronden (Aborisade, 2023).

Modus operandi. Het aantal slachtoffers van fraude blijft wereldwijd toenemen, met steeds meer frauduleuze benaderingen die gericht zijn op individuen (Cross, 2022). Het is belangrijk om te begrijpen hoe online fraude plaatsvindt, inclusief de gebruikte methoden zoals sociale manipulatie en psychologische misbruiktechnieken (Cross, 2022).

Rol medeplichtigen. De resultaten van Cretu-Adatte en collega's (2024) bieden geen duidelijkheid over (1) hoe eenvoudig het is om medeplichtigen van online te vinden, (2) wat hun beweegredenen zijn, (3) welke factoren hun betrokkenheid beïnvloeden, (4) in hoeverre online fraudeurs afhankelijk zijn van deze medeplichtigen of (5) hoe gemakkelijk ze door fraudeurs te benaderen zijn. Het onderzoeken van deze zaken zou volgens de auteurs meer inzicht geven in de coordinatie van illegale activiteiten en de pogingen om anti-witwasmaatregelen te omzeilen (Cretu-Adatte et al., 2024).

Timing waarschuwingsberichten. Jiang en collega's (2024) stellen dat toekomstig onderzoek verder zou moeten verkennen hoe de timing van waarschuwingen het responsgedrag beïnvloedt, bijvoorbeeld via risicoperceptie. Dit kan helpen om beter inzicht te krijgen in het gedrag van criminelen en in effectieve preventiestrategieën tegen online fraude (Jiang & collega's, 2024).

Interventies/trainingen

Slachtoffergericht

Detectie en monitoren. Meerdere onderzoeken stellen dat de focus moet komen te liggen op het detecteren van fraudeleuze activiteiten (Cross, 2022; Leong & collega's, 2024; Levi & Smith, 2022). Effectievere preventie zou zich volgens Cross (2022) moeten focussen op het herkennen van verzoeken om geld of persoonlijke informatie, aangezien dit de gemeenschappelijke factor is in alle frauduleuze praktijken. Hierbij AI-algoritmen kunnen helpen bij het detecteren en

beoordelen van fraude (Levi & Smith, 2022). Verder stellen Levi en Smith (2022) voor om fraude-monitoringsprogramma's op te zetten die in staat zijn nieuwe gevallen van online fraude tijdens pandemieën snel te detecteren. Real-time monitoring is volgens de auteurs noodzakelijk om de omvang en impact van online fraude te minimaliseren (Levi & Smith, 2022). Daarnaast stelt Cross (2022) dat financiële instellingen meer investeren in het begrijpen van fraude en het identificeren van relevante waarschuwingssignalen, aangezien die verschillen per type online fraude (Cross, 2022).

Documenteren aard en omvang fraude. Levi en Smith (2022) benadrukken dat het belangrijk is om de aard en omvang van online fraude tijdens eerdere pandemieën te documenteren en te begrijpen, zodat we beter voorbereid zijn op toekomstige crises.

Evaluatie maatregelen. Meerdere onderzoeken benadrukken het belang van het herzien en aanpassen van maatregelen (Cross, 2022; Levi & Smith, 2022; Ojolo & Singh, 2023). Zo stelt Cross (2022) bijvoorbeeld dat het belangrijk is om preventieprogramma's te evalueren aan de hand van wetenschappelijke maatstaven om te beoordelen of ze succesvol en effectief zijn.

Ondersteuning slachtoffers. In het onderzoek van Cross (2022) wordt verwezen naar een studie waarin slachtoffers van online fraude werd gevraagd naar hun ondersteuningsbehoeften na een incident. Uit dit onderzoek kwamen de volgende punten naar voren: (1) respectvolle en schuldvrije behandeling door autoriteiten, (2) eenvoudige meldprocedures, (3) goed getraind personeel bij instanties, (4), begrip en steun van vrienden en familie, (5) inzicht in beschikbare ondersteuningsdiensten en hoe deze te benaderen zijn en tegen welke kosten, (6) professionele ondersteuning door experts in financieel misbruik, en (7) hulp bij zowel de gevolgen van online fraude als de achterliggende oorzaken, zoals relatieproblemen of verslaving (Cross, 2022).

Impact verkleinen bij slachtoffers. Het ontbreken van duidelijk leiderschap in netwerken met veel online activiteit maakt duidelijk dat deze cybercrimenetwerken anders functioneren dan offline criminele organisaties die doorgaans hiërarchisch van aard zijn (Nguyen & Luong, 2021). Cybercrime netwerken werken vaak in een platte structuur met veel leden die mogelijk nooit fysiek met elkaar in contact komen (Nguyen & Luong, 2021). Daarom zouden wethandhavingsinstanties zich moeten richten op preventieve strategieën om de impact van online fraude op slachtoffers te beperken, aangezien de aard van deze netwerken moeilijk te bestrijden zijn (Nguyen & Luong, 2021).

Fraudebestrijdingsplan toekomstige crisis. In het onderzoek van Levi en Smith (2022) wordt er aangegeven dat het opnemen van fraudebestrijding in toekomstige pandemieplanningen en beleidsmaatregelen cruciaal is om ervoor te zorgen dat overheden, bedrijven en gemeenschappen voorbereid zijn op toekomstige crises (Levi & Smith, 2022).

Dadergericht

Armoedebestrijding. Het aanpakken van de armoede lijkt effectief te zijn om online fraude in ontwikkelingslanden te bestrijden (Aborisade, 2023; Kigerl, 2021). Het IMF en de Wereldbank zouden overheidsleningen kunnen verstrekken om e-commercebedrijven op te richten, wat op zijn beurt voor werkgelegenheid zou kunnen zorgen (Kigerl, 2021).

Gezins- en sociale omgeving. In het onderzoek van Aborisade (2023) wordt er benadrukt dat de gezins- en sociale omgeving van daders in Nigeria aandacht moet krijgen als onderdeel van correctionele therapie.

Strikte en onvermijdelijke straffen. Volgens Aborisade (2023) zou handhaving van wetten en beleid moeten worden versterkt en prioriteit moeten krijgen om ervoor te zorgen dat online fraudeurs met strikte en onvermijdelijke straffen worden geconfronteerd.

Aanpakken van neutralisaties en rationalisaties. In het onderzoek van Levi en Smith (2022) wordt er benadrukt hoe overheden en bedrijven online fraude effectiever kunnen bestrijden door neutralisatietechnieken en rationalisaties aan te pakken (Levi & Smith, 2022). Ten eerste door het aanbieden van duidelijke informatie over regels en verplichtingen, zodat individuen begrijpen wat rechtmatig gedrag inhoudt (Levi & Smith, 2022). Hierbij is het belangrijk dat conflicterende regels tussen rechtsgebieden worden vermeden (Levi & Smith, 2022). Maar ook door het maatschappelijke belang van naleving van regels te onderstrepen en een gevoel van morele verantwoordelijkheid te creëren (Levi & Smith, 2022). Public shaming zou op een re-integratieve wijze herhaling van online fraude kunnen minimaliseren (Levi & Smith, 2022). Als laatste zouden individuen moeten worden ondersteund bij het begrijpen en naleven van regels, zodat rationalisaties als onwetendheid of verwarring worden weggenomen (Levi & Smith, 2022).

Tabel 10. Samenvatting resultaten van de literatuur over online fraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	Gedeelde banden en gemeenschappelijke affiliaties	Internetgebruik	Neutralisatie bij ouders van fraudeurs	Anticiperen	Afwezigheid capabele bewaker	Effectiviteit van verliesgeframede waarschuwingen	Detectie en monitoren
			Groepsinteractie	Welvaart	Financieel gewin	Netwerk (actoren)	COVID-19 pandemie	Externe validiteit	Documenteren aard en omvang fraude
			Mentorschap		Hebzucht	Netwerk (structuur)		Generaliseerbaarheid en diversiteit	Evaluatie maatregelen
			Ouders			Samenwerking corrupte overheidsfunctionarissen	Obstakels voor opsporing en vervolging	Kwetsbaarheid demografische groepen	Ondersteuning slachtoffers
						Smurfen		Longitudinaal onderzoek	Impact verkleinen bij slachtoffers
						Technologie		Modus operandi	Fraudebestrijdingsplan toekomstige crisis
						Verliesaversie		Rol medeplichtigen	Armoedebestrijding

						Autoriteit	Timing waar-schuwings-berichten	Gezins- en so-ciale omgeving
						Schaarste		Strikte en on-vermijdelijke straffen
						Urgentie		Aanpakken van neutralisaties en rationalisa-ties
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*	***Grijs** = neutrale factor*	

3.1.5. Phishing

Introductie

Wetenschappelijke literatuur

Phishing is een wijdverbreide vorm van *social engineering* die gebruikersreferenties verzamelt door doelwitten ertoe te verleiden persoonlijke of financiële informatie vrij te geven, zoals creditcardgegevens, op een frauduleuze website (Bijmans et al., 2021, p. 3757). In totaal zijn er vijf studies geïdentificeerd die betrekking hebben op phishing. Dit betreffen de onderzoeken van Bijmans en collega's (2021), Chawki (2021), Hoheisel en collega's (2023), Khweiled en collega's (2021) en Kikerpill en Siibak (2021).

Bijmans en collega's (2021) hebben aan de hand van een longitudinaal onderzoek - uitgevoerd tussen september 2020 en januari 2021 - onderzocht hoe en in welke mate phishing kits worden ingezet bij phishing-aanvallen in Nederland en daarbij de *end-to-end* levenscyclus van Nederlandse phishing-aanvallen in kaart gebracht. Deze studie is van hoge kwaliteit.

Chawki (2021) heeft op zijn beurt middels een niet-systematische review onderzocht welke technieken er door cybercriminelen in de Europese Unie en VS werden gebruikt tijdens de COVID-19 pandemie en daarbij efficiënte methodes belicht om cyberaanvallen aan te pakken. De kwaliteit van deze studie is als laag beoordeeld.

Hoheisel en collega's (2023) onderzochten kenmerken en patronen van toegepaste phishing-technieken in Nederland tijdens de COVID-19-pandemie. De studie is met een hoge kwaliteitsscore beoordeeld.

Khweiled en collega's (2021) hebben middels een trend- en patroonanalyse onderzocht in welke mate tijdens de COVID-19 pandemie verschillende vormen van cyberaanvallen wereldwijd in de eerste helft van 2020 zijn toegenomen ten opzichte van dezelfde periode in 2019. Hierbij onderzochten de auteurs ook in hoeverre het gebrek aan bewustzijn bij gebruikers heeft bijgedragen aan de toename van deze aanvallen (Khweiled et al., 2021). De kwaliteit van deze studie is als laag beoordeeld.

Tenslotte hebben Kikerpill en Siibak (2021) nieuws-artikelen over online oplichtingen geanalyseerd om inzicht te krijgen in de technieken en strategieën die cybercriminelen gebruikten in hun social engineering-aanvallen tijdens de COVID-19-pandemie. Dit onderzoek kent een hoog kwaliteitsscore. Zie Tabel 11 voor een overzicht van de relevante studies, en zie Tabel 12 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met phishing.

Tabel 11.
De referenties en kwaliteitsboordeling van de relevante studies voor phishing.

Referentie	Kwaliteit
(Bijmans et al., 2021)	Hoog
(Chawki, 2021)	Laag
(Hoheisel et al., 2023)	Hoog
(Khweiled et al., 2021)	Laag
(Kikerpill & Siibak, 2021)	Hoog

Modus operandi

Algemene termen in e-mails**.** Uit het onderzoek van Bijmans en collega's (2021) komt naar voren dat tijdens COVID-19 phishing-criminelen bij het maken van frauduleuze links of domeinnamen vaak gebruikmaakten van algemene termen in plaats van te verwijzen naar specifieke namen van organisaties om slachtoffers ertoe te verleiden om op een phishing-link te klikken.

Autoriteit. Het gebruik van autoriteit lijkt een veelgebruikte techniek te zijn die cybercriminelen toepassen bij phishing-aanvallen. Meerdere onderzoeken constateren dat bijvoorbeeld tijdens de COVID-19 pandemie oplichters in hun phishing-aanvallen vaak gebruik maakten van legitieme bronnen, zoals gezondheids– en overheidsinstellingen, om slachtoffers te misleiden (Chawki, 2021; Khweiled et al., 2021; Kikerpill & Siibak, 2021).

Behulpzaamheid. Het lijkt erop dat cybercriminelen gebruik maken van behulpzaamheid om slachtoffers te misleiden (Hoheisel et al., 2023; Kikerpill & Siibak, 2021). In het onderzoek van Kikerpill en Siibak (2021) blijkt dat tijdens COVID-19 hoofdzakelijk de zogenoemde communicatiestrategie 'Barmhartige Samaritaan' werd toegepast door phishing-criminelen (Kikerpill & Siibak, 2021). Bij deze strategie doen cybercriminelen zich voor als behulpzame of goedbedoelende personen of organisaties die een slachtoffer willen helpen bij het vervullen van zijn of haar onmiddellijke behoeftes (Kikerpill & Siibak, 2021), zoals het aanvragen van financiële hulp of toegang tot goederen die beschermen tegen het virus (Hoheisel et al., 2023).

Bestaande technieken. Uit het onderzoek van Hoheisel en collega's (2023) komt naar voren dat tijdens de COVID-19 pandemie phishing e-mails vaak aanpassingen bevatten van bestaande technieken, zoals het gebruik van tekst die niet zichtbaar is voor de lezer en activiteiten van criminelen op specifieke dagen, in plaats van het gebruik van nieuwe technieken. Het aanpassen van bestaande strategieën vereist minder middelen dan het ontwikkelen van nieuwe methodes (Hoheisel et al., 2023). Dit sluit aan bij de *rationele keuzetheorie* (d.w.z. aanpassingen zijn minder risicovol en kosten effectief) en de *adaptie-innovatie theorie* (d.w.z. aanpassingen vereisen minder investeringen dan innovaties) (Hoheisel et al., 2023).

Decoy-pagina's. Onderzoek laat zien dat aanvallers steeds vaker gebruik maken van misleidende pagina's (Engels: *decoy pages*) die lijken op die van een echte organisatie om slachtoffers over te halen hun gegevens te delen (Bijmans et al., 2021). Ze vragen niet direct om inloggegevens, maar leiden uiteindelijk tot het delen ervan (Bijmans et al., 2021).

Dreiging**.** Een andere veelvoorkomende communicatiestrategie die tijdens COVID-19 door cybercriminelen werd toegepast is de zogenoemde 'Shock en Awe'-strategie (Kikerpill & Siibak, 2021). Deze strategie verwijst naar het oproepen van een gevoel van verlies bij een potentieel slachtoffer via misleidende communicatie, bijvoorbeeld door te dreigen de nutsvoorzieningen van de woning af te sluiten (Kikerpill & Siibak, 2021).

Levensduur phishing-aanval. In het onderzoek van Bijmans en collega's (2021) reconstrueerden de auteurs de volledige levenscyclus van veelvoorkomende phishing-aanvallen. Uit hun hun bevindingen kwam naar voren dat dat de meeste phishing domeinnamen slechts 24 uur online zijn (Bijmans et al., 2021). Dit suggereert volgens de auteurs dat phishing-criminelen snel handelen (Bijmans et al., 2021).

Phishingkits. Het lijkt erop dat criminelen veelvoudig gebruik van phishingkits om hun aanvallen te faciliteren (Bijmans et al., 2021). Een phishingkit is een kant-en-klare set tools met alle benodigdheden die het mogelijk maakt om eenvoudig een phishing-aanval te kunnen uitvoeren, zonder dat er specialistische ICT kennis nodig is (Bijmans et al., 2021). Deze phishingkits kunnen via verschillende bronnen worden verkregen, zoals darknetmarkten en online forums, maar zijn

ook verkrijgbaar op openbare chatapplicaties zoals Telegram (Bijmans et al., 2021). Zo werd er tijdens COVID-19 een phishingsoftware aangeboden op een online platform – een malware vermomd als een real-time kaart met WHO-informatie over de uitbraak – die tussen de 200 en 500 dollar kostte (Chawki, 2021). Bijmans en collega's (2021) ontdekten in hun onderzoek dat 1.363 Nederlandse phishing domeinnamen (gemiddeld 31 phishing domeinnamen online per dag) gebruik maakten van zulke phishingkits. Een ander opvallend gegeven is dat Nederlandse phishing-aanvallen voornamelijk gebruik maakten van hetzelfde softwareplatform waar phishingkits worden aangeschaft, namelijk uAdmin Framework (Bijmans et al., 2021). Dit platform wordt wereldwijd gebruikt en het stelt criminelen in staat om snel en efficiënt phishing-pagina's te bouwen die lijken op legitieme websites, zoals die van banken of online diensten (Bijmans et al., 2021). Dit met het doel om slachtoffers hun persoonlijke gegevens, zoals inloggegevens en creditcardinformatie, te laten invoeren (Bijmans et al., 2021).

Sociale context**.** De studie van Kikerpill en Siibak (2021) laat zien dat criminelen actuele gebeurtenissen en geloofwaardige sociale contexten, zoals de COVID-19 pandemie, gebruiken om phishing e-mails geloofwaardig te laten overkomen. Volgens de onderzoekers spelen drie hoofdelementen hierbij een rol, namelijk 'timing', 'plaats' en 'techniek' (Kikerpill & Siibak, 2021). Het element ‘timing’ kwam in phishing e-mails naar voren door in te spelen op de pandemie (Kikerpill & Siibak, 2021). Belangrijke thema's die in de oplichtingsberichten werden gebruikt, waren onder meer persoonlijke beschermingsmiddelen, geneesmiddelen en donaties (Kikerpill & Siibak, 2021). Wel constateren Hoheisel en collega's (2023) dat in eerste periode van de pandemie er weinig phishing-aanvallen waren die direct verwezen naar specifieke COVID-19-thema’s. Het element ‘plaats’ werd kwam tot uiting doordat cybercrimelen verschillende mediums [zoals e-mails, malafide websites en sociale media] gebruikten voor verschillende phishing e-mails (Kikerpill & Siibak, 2021). Zo werden bepaalde scams, zoals aanbiedingen voor valse vaccinaties, specifiek via nepwebsites verspreid (Kikerpill & Siibak, 2021). Ieder medium kent namelijk specifieke voordelen, bijvoorbeeld de mogelijkheid om sociale bewijskracht toe te voegen via nep-reviews op websites en sociale media (Kikerpill & Siibak, 2021). Het element ‘techniek’ werd volgens de auteurs ondersteund door het gebruik van overtuigingsprincipes in de phishing-e-mails (Kikerpill & Siibak, 2021).

Trends

Disproportionele aandeel**.** Het lijkt erop dat een zeer klein aantal criminelen verantwoordelijk is voor een groot aandeel phishing-aanvallen (Hoheisel et al., 2023).

Frequentie. Phishing is een van de meest voorkomende vormen van online criminaliteit (Khweiled et al., 2021). In de eerste helft van 2020 werden er wereldwijd 267.372 phishing-aanvallen gemeld, wat een stijging van 19,06% betreft ten opzichte van het jaar ervoor (Khweiled et al., 2021). Specifiek gericht op Nederland was er een grote toename van COVID-19-gerelateerde phishing-e-mails nadat de eerste beperkende maatregelen in Nederland waren ingevoerd (Hoheisel et al., 2023). Eerder onderzoek laat volgens Hoheisel en collega's (2023) ook zien dat criminaliteit met name plaatsvindt aan het begin van rampen.

Toekomstig onderzoek

Motivatie oplichter. Er zou meer onderzoek moeten worden gedaan naar de intenties van oplichters (Kikerpill & Siibak, 2021). Zo is er nog niet veel bekend over motivaties en gehanteerde strategieën van phishing-criminelen (Kikerpill & Siibak, 2021).

Sociale contexten. Volgens Kikerpill en Siibak (2021) zou toekomstig onderzoek zich moeten richten op andere sociale contexten dan de COVID-19 pandemie, zoals verkiezingen of natuurrampen, die een vergelijkbare context kunnen bieden voor phishing-aanvallen. Dit zou kunnen helpen bij het identificeren van risico's tijdens specifieke periodes of gebeurtenissen (Kikerpill & Siibak, 2021). Daarnaast zou toekomstig onderzoek zich moeten richten op hoe het gebruik van bepaalde sociale contexten, zoals de COVID-19 pandemie, de effectiviteit van phishing-aanvallen beïnvloedt (Kikerpill & Siibak, 2021).

Sociale manipulatie. Volgens Kikerpill & Siibak (2021) is weinig nog bekend of online criminelen bewust principes van sociale manipulatie in hun berichten verwerken of maar gewoon bestaande formats nabootsen (Kikerpill & Siibak, 2021).

Vergelijkend onderzoek**.** Het onderzoek van Hoheisel en collega's (2023) richtte zich op ontwikkeling van phishing-aanvallen tijdens de COVID-19 pandemie. In hun studie wordt er aangegeven dat toekomstig onderzoek zich zou kunnen richten op een grootschaliger longitudinaal onderzoek, zoals de periode van vóór en ná de COVID-19 pandemie, om zo veranderingen van phishing-tactieken bij sociale contexten beter bloot te kunnen leggen (Hoheisel et al., 2023). Daarnaast stellen de auteurs stellen dat het analyseren van phishing e-mails in meerdere talen, gericht op Nederlandse domeinnamen, waardevolle inzichten kunnen opleveren qua verschillen gebruikte ontwerpen en strategieën (Hoheisel et al., 2023).

Interventies/trainingen

Slachtoffer gericht

Adequaat handelen. Zoals uit resultaten naar voren kwam, zijn de meeste phishing domeinnamen slechts 24 uur online, wat suggereert dat criminelen snel handelen (Bijmans et al., 2021). Dit benadrukt volgens Bijmans en collega's (2021) de noodzaak tot snelle en doortastende reacties om dergelijke phishing-campagnes effectief te stoppen.

Bewustwording. Volgens Hoheisel en collega's (2023) zouden beleidsmakers meer de focus moeten leggen op bewustmakingscampagnes. Als het duidelijk is welke phishingkits het meest worden gebruikt, dan kan er beter worden bepaald welke informatie in bewustwordingscampagnes aan het publiek moet worden uitgelegd (Hoheisel et al., 2023).

Detectiemethoden. Wanneer phishing-campagnes aan wetshandhavingsinstanties worden gemeld, zijn de phishing domeinen vaak al verwijderd, waardoor het bijna onmogelijk wordt om de daders van de phishing-aanvallen te achterhalen (Bijmans et al., 2021). Daar komt bij dat WhatsApp en sms-berichten de interactie met slachtoffers versneld (Bijmans et al., 2021). Om die reden is er volgens Bijmans en collega's (2021) behoefte aan snellere detectiemethodes (Bijmans et al., 2021).

Monitoren. Het identificeren van de kenmerken van phishingkits maakt het mogelijk om het phishing-landschap continu te monitoren en nieuwe gerelateerde phishing-aanvallen te identificeren (Bijmans et al., 2021). Monitoring stelt organisaties in staat om hun anti-phishing maatregelen te verbeteren (Bijmans et al., 2021).

Phishingkits repository. Bijmans en collega's (2021) stellen voor om een soort van repository voor phishingkits in het leven te roepen, waarin kenmerken van phishingkits worden opgeslagen, zoals een overzicht van gebruikte misleidingstactieken en bestaande detectiemethodes. Als er bijvoorbeeld een overzicht is van bepaalde kwetsbaarheden in phishingkits, dan kunnen daarop gerichte interventies worden ontwikkeld (Bijmans et al., 2021). Binnen de cybersecuritygemeenschap kunnen verschillende partijen, zoals hostingproviders en onderzoekers, de

repository aanvullen met informatie over welke phishing-tactieken door criminelen veelal worden gebruikt (Bijmans et al., 2021). De auteurs geven wel aan dat het van belang is dat een standaardisatie ia voor hoe de informatie in de repository moet worden ingevoerd om uitwissing succesvol te maken (Bijmans et al., 2021)

Wetshandhaving. In Nederland wordt er door criminelen veel gebruik gemaakt van phishingkits die vaak gemeenschappelijke kenmerken vertonen (Bijmans et al., 2021). Door een duidelijk beeld te hebben van de populairste phishingkits die door cybercriminelen worden gebruikt, kunnen handhavingsinstanties zich richten op de phishingkits die de meeste impact hebben (Hoheisel et al., 2023). Als bijvoorbeeld kwetsbaarheden in phishingkits in kaart zijn gebracht, dan zouden phishing-aanvallen effectief kunnen worden verzwakt of onschadelijk worden gemaakt (Bijmans et al., 2021).

Tabel 12 . Samenvatting resultaten van de literatuur over phishing.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	Algemene termen in e-mails	Disproportioneel aandeel	Motivatie oplichter	Adequaat handelen
						Autoriteit	Frequentie	Sociale contexten	Bewustwording
						Behulpzaamheid		Sociale manipulatie	Detectiemethoden
						Decoy-pagina's		Vergelijkend onderzoek	Monitoren
						Dreiging			Phishingkits repository
						Levensduur phishing-aanval			Wetshandhaving
						Phishingkits			
						Sociale context			

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.6. Vishing

Introductie

Wetenschappelijke literatuur

Vishing, ofwel 'voice phishing', is een vorm van digitaliseerde fraude waarbij slachtoffers via telefoongesprekken, vaak uitgevoerd met behulp van Voice over Internet Protocol (VoIP), worden misleid om persoonlijke informatie of geld af te staan (Van Nguyen, 2022). In totaal zijn er drie studies geïdentificeerd die specifiek betrekking hebben op *vishing*. Dit betreffen de studies van Chawki (2021), Nguyen en Luong (2021) en Van Nguyen (2022).

Chawki (2021) heeft middels een niet-systematische review onderzocht welke technieken er door cybercriminelen in de Europese Unie en VS werden gebruikt tijdens de COVID-19 pandemie en daarbij efficiënte methodes belicht om cyberaanvallen aan te pakken. De kwaliteit van deze studie is als laag beoordeeld.

Het onderzoek van Nguyen en Luong (2021) heeft op basis van een sociale netwerkanalyse – gecombineerd met data van criminele profielen en interviews met de politie – de structuur van online fraudenetwerken (d.w.z. bankpasfraude en vishing) in Vietnam onderzocht. Het onderzoek is met een gemiddelde kwaliteitsscore beoordeeld.

De studie van Van Nguyen (2022) onderzocht bankpasfraude en vishing in Vietnam om meer inzicht te krijgen in hoe deze vormen van online fraude in de Vietnamese context plaatsvinden. Dit werd geanalyseerd aan de hand van crime script analysis, gebaseerd op 20 casestudies en interviews met 14 cyberpolitieagenten, waarbij drie fasen werden geïdentificeerd: voorbereiding, activiteit en na-activiteit (Van Nguyen, 2022). De studie is met een gemiddelde kwaliteitsscore beoordeeld. Zie Tabel 13 voor een overzicht met relevante studies, en zie Tabel 14 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met vishing.

Tabel 13.
De referenties en kwaliteitsboordelingen van de relevante studies voor vishing.

Referentie	Kwaliteit
(Chawki, 2021)	Laag
(Nguyen & Luong, 2021)	Gemiddeld
(Van Nguyen, 2022)	Gemiddeld

Motieven

Financieel gewin. Uit het onderzoek van Nguyen en Luong (2021) komt naar voren dat criminelen die onderdeel uitmaken van een netwerk uitsluitend zijn gericht op financieel gewin en niet worden gestuurd door ideologische, politieke of ethische overtuigingen.

Modus operandi

Interactie. In het onderzoek van Van Nguyen (2022) wordt er gesteld dat er bij vishing veel interactie met het slachtoffer nodig is om deze ervan te overtuigen geld over te maken naar de criminele bankrekening.

Netwerk. Het lijkt erop dat telefonische oplichtingnetwerken een hiërarchisch structuur kennen en bestaan uit vier actoren: *leiders* die aan het hoofd staan van een netwerk, *oplichters* die slachtoffers bellen, *geldezels* die financiële sporen verbergen en *recruiters* die geldezels

werven (Nguyen & Luong, 2021; Van Nguyen, 2022). Deze netwerken bestaan uit twee hoofdgroepen die beide verschillende structuren kennen: de bellers en de geldmollen (Nguyen & Luong, 2021). Bellers opereren in gecentraliseerde subgroepen, die zich op een afgelegen bevinden en wordt geleid door een baas worden die contact onderhoudt met andere subgroepen (Nguyen & Luong, 2021). De structuur van geldezel groepen verschilt met die van belgroepen. Geldezels verzamelen zich rond recruiters en kennen alleen hun identiteit, terwijl belgroepen een baas hebben die een centrale rol speelt. De combinatie van belgroepen en geldezel groepen creëert een vishing netwerk met een hybride structuur (Nguyen & Luong, 2021).

Rekrutering. Zoals eerder genoemd, bestaat een telefonische oplichtingnetwerken uit vier actoren: *leiders*, *bellers*, *geldezels* en *recruiters* (Nguyen & Luong, 2021; Van Nguyen, 2022). De eerste kennismaking tussen leiders en recruiters gebeurt online (Nguyen & Luong, 2021). Frauduleuze bellers worden meestal in hun eigen land via apps zoals WeChat geworven en ontvangen een salaris voor hun diensten (Van Nguyen, 2022). Geldezels worden vaak gerekruteerd via offline sociale banden met recruiters of online platforms (Van Nguyen, 2022). Ze worden ingeschakeld om de (financiële) sporen te verbergen en daarmee de kans op arrestatie te verkleinen (Van Nguyen, 2022). Geldezels gebruiken hun eigen of vervalste identiteitsbewijzen om bankrekeningen te openen en geld te beheren (Van Nguyen, 2022). Ze worden betaald per frauduleuze zaak en ontvangen een percentage van de fraudeopbrengsten (Van Nguyen, 2022).

Tussenrekeningen. Het onderzoek van Van Nguyen (2022) toont aan dat in Vietnam het gestolen geld bij telefoonfraude door geldezels of recruiters werd opgehaald en via verschillende tussenrekeningen naar de bendeleiders werd doorgestuurd. In sommige gevallen werd het geld op diverse manieren verwerkt voordat het de fraudeurs bereikte (Van Nguyen, 2022). Een manier die in de studie werd genoemd, was dat geldezels het geld uit banken haalden en dit vervolgens via recruiters naar Chinese bendeleden stuurden (Van Nguyen, 2022). Een andere methode was dat het geld werd opgehaald bij een geldautomaat en daarna via tussenrekeningen naar de Chinese fraudeurs werd gestuurd (Van Nguyen, 2022).

VoIP-technologie. Het lijkt erop dat criminelen van vishing gebruik maakt van VoIP-technologie waarmee ze slachtoffers kunnen bellen vanuit het buitenland met vervalste nummers (Nguyen & Luong, 2021; Van Nguyen, 2022). Het verkrijgen van tools en telefoonnummers lijkt relatief eenvoudig, omdat abonnementen gemakkelijk kunnen worden aangeschaft bij legale VoIP-serviceproviders (Van Nguyen, 2022). In gevallen met buitenlandse slachtoffers kwamen bellers naar Vietnam om de VoIP-systemen in te stellen, terwijl Vietnamese bellers buiten Vietnam opereerden onder leiding van Chinese of Taiwanese leiders (Van Nguyen, 2022). Ze werkten vaak in kleine teams vanuit afgelegen huizen of appartementen die beveiligd waren met camera's en fysieke barrières (Van Nguyen, 2022).

Misleidingstechnieken

Autoriteit. Het lijkt erop dat fraudeurs een lijst met telefoonnummers gebruiken om willekeurige mensen op te bellen, waarin ze een script volgen, en zich voordoen als wetshandhavers (zoals politie of aanklagers) om mensen te overtuigen om geld over te maken naar rekeningen van geldezels (Van Nguyen, 2022).

Onder druk zetten. In de studie van Van Nguyen (2022) gebruikten fraudeurs internetbellen (VoIP) om slachtoffers onder druk te zetten en hen te dwingen geld over te maken.

Trends

Reverse phishing. Reverse phishing is een nieuwe vorm van oplichting waarbij aanvallers via e-mails of sociale mediaberichten slachtoffers lokken om hen onbewust te bellen (Chawki, 2021). Deze e-mails doen vaak alsof betalingen niet zijn ontvangen en vragen slachtoffers om contact op te nemen met de klantenservice van de bank via een meegeleverd VoIP-nummes (Chawki, 2021). De oplichters doen zich voor als medewerkers van financiële instellingen en zetten slachtoffers onder druk met dreigementen over grote verliezen als ze niet meewerken (Chawki, 2021).

Toekomstig onderzoek

Misdaadscripts. Het onderzoek van Van Nguyen (2022) geeft aan dat er weinig informatie is over bepaalde aspecten van de misdaadscripts van transnationale computerfraude, zoals het werven van frauduleuze bellers, het verkrijgen van telefoonnummers van slachtoffers en het in rekening brengen van kosten. Volgens de auteur zou toekomstig onderzoek kunnen bijdragen aan het verduidelijken van deze misdaadscripts, bijvoorbeeld door cyberfraudeurs te interviewen (Van Nguyen (2022).

Trainingen/interventies

Slachtoffergericht

Bewustwording. Volgens Van Nguyen (2022) moeten strategieën zich richten vergroten van het bewustzijn bij mensen, omdat iedereen in potentie slachtoffer kan worden.

Samenwerking. Van Nguyen (2022) stelt dat het grensoverschrijdende karakter van online criminaliteit internationale samenwerking vereist tussen opsporingsdiensten om bankpasfraude effectief aan te kunnen pakken (Van Nguyen, 2022).

Tabel 14. Samenvatting resultaten van de literatuur over vishing.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	Financieel gewin	Interactie Netwerk Rekrutering VoIP-technologie Autoriteit Onder druk zetten	Reverse phishing	Misdaad-scripts	Bewustwording Misdaadscripts Samenwerking
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.7. Datingfraude

Introductie

Wetenschappelijke literatuur

Datingfraude, ook wel bekend als online romantische fraude,is een vorm van online fraude waarbij oplichters op digitale platforms romantische interesses wekken met als doel hun slachtoffers (grote sommen) geld afhandig te maken (Abubakari, 2024, p. 710). In totaal hebben zijn er tien studies geïdentificeerd die betrekking hebben op datingfraude. Dit betreffen de onderzoeken van Abubakari, (2024), Abubakari en Amponsah (2024), Alam (2021), Cross (2022), Dickinson en collega's (2023), Dickinson en Wang (2024), Eseadi en collega's (2021), Offei en collega's (2022), Wang en collega's (2021) en Wang en Dickinson (2024).

Abubakari (2024) heeft aan de hand interviews onderzoek gedaan naar de invloed van sociaal-culturele ervaringen en technologische factoren op de betrokkenheid van vrouwen bij datingfraude in de regio Tamale, Ghana. De kwaliteit van deze studie is als hoog beoordeeld.

De studie van Abubakari en Amponsah (2024) onderzocht op basis van een documentenanalyse misleidingsstrategieën en rollen die Ghanese diasporagroepen in de VS innemen bij verschillende vormen van online criminaliteit. Dit onderzoek kent een lage kwaliteitsscore.

Alam (2021) heeft middels een experiment onderzocht - waarbij manipulatietechnieken van daders inzichtelijk zijn gemaakt - hoe theoretische modellen kunnen worden geïntegreerd om de ontwikkeling van kwetsbaarheid voor datingfraude te begrijpen. Deze studie is beoordeeld met een gemiddelde kwaliteitsscore.

Cross (2022) heeft via een niet-systematische review geschetst wat er momenteel bekend is van online fraude, waaronderdatingfraude , omtrent de gehanteerde modus operandi van daders en effectieve interventies om fraude te bestrijden. De studie is met een laag kwaliteitsscore beoordeeld.

Dickinson en collega's (2023) hebben middels een experiment onderzocht in welke mate daders van datingfraude hun misleidingsstrategieën aanpassen als reactie op het gedrag van hun slachtoffers. De kwaliteit van deze studie is als gemiddeld beoordeeld.

Dickinson en Wang (2024) hebben aan de hand van experimenteel onderzoek onderzocht of en hoe datingfraudeurs neutralisaties aan hun slachtoffers voorstellen om zo hun misdaden te vergemakkelijken. Dit onderzoek kent een hoog kwaliteitsscore.

Eseadi en collega's (2021) hebben in hun niet-systematische review over datingfraudeonder andere gehanteerde misleidingstechnieken van daders in kaart gebracht en aanbevelingen geschetst voor toekomstig onderzoek en preventiebeleid. De studie is met een lage kwaliteitsscore beoordeeld.

Offei en collega's (2022) hebben aan de hand van een vragenlijst onderzocht hoe technieken, zoals neutralisatie en het ontkennen van risico’s, invloed hebben op de intentie van daders om datingfraudete plegen. Het onderzoek is met een hoge kwaliteitsscore beoordeeld.

Wang en collega's (2021) hebben in hun experimenteel onderzoek onderzocht in hoeverre de inhoud van berichten die rechtstreeks naar actieve datingfraudeurs worden gestuurd hun gedragspatronen beïnvloeden. Dit onderzoek kent een hoge kwaliteitsscore.

Tenslotte hebben Wang en Dickinson (2024) in hun experimentele onderzoek onderzocht hoe bij datingfraude variaties in de potentiële beloning, die een (fictief) slachtoffer aanbiedt aan een dader, de misleidingsstrategieën van fraudeurs beïnvloeden. De studie is met een hoge

kwaliteitsscore beoordeeld. Zie Tabel 15 voor een overzicht van de relevante studies, en zie Tabel 16 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met datingfraude.

Tabel 15.
De referenties en kwaliteitsboordeling van de relevante studies voordatingfraude.

Referentie	Kwaliteit
(Abubakari, 2024)	Hoog
(Abubakari & Amponsah, 2024)	Laag
(Alam, 2021)	Gemiddeld
(Cross, 2022)	Laag
(Dickinson et al., 2023)	Gemiddeld
(Dickinson & Wang, 2024)	Hoog
(Eseadi et al., 2021)	Laag
(Offei et al., 2022)	Hoog
(Wang et al., 2021)	Hoog
(Wang & Dickinson, 2024)	Hoog

Routineactiviteiten

Anonimiteit. Het lijkt erop dat het anonieme karakter van datingfraude van invloed is waarom mensen deze vorm van online fraude plegen (Abubakari, 2024). Het wordt door daders als minder riskant ervaren dan traditionele criminaliteit, omdat door het anonieme karakter van het internet ze vaak buiten het directe bereik van wetshandhavingsinstanties opereren (Abubakari, 2024). Daar komt bij dat voor veel vrouwen de anonimiteit van het internet een extra voordeel (Abubakari, 2024). Ze kunnen deze activiteiten namelijk uitvoeren zonder hun persoonlijke of sociale identiteit prijs te hoeven geven (Abubakari, 2024). Dit is een belangrijk voordeel in samenlevingen waar vrouwen een maatschappelijke druk voelen om zich te conformeren aan de rol van 'deugdzame vrouw' en waarbij crimineel gedrag voornamelijk toch wordt geassocieerd met mannengedrag (Abubakari, 2024).

Betaalbaarheid. Het lijkt erop dat betaalbaarheid een belangrijke rol speelt waarom individuen datingfraude plegen (Abubakari, 2024). Vrouwelijke oplichters hebben in Tamale vaak te kampen met financiële beperkingen (vrouwen krijgen bijvoorbeeld weinig financiële steun vanuit de familie) die hen ervan weerhouden om op een legale wijze geld te verdienen, zoals het opstarten van een onderneming (Abubakari, 2024). Datingfraude vereist minimale financiële uitgaven, slechts het hebben van een smartphone en internetbundel is voldoende, die de meeste fraudeur toch al bezitten (Abubakari, 2024). Dit maakt deze vorm van online fraude daarom erg aantrekkelijk voor vrouwelijke oplichters (Abubakari, 2024).

Sociale relaties

Diaspora. Onderzoek van Abubakari en Amponsah (2024) benadrukt de belangrijke rol die Ghanese burgers in de VS hebben bij het faciliteren van datingfraude voor daders in Ghana en andere Afrikaanse landen. Daders in Ghana werken vaak samen met diaspora-leden in de VS om oplichting met zo min mogelijk belemmeringen uit te kunnen voeren (Abubakari & Amponsah, 2024).

Sociale banden. Het onderzoek van Abubakari (2024) benadrukt dat sociale banden - zoals vriendschapsnetwerken, romantische relaties en familiebanden - de kans op het plegen van de datingfraude vergroten. Sociale relaties fungeren in zekere zin als toegangspoorten tot de wereld

van deze vorm van online fraude (Abubakari, 2024). Ze bieden vrouwelijke fraudeurs essentiële bronnen, waaronder informatie, vaardigheden en technologische middelen, die cruciaal zijn om de oplichting succesvol te kunnen uitvoeren (Abubakari, 2024).

Macrofactoren

Economische marginalisatie. De resultaten uit de studie van Abubakari (2024) laten zien dat de toenemende betrokkenheid van vrouwen bij datingfraude kan worden toegeschreven aan economische marginalisering (Abubakari, 2024). Genderdiscriminatie belemmeren vrouwen in het verwerven van een legitieme sociaaleconomische positie (Abubakari, 2024). Deze patricische dynamieken drijft vrouwen tot het plegen van datingfraude als een coping mechanisme (Abubakari, 2024). Het is de economische spanning die vrouwen drijft richting het plegen van datingfraude om in hun financiële behoeften te voorzien (Abubakari, 2024).

Patriarchale normen. Om het plegen van online romantische te kunnen verklaren, kan volgens Abubakari (2024) ook gekeken worden naar veranderende culturele verwachtingen rondom het huwelijk. Waar traditionele patriarchale normen eerst minder nadruk legden op vrouwelijke financiële bijdragen, wordt het respect van een vrouw binnen een huwelijk nu steeds vaker gekoppeld aan de financiële bijdrage die zij levert (Abubakari, 2024). Dit is namelijk van wezenlijk belang voor de sociale status en huwelijkswelzijn van deze vrouwen (Abubakari, 2024). Vrouwen moeten daardoor een steeds belangrijkere rol innemen bij het onderhouden van het gezin, wat extra financiële druk op hen legt (Abubakari, 2024).

Neutralisatietechnieken

Altercasting. De bevindingen uit de studie van Dickinson en Wang (2024) suggereren dat *altercasten*, waarbij iemand een andere identiteit aanneemt, kan functioneren als een vorm van neutralisatie. Daders gebruiken neutralisaties niet alleen om schuldgevoelens te verminderen, maar ook als hulpmiddelen om misdaden tegen anderen gemakkelijker te maken. Zo kunnen daders ze aan slachtoffers aanbieden in de hoop dat slachtoffers deze technieken aanleren en daardoor hun eigen slachtofferrol neutraliseren (Dickinson & Wang, 2024). Eerder onderzoek waaraan de auteurs refereren, constateert dat het leren gebruiken van neutralisaties belangrijk is voor het vormen van iemands zelfbeeld (Dickinson & Wang, 2024). Dit lijkt te gebeuren wanneer fraudeurs doen alsof er een noodsituatie is of een intieme relatie bestaat (Dickinson & Wang, 2024).

Ontkennen van slachtofferschap. Uit het onderzoek van Offei en collega's (2022) komt naar voren dat criminelen van datingfraude uitsluitend de neutralisatietechniek ‘ontkenning van slachtofferschap’ gebruiken om hun daden te rechtvaardigen. Een mogelijke verklaring hiervoor is dat daders beweren dat ook het slachtoffer profiteert van de situatie (Offei et al., 2022). Daders beseffen tegelijkertijd wel dat het moeilijk is om te beweren is dat er zowel géén verantwoordelijkheid als géén schade is, omdat slachtoffers emotionele en financiële schade kunnen aantonen (Offei et al., 2022). Dus als de dader kan aantonen dat er geen slachtoffer is, dan kunnen ze niet alleen verantwoordelijk worden gehouden en wordt daarmee de verantwoordelijkheid naar beide partijen verschoven of wordt de schuld in zijn geheel weggenomen bij de dader (Offei et al., 2022).

Modus operandi

Beloning. Het lijkt erop dat fraudeurs hun gedrag aanpassen op basis van veranderingen in de potentiële beloning (d.w.z. het gedrag van het slachtoffer) (Dickinson et al., 2023; Wang &

Dickinson, 2024). Dit gebeurt met name in fasen waarin geld wordt geïntroduceerd, beloofd of aangeboden (Wang & Dickinson, 2024). Wanneer fraudeurs denken geld te krijgen of te hebben gehad van het slachtoffer, dat ze dan eerder geneigd zijn om bijvoorbeeld voor te stellen om het gesprek op een ander platform voort te zetten of door meer woorden en tekens te gebruiken in hun communicatie, maar ook de intieme band met het slachtoffer te benadrukken (Wang & Dickinson, 2024). Dit heeft volgens Wang en Dickinson (2024) ermee te maken dat mensen meer geneigd zijn tot zelfgemotiveerd gedrag wanneer ze grotere beloningen verwachten. Fraudeurs intensiveren zogezegd hun communicatie wanneer slachtoffers bereid lijken te zijn om iets te geven (Wang & Dickinson, 2024).

Opvolgberichten. Criminelen stellen vaak ogenschijnlijk onschuldige vragen aan het slachtoffer door bijvoorbeeld te vragen hoe het met het slachtoffer gaat om het slachtoffer betrokken te houden en sneller te laten reageren op berichtjes (Dickinson et al., 2023). Wang en Dickinson (2024) in hun onderzoek ook dat vervolgberichten de respons van slachtoffers verhogen (Wang & Dickinson, 2024). Dit vergroot de kans dat slachtoffers meer geld sturen (Wang & Dickinson, 2024). Fraudeurs die al een beloning hebben ontvangen, maken vaker gebruik van opvolgberichten met als om meer geld te krijgen (Wang & Dickinson, 2024).

Fases. Uit meerdere studies komt naar voren dat het proces datingfraude meerdere fases doorloopt (Cross, 2022; Eseadi et al., 2021). Dit proces kan *grosso modo* in vijf opeenvolgende fases worden ingedeeld. Allereerst maken fraudeurs valse profielen aan op datingsites, sociale media of via e-mail, waarbij ze gestolen of verzonnen identiteiten gebruiken, zoals van militairen, hulpverleners of buitenlandse professionals (Eseadi et al., 2021). Vervolgens tonen criminelen snel sterke emoties en verplaatsen de communicatie naar privékanalen - zoals telefoongesprekken, berichten of e-mail - om vertrouwen en emotionele betrokkenheid bij het slachtoffer op te wekken (Eseadi et al., 2021). Soms gebruiken criminelen ook speciale apps om hun eigen stem te verbergen (Eseadi et al., 2021). Vervolgens wordt de zogenoemde ‘foot-in-door’-techniek toegepast, waarbij fraudeurs om kleine geschenken vragen, in plaats van grote bedragen, om zo het vertrouwen van het slachtoffer verder te versterken (Eseadi et al., 2021). Daarna vragen daders om grotere bedragen onder valse voorwendselen, zoals een noodsituatie of reiskosten om het slachtoffer te kunnen ontmoeten (Eseadi et al., 2021). Als het slachtoffer betaalt, dan verzinnen de oplichters nieuwe redenen om nog meer geld te kunnen vragen (Eseadi et al., 2021). Uiteindelijk als het slachtoffer de fraude ontdekt en vervolgens stopt met betalen, dan proberen sommige daders alsnog hen opnieuw te bedriegen, waardoor het slachtoffer opnieuw slachtoffer wordt (Eseadi et al., 2021).

Gesprek voortzetten op ander platform. Het lijkt erop dat al een dader contact heeft gemaakt met het slachtoffer, dat daders het slachtoffer aan te moedigen om via andere kanalen (zoals WhatsApp, sms-bericht of telefonisch) het gesprek voort te zetten (Cross, 2022; Dickinson et al., 2023; Wang en Dickinson, 2024).

Passend profiel. Fraudeurs maken profielen op online datingplatforms die aansluiten bij de romantische fantasieën van het slachtoffer (Eseadi et al., 2021). Deze profielen bevatten meestal fictieve namen of gestolen identiteiten van betrouwbare personen zoals modellen, militairen, hulpverleners of professionals die in het buitenland werkzaam zijn (Eseadi et al., 2021). Hierbij constateren Eseadi en collega's (2021) dat mannelijke fraudeurs zichzelf vaak presenteren zichzelf als rijke, hoogopgeleide professionals, waarbij een hoog sociaal-culturele status doorgaans als aantrekkelijk door vrouwen wordt bevonden (Eseadi et al., 2021). Vrouwelijke

fraudeurs lijken zich juist voor te doen als een knappe jonge vrouw die behoefte heeft aan financiële steun (Eseadi et al., 2021)

Opvragen persoonlijke informatie. Fraudeurs lijken ook vaak persoonlijk informatie, zoals foto's, leeftijd en beroep, op te vragen van het slachtoffer (Dickinson et al., 2023). Deze informatie kan vervolgens worden gebruikt voor identiteitsdiefstal of om vertrouwelijker en betrouwbaarder te doen overkomen (Dickinson et al., 2023).

Inschakelen handlangers. Het lijkt erop dat Ghanese criminelen handlangers in het buitenland inschakelen om datingfraude mogelijk te kunnen maken (Abubakari & Amponsah, 2024). Vanwege beperkingen in Ghana schakelen ze handlangers in de VS in om geloofwaardige profielen te beheren en valse Amerikaanse identiteiten te gebruiken, inclusief Amerikaanse telefoonnummers, om betrouwbaarder over te komen (Abubakari & Amponsah, 2024).

Platform. Oplichters maken vaak valse online profielen aan op datingsites, hoewel ook gebruik wordt gemaakt van sociale media of de e-mail om in contact te komen met potentiële slachtoffers (Eseadi et al., 2021).

Vertrouwen opbouwen. Uit meerdere onderzoeken komt naar voren dat criminelen een emotionele band met het slachtoffer opbouwen om slachtoffers te manipuleren om geld over te maken (Abubakari, 2024; Cross, 2022; Dickinson et al., 2023; Eseadi et al., 2021; Wang & Dickinson, 2024).

Misleidingstechnieken

Begeerlijk. Onderzoek laat zien dat fraudeurs vaak gebruik maken gebruik van vleiende taal, zoals slachtoffers ‘knap’ of ‘liefje’ te noemen (Dickinson et al., 2023; Dickinson & Wang, 2024; Eseadi et al., 2021). Dit doen ze om zo het slachtoffer aantrekkelijk of begeerlijk te laten voelen (Dickinson et al., 2023; Eseadi et al., 2021), wat de emotionele band met het slachtoffer versterkt (Eseadi et al., 2021) en hun vermogen om risico's in te schatten verkleint (Dickinson et al., 2023).

Geloofwaardig overkomen. Om het vertrouwen van slachtoffers te winnen, laat het onderzoek van Dickinson en collega's (2023) zien dat fraudeurs zichzelf presenteren als niet-bedreigende personen die geen slechte foute intenties hebben. Ze doen dit bijvoorbeeld door persoonlijke informatie (zoals hun naam, woonplaats en privé-foto’s) van henzelf te delen of de schijn op te houden dat ze oprecht op zoek zijn naar een relatie (Dickinson et al., 2023). Daarnaast benadrukken fraudeurs gemeenschappelijke interesses, achtergronden of religieuze verbondenheid om vertrouwen bij het slachtoffer te winnen (Eseadi et al., 2021). Deze tactiek werkt vooral in de vroegste stadia van de relatie; de intentie van de oplichter is er dan op gericht om een vertrouwelijke band op te bouwen met het slachtoffer (Eseadi et al., 2021).

Gevoel van controle en zelfvertrouwen. Het lijkt erop dat daders op subtiele wijze een gevoel van controle en zelfvertrouwen overbrengen aan potentiële slachtoffers (Dickinson et al., 2023). Hierdoor gaan slachtoffers minder snel twijfelen dat ze worden misleid (Dickinson & Wang, 2024). Dit maakt ze ontvankelijker voor manipulatie en zijn dan eerder geneigd om geld te sturen (Dickinson & Wang, 2024). Fraudeurs maken gebruik van niet-dwingende taal, zoals vrijheid suggereren in geldgebruik, waardoor slachtoffers de risico’s om opgelicht te worden lager inschatten (Dickinson et al., 2023). Een andere manier is door subtiele instemming, waarbij fraudeurs terughoudend reageren als het slachtoffers geld wil toesturen (Dickinson & Wang, 2024). Deze subtiele benadering geeft het slachtoffer het idee dat het initiatief volledig bij hen ligt (Dickinson & Wang, 2024).

Herhaaldelijke verzoeken. Uit het studie van Eseadi en collega's (2021) blijkt dat zodra het slachtoffer eenmaal is ingegaan op een betaalverzoek, dat dan oplichters nieuwe situaties blijven verzinnen om verdere betalingen uit te kunnen lokken (Eseadi et al., 2021).

Persoonlijke verhalen. Het lijkt erop dat dat fraudeurs gebruik maken van persoonlijke verhalen om het vertrouwen bij slachtoffers te winnen (Abubakari en Amponsah, 2024; Dickinson et al., 2023; Eseadi et al., 2021). Voor het creëren van een emotionele band, delen fraudeurs persoonlijke en tragische verhalen, zoals het overlijden van een partner, wat essentieel is voor het opbouwen van vertrouwen (Abubakari & Amponsah, 2024; Eseadi et al., 2021). Uiteindelijk is het doel om slachtoffers aan te moedigen om verschillende soorten acties te ondernemen, met name het sturen van geld (Dickinson et al., 2023).

Religieuze band. Het lijkt erop dat sommige fraudeurs religieuze aspecten benadrukken om wantrouwen bij slachtoffers weg te nemen (Eseadi et al., 2021), zodat slachtoffers uiteindelijk geld gaan sturen (Dickinson & Wang, 2024; Eseadi et al., 2021). Dit doen daders bijvoorbeeld door te stellen dat hun ontmoeting door een Goddelijke wil heeft plaatsgevonden of door een beroep op de morele plichten om anderen te helpen – het helpen van een behoeftige is een centraal principe in veel religies (Dickinson & Wang, 2024). Fraudeurs hopen door zichzelf als een religieus persoon te presenteren, dat het slachtoffer zich in deze identiteit gaat verplaatsen en zichzelf ziet als iemand die volgens deze religieuze waardes handelt (Dickinson & Wang, 2024).

Romantische band. Een andere misleidingsstrategie die oplichters gebruiken, is het suggereren van een toekomstige of al bestaande romantische met het slachtoffer (Dickinson et al., 2023). Daders suggereren bijvoorbeeld dat het geld zal worden gebruikt om het slachtoffer te bezoeken (Dickinson & Wang, 2024) of in een vroeg stadium al huwelijksvoorstellen te doen om een gevoel van 'toekomst' te creëren (Eseadi et al., 2021). Deze tactieken zorgen ervoor dat slachtoffers minder snel denken dat ze worden opgelicht (Dickinson et al., 2023) en geld geven als een normale uiting van liefde beschouwen (Dickinson & Wang, 2024).

Toewijding. Het onderzoek van Alam (2021) laat zien dat met name *commitment berichten* – welke zijn gericht op diepgaande emotionele betrokkenheid of een serieuze toewijding – gebruikers extra kwetsbaar maken voordatingfraude .

Urgentie. Het lijkt erop daders dat hun slachtoffers manipuleren om geld te sturen door gebruik te maken van urgentie (Dickinson & Wang, 2024; Eseadi et al., 2021). Daders claimen vaak in een nood- crisissituatie te verkeren en daarom zo snel mogelijk geld nodig hebben (Dickinson & Wang, 2024; Eseadi et al., 2021). Zulke claims vallen meestal in drie categorieën: (1) urgente kosten (bijvoorbeeld het kunnen betalen van de huur, voedsel, rekeningen), (2) kosten gericht op gezondheid en veiligheid (zoals geld voor medicijnen of het beweren in een vluchtelingenkamp te zitten) en (3) familiare kosten (geld dat nodig zou zijn om familie te kunnen ondersteunen) (Dickinson & Wang, 2024). Het lijkt erop dat het gebruik van deze verhalen het schuldgevoel en de twijfel bij slachtoffer wegneemt, aangezien het wordt geframed als een daad van liefdadigheid in plaats van een risicovolle transactie (Dickinson & Wang, 2024).

Trends

Frequentie. De populariteit van datingplatforms en sociale media heeft geleid tot een toename van benaderingen vandatingfraude , waarbij online communicatiekanalen (zoals e-mail, berichtenapps, telefoongesprekken) veelgebruikte en effectieve methode zijn om slachtoffers te bereiken (Cross, 2022).

Nepaccounts identficeren. Datingfraude via online datingsites neemt toe door de moeilijkheid om nepaccounts te herkennen (Eseadi et al., 2021). Onderzoek wijst uit dat gebruikers vaak niet in staat zijn oplichters te identificeren op basis van hun profielen (Eseadi et al., 2021). Volgens Eseadi en collega's (2021) reageren datingsites traag op meldingen en nemen onvoldoende actie, terwijl oplichters eenvoudig nieuwe accounts kunnen aanmaken als de oude accounts zijn geblokkeerd (Eseadi et al., 2021).

Ondersteunende rol vrouw. Vrouwen lijken een grote ondersteunende rol te hebben in de datingfraude -industrie (Abubakari, 2024). Ze worden door mannelijke oplichters gerekruteerd die verband houden met hun biologische kenmerken, waaronder het voeren van gesprekken met slachtoffers en het uitvoeren van transacties (Abubakari, 2024).

Toekomstig onderzoek

Blokkeren communicatie. Eseadi en collega's (2021) opperen dat er onderzoek moet worden gedaan naar algoritmes die verdachte communicatie, met of zonder toestemming van het slachtoffer, kunnen blokkeren. Hierbij zou er ook gekeken moeten worden naar de ethische bezwaren ervan (Eseadi et al., 2021).

Meldingsgedrag. Toekomstige onderzoeken zou zich meer moeten focussen welke factoren slachtoffers ertoe aanzetten om fraudegevallen te melden (Eseadi et al., 2021).

Menselijk gedrag. Er zou volgens Wang en collega's (2021) meer onderzoek gedaan moet worden naar menselijke factoren, aangezien menselijk gedrag constant is, terwijl technologie constant verandert.

Methode en data-analyse. Ten eerste door het verzamelen van objectieve gegevens kan er meer inzicht worden verkregen in neutralisatiestrategieën en psychologische factoren die een rol spelen bij datingfraude (Offei et al., 2022). Toekomstig onderzoek zou daarom gebruik moeten maken van andere methoden, dan louter het gebruik van vragenlijsten (Offei et al., 2022). Dit maakt volgens de auteurs het mogelijk objectieve informatie te verzamelen van deelnemers uit diverse contexten (Offei et al., 2022). Dit kan helpen om het fenomeen beter te begrijpen (Offei et al., 2022). Ten tweede kan interviewen van fraudeurs diepere inzichten bieden in hun motivaties en strategieën (Wang & Dickinson, 2024). Ten derde kan het vergelijken van interviews met experimentele methoden een (1) volledigere beeld geven van datingfraude , (2) experimentele bevindingen valideren en (3) aanvullende tactieken van fraudeurs onthullen (Wang & Dickinson, 2024). Als laatste zijn romantische relaties over het algemeen tijdsafhankelijk en evoluerend van aard (Alam, 2021). Daarom zou experimenteel onderzoek met meerdere meetmomenten interessant zijn om meer inzicht te krijgen in deze vorm van fraude (Alam, 2021).

Modus operandi. Toekomstig onderzoek zou zich moeten richten op het belichten van verschillende technieken die fraudeurs gebruiken om hun slachtoffers te misleiden (Eseadi et al., 2021).

Psychologische kenmerken en gevolgen. Volgens Eseadi en collega's (2021) zou er meer onderzoek moeten komen naar de psychologische gevolgen van slachtofferschap vandatingfraude . Daarnaast zou toekomstig onderzoek zich moeten focussen op de relatie tussen fraudeurs en slachtoffers om daarbij te kijken naar specifieke psychiatrische stoornissen, zoals afhankelijkheidsstoornissen bij slachtoffers en antisociale persoonlijkheidskenmerken bij daders (Eseadi et al., 2021).

Steekproef. Er is behoefte aan toekomstig onderzoek dat zich richt op diverse onderzoekspopulaties uit verschillende sociaal-culturele en politieke contexten om meer inzicht te krijgen in de dynamieken van datingfraude (Abubakari, 2024; Alam, 2021; Wang & Dickinson, 2024).

Interventies/trainingen

Slachtoffergericht

Bewustzijn. Meerdere onderzoeken pleitten voor een verhoogder zelfbewustzijn bij gebruikers om hen minder vatbaarder te laten maken voor oplichtingspraktijken (Alam, 2021; Eseadi et al., 2021; Offei et al., 2022; Wang et al., 2021; Wang & Dickinson, 2024). Zo zouden datingplatforms gebruikers potentiële slachtoffers moeten informeren over de risico's en toegepaste midsleidingsstrategieën (Eseadi et al., 2021; Wang & Dickinson, 2024). Dit kan bijvoorbeeld worden gedaan door het verstrekken van een checklist of gids met veelgebruikte toegepaste misleidingstechnieken [bij registratie op datingsites] (Eseadi et al., 2021; Offei et al., 2022) of via bewustwordingscampagnes waarbij ook het belang wordt benadrukt om niet zomaar geld over te maken naar vreemdem (Wang & Dickinson, 2024).

Certificering van datingsites. Landen zoals Singapore hebben een register van gecertificeerde datingplatforms (Eseadi et al., 2021). Het bevorderen van het gebruik van deze goedgekeurde platforms kan bijdragen aan het verminderen van nepwebsites en het verbeteren van de veiligheid (Eseadi et al., 2021).

Detectie. Het ontwikkelen van systemen bij het aanmaken van een datingprofiel verdachte profielen automatisch detecteren, kan datingsites helpen om fraudeurs vroegtijdig te identificeren (Eseadi et al., 2021).

Empathieniveau. Beheerders van datingplatforms zouden ook het empathieniveau van gebruikers kunnen meten (Offei et al., 2022). Dit kan helpen te begrijpen of slachtoffers vatbaar zijn voor fraude en zo voorkomen dat mensen met goede bedoelingen slachtoffer worden (Offei et al., 2022).

Geestelijke gezondheid. Eseadi en collega's (2021) betogen voor het ontwikkelen van effectieve programma's, interventies en hulpmiddelen om geestelijke gezondheid van slachtoffers te verbeteren.

Genderdiscours. De studie Abubakari (2024) benadrukt de noodzaak om genderdynamiek binnen online romantische oplichting en cybercriminaliteit te herzien. Op maat gemaakte interventie- en preventiestrategieën zijn nodig, waarbij rekening wordt gehouden met sociaal-culturele en technologische factoren die de betrokkenheid van vrouwen beïnvloeden (Abubakari, 2024). Daarnaast kunnen initiatieven voor gendergelijkheid kunnen vrouwen legitieme economische kansen bieden en zo de kans verkleinen dat zij illegale middelen zoeken voor hun levensonderhoud (Abubakari, 2024). Ook vragen veranderde genderdynamieken om gespecialiseerde training (Abubakari, 2024). Zulke trainingen zijn essentieel om instanties de vaardigheden te geven die nodig zijn om hun onderzoeksmethoden en interventies effectief te aan te kunnen passen (Abubakari, 2024).

Heersende norm. Fraudeur brengen niet alleen schade toe aan slachtoffers, maar ook (indirect) aan de eigen gemeenschap (Offei et al., 2022). PayPal heeft bijvoorbeeld bepaalde landen waar veel fraude voorkomt op de zwarte lijst gezet (Offei et al., 2022). Daarom is het belangrijk dat gemeenschappen online fraude afkeuren, omdat iedereen in de gemeenschap de nadelige gevolgen kan voelen, zelfs als er ogenschijnlijk geen directe slachtoffers zijn (Offei et al., 2022).

Meldingspunt voor slachtoffers. Vanuit meerdere onderzoeken wordt er voorgesteld om meldingskanalen voor slachtoffers in het leven te roepen (Eseadi et al., 2021; Offei et al., 2022). Zo stellen Offei en collega's (2022) voor om een anoniem meldingspunt op datingsites te implementeren waar potentiële slachtoffers kunnen controleren of ze mogelijk slachtoffer worden van fraude (Offei et al., 2022). Dit zou hen in staat stellen waakzamer te zijn en de kans op slachtofferschap verkleinen (Offei et al., 2022). Daarnaast zou een toegankelijke en veilige manier om fraude te melden de schaamte om fraude niet te melden bij slachtoffers wegnemen (Eseadi et al., 2021). Daarnaast kan er dan ook beter worden vastgesteld de werkelijke impact van datingfraude worden vastgesteld (Eseadi et al., 2021).

Monitoren. Beveiligingsdiensten kunnen IP-adressen in de gaten houden, met name uit fraudegevoelige regio's, om oplichting vroegtijdig te identificeren (Eseadi et al., 2021).

Risico-identificatie. Eseadi en collega's (2021) stellen ook voor om kennis over psychologische kenmerken die mensen vatbaar maken voor oplichting toe te laten passen door datingplatforms. Persoonlijkheidsvragenlijsten kunnen helpen om risicogebruikers te identificeren voor gerichte interventies (Eseadi et al., 2021).

Samenwerking. Doordat veel datingfraude wordt gepleegd door criminelen uit Afrikaanse landen wordt er geadviseerd samen te werken met Westerse landen, zodat om middelen en informatie efficiënt kan worden gedeeld (Eseadi et al., 2021). Afrikaanse landen zouden ook kunnen samenwerken op het gebied van informatiewisseling met buitenlandse agentschappen die ervaring hebben in het bestrijden van datingfraude (Eseadi et al., 2021). Deze samenwerking zou kunnen leiden tot effectievere opsporing van daders, beter internetbeveiligingsbeleid en betere afstemming op internationale normen (Eseadi et al., 2021). Daarnaast zou nauwere samenwerking tussen onderzoekers en datingsites betere inzichten kunnen opleveren in de ervaringen van online daters om zo tot effectievere preventiestrategieën te kunnen komen (Eseadi et al., 2021).

Screeningtools. Datingwebsites kunnen helpen bij het voorkomen van datingfraude door het gebruik van screeningsystemen en preventieve tools (Offei et al., 2022). Beheerders zouden een systeem moeten ontwikkelen om mensen te identificeren die risico's op slachtofferschap negeren (Offei et al., 2022). Als bijvoorbeeld een deelnemer te veel zelfvertrouwen toont, kan dit een waarschuwing zijn voor beheerders en andere gebruikers dat diegene mogelijk risico loopt om slachtoffer te worden (Offei et al., 2022).

Victim-blaming voorkomen. Dickinson en Wang (2024) stellen om *victim blaming* te voorkomen dat het belangrijk is om te benadrukken aan het grote publiek wordt gedeeld dat fraudeurs gebruik maken van technieken om slachtoffers in bepaalde rollen te duwen (Dickinson & Wang, 2024).

Voorlichting. Volgens Offei en collega's (2022) zouden datingplatforms en overheidsinstanties gebruikers van datingsites moeten informeren over de technieken die daders gebruiken om hun criminele gedrag te rationaliseren en de methoden die zij inzetten om dergelijke acties te rechtvaardigen.

Waarschuwingsberichten. Online platforms, zoals Tinder en Meta, en financiële diensten kunnen waarschuwingsmeldingen ontwikkelen die dan worden gestuurd naar gebruikers als gesprekken wijzen op geldverzoeken (Wang & Dickinson, 2024). Dit kan slachtoffers helpen bij het herkennen dat ze mogelijk worden opgelicht, zodat grondiger gaan nadenken om al dan niet geld over te maken (Wang & Dickinson, 2024). Het onderzoek van Alam (2021) laat zien dat met name *commitment berichten* – welke zijn gericht op diepgaande emotionele betrokkenheid of serieuze

toewijding – gebruikers extra kwetsbaar maken voordatingfraude . Platforms zouden dergelijke berichten kunnen herkennen en gebruikers waarschuwen voor mogelijke oplichting (Alam, 2021).

Zelfbeschermingsmaatregelen. Resultaten uit het onderzoek van Wang en Dickinson (2024) laten zien dat fraudeurs vaak hun zelfpresentatiestrategieën afstemmen op de interesses van slachtoffers en aanpassen op basis van de positieve of negatieve reacties van de slachtoffers. Potentiële slachtoffers van datingfraude kunnen zichzelf daarom beschermen door omgekeerde beeldzoekhulpmiddelen te gebruiken om informatie van fraudeurs te verifiëren (Wang & Dickinson, 2024).

Dadergericht

Afschrikking. Resultaten uit de studie van Wang en collega's (2021) laten zien dat fraudeurs ontmoedigd kunnen worden door sanctiedreigingen. Datingsites zouden een algoritme kunnen ontwikkelen dat mogelijke fraudeurs identificeert en hen vervolgens een geautomatiseerd en geloofwaardig afschrikkingsbericht stuurt (Wang et al., 2021). Hierdoor passeren ze mogelijk niet succesvol door het screeningsprotocol (Wang et al., 2021).

Culturele normen veranderen. Volgens Abubakari (2024) zou de culturele verwachtingen over de rol van vrouwen in het huwelijk en hun financiële bijdragen aan het gezin moeten worden aangepakt (Abubakari, 2024). Een open maatschappelijke debat zou volgens de onderzoekers hierbij kunnen helpen (Abubakari, 2024).

Morele en juridische gevolgen. Zoals in het onderzoek van Offei en collega's (2022) naar voren komt, rechtvaardigen fraudeurs hun daden door verantwoordelijkheid te ontkennen en hun slachtoffers niet als echte doelwitten te zien. Om dit tegen te gaan, zouden onderwijsprogramma's de gevolgen van hun daden moeten benadrukken (Offei et al., 2022). Dit kan worden gedaan door het laten zien van het ernstige psychische problemen die het bij slachtoffers kan veroorzaken (Offei et al., 2022). Het doel is om het geweten van daders te beïnvloeden en hen te laten inzien dat hun neutralisaties onjuist zijn (Offei et al., 2022). Abubakari (2024) benadrukt eveneens dat interventies ook gericht moeten zijn op daders, waarbij de nadruk moet komen te liggen op de morele en juridische gevolgen van het deelnemen aan datingfraude .

Tabel 16. Samenvatting resultaten van de literatuur over datingfraude

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	Anonimiteit	Diaspora	Economische marginalisatie	Altercasting	Beloning	Frequentie	Blokkeren communicatie	Bewustzijn
		Betaalbaarheid	Sociale banden	Patriarchale normen	Ontkennen van slachtofferschap	Opvolgberichten	Nepaccounts identificeren	Meldingsgedrag	Certificering van datingsites
						Fases	Ondersteunende rol vrouw	Menselijk gedrag	Detectie
						Gesprek voortzetten op ander platform		Methode en data-analyse	Empathieniveau
						Passend profiel		Modus operandi	Geestelijke gezondheid
						Opvragen persoonlijke informatie		Psychologische kenmerken en gevolgen	Genderdiscours
						Inschakelen handlangers		Steekproef	Heersende norm
						Platform			Meldingspunt voor slachtoffers

						Vertrouwen opbouwen Begeerlijk Geloofwaar-dig overko-men Gevoel van controle en zelfvertrou-wen Herhaalde-lijke ver-zoeken Persoonlijke verhalen Religieuze band Romantische band Toewijding Urgentie	Monitoren Risico-identifica-tie Samenwerking Screeningtools *Victim-blaming* voorkomen Voorlichting Waarschuwings-berichten Zelfbescher-mingsmaatrege-len Afschrikking Culturele nor-men veranderen Morele en juridi-sche gevolgen
	Legenda	***Groen*** *= positieve relatie*	***Rood*** *= negatieve relatie*	***Blauw*** *= ambigue relatie*	***Grijs*** *= neutrale factor*			

3.1.8. Pig-butchering scam

Introductie

Wetenschappelijke literatuur

Pig-butchering scam, in het Nederlands betekent het letterlijk 'varkensslachtingsfraude', is een nieuwe vorm van datingfraude waarbij criminelen vooropgezette romantische misleidingsstrategieën gebruiken om vertrouwen te winnen bij hun slachtoffers (Wang, 2024). Uiteindelijk maken ze gebruik van valse investeringsplatformen en cryptovalutakanalen om de fraude uit te voeren (Wang, 2024). Het is daarbij een vorm van mensenhandel waarbij slachtoffers niet alleen moeten werken, maar ook criminele activiteiten moeten uitvoeren (Wang, 2024). Het verschil met andere vormen van mensenhandel is dat slachtoffers worden behandeld als verhandelbare goederen, totdat ze geen waarde meer hebben (Wang, 2024).

In totaal is er één studie geïdentificeerd die betrekking heeft op pig-butchering scam. Dit betreft de studie van Wang (2024). Dit onderzoek richt zich op het begrijpen van de identiteitstransformatie van kwetsbare Chinese werknemers die betrokken zijn bij illegale arbeidspraktijken, waarbij de focus ligt op de manier waarop sociale manipulatie en mensenhandel hierbij een rol spelen (Wang, 2024). De studie onderzoekt de overlap tussen deze praktijken en hoe werknemers omgaan met hun kwetsbaarheid en veerkracht in dit proces (Wang, 2024). Bovenstaande is onderzocht aan de hand van slachtoffergetuigenissen op Chinese sociale mediaplatformen (Wang, 2024). De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 17 voor een overzicht van de relevante studie, en zie Tabel 18 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met pig-butchering scam.

Tabel 17.
De referentie en kwaliteitsboordeling van de relevante studie over pig-butchering scam.

Referentie	Kwaliteit
(Wang, 2024)	Hoog

Modus operandi

Fases. Het onderzoek van Wang (2024) identificeerde vier fasen in de transformatie van slachtoffer naar fraudeur, namelijk (1) de aanvang, (2) de acculturatie, (3) het keerpunt en (4) de ontsnapping. In de aanvangsfase werden arbeiders misleid door aantrekkelijke werkgelegenheidsaanbiedingen (Wang, 2024). De acculturatiefase laat zien dat bij aankomst slachtoffers in Noord-Myanmar werden geïsoleerd en onderworpen aan dwang, mishandeling, drugsgebruik en hersenspoeling en zo werden gedwongen om fraudeur te worden (Wang, 2024). Het keerpunt speelde op het moment dat werknemers die niet meer goed presteerden, werden doorverkocht aan andere criminele groepen (Wang, 2024). Gedurende dit proces wordt de identiteit van de werknemer als dader steeds sterker, terwijl ze zowel lichamelijk als psychologisch worden misbruikt (Wang, 2024). Veel arbeiders weten uiteindelijk te ontsnappen door geluk en hun vastberadenheid (Wang, 2024).

Misleiding. Wang (2024) constateert dat slachtoffers van pig-butchering scam op diverse manieren worden misleid, voordat ze worden gerekruteerd (Wang, 2024). De studie laat zien dat slachtoffers vaak werden verleid door online advertenties die hoge lonen en aantrekkelijke

voordelen aanboden of ze werden benaderd door oplichters die zich uitgaven voor vertegenwoordigers van betrouwbare bedrijven (Wang, 2024). In sommige gevallen werden slachtoffers via vrienden of familie geïntroduceerd bij de oplichters, wat het vertrouwen bij slachtoffers versterkte (Wang, 2024). De beloftes van een beter leven maakten slachtoffers extra vatbaar voor uitbuiting (Wang, 2024).

Toekomstige studies

Mixed method. Om de modus operandi van pig-butchering scam te onderzoeken, heeft de studie van Wang (2024) gebruik gemaakt van verklaringen van slachtoffers op Chinese sociale mediaplatforms. Volgens de auteur kunnen de getuigenissen mogelijk bestaan uit gefragmenteerde of verdrongen herinneringen door traumatische ervaringen (Wang, 2024). Dit kan de objectiviteit van de data beïnvloeden (Wang, 2024). Toekomstig onderzoek zou daarom volgens de auteurs meerdere methodes moeten gebruiken, zoals interviews en vragenlijsten, om dit probleem te verminderen, maar ook om zo beter begrip te krijgen in de omstandigheden van slachtoffers van mensenhandel (Wang, 2024). Het verkrijgen van data van de slachtoffers zelf kan waardevolle kwalitatieve en kwantitatieve resultaten opleveren die dieper ingaan op de identiteitstransformatie die (verhandelde) werknemers doormaken (Wang, 2024).

Onderzoekssubject. Meer onderzoek is volgens Wang (2024) noodzakelijk om beter inzicht te krijgen welke groepen er allemaal betrokken zijn bij pig-butchtering scam.

Trainingen/interventies

Slachtoffergericht

Herstel en re-integratie. Het is volgens Wang (2024) mogelijk dat een aanzienlijk deel van de slachtoffers voortdurend zijn blootgesteld aan fysieke en psychologisch misbruik. Hierdoor kunnen slachtoffers zich vervreemd voelen van de maatschappij of moeite hebben om het vertrouwen in anderen terug te winnen (Wang, 2024). Daarom stelt de auteur dat slachtoffers door overheden of onderwijsinstellingen moeten worden ondersteund in het verbeteren van hun fysieke en mentale welzijn, zodat ze weer deel kunnen gaan uitmaken van de maatschappij (Wang, 2024).

Samenwerking. Volgens Wang (2024) is het essentieel dat de wereldgemeenschap de criminele activiteiten in Noord-Myanmar erkent. Veel van de betrokkenen, voornamelijk Chinese staatsburgers, maar ook mogelijk burgers van andere landen, worden gedwongen deel te nemen aan deze frauduleuze activiteiten (Wang, 2024). Landen, vooral die in Azië, zouden moeten samenwerken om deze vorm van mensenhandel te stoppen (Wang, 2024). De auteurs stelt verder dat internationale organisaties als de Verenigde Naties zouden moeten helpen bij het versterken van de samenwerking tussen landen en deze landen moeten ondersteunen bij het opstellen van actieplannen (Wang, 2024). Deze plannen zouden militaire, economische en sociale initiatieven kunnen omvatten (Wang, 2024).

Sociaal en juridisch perspectief. Wang (2024) stelt in zijn studie technologische vooruitgangen, zoals ChatGPT en Deepfake, criminelen kunnen helpen bij het plegen van fraude een efficiëntere manier. Dit kan het risico op slachtofferschap vergroten (Wang, 2024). Daarom zouden overheden zich vanuit sociaal en juridisch perspectief moeten voorbereiden op deze uitdagingen (Wang, 2024).

Tabel 18. Samenvatting resultaten van de literatuur over pig-butchering scam.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	Fases Misleiding	-	Mixed method Onderzoekssubject	Herstel en re-integratie Samenwerking
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.9. Advance fee fraud (AFF)

Introductie

Wetenschappelijke literatuur

Advance fee fraud (AFF) is een vorm van oplichting waarbij fraudeurs gebruikmaken van digitale communicatiemiddelen om slachtoffers te misleiden (Tambe Ebot, 2023, p. 1). Criminelen proberen slachtoffers te overtuigen om vooraf een bedrag te betalen voor beloofde goederen of diensten die in werkelijkheid niet bestaan (Tambe Ebot, 2023, p. 1). Zodra fraudeurs een eerste betaling ontvangen, verzinnen ze nieuwe of herhalen ze eerdere leugens om maar extra betalingen van het slachtoffer te ontvangen (Tambe Ebot, 2023, p. 1). Ze blijven dit doen totdat het slachtoffer de fraude ontdekt en stopt met betalen (Tambe Ebot, 2023, p. 1). In totaal hebben zijn er drie studies geïdentificeerd die betrekking hebben op AFF. Dit betreffen de onderzoeken van Okosun en Ilo (2023), Cross (2022) en Tambe Ebot (2023).

Okosun en Ilo (2023) hebben een niet-systematische review uitgevoerd naar de ontwikkeling van AFF en de sociaal-culturele impact ervan in Nigeria. Dit onderzoek kent een lage kwaliteitsscore.

Cross (2022) heeft via een niet-systematische review geschetst wat er momenteel bekend is van onder andere AFF omtrent de gehanteerde modus operandi van daders en effectieve interventies om fraude te bestrijden. De studie is met een lage kwaliteitsscore beoordeeld.

Tambe Ebot (2023) aan de hand van interviews de motivaties en misleidingsstrategieën van hedendaagse AFF-oplichters onderzocht. De auteur richtte zich daarbij op de rol van de digitale omgeving en de toepasbaarheid van sociaal-leertheorieën bij het begrijpen en voorspellen van zulk crimineel gedrag. De kwaliteit van deze studie is als gemiddeld beoordeeld. Zie Tabel 19 voor een overzicht van de relevante studies, en zie Tabel 20 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met AFF.

Tabel 19.
De referenties en kwaliteitsboordeling van de relevante studies voor AFF.

Referentie	Kwaliteit
(Okosun & Ilo, 2023)	Laag
(Cross, 2022)	Laag
(Tambe Ebot, 2023)	Gemiddeld

Macrofactoren

Politieke en economische klimaat. Volgens Okosun en Ilo (2023) wordt het bestrijden van AFF in Nigeria bemoeilijkt door falend leiderschap. Het onderzoek bespreekt de invloed van corruptie en slecht *governance* op de opkomst en het voortbestaan van online criminaliteit (Okosun & Ilo, 2023). Het land heeft meer dan 250 etnische groepen, maar de politieke macht ligt voornamelijk in handen van drie grote etnische groepen, wat leidt tot een focus op etnische belangen in plaats van op de kwaliteit van politieke leiders (Okosun & Ilo, 2023). Dit heeft geleid tot een cultuur van corruptie, waarbij politici vaak worden beschermd door hun etnische of politieke netwerken (Okosun & Ilo, 2023). Het slechte politieke en economische klimaat (d.w.z. hoge werkeloosheid, lage lonen en hoge inflatie) in Nigeria spoort (jonge) mensen aan tot het plegen van online

criminaliteit (Okosun & Ilo, 2023). Via deze weg proberen ze snel geld te verdienen en een hoge sociale status te verwerven (Okosun & Ilo, 2023).

Modus operandi

Digitale omgeving. Tambe Ebot (2023) constateert dat een aantal kenmerken van de digitale omgeving het plegen van AFF versterkt. Deze kenmerken omvatten de mogelijkheden van (1) sociale mediaplatforms, (2) anonimiteit op het internet, (3) een lage afschrikking en (4) rechtvaardiging van online gedrag (Tambe Ebot, 2023). Ten eerste sociale mediaplatforms. Oplichters worden aangemoedigd door eerdere succesvolle oplichtingen en de verwachting van toekomstige beloningen (Tambe Ebot, 2023). Sociale mediaplatforms versnellen dit proces door het voor oplichters eenvoudig te maken om bijvoorbeeld accounts te creëren en verwijderen, en identiteiten en locaties te fingeren (Tambe Ebot, 2023). Ten tweede anonimiteit op het internet. Fraudeurs worden in hun activiteiten aangemoedigd door het gevoel van straffeloosheid dat door het anonieme karakter van het internet wordt versterkt (Tambe Ebot, 2023). Ten derde beperkte afschrikking. Het gebrek aan afschrikking zorgt ervoor dat oplichters zich geen zorgen maken om gepakt te worden (Tambe Ebot, 2023). Aangezien anonimiteit het moeilijk maakt om effectief af te schrikken, geloven daders dat ze straffeloos hun oplichting kunnen voortzetten (Tambe Ebot, 2023). Tenslotte rechtvaardiging van online gedrag. De veelal (afstandelijke) tekst gebaseerde aard van online interacties, waarbij de morele druk van *face-to-face* interacties ontbreekt, maakt het gemakkelijker voor oplichters om hun gedrag te rechtvaardigen (Tambe Ebot, 2023).

Hybride interactie. Bij digitale misdaden, zoals AFF-fraude, begint de interactie met oplichters vaak in de fysieke wereld, waarbij de overstap naar de digitale omgeving zowel het leerproces als de betrokkenheid bij criminaliteit versnelt (Tambe Ebot, 2023). Dit komt doordat online oplichtingsinteracties en -modellen vrijwel onbeperkt zijn wat betreft beschikbaarheid, schaalgrootte, tijd en locatie (Tambe Ebot, 2023).

Profiel. In de loop van de tijd worden er bij AFF nieuwe profielen door criminelen gebruikt (Okosun & Ilo, 2023). Bijvoorbeeld een Amerikaanse soldaat die financiële hulp vraagt of een aantrekkelijke Afrikaanse vrouw die westerse mannen aanspreekt (Okosun & Ilo, 2023).

Social engineering. De bevindingen tonen verder aan hoe de digitale omgeving het handelen van oplichters beïnvloedt door het gebruik van social engineering-technieken (Tambe Ebot, 2023). Deze technieken stellen oplichters in staat om geloofwaardige, misleidende berichten te creëren die gebruikers verleiden tot het doen van betalingen (Tambe Ebot, 2023). Oplichters passen hun gedrag aan door het observeren van slachtoffers, sociale media en andere criminelen (Tambe Ebot, 2023).

Veelvoorkomende methodes. Uit de studie Cross (2022) komt naar voren dat Veelvoorkomende methoden die fraudeurs hanteren zijn nep-investeringen, erfenissen, loterijprijzen, werkvoorstellen en liefdadigheidsverzoeken.

Verhogen van eisen. Op het moment dat een slachtoffer geld overmaakt, verhogen daders vaak hun eisen, wat kan resulteren in aanzienlijke financiële verliezen (Cross, 2022). Slachtoffers vinden het moeilijk om zich los te maken en blijven vaak geld sturen, zelfs wanneer ze doorhebben dat ze zijn opgelicht (Cross, 2022).

Trends

Normalisatie. In het onderzoek van Okosun en Ilo (2023) wordt er gesteld dat de positieve houding tegenover fraudeurs bijdraagt aan de normalisatie van AFF-praktijken. Veel jongeren in

Nigeria zien deze oplichters als helden die wraak nemen op de onderdrukking van hun voorouders tijdens de slavernij en het koloniale tijdperk (Okosun & Ilo, 2023). Deze rechtvaardiging wordt gebruikt om buitenlandse slachtoffers op te lichten, hoewel oplichters zich ook steeds meer richten op het binnenland (Okosun & Ilo, 2023). Zo blijkt dat online fraudeurs nu niet alleen buitenlandse slachtoffers aanvallen, maar ook hun eigen landgenoten, wat leidt tot een groeiende kwetsbaarheid in de samenleving (Okosun & Ilo, 2023).

Robin Hood. Veel fraudeurs investeren in het kopen van *goodwill* en presenteren zichzelf als weldoeners, ofwel moderne Robin Hoods (Okosun & Ilo, 2023).

Zoekmachines. Oplichters gebruiken zoekmachines om toegang te krijgen tot informatie over hoe ze hun social engineering skills kunnen uitbreiden en verbeteren (Tambe Ebot, 2023).

Toekomstig onderzoek

Real-time data. Online misdrijven zijn sterk verbonden met sociale media. Het verzamelen van *real-time* data is daarom cruciaal om actuele informatie over online criminaliteit te verkrijgen (Tambe Ebot, 2023). De verwachting is ook dat technieken die in AFF worden gebruikt in de toekomst zullen veranderen of evolueren (Tambe Ebot, 2023).

Social engineering-technieken. Toekomstig onderzoek zou vanuit het perspectief van de dader zich meer moeten richten op het verder documenteren en begrijpen van de ontwikkeling en veranderingen in de *social engineering*-technieken van oplichters (Tambe Ebot, 2023).

Theoretische modellen. Het onderzoek van Tambe Ebot (2023) wijst uit dat oplichters neutralisaties toepassen om hun criminele praktijken te rechtvaardigen, hoewel er andere perspectieven volgens de auteur kunnen bijdragen aan het begrijpen van de oorzaken van AFF (Tambe Ebot, 2023). Toekomstig onderzoek zou dan ook AFF moeten onderzoeken aan de hand van bijvoorbeeld de *strain-theorie*, *sociale controle theorieën* en *rationele keuze theorieën* (Tambe Ebot, 2023).

Verklaren dadergedrag. Tambe Ebot (2023) stelt dat de focus moet worden verschoven van het verklaren van het gedrag van AFF-oplichters op basis van indirecte data - zoals vrienden en familie van de daders - naar longitudinale (etnografisch) onderzoek dat direct gegevens verzamelt van daders en wetshandhavers.

Interventies/trainingen

Slachtoffergericht

Bewustwording. Okosun en Ilo (2023) benadrukken de noodzaak van het vergroten van het bewustzijn bij potentiële slachtoffers over online risico's. Een groter bewustzijn zorgt ervoor dat mensen beter in staat zijn om te anticiperen op cyber-aanvallen en daarmee een lager risico hebben om slachtoffer te worden (Okosun & Ilo, 2023).

Dadergericht

Attitudes. Tambe Ebot (2023) suggereert dat de huidige anti-oplichting aanbevelingen vooral gericht zijn op het beschermen van slachtoffers, terwijl er meer nadruk zou moeten komen te liggen op het gedragsverandering bij oplichters (Tambe Ebot, 2023). Hoewel het belangrijk is om gebruikers te helpen zichzelf te beschermen, versterken technologische vooruitgangen en de overtuigingskracht van oplichters het succes van oplichterspraktijken (Tambe Ebot, 2023). Daarom zouden onderzoekers, professionals en wetshandhavers zich moeten richten op het veranderen van

de attitudes van oplichters, aangezien zij vaak rationalisaties gebruiken om hun acties te rechtvaardigen (Tambe Ebot, 2023).

Maatschappelijke norm. Er moet veel gedaan worden om de houding van de brede bevolking ten opzichte van internetfraude te veranderen (Okosun & Ilo, 2023). De heersende gedachte is namelijk dat AFF als een vorm van herstelbetalingen voor het koloniale verleden kan worden beschouwd (Okosun & Ilo, 2023).

Rehabilitatie- en preventieprogramma's. Volgens Okosun en Ilo (2023) zouden beleidsmakers zich moeten richten op het ontwikkelen van rehabilitatie- en preventieprogramma', die gericht zijn op het positief beïnvloeden van gedrag (zoals mentoring, peer-counseling en gedragsmodificatie). Deze initiatieven zijn gebaseerd op het idee dat positieve rolmodellen en ervaringen jongeren helpen om in lijn te komen met de legitieme maatschappelijke waarden (Okosun & Ilo, 2023).

Routine-activiteiten theorie. Okosun en Ilo (2023) stellen dat AFF worden verklaard door de routine-activiteitentheorie. Zo vindt AFF-oplichting plaats wanneer (1) een gemotiveerde dader (2) een geschikt doelwit vindt en daarbij (3) goede bewaking ontbreekt (Okosun & Ilo, 2023). Beleidsmaatregelen die één van deze drie elementen weg weten te nemen, kunnen helpen om dit soort misdrijven te verminderen (Okosun & Ilo, 2023).

Sancties. Er zijn uitdagingen voor programma's die oplichters aanpakken, aangezien oplichtingstechnieken snel veranderen en moeilijk te bestrijden zijn (Tambe Ebot, 2023). Bovendien is het problematisch dat sommige slachtoffers, ondanks waarschuwingen, zich toch laten misleiden door oplichters (Tambe Ebot, 2023). Om de effectiviteit van de beschermingsmaatregelen te vergroten, zouden er zichtbare sancties tegen oplichters moeten komen (Tambe Ebot, 2023).

Voorlichting. Tambe Ebot (2023) stelt dat er een risico bestaat dat studenten oplichters worden door socialisatie met andere oplichters. Om die reden moet er volgens de auteur aandacht worden besteed aan de risico's van oplichting op scholen worden gedoceerd, aangezien vriendschapsactiviteiten die individuen motiveren om online oplichting te plegen voornamelijk plaatsvinden op scholen (Tambe Ebot, 2023).

Tabel 20. Samenvatting resultaten van de literatuur over advance fee fraud.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	Politieke en economische klimaat	-	Digitale omgeving	Normalisatie	Real-time data	Bewustwording
						Hybride interactie	Robin Hood	Social engineering-technieken	Attitudes
						Profiel	Zoekmachines	Theoretische modellen	Maatschappelijke norm
						Social engineering		Verklaren dadergedrag	Rehabilitatie- en preventieprogramma's
						Veelvoorkomende methodes			Routine-activiteiten theorie
						Verhogen van eisen			Sancties
									Voorlichting

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.10. E-commerce fraude

Introductie

Wetenschappelijke literatuur

E-commerce fraude, ook wel bekend als *customer-to-customer* (C2C) *fraude*, is een vorm van online fraude dat plaatsvindt via online platformen voor handel en transacties (Lee, 2022, p. 2530). Hierbij worden internet en sociale media vaak ingezet om vertrouwen en een goede relatie tussen verkopers en kopers op te bouwen (Lee, 2022, p. 2530). E-commercefraude kan verschillende vormen aannemen, waaronder fraude met leveringen, betalingen, retouren en restituties, en wordt zowel door verkopers als kopers gepleegd (Lee, 2022, p. 2530). In totaal is er één studie geïdentificeerd die betrekking heeft op e-commerce fraude. Dit betreft de studie van Lee (2022).

Het onderzoek van Lee (2022) heeft middels een crime script analyse onderzocht hoe C2C fraude plaatsvindt op de Chinese onlineplatforms *Baidu Tieba*[7], met bijzondere aandacht voor de rol van *Tencent QQ* (QQ), een *instant messenger* in China die vergelijkbaar is met WhatsApp. Dit onderzoek kent een gemiddelde kwaliteitsscore. Zie Tabel 21 voor een overzicht van de relevante studie, en zie Tabel 22 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met e-commerce fraude.

Tabel 20.
De referentie en kwaliteitsboordeling van de relevante studie voor *e-commerce* fraude.

Referentie	Kwaliteit
(Lee, 2022)	Gemiddeld

Demografische kenmerken

Geslacht. Onderzoek van Lee (2022) laat zien dat ongeveer 63% van de fraudeurs mannen zijn.

Leeftijd. Lee (2022) constateert dat de meeste gerapporteerde fraudeurs jong waren. De jongste fraudeur was 18 jaar oud, terwijl de overige fraudeurs voornamelijk in de leeftijdscategorie van 20 tot 39 jaar vielen (Lee, 2022).

Modus operandi

Fases. Uit het onderzoek van Lee (2022) lijkt het fraudeproces uit vier opeenvolgende fases te bestaan, namelijk (1) voorfase, (2) uitvoeringsfase, (3) afrondingsfase en (4) afsluitingsfase. In de *voorfase* van frauduleuze C2C-transacties bouwen fraudeurs via het platform QQ vertrouwen op met potentiële klanten (Lee, 2022). Fraudeurs bereiden zich voor door een QQ-account aan te maken, betalingsopties in te stellen en het zorgvuldig kiezen van producten of diensten om te verkopen (Lee, 2022). Verkopers gebruiken advertenties en chatgroepen om klanten aan te werven (Lee, 2022). Dit wordt vaak gedaan met behulp van lage prijzen of door direct contact op te nemen via hun QQ-ID (Lee, 2022). Reputatie en geloofwaardigheid worden versterkt door het kopen van zogenoemde 'QQ friends/fans' en het delen van gedetailleerde profielinformatie (Lee, 2022). Het doel van deze fase is om vertrouwen te wekken en een basis te leggen voor

[7] *Baidu Tieba* is een Chinees platform waar gebruikers advertenties kunnen plaatsen en reageren op lokale aanbiedingen, wat het volgens Lee (2022) een geschikte plek maakt om de dynamiek van C2C-fraude te onderzoeken.

toekomstige transacties (Lee, 2022). In de operationele fase verifiëren verkopers eerst de persoonlijke informatie van de koper, zoals naam, geboortedatum en geboorteplaats, en vragen soms om een identiteitskaart (Lee, 2022). Fraudeurs kunnen ook vragen naar de financiële situatie van de koper om vertrouwen en de bereidheid van de koper om een deal te sluiten te peilen (Lee, 2022). Nadat de informatie is geverifieerd, onderhandelen de partijen over de prijs (Lee, 2022). Aangezien C2C-handel niet is gereguleerd, proberen verkopers vaak een hogere prijs te bedingen dan de oorspronkelijk prijs (Lee, 2022). Dit leidt tot heronderhandelingen, waarbij kopers doorgaans akkoord gaan als de prijs nog steeds onder de marktprijs ligt (Lee, 2022). De afrondings- en afsluitingsfase van C2C-fraude begint nadat de betaling is verzonden en slachtoffers ontdekken dat er iets mis is gegaan met de transactie (Lee, 2022). Kopers worden vaak gevraagd om hun QQ Pay Wallet-saldo te tonen of direct geld over te maken naar een bankrekening van de verkoper (Lee, 2022). Na de betaling verdwijnt de frauduleuze verkoper, en kopers blijven achter zonder compensatie (Lee, 2022). C2C-fraude maakt meestal geen gebruik van hightech-betaalmethoden, zoals cryptocurrency, omdat het is gebaseerd op het uitwisselen van legitieme goederen en diensten (Lee, 2022). Het crime-script beschrijft zogezegd hoe frauduleuze verkopers communiceren met potentiële slachtoffers (Lee, 2022). Criminelen adverteren met goederen via individuele of groepsberichten om het vertrouwen van potentiële slachtoffers te winnen (Lee, 2022). Deze advertenties zijn effectiever wanneer ze binnen vertrouwde kringen worden gedeeld (Lee, 2022). Klanten die denken een goede deal te kunnen krijgen, nemen contact op met de verkoper, bespreken de details en doen een betaling (Lee, 2022). Na de betaling verdwijnt de verkoper en worden er geen producten of diensten geleverd, waarna slachtoffer zich realiseert te zijn opgelicht (Lee, 2022).

Platforms. De studie van Lee (2022) benadrukt dat het gebruik van technologische hulpmiddelen e-commercefraude vergemakkelijkt. Fraudeurs maken gebruik van de basisfuncties van platforms zoals QQ en ontwikkelen manieren om detectie door klanten te omzeilen (Lee, 2022). In veel gevallen wordt QQ Pay gebruikt, dat is gekoppeld aan de QQ-app (Lee, 2022). Sommige fraudeurs manipuleren QQ-app instellingen, zoals het versnellen van betalingen naar de verkopersrekening, terwijl andere slachtoffers onder druk zetten om bankoverschrijvingen te gebruiken zodat mogelijk gestolen geld snel kan worden uitbetaald (Lee, 2022).

Toekomstig onderzoek

Meerdere landen. Het onderzoek van Lee (2022) was op de Chinese context gericht en om de resultaten verder te kunnen generaliseren oppert de auteur dat toekomstig onderzoek ook in andere landen moet worden uitgevoerd.

Modus operandi. De resultaten uit het onderzoek van Lee (2022) zijn gebaseerd op slachtofferervaringen van QQ-gebruikers, maar voor een volledige verklaring van gehanteerde modus operandi zou volgens de auteur onderzoek ook gericht moeten zijn op de dader zelf.

Interventies/trainingen

Slachtoffergericht

Bewustzijn. Volgens Lee (2022) wijzen de bevindingen op een duidelijke behoefte om het bewustzijn over de e-commerce fraude bij mensen te vergroten. Interventies zouden zich kunnen richten op jongere generaties, aangezien die vaker online zijn en meer kans lopen om slachtoffer te worden van C2C-fraude (Lee, 2022).

Tabel 22. Samenvatting resultaten van de literatuur over e-commerce fraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
Geslacht (man) Leeftijd	-	-	-	-	-	Fases Platforms	-	Meerdere landen Modus operandi	Bewustzijn
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.11. Concession-Abuse-as-a-Service (CAaaS)-fraude

Introductie

Wetenschappelijke literatuur

Concession-Abuse-as-a-Service (CAaaS)-fraude is een vorm van online fraude waarbij fraudeleuze klanten proberen een gratis vervangingsproduct of terugbetaling van online winkels te krijgen door klantenservicemedewerkers te manipuleren en het retourproces uit te buiten (Sun et al., 2021, p. 4170). De klanten van CAaaS (de initiators van de oplichting) verzoeken aanvallers (dienstverleners) om contact op te nemen met een handelaar om de oplichting uit te voeren (Sun et al., 2021, p. 4169). Als de oplichting slaagt, kan de misdadiger het vervangingsproduct of de terugbetaling doorverkopen via tussenpersonen (Sun et al., 2021, p. 4170). CAaaS-oplichting bestaat uit twee hoofdrolspelers: de CAaaS-oplichter (de klant die een gratis concessie wil zoals terugbetaling) en de afnemer (de oplichter die de dienst aanbiedt voor het misbruiken van de terugbetaling) (Sun et al., 2021). Er zijn ook ondersteunende criminelen die helpen het succes van de oplichting te vergroten en de identiteit van de oplichters te verbergen (Sun et al., 2021). In totaal is er één studie geïdentificeerd die betrekking heeft op CAaaS-oplichting. Dit betreft de studie van Sun en collega's (2021). In dit onderzoek werden ondergrondse forums geanalyseerd om de personen achter de CAaaS-fraude te identificeren en de werking ervan te kunnen begrijpen (Sun et al., 2021). De kwaliteit van deze studie is als gemiddeld beoordeeld. Zie Tabel 23 voor een overzicht van de relevante studie, en zie Tabel 24 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met CAaaS-fraude.

Tabel 23.
De referentie en kwaliteitsboordeling van de relevante studie voor CAaaS-fraude.

Referentie	Kwaliteit
(Sun et al., 2021)	Gemiddeld

Criminaliteit

Betrokkenheid bij niet-oplichterspraktijken. Uit het onderzoek van Sun en collega's (2021) komt naar voren dat een aantal CAaaS-oplichter betrokken is bij niet-scam activiteiten en dan met name bij hacking (12,83%) en gestolen inloggegevens (25,80%). Een verklaring hiervoor is dat deze activiteiten vaak zijn gerelateerd aan CAaaS, zoals het verkrijgen van gecompromitteerde online accounts voor CAaaS-diensten (Sun et al., 2021).

Modus operandi

Fases. CAaaS-oplichting bestaat uit twee hoofdrolspelers: de CAaaS-oplichter (de klant die een gratis concessie wil zoals terugbetaling) en de afnemer (de oplichter die de dienst aanbiedt voor het misbruiken van de terugbetaling) (Sun et al., 2021). Er zijn ook ondersteunende criminelen die helpen het succes van de oplichting te vergroten en de identiteit van de oplichters te verbergen (Sun et al., 2021). De oplichtingspraktijk verloopt in drie fases: (1) voorbereiding, (2) uitvoering en (3) monetisatie (Sun et al., 2021). In de voorbereidingsfase maken afnemer en dienstverlener een deal, waarbij de initiatiefnemer informatie over de bestelling verstrekt (Sun et al., 2021). Eventueel worden er compromitterende accounts of hacktools aangeschaft voor betere

anonimiteit (Sun et al., 2021). In de uitvoeringsfase misleidt de dienstverlener de klantenservice medewerker om een overeenkomst (zoals een terugbetaling of een nieuw product) te verkrijgen (Sun et al., 2021). Hierbij krijgen ze soms hulp van anderen, zoals vervalsers en mensen die lege dozen of vervalste goederen leveren om het retourproces te manipuleren (Sun et al., 2021). In de monetisatiefase worden na het verkrijgen van de concessie de goederen of cadeaubonnen omgezet in geld via ondergrondse marktplaatsen of de goederen worden doorverkocht via tussenpersonen (Sun et al., 2021).

Gecompromitteerde accounts. Het onderzoek van Sun en collega's (2021) wijst uit dat oplichters actief naar gecompromitteerde winkelaccounts met recente bestellingen voor restitutieverzoeken, omdat deze minder controle vereisen en vaak als routine worden beschouwd door klantenservicemedewerkers. Daarbij zijn bestellingen hoge waarde minder aantrekkelijk zijn vanwege het risico op extra onderzoeken en daarom stellen veel oplichters een limiet in voor de waarde van bestellingen bij elke verkoper (Sun et al., 2021). Daarnaast verkiezen fraudeurs winkelaccounts met een lange bestelgeschiedenis en weinig claims, omdat die als minder verdacht worden gezien (Sun et al., 2021). Op ondergrondse forums adverteren verkopers gecompromitteerde accounts met deze eigenschappen als ideale accounts voor restitutie- of oplichtingsdoeleinden (Sun et al., 2021)

Keuze slachtoffer. CAaaS-oplichters richten zich vaak op grote handelaren omdat zij een robuuste klantenservice hebben en bereid zijn financieel verlies te accepteren voor klanttevredenheid (Sun et al., 2021). Grote bedrijven zijn daardoor kwetsbaarder voor CAaaS oplichting (Sun et al., 2021).

Misbruik retourbeleid. Het onderzoek van Sun en collega's (2021) laat zien dat CAaaS-oplichters dikwijls gebruik van een aantal veelvoorkomende redenen om terugbetaling aan te vragen. Ten eerste dat het pakket niet is geleverd (Sun et al., 2021). Oplichters nemen contact op met de klantenservice nadat het pakket is geleverd en beweren dat het nooit is aangekomen (Sun et al., 2021). Ze volgen de instructies van de klantenservicemedeweker op, bijvoorbeeld het doen van navraag bij de buren of daar het pakketje is bezorgd, om vertrouwen op te bouwen, maar beweren uiteindelijk dat van het pakket geen spoor te bekennen is (Sun et al., 2021). Ten tweede dat de doos leeg is (Sun et al., 2021). Oplichters beweren een lege doos te hebben ontvangen met alleen verpakkingsmateriaal, wat hen in staat stelt om een terugbetaling aan te vragen (Sun et al., 2021). In zulke gevallen verstrekken klantenservice medewerkers meestal een terugbetaling (Sun et al., 2021). Ten derde dat (een deel van) het product ontbreekt (Sun et al., 2021). Zo kunnen oplichters beweren dat sommige artikelen ontbreken om zo een terugbetaling te kunnen aanvragen (Sun et al., 2021). Ten vierde dat er een verkeerd item is geleverd (Sun et al., 2021). Oplichters beweren dat ze een verkeerd item hebben ontvangen van mindere waarde, sturen een goedkopere versie terug en houden vervolgens het originele item (Sun et al., 2021). Een andere reden is dat het product beschadigd is (Sun et al., 2021). Oplichters kunnen beweren dat een item beschadigd is aangekomen, bijvoorbeeld schade door lekkende vloeistoffen, en vragen om een terugbetaling of vervangend product (Sun et al., 2021).

Telefoongesprekken. Oplichters lijken de voorkeur te hebben voor telefoongesprekken met klantenservicemedewerkers (Sun et al., 2021). Dit heeft ermee te maken dat in een telefoongesprek de medewerker meteen moet reageren en social engineering-tactieken beter door de oplichter kunnen worden toegepast (Sun et al., 2021).

Misleidingstactieken

Beleefdheid. Uit het onderzoek van Sun en collega's (2021) komt naar voren dat CAaaS-oplichters zich doorgaans positieve opstellen door zich charmant en beleefd te gedragen tijdens interacties met klantenservice medewerkers. CAaaS-oplichters noemen bijvoorbeeld klantenservice medewerkers bij hun naam, tonen begrip voor eventuele fouten en uiten hun waardering voor de hulp (Sun et al., 2021).

Medelijden en urgentie. Dienstverleners verzinnen vaak verhalen die gevoelens van medelijden en urgentie oproepen. Criminelen zeggen bijvoorbeeld het cadeau voor hun zieke zoon niet is bezorgd om de klantenservice te overtuigen dat snel een terugbetaling moet worden geregeld (Sun et al., 2021).

Liegen over eerdere gesprekken. Sommige CAaaS-oplichters bellen meerdere keren met een verkoper en liegen vervolgens tegen de betreffende klantenservicemedewerker over wat er in eerdere gesprekken is afgesproken (Sun et al., 2021). In het onderzoek van Sun en collega's (2021) wordt als voorbeeld gegeven dat oplichters beweren dat het vorige gesprek werd verbroken op het moment dat de terugbetaling werd verwerkt, zodat de tweede klantenservicemedewerker de niet-bestaande overeenkomst (bijv. de terugbetaling) toch toekent (Sun et al., 2021).

Wettelijke voorschriften uitbuiten. Dienstverleners kunnen wettelijke voorschriften gebruiken om te voorkomen dat ze goederen retourneren (Sun et al., 2021). In het onderzoek van Sun en collega's (2021) wordt er een voorbeeld aangehaald dat een CAaaS-serviceprovider bijvoorbeeld kan klagen over een batterijlekkage in een gekochte laptop en aangeven dat hij deze niet kan retourneren vanwege een bepaalde wetsartikel (Lithium Battery Regulation).

Trends

Mislukte oplichtingen. Volgens Sun en collega's (2021) zijn er verschillende oorzaken voor mislukte oplichtingspraktijken. De oplichting wordt ontdekt door onderzoek *verzendagenten* (verifieren identiteit, goederen en internationale verzending bij verdachte zendingen) of *handelaren* (gebruiken data zoals tijdstempels en pakketinformatie om leveringen te controleren) (Sun et al., 2021). Daarnaast zijn duurdere goederen vatbaarder voor onderzoek, waardoor oplichters door de mand kunnen vallen bij automatische controles (Sun et al., 2021). Ook kan een ongebruikelijke activiteit op een winkelaccount, vooral als een account een geschiedenis van misbruik heeft, leiden tot onderzoek waardoor de oplichting wordt ontdekt (Sun et al., 2021). Een andere oorzaak is dat onvoldoende of onbetrouwbaar bewijs leiden tot ontdekking, doordat bijvoorbeeld oplichters geen ‘vervalsen’ bewijs kunnen leveren of juist fouten maken bij vervalsingen (Sun et al., 2021). Als laatste kunnen oplichters falen als ze worden gedwongen om hun identiteit te onthullen bij ontvangst van de goederen of als ze goederen moeten retourneren (Sun et al., 2021). Laatstgenoemde is vooral het geval als inspectie of persoonlijke afhaling vereist is (Sun et al., 2021).

Tarieven service providers. Serviceproviders in ondergrondse forums rekenen meestal een percentage van de orderwaarde (Sun et al., 2021). De kosten hangen af van de handelaar, orderprijs en betaalmethode. Het ontvangen percentage varieert vaak tussen de 15% tot 25% met een minimumbedrag van 35 dollar (Sun et al., 2021).

Tutorials en begeleiding forum. Het onderzoek van Sun en collega's (2021) toont aan dat op ondergrondse forums tutorials en begeleiding worden aangeboden en oplichters hun ervaringen hierop met elkaar delen. Oplichters kunnen op die manier snel (van elkaar) leren en worden ze

als het ware van A tot Z begeleidt in het uitvoeren van CAaaS-oplichting (Sun et al., 2021). Oplichters lijken binnen 47 tot 293 dagen hun eerste successen te boeken (Sun et al., 2021)

Interventie/trainingen

Slachtoffergericht

Account Abuse Detection Principles (AADP). Om concessiefraude te voorkomen, moeten er volgens Sun en collega's (2021) proactieve maatregelen worden genomen om gecompromitteerde accounts vroegtijdig te detecteren. De auteurs stellen een Account Abuse Detection Principles (AADP) voor om deze vorm van fraude beter te kunnen identificeren en bestaat uit een vijftal punten (Sun et al., 2021). Ten eerste kunnen tijdige meldingen aan de accountbezitter CAaaS-oplichting helpen voorkomen, vooral bij accounts die verkocht zijn op ondergrondse platforms of betrokken zijn bij datalekken (Sun et al., 2021). Ten tweede moeten accounts met ongebruikelijke activiteit, zoals frequente restitutieverzoeken, worden gemonitord (Sun et al., 2021). Hierbij de datum van bestellingen ook een belangrijke risicofactor zijn (Sun et al., 2021). Ten derde kunnen nieuwe accounts met weinig bestelgeschiedenis zijn (Sun et al., 2021). Ook als een nieuw account is gekoppeld aan een eerder gesloten oplichters-account, moet het volgens de auteurs als verdacht worden gemarkeerd (Sun et al., 2021). Het laatste vierde principe betreft het gebruik van technische authenticatiemethoden, zoals twee-factor-authenticatie, die kunnen helpen om misbruik van gecompromitteerde accounts te voorkomen (Sun et al., 2021). Als laatste kunnen snelle uitgaven van e-giftcard-saldi en verzendingen naar een nieuw adres wijzen op misbruik van gecompromitteerde accounts (Sun et al., 2021).

Merchant Operation Protocol (MER-OP). Om fraude effect te voorkomen, stellen Sun en collega's (2021) een Merchant Operation Protocol (MER-OP) voor die gericht is op algemene bedrijfsvoering voor handelaren van goederen (Sun et al., 2021). Dit protocol bestaat uit een zevental punten. Het eerste punt betreft dat handelaren klantenservicemedewerkers moeten voorzien van een dashboard met klantinformatie en risicoscore, in combinatie met scam detectie tools en eerdere chatrecord, om authenticiteit te verifiëren (Sun et al., 2021). Als tweede moeten er foto’s van goederen worden gemaakt tijdens het verpakken. Dit zou helpen bij het verminderen van claims voor ontbrekende of verkeerd geleverde items (Sun et al., 2021). Daarnaast kan een offline retourbeleid voor dure goederen, waarbij directe inspectie van het product en verificatie van de identiteit van de klant, bijdragen aan het voorkomen van CAaaS-fraude (Sun et al., 2021). Ook kan apart verpakken van dure artikelen helpen tegen fraudeclaims als ontbrekende producten of lege dozen (Sun et al., 2021). Verder stellen Sun en collega's (2021) dat handelaren extra verificatie moeten instellen voor e-giftcard betalingen om de kans op oplichting te verkleinen. Een ander punt is dat klanten een tweede contactadres moeten aangeven om meldingen over accountactiviteit te ontvangen (Sun et al., 2021). Als laatste zouden handelaren actief moeten samenwerken met betalingsverwerkers bij frauduleuze claims, aangezien oplichters soms proberen om anti-fraude systemen te omzeilen via derden (Sun et al., 2021). Een minpunt aan dit protocol is volgens de auteurs wel dat klanten sommige maatregelen als ongemakkelijk kunnen ervaren (Sun et al., 2021)

Tabel 24. Samenvatting resultaten van de literatuur over Concession-Abuse-as-a-Service (CAaaS)-fraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	Betrokkenheid bij niet-oplichters-praktijken	-	-	-	-	Fases Gecompromitteerde accounts Keuze slachtoffer Misbruik retourbeleid Telefoongesprekken Beleefdheid Medelijden en urgentie Liegen over eerdere gesprekken Wettelijke voorschriften uitbuiten	Mislukte oplichtingen Tarieven service providers Tutorials en begeleiding forum	-	Account Abuse Detection Principles (AADP) Merchant Operation Protocol (MER-OP)

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.12. Online werkgelegenheidsfraude

Introductie

Wetenschappelijke literatuur

Online werkgelegenheidsfraude is een vorm van online fraude waarbij niet-bestaande vacatures worden aangeboden met als doel om persoonlijke, gevoelige en/of financiële informatie van het slachtoffer te verkrijgen (Cole, 2022). In totaal is er drie studies geïdentificeerd die betrekking heeft op online werkgelegenheidsfraude. Dit betreft het onderzoek van Cole (2022), Goyal en collega's (2023) en Ridho (2024).

Cole (2022) onderzocht hoe de social-engineeringaanvallen van fraudeurs, zoals taalkundige signalen en tactieken, variëren op basis van de online presentatie van gebruikers-cv's op vacaturewebsites. De kwaliteit van deze studie is als hoog beoordeeld.

Goyal en collega's (2023) hebben op basis van 17.000 klachten een kennisgrafiek ontwikkeld omtrent werkgelegenheidsfraudes om consumenten te waarschuwen en fraudepatronen te identificeren. De studie is met een lage kwaliteitsscore beoordeeld.

De studie van Ridho (2024) heeft aan de hand van slachtofferervaringen van Twitter-gebruikers onderzoek gedaan naar de werkwijze en misleidingstechnieken die door criminelen worden toegepast bij online vacaturefraude. De kwaliteit van deze studie is als gemiddeld beoordeeld. Zie Tabel 25 voor een overzicht van de relevante studie, en zie Tabel 26 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met online werkgelegenheidsfraude.

Tabel 25.
De referenties en kwaliteitsboordeling van de relevante studies voor **online werkgelegenheidsfraude**.

Referentie	Kwaliteit
(Cole, 2022)	Hoog
(Goyal et al., 2023)	Laag
(Ridho, 2024)	Gemiddeld

Modus operandi

Autoriteit. Goyal en collega's (2023) constateren dat oplichters zich vaak voordoen als bekende retailers, zoals Amazon en Walmart, door nep-vacatures te plaatsen op grote online platformen.

Beleefde toon. Cole (2022) constateert in zijn studie dat Social engineerings-techieken, zoals linguïstische aanwijzingen van beleefdheid, een grotere rol spelen in fraudegevallen als geheel dan individuele kenmerken van fraudeurs. In 60% van de fraudegevallen gebruikten oplichters een beleefde toon om slachtoffers te overtuigen hun sollicitatie voort te zetten of extra informatie te geven (Cole, 2022).

E-mail. Het lijkt erop dat de e-mail voor oplichters de meest gebruikelijke manier is om hun slachtoffer te benaderen (Goyal et al., 2023).

Fases. Volgens het onderzoek van Ridho (2024) lijkt online vacaturefraude een gestructureerd proces te verlopen, waarbij slachtoffers geleidelijk aan financieel en psychologisch meer betrokken raken (Ridho, 2024). Het doel van criminelen is om de investeringen en betrokkenheid

van slachtoffers stap voor stap te vergroten (Ridho, 2024). De verschillende stappen die in het onderzoek zijn benoemd, worden in chronologische volgorde besproken. De oplichting begint met ongevraagde werkaanbiedingen waarbij slachtoffers eenvoudige taken, zoals YouTube-video's liken, moeten uitvoeren in ruil voor kleine beloningen (Ridho, 2024). Vervolgens worden ze toegevoegd aan een grote Telegram-groep om de geloofwaardigheid van oplichting te vergroten en slachtoffers krijgen hogere beloningen voor uitgevoerde taken (Ridho, 2024). Slachtoffers worden aangemoedigd geld over te maken om de activiteit van een cryptocurrency-website te stimuleren met de belofte van beloningen (Ridho, 2024). Naarmate de scam vordert, stijgen de bedragen die slachtoffers moeten storten (Ridho, 2024). Slachtoffers worden overgeplaatst naar een kleinere VIP-groep, waar de druk wordt opgevoerd om door te gaan (Ridho, 2024). Ze worden gedwongen grotere bedragen te storten, onder de dreiging van verlies van eerdere betalingen (Ridho, 2024). Het komt voor dat, ondanks waarschuwingen van familie, slachtoffers hun spaargeld en leningen van familieleden inzetten (Ridho, 2024). De laatste fase betreft het vragen van een zeer hoog bedrag, vanwege een zogenaamde ‘systeemupdate’, waarna ze uiteindelijk doorhebben dat ze het slachtoffer zijn geworden van de oplichting (Ridho, 2024).

Focus op niet-technologisch beroep. Oplichters lijken vaak gericht te zijn op gebruikers wiens beroep minder afhankelijk is van technologie, zoals babysitters (Cole, 2022). Dit suggereert volgens Cole (2022) dat oplichters bepaalde profielen selecteren op basis van hun verwachte kennis van online fraude.

Gedrag aanpassen en imitatie. De studie van Cole (2022) toont aan dat fraudeurs hun tactieken aanpassen aan de online omgeving en de presentatie van cv-profielen op vacaturewebsites. Ze imiteren legitieme werkgevers door onder andere gevoelige informatie op te vragen en hyperlinks te sturen (Cole, 2022). In het onderzoek het wordt er gesteld dat de sociale leertheorie hierbij een rol speelt: fraudeurs leren en passen zich aan door gedrag van legitieme aanbieders te kopiëren (Cole, 2022).

Schaarste. Fraudeurs maken gebruik van de neiging van mensen om meer waarde te hechten aan kansen die als zeldzaam of beperkt worden gepresenteerd (Ridho, 2024). Door het introduceren van zogenoemde ‘upgrading tasks’ en VIP-groepen, creëren criminelen het gevoel van exclusiviteit, waardoor slachtoffers denken dat ze toegang hebben tot iets unieks (Ridho, 2024). Deze schijnbare schaarste zetten slachtoffer ertoe aan om meer te investeren uit angst om iets unieks mis te lopen (Ridho, 2024). Dit leidt tot risicovoller gedrag, waarbij slachtoffers grotere financiële risico's nemen en subtiele aanwijzingen van de oplichting negeren (Ridho, 2024).

SES en opleidingsniveau. Het lijkt erop demografische gegevens van cv-profielen een belangrijke rol spelen bij fraude aanvallen (Cole, 2022). Profielen met een lagere sociaal economische status (SES) en lager onderwijsniveau werden vaker getroffen door oplichters (Cole, 2022).

Sociale bewijskracht. Het lijkt erop dat sociale bewijskracht een rol speelt in **vacaturefraude** doordat slachtoffers hun gedrag afstemmen op de acties van anderen (Ridho, 2024). Telegram-groepen met veel leden, waarin succesverhalen worden gedeeld, wekken de indruk dat zulke investeringen legitiem zijn (Ridho, 2024). Het idee dat anderen zogenaamd succesvol zouden zijn, vermindert het risicobesef en moedigt slachtoffers aan om door te gaan (Ridho, 2024).

Sociale nabijheid. Het lijkt erop dat cybercriminelen hun doelwitten motiveren door sociale nabijheid op te bouwen (Ridho, 2024). Ze bouwen een vertrouwensband op om hun doelwitten te overtuigen, omdat mensen van nature geneigd zijn anderen te helpen (Ridho, 2024). Fraudeurs creëren situaties waarin het lijkt alsof ze maar een beetje hulp nodig hebben, waardoor er minder twijfel ontstaat bij het slachtoffer (Ridho, 2024).

Verliesaversie. Fraudeurs lijken gebruik te maken van psychologische principes als verliesaversie, waarbij mensen meer bang zijn voor verlies dan voor winst (Ridho, 2024). Slachtoffers blijven steeds meer investeren om eerdere verliezen te vermijden (Ridho, 2024). Dit wordt versterkt doordat ze zich steeds verder (psychologisch) vastklampen aan hun investeringen uit angst voor grotere verliezen (Ridho, 2024).

Toekomstig onderzoek

Maatschappelijke impact. Ridho (2024) betoogt dat er onderzoek moet worden gedaan naar de bredere maatschappelijke impact van online **werkgelegenheidsfraude**.

Psychologische mechanismen. Er is behoefte aan toekomstig onderzoek om meer inzicht te krijgen in de psychologische processen en dynamieken van **online werkgelegenheidsfraude** (Cole, 2022; Ridho, 2024). Zo benadrukt de studie van Cole (2022) de noodzaak om verder onderzoek te doen naar hoe oplichters hun gedrag en tactieken aanpassen aan verschillende platforms, zoals datingsites, om hun motivaties en imitatiegedrag beter te begrijpen.

Verschillende demografie. Volgens Ridho (2024) zou toekomstig onderzoek zich ook kunnen richten op de vraag of de misleidingstechnieken genoemd bij verschillende groepen mensen op dezelfde manier werken.

Trainingen/interventies

Slachtoffergericht

Onderwijs en bewustwording. De studie van Cole (2022) benadrukt dat toezicht en educatie door zogenoemde *guardians*, zoals onderzoekers, politie en websitehosts, cruciaal zijn. Deze partijen zouden slachtoffers moeten helpen om fraudeurs te herkennen en verdachte activiteiten te melden, zodat er sneller kan worden ingegrepen (Cole, 2022). Daarnaast benadrukt Ridho (2024) het belang van publieke bewustwording, waarbij campagnes uitleggen welke gevaren er zijn en welke misleidingstactieken worden gebruikt bij online werkgelegenheidsfraude. Bovendien zouden bedrijven hun klanten moeten informeren over de risico's die dergelijke oplichting met zich meebrengt en met preventieve strategieën aanreiken (Ridho, 2024).

Samenwerking. Ridho (2024) stelt dat bedrijven, met name die in de financiële en technologische sector, hun beveiliging moeten verbeteren en moeten samenwerken met wetshandhavingsinstanties om frauduleuze activiteiten te onderzoeken.

Wetgeving. In het onderzoek van Ridho (2024) wordt er gepleit dat beleidsmakers strengere regels invoeren voor online gemeenschappen en hun financiële transacties. Verder stelt de auteur dat er juridische kaders moeten zijn om snel op frauduleuze activiteiten te kunnen inspelen en om zo slachtoffers beter te kunnen beschermen (Ridho, 2024).

Tabel 26. Samenvatting resultaten van de literatuur over online werkgelegenheidsfraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	Autoriteit Beleefde toon E-mail Fases Focus op niet-technologisch beroep Gedrag aanpassen en imitatie Schaarste SES en opleidingsniveau Sociale bewijskracht Sociale nabijheid Verliesaversie	-	Maatschappelijke impact Psychologische mechanismen Verschillende demografie	Onderwijs en bewustwording Samenwerking Wetgeving

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.13. Online werknemersfraude

Introductie

Wetenschappelijke literatuur

Online werknemersfraude is een vorm van online fraude wordt aan de hand van online computertoegang gepleegd tegen het bedrijf of organisatie waar iemand voor werkt met als doel financiële voordelen te behalen (Othman & Ameer, 2022). In totaal is er één studie geïdentificeerd die betrekking heeft op online werknemersfraude. Dit betreft het onderzoek van Othman en Ameer (2022). De studie van Othman en Ameer (2022) heeft aan de hand van het bestuderen van strafdossiers onderzocht hoe en waarom werknemers computertoegang gebruiken om fraude te plegen bij kleine bedrijven in Nieuw-Zeeland. De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 27 voor een overzicht van de relevante studie, en zie Tabel 28 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met online werknemersfraude.

Tabel 27.
De referentie en kwaliteitsboordeling van de relevante studie voor online werknemersfraude.

Referentie	Kwaliteit
(Othman & Ameer, 2022)	Hoog

Demografische kenmerken

Geslacht en werkpositie. De relatie tussen geslacht en werknemersfraude is niet geheel duidelijk. Uit het onderzoek van Othman en Ameer (2022) komt naar voren dat in de meeste gevallen (vrouwelijke) managers online werknemersfraude plegen (Othman & Ameer, 2022). Hogere functies bieden meer mogelijkheden voor fraude, omdat de verantwoordelijkheid en toegang tot middelen hierbij een belangrijke rol spelen (Othman & Ameer, 2022). Een gedeelte van eerder onderzoek laat daarentegen zien dat met name mannen online werknemersfraude plegen(Othman & Ameer, 2022).

Leeftijd. De relatie tussen leeftijd en online werknemersfraude is niet geheel duidelijk. Het onderzoek van Othman en Ameer (2022) laat zien dat medewerkers van rond de 48 jaar, die een senior functie van enige invloed bekleden, vaker medewerkersfraude plegen. Jongere werknemers, zowel in leidinggevende als niet-leidinggevende functies, hadden niettemin meer mogelijkheden tot fraude en veroorzaakten de grootste en langdurigste verliezen (Othman & Ameer, 2022). Jongeren worden als impulsiever beschouwd en hebben daardoor een grotere kans op het plegen van werknemersfraude (Othman & Ameer, 2022). Fraude gepleegd door managers duurde gemiddeld langer dan door niet-managers, wat vervolgens resulteerde in hogere verliezen (Othman & Ameer, 2022). Dit komt overeen met eerdere bevindingen dat een langere detectietijd leidt tot grotere schade (Othman & Ameer, 2022).

Intrinsieke en persoonlijkheidskenmerken

Ondeugd. In tegenstelling tot eerdere onderzoeken toonde de studie van Othman en Ameer (2022) aan dat ondeugd tot de belangrijkste motieven behoort om werknemersfraude te plegen. Dit sluit aan bij Nieuw-Zeelands onderzoek, waaruit blijkt dat gokken kan leiden tot crimineel

gedrag en het verwaarlozen van verantwoordelijkheden, evenals de gevolgen daarvan (Othman & Ameer, 2022).

Criminaliteit

Strafblad. Het lijkt erop dat de meeste oplichters van online werknemersfraude *first offenders* zijn (Othman & Ameer, 2022). Uit eerdere studies blijkt dat fraude vaak begint met kleine bedragen, zonder aanvankelijke criminele intentie (Othman & Ameer, 2022).

Routine activiteiten

Ongebruikelijk gedrag. Het onderzoek van Othman en Ameer (2022) laat zien dat sommige fraudeurs te zijn herkennen aan ongebruikelijk gedrag op de werkvloer. Ongebruikelijk gedrag, zoals lange werkuren en het weigeren van vakantiedagen, kan wijzen op fraude (Othman & Ameer, 2022). Hardwerken was een manier om afwijkend gedrag te camoufleren (Othman & Ameer, 2022). Verdachte patronen kunnen zich zowel op gedrags- als financieel vlak voordoen (Othman & Ameer, 2022).

Sociale relaties

Misbruik door familie. Het lijkt erop dat familiekwesties, zoals op jonge leeftijd fysiek en seksueel misbruikt te zijn geweest, verband te hebben met het plegen van online werknemersfraude (Othman & Ameer, 2022).

Neutralisatietechnieken

Rationalisaties. Fraudeurs lijken vaak hun daden te rechtvaardigen om schuldgevoelens te vermijden (Othman & Ameer, 2022). Dit lijkt vaker voor te komen bij managers dan niet-managers (Othman & Ameer, 2022).

Modus operandi

Salaristarieven manipuleren. De studie van Othman en Ameer (2022) wijst uit dat fraudeurs hun online computertoegang manipuleerden om hun eigen salaristarieven te verhogen, zonder dat de bedrijfseigenaren hiervan wisten (Othman & Ameer, 2022). Het vermogen om het uurtarief, de loonbetaling of de werkuren te wijzigen, wees erop dat de fraudeur toegang had tot systemen die uitsluitend voor de bedrijfseigenaar bedoeld zijn (Othman & Ameer, 2022).

Trends

Duur. Het onderzoek van Othman en Ameer (2022) laat zien dat werknemersfraude gemiddeld 25 maanden duurt.

Ongecontroleerde toegang. Het risico op online werknemersfraude lijkt groter te zijn wanneer een werknemer meer toegangsrechten heeft dan noodzakelijk is voor zijn of haar functie (Othman & Ameer, 2022). Dit geldt met name wat betreft toegang tot bankrekeningen en vertrouwelijke informatie (Othman & Ameer, 2022).

Preventiemaatregelen en vertrouwen. Resultaten uit het onderzoek van Othman en Ameer (2022) laten zien dat fraudepreventie de meest kosteneffectieve manier is om online werknemersfraude te bestrijden. Deze maatregelen zijn echter ineffectief op het moment dat controles, bijvoorbeeld van het verifiëren van leveringen, loonlijstgegevens of overuren, onzorgvuldig worden uitgevoerd en er teveel vertrouwen is in werknemers (Othman & Ameer, 2022). Kleine

bedrijven vertrouwen vaak te veel op sleutelwerknemers, wat kan leiden tot een gebrek aan toezicht (Othman & Ameer, 2022). Vertrouwen alleen is volgens Othman en Ameer (2022) geen effectieve manier om online werknemersfraude te voorkomen.

Toekomstig onderzoek

Meerdere landen. Het onderzoek van Othman en Ameer (2022) was gericht op het rechtsgebied van Nieuw-Zeeland. Daarom zijn volgens de auteurs de resultaten niet generaliseerbaar, omdat vergelijkbare zaken in andere landen anders kunnen worden behandeld door verschillende waarden en culturen (Othman & Ameer, 2022).

Sectorvergelijking. De bevindingen uit de studie van Othman en Ameer (2022) zijn beperkt tot de gevallen in de database, waardoor geen generalisaties naar andere werknemersfraudegevallen in Nieuw-Zeeland mogelijk zijn. Ook is het mogelijk dat veel fraudegevallen niet ontdekt of gemeld zijn (Othman & Ameer, 2022). Toekomstig onderzoek zou meer gevallen kunnen analyseren om sectorvergelijkingen en longitudinaal onderzoek mogelijk te maken (Othman & Ameer, 2022).

Interventies/trainingen

Slachtoffergericht

Audits. Audits worden als waardevolle detectiemethode beschouwd, waar zowel een preventieve als opsporende werking vanuit gaat (Othman & Ameer, 2022). Othman en Ameer (2022) geven hierbij wel aan dat door een audit nog steeds fraude over het hoofd kan worden zien en dat de kosten de voordelen ervan kan overtreffen (Othman & Ameer, 2022).

Het vier-ogen-principe. De studie van Othman en Ameer (2022) benadrukt dat hoewel voor kleine bedrijven audits vaak duur zijn, dat het toepassen van interne controleprincipes, zoals het vier-ogen-principe, kan helpen bij controles. Verdachte patronen en ongebruikelijke transacties zouden regelmatig moeten worden gecontroleerd (Othman & Ameer, 2022). Verder zouden leidinggevenden/eigenaren de enige personen moeten zijn die toegang hebben tot bedrijfsbankrekeningen of het beheren van elektronische betalingen (Othman & Ameer, 2022). Daarnaast zouden aankopen moeten worden goedgekeurd door de eigenaar of een onafhankelijke partij voordat ze plaatsvinden (Othman & Ameer, 2022). Tenslotte zouden betalingen aan leveranciers altijd moeten worden ondersteund door gecontroleerde documenten (Othman & Ameer, 2022).

Verplichte vakanties en functiewisselingen. Othman en Ameer (2022) betogen dat goedkope controlemaatregelen, zoals verplichte vakanties en functiewisselingen, effectief kunnen zijn bij het opsporen van online werknemersfraude, omdat fraude vaak ontdekt wordt wanneer medewerkers afwezig zijn.

Dadergericht

Achtergrondinformatie werknemer. Othman en Ameer (2022) stellen in hun onderzoek dat preventieve strategieën tegen online werknemersfraude zouden moeten beginnen voor indienstneming en tijdens het dienstverband. Achtergrondcontrole, zoals referenties opvragen bij vorige werkgevers, kan de kans op slachtofferschap verminderen (Othman & Ameer, 2022). Het risico op fraude lijkt immers toe te nemen wanneer personen met eerdere fraudeveroordelingen worden aangenomen (Othman & Ameer, 2022).

Afschrikking. Othman en Ameer (2022) stellen dat kleine bedrijven een sterke ethische cultuur kunnen opbouwen door duidelijk te communiceren met het personeel over de verwachte

waarden van werknemers. De grootste afschrikking tegen online werknemersfraude is de angst voor sociale en informele sancties en de overtuiging dat onethisch gedrag niet wordt getolereerd (Othman & Ameer, 2022). Eigenaren zouden volgen de auteurs het goede voorbeeld moeten geven, en moeten worden aangemoedigd om fraudeurs bij de autoriteiten aan te geven (Othman & Ameer, 2022)

Tabel 28. Samenvatting resultaten van de literatuur over online werknemersfraude.

Demografische kenmerken	Intrinsieke en persoonlijkheidskenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macrofactoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
Geslacht en werkpositie	Ondeugd	Ongebruikelijke gedrag	Misbruik door familie	-	Rationalisaties	Salaris-tarieven manipuleren	Duur	Meerdere landen	Audits
Leeftijd	Strafblad						Ongecontroleerde toegang	Sectorvergelijking	Het vier-ogen-principe
							Preventiemaatregelen en vertrouwen		Verplichte vakanties en functiewisselingen
									Achtergrondinformatie werknemer
									Afschrikking
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		***Grijs** = neutrale factor*	

3.1.14. Online bankpasfraude

Introductie

Wetenschappelijke literatuur

Online bankpasfraude is een vorm van identiteitsdiefstal waarbij de creditcardgegevens van een ander zonder toestemming worden overgenomen om aankopen op de rekening te boeken of er geld van af te halen (Nguyen & Luong, 2021, p. 422). In totaal zijn er twee studie geïdentificeerd die specifiek betrekking hebben op bankpasfraude. Dit betreft het onderzoek van Nguyen en Luong (2021) en Van Nguyen (2022). Het onderzoek van Nguyen en Luong (2021) heeft op basis van een sociale netwerkanalyse – gecombineerd met data van criminele profielen en interviews met de politie – de structuur van online fraudenetwerken (d.w.z. bankpasfraude en vishing) in Vietnam onderzocht. Het onderzoek is met een gemiddelde kwaliteitsscore beoordeeld. De studie van Van Nguyen (2022) onderzocht bankpasfraude en vishing in Vietnam om meer inzicht te krijgen in hoe deze vormen van online fraude in de Vietnamese context plaatsvinden. Dit werd geanalyseerd aan de hand van crime script analysis, gebaseerd op 20 casestudies en interviews met 14 cyberpolitieagenten, waarbij drie fasen werden geïdentificeerd: voorbereiding, activiteit en na-activiteit (Van Nguyen, 2022). De studie is met een gemiddelde kwaliteitsscore beoordeeld. Zie Tabel 29 voor een overzicht van de relevante studie, en zie Tabel 30 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met online bankpasfraude.

Tabel 29.
De referenties en kwaliteitsboordeling van de relevante studies voor online bankpasfraude.

Referentie	Kwaliteit
(Nguyen & Luong, 2021)	Gemiddeld
(Van Nguyen, 2022)	Gemiddeld

Motieven

Financieel gewin. Uit het onderzoek van Nguyen en Luong (2021) komt naar voren dat criminelen die onderdeel uitmaken van een netwerk uitsluitend zijn gericht op financieel gewin en niet worden gestuurd door ideologische, politieke of ethische overtuigingen.

Modus operandi

Aankopen bankkaartgegevens. De studie van Van Nguyen (2022) wijst uit veel cybercriminelen in Vietnam bankpasgegevens kopen van vertrouwde leveranciers op hackingforums. Betalingen worden meestal verricht via digitale diensten, zoals PayPal of bankoverschrijvingen (Van Nguyen, 2022). Verder gebruiken de meeste fraudeurs software zoals QQ voor communicatie met anderen om de gegevens te verkrijgen, waarbij aanbieders van deze gegevens veelal 40% van de opbrengsten krijgen (Van Nguyen, 2022).

Directe interactie. Bankkaartfraude vereist geen directe interactie omdat technologie, zoals skimming en online aankopen, de fraude automatiseert (Van Nguyen, 2022).

Fases. Uit de studie van Van Nguyen (2022) blijkt dat, nadat slachtoffers geld hadden overgemaakt, het snel werd opgenomen door geldezels of via tussenpersonen naar de leiders werd doorgestuurd. In Vietnam gebeurde dit proces soms door het geld via verschillende bankrekeningen te verplaatsen of via goudwinkels (Van Nguyen, 2022). Vietnamese criminelen gebruiken

gestolen betaalkaartgegevens om dure, lichtgewicht producten op Amerikaanse websites, zoals Amazon en eBay, te kopen. Ze verdoezelen hun IP-adressen, betalen met gestolen kaarten en sturen de producten via logistieke bedrijven naar Vietnam (Van Nguyen, 2022). Buitenlandse helpers, zoals 'shipping mules', verpakken de goederen voordat ze werden doorgestuurd (Van Nguyen, 2022, p. 237). Soms helpen vrienden of familie bij het transport (Van Nguyen, 2022). Daarnaast schaffen fraudeurs ook software en domeinnamen aan met de gestolen passen (Van Nguyen, 2022).

Geldezels. In netwerken voor bankpasfraude spelen geldezels een cruciale rol door producten, gekocht met gestolen creditcards, te ontvangen en door te sturen naar de *kernleden* (d.w.z. degene die criminele activiteiten aansturen) (Van Nguyen, 2022). Het gebruik van geldezels maakt het voor opsporingsdiensten moeilijker om deze criminelen op te pakken (Van Nguyen, 2022). Cybercriminelen hebben vaak moeite om voldoende actieve geldezels te vinden en zetten daarom diverse rekruteringsmethoden in, zoals via online forums of (offline) sociale netwerken (Van Nguyen, 2022).

Netwerk. Het netwerk van online aankopen bestaat uit verschillende subnetwerken die draaien om een hoofdcrimineel (Nguyen & Luong, 2021). Kernleden werken samen met ondersteunende actoren, zoals hackers en gelezels, bij het uitwisselen van bankkaartgegevens, hackingtools en geldezels (Nguyen & Luong, 2021). De leiderschapsrol binnen online aankoopnetwerken is vaak onduidelijk (Nguyen & Luong, 2021). Er is vaak een platte structuur zonder duidelijke hiërarchie waarbij de leiderschapsrol flexibel kan. Dit betekent dat één lid meerdere posities kan bekleden (Nguyen & Luong, 2021). Relaties binnen online aankoopnetwerken zijn doorgaans los van aard en er is weinig offline interactie (Nguyen & Luong, 2021). Virtuele fora dienen als plaatsen waar criminelen informatie en tools kunnen uitwisselen en netwerken opbouwen voor fraude (Nguyen & Luong, 2021). Leden communiceren via fora, e-mail en chatrooms, en kernactoren verdelen financiële voordelen via digitale betalingen (Nguyen & Luong, 2021). In de beginfase functioneren de forums als zwermgroepen, waarbij cybercriminelen vrij informatie en gestolen gegevens uitwisselen (Nguyen & Luong, 2021). Na verloop van tijd ontstaat er meer een hierarchische structuur, wat de forums meer doet lijken op traditionele criminele groepen (Nguyen & Luong, 2021). Netwerken die vervalste kaarten maken, vertonen meer offline activiteiten en hebben een duidelijkere leiderschapsstructuur dan online aankoopnetwerken (Nguyen & Luong, 2021). Offline ontmoetingen leiden tot hechtere netwerken met nauwere relaties in kleinere groepen (Nguyen & Luong, 2021). Deze netwerken kennen een centrale actor die de rol van kernlid (die de activiteiten leidt) of enabler vervult (die diensten zoals hacktools leveren) (Nguyen & Luong, 2021; Van Nguyen, 2022).

Skimming. Uit de studie van Van Nguyen (2022) komt naar voren dat fraudeurs apparaten gebruiken om bankpasgegevens te stelen bij geldautomaten, zoals in Vietnam waar Chinese fraudeurs skimmingapparaten installeerden (Van Nguyen, 2022). Bankpasgegevens worden gebruikt om valse magneetstripkaarten te maken, die vervolgens werden gebruikt voor geldopnames bij pinautomaten of voor nepaankopen bij betaalterminals. Geldopnames werden vaak 's avond laat of uitgevoerd om detectie door slachtoffers of autoriteiten te voorkomen (Van Nguyen, 2022). Kortom, Zodra oplichters de bankpasgegevens hebben bemachtigd, stelen ze geld door middel van verschillende carding-methodes: online aankopen, frauduleuze aankopen in winkels of het klonen van kaarten om geld op te kunnen nemen bij geldautomaten (Van Nguyen, 2022).

Software voor transacties. In het onderzoek van Van Nguyen (2022) wordt er geconstateerd dat criminelen software gebruiken om valse transacties uit te voeren, vaak met gestolen e-

mailaccounts en vervalste kaarten. Ze stelen geld via online aankopen, geldautomaten of betaalterminals (Van Nguyen, 2022).

SQL-injectie. Hackers gebruiken technieken zoals *SQL-injectie* (= een type beveiligingslek waarbij een aanvaller kwaadaardige SQL-code invoegt in een invoerveld) om toegang te krijgen tot bankpasgegevens op buitenlandse e-commercewebsites, inclusief kaartnummers, vervaldatums en persoonlijke gegevens (Van Nguyen, 2022).

Verbergen identiteit. De studie van Van Nguyen (2022) laat zien dat fraudeurs verschillende methodes gebruiken om detectie door wetshandhavers te voorkomen. Ze verbergen hun echte IP-adressen met nep-IP-software of VPN's, of gebruiken gestolen e-mailaccounts voor transacties (Van Nguyen, 2022).

Vluchtgedrag. Van Nguyen (2022) constateerde in zijn onderzoek dat bij online aankopen fraudeurs alleen vluchtten bij vermoedens van ontdekking, terwijl kaartvervalsers na geldopnames al direct vertrokken. Chinese netwerken opereerden mobiel, verhuisden vaak tussen steden en bleven slechts enkele dagen per locatie (Van Nguyen, 2022). Andere fraudeurs verbleven enkele maanden op dezelfde plek, waarna ze verder trokken om opnieuw te frauderen (Van Nguyen, 2022). Geldezels bleven meestal in één gebied en vluchtten bij verdenking van onderzoek door opsporingsdiensten (Van Nguyen, 2022).

Interventies/trainingen

Slachtoffergericht

Bewustwording. Volgens Van Nguyen (2022) moeten strategieën zich richten vergroten van het bewustzijn bij mensen, omdat iedereen in potentie slachtoffer kan worden.

Samenwerking. Van Nguyen (2022) stelt dat het grensoverschrijdende karakter van online criminaliteit internationale samenwerking vereist tussen opsporingsdiensten om bankpasfraude effectief aan te kunnen pakken (Van Nguyen, 2022).

Dadergericht

Bewustwording. Bewustwordingscampagnes moet volgens Van Nguyen (2022) gericht zijn op het voorkomen van de rekrutering van geldezels.

Tabel 30. Samenvatting resultaten van de literatuur over online bankpasfraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	Financieel gewin	Aankopen bankkaartgegevens Directe interactie Fases Geldezels Netwerk Skimming Software voor transacties SQL-injectie Verbergen identiteit Vluchtgedrag	-	-	Bewustwording Samenwerking Bewustwording (dader)

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.15. Social engineering

Introductie

Wetenschappelijke literatuur

Social engineering refereert aan het manipuleren van mensen door middel van bedrog om toegang te krijgen tot gevoelige informatie of beveiligde systemen (Steinmetz et al., 2021, p. 1). Dit kan verschillende vormen aannemen, zoals phishing (e-mailfraude), smishing (sms-fraude), spear-phishing (gerichte e-mailfraude), vishing (telefonische fraude) en bedrog in persoon (Steinmetz et al., 2021, p. 1). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op *social engineering*. Dit betreft het onderzoek van Steinmetz en collega's (2021). (Steinmetz et al., 2021). De studie van Steinmetz en collega's (2021) bestudeert middels interviews met social engineers welke eigenschappen zij koppelen aan succesvolle misleidingen. De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 31 voor een overzicht van de relevante studie, en zie Tabel 32 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met social engineering.

Tabel 31.
De referentie en kwaliteitsboordeling van de relevante studie voor social engineering.

Referentie	Kwaliteit
(Steinmetz et al., 2021)	Hoog

Modus operandi

Gedrag afstemmen. Uit de studie van Steinmetz en collega's (2021) komt naar voren dat sociale ingenieurs in staat moeten zijn om de emoties, lichaamstaal en reacties van hun doelwit te lezen en hun benadering daarop aan te passen. Als het slachtoffer weerstand biedt of het gesprek afbreekt, kunnen social engineers volhouden of wachten tot de situatie is gekalmeerd voordat ze opnieuw proberen het slachtoffer proberen te misleiden (Steinmetz et al., 2021).

Normaal overkomen. Het lijkt erop dat social engineers proberen om zo normaal en alledaagse mogelijk over te komen om geen argwaan te creëren bij het slachtoffer (Steinmetz et al., 2021).

Overtuigend profiel. Sociale lijken hun persoonlijke eigenschappen en ervaringen te evalueren om een overtuigend (fictief) overkomen te creëren (Steinmetz et al., 2021). Dit omvat onder andere relevante ervaringen (bijv. IT-ervaring), fysieke kenmerken (zoals leeftijd of aantrekkelijkheid) en het gebruik van gebruik van stereotypen (bijv. het spelen van een hulpeloze dame in nood) (Steinmetz et al., 2021). Ze passen hun aanpak aan op basis van deze factoren en maken strategisch gebruik van stereotypen en sociale percepties om effectief te misleiden (Steinmetz et al., 2021). Bij digitale of telefonische fraude zijn fysieke beperkingen minder relevant, maar stereotypen kunnen zowel online als persoonlijk worden gebruikt om doelwitten te beïnvloeden (Steinmetz et al., 2021).

Realistisch scenario schetsen. Het lijkt erop dat social engineers realistische en geloofwaardige scenario's bedenken door zich in een rol te verplaatsen, met een passend verhaal, relevante vaardigheden en vakjargon (Steinmetz et al., 2021). Daarbij speelt controle hebben over lichaamstaal en gezichtsuitdrukkingen een belangrijke rol om argwaan bij het slachtoffer te voorkomen (Steinmetz et al., 2021).

Snel en eenvoudig. Voor succesvolle sociale manipulatie blijkt uit de studie Steinmetz en collega's (2021) dat snelheid en eenvoud cruciaal zijn. De interacties moeten snel en zonder complicaties verlopen, zodat het slachtoffer geen tijd heeft om de situatie te analyseren of de misleiding te doorzien (Steinmetz et al., 2021). De social engineer moet hierbij een evenwicht vinden: de interactie mag niet te snel verlopen om argwaan te vermijden, maar ook niet te ingewikkeld, zodat het slachtoffer niet te veel gaat nadenken (Steinmetz et al., 2021).

Sociale norm. Uit de studie van Steinmetz en collega's (2021) komt naar voren dat criminelen zich bewust zijn van de sociale normen en verwachtingen om de interactie soepel en overtuigend te laten verlopen (Steinmetz et al., 2021).

Technologie. Uit de studie van Steinmetz en collega's (2021) komt naar voren dat technologie een dubbele rol speelt bij social engineering: het biedt middelen om informatie te verzamelen die de misleiding ondersteunt, maar fungeert ook als einddoel, zoals het verleiden van een slachtoffer tot het klikken op een schadelijke link of het downloaden van een bijlage (Steinmetz et al., 2021).

Timing. Timing lijkt essentieel te zijn voor het succes van social engineering. De tijd van het jaar, het tijdstip van de dag en actuele gebeurtenissen kunnen van invloed zijn op het succes van de oplichting (Steinmetz et al., 2021). Tijdens feestdagen kunnen bijvoorbeeld gevoelens van vrijgevigheid worden benut (Steinmetz et al., 2021). Het vermijden van specifieke momenten, zoals lunch of de ochtend, kan ook de effectiviteit verhogen, aangezien mensen op die momenten dan vaak minder aandacht besteden aan e-mails (Steinmetz et al., 2021).

Misleidingstechnieken

Authenticiteit. Het onderzoek van Steinmetz en collega's (2021) beschrijft hoe cybrcriminelen authenticiteit creëren om het vertrouwen van hun doelwitten te winnen. Dit wordt bereikt door (1) een geloofwaardige indruk te maken (d.w.z. achtergrondverhaal, consistentie pretext en beheersen van jargon), (2) angstige signalen te vermijden, zoals lichaamstaal en gezichtsuitdrukking, omdat deze van invloed zijn op de geloofwaardigheid, (3) sociale normen en scripts te volgen want dat voorkomt argwaan, (4) gebruik te maken van visuele hulpmiddelen zoals kostuums of nepidentificaties, en (5) technologische manipulatie door bijvoorbeeld telefoonnummers te *spoofen* of phishing e-mails geloofwaardig te maken (Steinmetz et al., 2021).

Autoriteit. Het lijkt erop dat social engineers sociale netwerken en vertrouwensrelaties gebruiken om vertrouwen te winnen en misleidende doelen te bereiken (Steinmetz et al., 2021). Ze doen vooraf onderzoek om zichzelf strategisch in het netwerk van hun doelwit te plaatsen en maken gebruik van 'transitief vertrouwen' door zich voor te doen als een vertrouwde derde partij (Steinmetz et al., 2021). Ze kunnen ook toegang krijgen tot fysieke locaties met nep-identificatie of via sociale media en nepprofielen (Steinmetz et al., 2021). Het risico bestaat wel dat de oplichting wordt ontdekt als het doelwit de persoon of organisatie goed kent (Steinmetz et al., 2021).

Beloning en behulpzaam zijn. Het lijkt erop social engineers proberen het doelwit te motiveren door kleine beloningen aan te bieden, zoals een cadeaubon van 10 dollar (Steinmetz et al., 2021). Het doel is om het slachtoffer te motiveren tot actie zodat het geen wantrouwen oproept (Steinmetz et al., 2021). Een te grote beloning, zoals een cadeaubon van honderd dollar, is onrealistisch en wekt wantrouwen op (Steinmetz et al., 2021). Kortom, de prikkel moet groot genoeg zijn om te overtuigen, maar niet te groot om argwaan op te roepen (Steinmetz et al., 2021).

Urgentie en druk. Een andere tactiek die social engineers gebruiken is het onder druk zetten van het slachtoffer door urgente en emotioneel beladen verhalen te verzinnen (Steinmetz et al.,

2021). Dit kan het slachtoffer ertoe brengen om snel te handelen zonder er goed erover te kunnen nadenken (Steinmetz et al., 2021). Daarbij kan het verstrekken van een overvloed aan informatie de focus van het slachtoffer afleiden, waardoor het doelwit minder kritisch wordt (Steinmetz et al., 2021).

Toekomstig onderzoek

Demografische factoren. Toekomstig onderzoek zou volgens Steinmetz en collega's (2021) zich moeten richten op de demografische factoren van slachtoffers, zoals leeftijd en geslacht, en hoe deze invloed hebben op hun vatbaarheid voor fraude - vooral wanneer deze kenmerken zichtbaar zijn tijdens interacties. Volgens de auteurs moet er ook onderzocht worden welke rol de eigenschappen van de dader, zoals geslacht, leeftijd en vaardigheden, in het social engineering proces spelen en hoe deze factoren het succes van bedrog beïnvloeden (Steinmetz et al., 2021).

Modus operandi en detectiemechanismen. Toekomstig onderzoek zou kunnen verkennen hoe sociale ingenieurs hun technieken aanpassen om detectie te voorkomen en hoe verschillende detectiemechanismen daadwerkelijk functioneren in realistische situaties (Steinmetz et al., 2021).

Motivatie. Onderzoek zou moeten verkennen hoe de motivatie van de dader, zoals het streven naar financiële winst of de uitdaging, de uitvoering van sociale engineeringdecepties beïnvloedt (Steinmetz et al., 2021). Daarnaast zou het moeten onderzoeken of daders met andere motivaties, zoals persoonlijke expressie, verschillende strategieën hanteren dan diegene die primair gericht zijn op financieel gewin (Steinmetz et al., 2021).

Psychologische en sociale mechanismen van slachtoffers. Toekomstig onderzoek kan zich ook richten op het verder begrijpen van de psychologische en sociale mechanismen die slachtoffers gebruiken om bedrog te herkennen, inclusief de specifieke ‘uncovering moves’ die ze toepassen (Steinmetz et al., 2021, p. 10).

Tabel 32. Samenvatting resultaten van de literatuur over social engineering.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	Gedrag afstemmen Normaal overkomen Overtuigend profiel Realistisch scenario schetsen Snel en eenvoudig Sociale norm Technologie Timing Authenticiteit Autoriteit Beloning en behulpzaam zijn Urgentie en druk	-	Demografische factoren Modus operandi en detectie-mechanismen Motivatie Psychologische en sociale mechanismen van slachtoffers	-

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.16. Geldezels

Introductie

Wetenschappelijke literatuur

Geldezels, ofwel money mules of katvangers, worden door cybercriminelen gebruikt om het spoor tussen slachtoffers en criminelen te verdoezelen, waardoor het voor wetshandhavingsinstanties moeilijker wordt om mensen achter de criminele netwerken op te sporen (Bekkers & Leukfeldt, 2023). Bij verschillende vormen van fraude worden gelden overgeboekt van de bankrekeningen van slachtoffers naar de bankrekeningen van geldezels (Bekkers & Leukfeldt, 2023, p. 604). Vervolgens wordt zo snel mogelijk het geld opgenomen bij geldautomaten of gebruikt om goederen te kopen (Bekkers & Leukfeldt, 2023, p. 604). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op money mules. Dit betreft het onderzoek van Bekkers en Leukfeldt (2023). De onderzoekers hebben Instagram-accounts en -post, gericht op rekruteren van geldezels, onderzocht om een beter begrip te krijgen van de online rekruteringsprocessen van geldezels (Bekkers & Leukfeldt, 2023). De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 33 voor een overzicht van de relevante studie, en zie Tabel 34 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met geldezels .

Tabel 33.
De referentie en kwaliteitsboordeling van de relevante studie voor money mules.

Referentie	Kwaliteit
(Bekkers & Leukfeldt, 2023)	Hoog

Modus operandi

Gesloten netwerken. Meer dan een derde van de onderzochte accounts in de studie van Bekkers en Leukfeldt (2023) was afgeschermd, wat suggereert dat dergelijke activiteiten plaatsvinden binnen besloten netwerken. Toegang lijkt afhankelijk te zijn van bestaande connecties, vergelijkbaar met traditioneel criminele structuren (Bekkers & Leukfeldt, 2023).

Instagram. Criminelen gebruiken Instagram als een anoniem en laagdrempelig platform om geldezels te rekruteren. Bekkers en Leukfeldt (2023) constateren dat de visuele en tekstuele elementen van criminele accounts sterk variëren. Er zijn Instagram-accounts die slechts eenvoudige beelden tonen van geld tot aan professionele strategieën met uiteenlopend taalgebruik en emoticons (Bekkers & Leukfeldt, 2023). Opvallend is dat meer dan de helft van de onderzochte accounts weinig tot geen activiteit vertoonde, wat volgens de auteurs suggereert dat actieve werving vaak niet nodig is omdat potentiële geldezels zelf contact zoeken via verhalen en netwerken (Bekkers & Leukfeldt, 2023). De digitale structuur van Instagram biedt criminelen daarmee eenvoudige en toegankelijke mogelijkheden voor online rekrutering (Bekkers & Leukfeldt, 2023).

Misbruik financiële problemen. Uit het onderzoek van Bekkers en Leukfeldt (2023) blijkt financiële problemen soms door criminelen werden misbruikt om slachtoffers te lokken. Zo lijken geldezels zich doorgaans bewust te zijn van de illegaliteit ervan, maar zijn ze bereid om dit te accepteren zolang er een financiële beloning tegenover staat (Bekkers & Leukfeldt, 2023).

Neutralisatie- en normalisatietechnieken. Daders maken bij het rekruteren van geldezels vaak gebruik van neutralisatietechnieken om de morele drempel te verlagen en de bereidheid tot medewerking te vergroten (Bekkers & Leukfeldt, 2023). Er wordt bijvoorbeeld benadrukt dat het

verdienen van geld via deze praktijken volledig risicoloos is en of dat dergelijke activiteiten legaal zijn, zonder dat verdere uitleg of onderbouwing wordt gegeven (Bekkers & Leukfeldt, 2023). Daders delen succesverhalen, zoals screenshots van bankoverschrijvingen en chatgesprekken met tevreden 'klanten', om de indruk te wekken dat deze activiteiten winstgevend en betrouwbaar zijn (Bekkers & Leukfeldt, 2023). Verder laat de studie zien dat het aanbieden van bankpassen worden gepresenteerd als legitiem werk door termen te gebruiken zoals "werk," 'werknemers', en 'klanten' (Bekkers & Leukfeldt, 2023). Sommige wervers onderscheiden zich bovendien door zichzelf te profileren als eerlijker of betrouwbaarder dan hun concurrenten (Bekkers & Leukfeldt, 2023).

Presenteren als reguliere bedrijven. Sommige rekruteerders/daders presenteren zichzelf als reguliere bedrijven en gebruiken strategieën die lijken op online vacaturecampagnes (Bekkers & Leukfeldt, 2023).

Privé-chats. Privé-chats lijken een essentiële rol te spelen bij het overdragen van bankpassen en rekeningen aan criminelen (Bekkers & Leukfeldt, 2023). Volgens de auteurs blijft het echter onduidelijk hoeveel geldezels daadwerkelijk reageren en waarom sommige accounts succesvoller zijn in rekruteren dan andere (Bekkers & Leukfeldt, 2023).

Regionale gerichtheid. Bekkers en Leukfeldt (2023) constateren dat rekruteerders zich vaak richten op specifieke doelgroepen op basis van leeftijd of locatie, vanwege waarschijnlijk praktische redenen als hogere banklimieten en nabijheid. Dit suggereert volgens de auteurs dat lokale criminele netwerken online platforms gebruiken om mensen in hun regio te bereiken (Bekkers & Leukfeldt, 2023).

Trends

Subcultuur. Het lijkt erop dat er een subcultuur is rondom money muling, waarbij straattaal en afbeeldingen van grote hoeveelheden contant geld, luxe goederen en rappers worden gebruikt om een luxe levensstijl te verkopen en deze praktijken te normaliseren (Bekkers & Leukfeldt, 2023).

Interventies/trainingen

Slachtoffergericht

Bewustwording. Hoewel uit de studie van Bekkers en Leukfeldt (2023) blijkt dat neutralisatietechnieken op Instagram nauwelijks voorkwamen, kan niettemin bewustmaking van de gevolgen voor slachtoffers volgens de auteurs helpen om de excuses van daders te doorbreken.

Peer pressure en subculturele normen. Peer pressure en subculturele normen kunnen worden beïnvloed door positieve alternatieven, zoals schuldhulp of legaal werk, te bevorderen (Bekkers & Leukfeldt, 2023).

Voorlichting. Bekkers en Leukfeldt (2023) geven aan dat het belangrijk is om potentiële geldezels voor te lichten over de risico's van snel geld verdienen en het proces van money muling om deze groep minder kwetsbaar te maken voor rekruteerders (Bekkers & Leukfeldt, 2023). Ook zou het benadrukken van de risico's en het feit dat de beloofde beloning vaak uitblijft de aantrekkingskracht kunnen verminderen (Bekkers & Leukfeldt, 2023).

Dadergericht

Accounts blokkeren. Toegang tot rekruteringsaccounts kan worden belemmerd door strengere toegangscontrole of het vroegtijdig blokkeren van accounts (Bekkers & Leukfeldt, 2023). Social media-platforms kunnen ook zoekwoorden blokkeren en strengere contentregels invoeren (Bekkers & Leukfeldt, 2023). Administrators kunnen het moeilijker maken om geldezel accounts te vinden door relevante zoekwoorden te blokkeren en nieuwe gebruikers strengere regels op te leggen (Bekkers & Leukfeldt, 2023).

Anonimiteit verminderen. Anonimiteit kan volgens Bekkers en Leukfeldt (2023) worden verminderd door strengere registratie-eisen voor sociale media in te stellen.

Monitoren en waarschuwingen. Bekkers en Leukfeldt (2023) stellen dat de politie social media-platformen actief zouden moeten monitoren om criminelen en bezoekers van rekruteringsaccounts te waarschuwen dat ze onder toezicht staan. Openbare waarschuwingen over de gevolgen van deelname aan criminele netwerken kunnen preventief werken en potentiële geldezels ervan bewust maken dat hun persoonlijke gegevens uiteindelijk door de wetshandhaving worden achterhaald (Bekkers & Leukfeldt, 2023). Verder kunnen algoritmes worden gebruikt om verdachte accounts op te sporen en gebruikers aan te moedigen om verdachte activiteiten te melden (Bekkers & Leukfeldt, 2023).

Tabel 34. Samenvatting resultaten van de literatuur over money mules.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	Misbruik financiele problemen Gesloten netwerken Neutralisatie- en normalisatie-technieken Instagram Presenteren als reguliere bedrijven Privé-chats Regionale gerichtheid	Subcultuur	-	Bewustwording Peer pressure en subculturele normen Voorlichting Accounts blokkeren Anonimiteit verminderen Monitoren en waarschuwingen

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

3.1.17. Bitcoin-gerelateerde online criminaliteit

Introductie

Wetenschappelijke literatuur

Bitcoin gerelateerde online criminaliteit betreffen onder andere blackmail, sextortion en ramsomware waarbij betalingen via Bitcoin plaatsvinden (Buil-Gil et al., 2021). In totaal is er **één studie** geïdentificeerd die specifiek betrekking heeft op bitcoin-gerelateerde online criminaliteit. Een bitcoin-gebruiker kan een wallet aanmaken en onbeperkt adressen genereren om transacties uit te voeren (Buil-Gil et al., 2021). Wallets beheren alleen de sleutels voor toegang tot adressen, waardoor één gebruiker meerdere adressen en wallets kan beheren (Buil-Gil et al., 2021). Dit betreft het onderzoek van Buil-Gil en collega's (2021). Het onderzoek van Buil-Gil en collega's (2021) analyseerde 186.735 meldingen van Bitcoin-gerelateerde online criminaliteit (d.w.z. blackmail, ransomware, sextortion, darknet-marktfraude, Bitcoin-tumblerfraude) om de mate van concentratie van cybercrimineel gedrag te onderzoeken en groepen daders te identificeren die betrokken zijn bij deze online misdrijven. De kwaliteit van deze studie is als hoog beoordeeld. Zie Tabel 35 voor een overzicht van de relevante studie, en zie Tabel 36 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met bitcoin gerelateerde online criminaliteit.

Tabel 35.
De referentie en kwaliteitsboordeling van de relevante studie voor bitcoin gerelateerde online criminaliteit.

Referentie	Kwaliteit
(Buil-Gil et al., 2021)	Hoog

Trends

Concentratie criminaliteit. Het lijkt erop dat bitcoin-gerelateerde online criminaliteit sterk is geconcentreerd. Uit de studie van Buil-Gil en collega's (2021) blijkt dat een klein aantal adressen verantwoordelijk is voor een groot deel van de misdaden. Het internet vergroot de rijkwijdte van criminaliteit aanzienlijk, waardoor één dader in korte tijd veel slachtoffers kan bereiken (Buil-Gil et al., 2021). Bovendien zorgt de complexiteit van Bitcoin-gerelateerde cybercriminaliteit ervoor dat technisch bekwame daders langdurig en onopgemerkt actief kunnen blijven (Buil-Gil et al., 2021). Verder lijkt online criminaliteit variërende concentratiepatronen te tonen die afhankelijk zijn van het type misdaad (Buil-Gil et al., 2021). Misdrijven (bijv. ransomware en sextortion) gericht op gebruikers van veelgebruikte diensten, zoals e-mail en sociale media, concentreren zich sterk op enkele Bitcoin-adressen vanwege hun schaalbaarheid en brede bereik (Buil-Gil et al., 2021). Daarentegen zijn misdaden via minder gangbare diensten, zoals darknetmarkten, minder geconcentreerd door hun één-op-één interacties (Buil-Gil et al., 2021). Bitcoin-adressen met veel meldingen zijn vaak betrokken bij grootschalige, eenvoudige aanvallen, zoals afpersing, fraude en witwassen (Buil-Gil et al., 2021). Bitcoin-adressen met grote transacties kunnen diverse criminele activiteiten omvatten, terwijl accounts met weinig meldingen en grotere transactievolumes vaak individuen betreffen die Bitcoins voor persoonlijk gewin bewaren (Buil-Gil et al., 2021).

Toekomstig onderzoek

Methode en data-analyse. Volgens Buil-Gil en collega's (2021) zou toekomstig onderzoek moeten vaststellen welke Bitcoin-adressen betrokken zijn bij criminaliteit. Dit kan worden bereikt door technieken zoals sociale netwerkanalyse en blockchain-tracking te gebruiken om de verplaatsing van criminele opbrengsten tussen adressen te volgen (Buil-Gil et al., 2021).

Trainingen/interventies

Slachtoffergericht

Bewustwording. Bewustwordingscampagnes moeten volgens Buil-Gil en collega's (2021) slachtoffers leren hoe ze aanvallen kunnen voorkomen en adequaat moeten reageren op ransomware of afpersing via e-mail (Buil-Gil et al., 2021).

Dadergericht

Detectie. Het combineren van misdaadrapporten met openbare blockchain-data zou kunnen helpen om bitcoin-adressen die mogelijk betrokken zijn bij uiteenlopende criminele activiteiten te kunnen identificeren (Buil-Gil et al., 2021). Daarnaast stellen de auteurs dat door te onderzoeken hoe cybercriminelen zich specialiseren, beleidsmaatregelen ontwikkeld kunnen worden die effectiever zijn in het identificeren van criminelen die steeds dezelfde misdrijven plegen (Buil-Gil et al., 2021).

Tabel 36. Samenvatting resultaten van de literatuur over bitcoin-gerelateerde online criminaliteit.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidings-technieken	Trends	Toekomstig onderzoek	Interventies/ trainingen (slachtoffer / dader)
-	-	-	-	-	-	-	Concentratie criminaliteit	Methode en data-analyse	Bewustwording Detectie
	Legenda	***Groen** = positieve relatie*	***Rood** = negatieve relatie*	***Blauw** = ambigue relatie*	***Grijs** = neutrale factor*				

3.1.18. Overige vormen van online criminaliteit

BEC-fraude

Bij *Business Email Compromise* (BEC)-fraude omvat het imiteren van e-mailadressen van leidinggevenden, medewerkers of zakenpartners, door middel van hacking of e-mailspoofing (Abubakari & Amponsah, 2024). Met deze vervalste e-mails worden financiële overboekingen aangevraagd, vaak met vervalste machtigingsbrieven en handtekeningen (Abubakari & Amponsah, 2024). In totaal zijn er twee studies geïdentificeerd die specifiek betrekking hebben op BEC-fraude. Dit betreffen de onderzoeken van Abubakari en Amponsah (2024) en Cross (2022).

Cross (2022) heeft via een niet-systematische review geschetst wat er momenteel bekend is van online fraude, waaronderdatingfraude , omtrent de gehanteerde modus operandi van daders en effectieve interventies om fraude te bestrijden. De studie is met een lage kwaliteitsscore beoordeeld.

De studie van Abubakari en Amponsah (2024) onderzocht op basis van een documentenanalyse misleidingsstrategieën en rollen die Ghanese diasporagroepen in de VS innemen bij verschillende vormen van online criminaliteit. Dit onderzoek kent een lage kwaliteitsscore. Zie Tabel 37 voor een overzicht van de relevante studies, en zie Tabel 38 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met BEC-fraude.

Computer-gerelateerde cybercriminaliteit (computer)

De belangrijkste vormen van *computer-gerelateerde cybercriminaliteit* zijn cybertransacties en cyberfinanciering (Lee et al., 2023, p. 2). Bij een cybertransactie kan een crimineel proberen winst te maken uit nepverkopen (Lee et al., 2023, p. 2). Wat betreft cyberfinanciering kan een crimineel proberen een microbetaling te doen door de mobiele telefoongegevens van het slachtoffer te gebruiken zonder toestemming (Lee et al., 2023, p. 2). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op computer-gerelateerde cybercriminaliteit. Dit betreft het onderzoek van Lee en collega's (2023).

Lee en collega's (2023) hebben middels het interviewen van politie rechercheurs criminele factoren voor verschillende vormen van online criminaliteit onderzocht om vervolgens met suggesties te komen voor preventieve maatregelen. De kwaliteit van dit onderzoek is als hoog beoordeeld. Zie Tabel 37 voor een overzicht van de relevante studie, en zie Tabel 39 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met computer-gerelateerde cybercriminaliteit.

Content-gerelateerde cybercriminaliteit (content)

De belangrijkste vormen van *content-gerelateerde cybercriminaliteit* zijn cyberstalking, en cyberbelediging en -laster (Lee et al., 2023, p. 2). Bij cyberstalking kan een crimineel proberen een slachtoffer te bombarderen met kwaadaardige berichten (Lee et al., 2023, p. 2). Wat betreft cyberlaster en -beledigingen kan een crimineel proberen kwaadaardige opmerkingen over een slachtoffer te plaatsen op online bulletinboards (Lee et al., 2023, p. 2). In deze studie analyseren en vergelijken we de criminele factoren die betrokken zijn bij deze drie soorten cybercriminaliteit (Lee et al., 2023, p. 2). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op content-gerelateerde cybercriminaliteit. Dit betreft het onderzoek van Lee en collega's (2023).

Zie Tabel 37 voor een overzicht van de relevante studie, en zie Tabel 40 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met content-gerelateerde cybercriminaliteit.

GPF

Goudhandelfraude (GPF) is een vorm van online criminaliteit waarbij slachtoffers worden misleid met investeringen in goudprojecten (Abubakari & Amponsah, 2024). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op GPF. Dit betreft de studie van Abubakari en Amponsah (2024). Zie Tabel 37 voor een overzicht van de relevante studie, en zie Tabel 41 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met GPF.

Witwassen

Witwassen is het proces waarbij bezittingen afkomstig uit criminele activiteiten worden omgezet of overgeboekt om de illegale herkomst te verbergen of om criminelen te faciliteren (Abubakari & Amponsah, 2024). In totaal is er één studie geïdentificeerd die specifiek betrekking heeft op witwassen. Dit betreft de studie van Abubakari en Amponsah (2024). Zie Tabel 37 voor een overzicht van de relevante studie, en zie Tabel 42 voor een overzicht van de geïdentificeerde risicofactoren en hun relatie met witwassen.

Tabel 37.
De referenties en kwaliteitsboordeling van de relevante studies.

Referentie	**Kwaliteit**
(Cross, 2022)	Laag
(Abubakari & Amponsah, 2024)	Laag
(Lee et al., 2023)	Hoog

Demografische kenmerken

Burgerlijke staat (content). Uit de de studie van Lee en collega's (2023) kwam naar voren dat de meeste verdachte van content-gerelateerde cybercriminaliteit ongetrouwd waren (75, 81%).

Geslacht (computer). Het lijkt erop dat daders van computer-gerelateerde cybercriminaliteit voornamelijk mannen zijn (Lee et al., 2023). Zo constateren Lee en collega's (2023) in hun onderzoek dat in bijna alle gevallen het betrof om mannelijke verdachten (93,94%).

Geslacht (content). Lee en collega's (2023) constateren dat bij content-gerelateerde cybercriminaliteit het leeuwendeel van de verdachten mannen waren (62,39%).

Leeftijd (computer). Het lijkt erop dat de meeste criminelen die computer-gerelateerde cybercriminaliteit plegen tieners en twintigers zijn (Lee et al., 2023).

Leeftijd (content). Het lijkt erop dat de meeste criminelen die content-gerelateerde cybercriminaliteit plegen tussen de 20 en 40 jaar zijn (Lee et al., 2023).

Criminaliteit

Recidive (computer). Uit de studie van Lee en collega's (2023) blijkt dat 52,11% van de verdachten van cybertransacties herhaalde overtreders zijn, en voor cyberfinanciering is dit percentage 35,71.

Recidive (content). Mogelijk is slechts een kleine groep daders die content-gerelateerde cybercriminaliteit plegen recidivist. Uit de studie van Lee en collega's (2023) blijkt dat 12,20% van

de verdachten recidivisten waren van cyberlaster en -beledigingen, en er waren geen recidiverende verdachten voor cyberstalking.

Strafblad (computer). Het lijkt erop dat een substantiële groep die computer-gerelateerde cybercriminaliteit plegen wel een eerdere veroordeling op zijn haar naam heeft staan. Zo constateren Lee en collega's (2023) in hun studie dat van de verdachten 30,30% geen strafblad had, 30,30% een eerdere veroordeling kent en 18,19% 2 tot 5 eerdere veroordelingen op hun namen hebben.

Strafblad (content). Het lijkt erop dat de helft van de criminelen die content-gerelateerde cybercriminaliteit plegen een strafblad heeft. Uit het onderzoek van Lee en collega's (2023) blijkt dat bij de verdachten van content-gerelateerde cybercriminaliteit 50% geen strafblad had, 22,58% een eerdere veroordeling heeft, 16,13% 2 tot 5 eerdere veroordelingen heeft en 11,29% meer dan 5 eerdere veroordelingen kent.

Motieven

Financieel gewin (computer). Het lijkt erop dat het verdienen van geld de meest voorkomende motieven waren voor computer-gerelateerde cybercriminaliteit.

Persoonlijke veroordeling (content). Het lijkt erop dat een motief om cyberlaster en -belediging te plegen is persoonlijke veroordeling. Lee en collega's (2023) constateren dat in 19,35% van de gevallen verdachten cyberlaster en beledigingen plegen tegen een specifieke persoon, vaak iemand met wie ze een persoonlijke relatie hebben. In tegenstelling tot andere motieven, die vaak openbaar of grootschalig zijn, is deze vorm van online criminaliteit gericht op een individu door bijvoorbeeld herhaaldelijk berichten te sturen om iemand lastig te vallen of te bekritiseren (Lee & collega's, 2023).

Plezier en verveling (content). Plezier en verveling zijn ook van invloed waarom mensen content-gerelateerde cybercriminaliteit plegen (Lee & collega's, 2023). In het onderzoek van Lee en collega's (2023) blijkt dat 24,19% van de verdachten deze misdaden begaan uit verveling of om zich te amuseren, bijvoorbeeld het plaatsen van valse informatie uit verveling.

Slechte ervaringen (content). Het hebben van slechte ervaringen met een persoon of organisatie kan ook een motief zijn om content-gerelateerde cybercriminaliteit te plegen. Lee en collega's (2023) constateren dat in 19,35% van de gevallen verdachten cyberlaster en -belediging plegen om slechte ervaringen met een persoon of organisatie te delen. Een voorbeeld hiervan is een verdachte die negatieve ervaringen met een tandarts publiceert na een slechte behandeling (Lee & collega's, 2023).

Solidariteit met pestkop (content). In slechts een klein aantal gevallen lijken mensen content-gerelateerde cybercriminelen te plegen uit solidariteit met pestkoppen. Lee en collega's (2023) constateren dat in 8,06% van de gevallen verdachten cyberlaster en -belediging plegen uit solidariteit met anderen die kwaadaardige berichten plaatsen. Ze voelen zich verbonden met deze pestkoppen en sluiten zich bij hen aan, bijvoorbeeld omdat ze het eens zijn met de berichten of omdat anderen op het platform hetzelfde gedrag vertonen (Lee & collega's, 2023).

Woede (content). Woede lijkt ook een rol te spelen waarom mensen content-gerelateerde cybercriminaliteit plegen. Zo komt uit het onderzoek van Lee en collega's (2023) naar voren dat in 29,03% van de gevallen verdachten misdrijven begaan om hun woede te uiten over een onderwerp of persoon. Bijvoorbeeld het plaatsen van beledigende berichten na het lezen van een artikel online (Lee & collega's, 2023).

Modus operandi

Anonimiteit (content). Verdachten maken vaak gebruik van anonimiteit bij het plaatsen van berichten (Lee et al., 2023).

Contact via berichten of telefonisch (content). Het lijkt erop dat cyberstalking voornamelijk plaatsvinden via berichten of telefonisch. In 33,87% van de gevallen plegen verdachten cyberstalking door herhaaldelijk berichten te sturen of telefonisch contact op te nemen met hun slachtoffers via mobiele telefoons (Lee et al., 2023). Vaak hebben ze een persoonlijke relatie met het slachtoffer en benaderen ze hen op een agressieve of bedreigende manier (Lee et al., 2023). Dit vindt met name plaatst via tekst- of SNS-berichten (90.48%), en in mindere mate via spraakoproepen (9.52%) (Lee et al., 2023).

E-mail en mobile messenger (computer). De resultaten uit het onderzoek van Lee en collega's (2023) suggereren dat de belangrijkste kanalen die daders van computer-gerelateerde cybercriminaliteit gebruiken zijn: *online sites* (bijv. tweedehands handelssites, gamesites, App Store, SNS-sites) die verantwoordelijk waren voor 90,91% van de gevallen en *mobile messenger-apps* (zoals KakaoTalk) die goed waren voor 9.09% van de gevallen.

Fases (BEC). In tegenstelling tot veel vormen van AFF- en datingfraude , richt BEC-fraude zich op bedrijven in plaats van op individuen (Cross, 2022). Deze vorm van fraude maakt misbruik van bestaande relaties tussen zakelijke collega's of betrouwbare leveranciers om financieel gewin te behalen (Cross, 2022). BEC-fraude vindt vaak plaats wanneer een dader zich voordoet als een werknemer, leverancier of ander vertrouwd lid van het bedrijfspersoneel om geld, rekeningnummers, toegangscodes of andere gevoelige informatie te verkrijgen (Cross, 2022). Het slachtoffer vaak gevraagd om geld over te maken naar de rekening van de dader, bijvoorbeeld door het onderscheppen van een betaling of het opstellen van een valse factuur (Cross, 2022). De slachtoffers zijn zowel de organisatie die de betaling niet heeft ontvangen als de persoon die de betaling naar de verkeerde rekening heeft gestuurd (Cross, 2022). De fraude wordt pas ontdekt op het moment dat de echte facturen niet zijn betaald en de betalingen naar andere rekeningen zijn gegaan (Cross, 2022).

Fases (GPF). GPF is een vorm van gedigitaliseerde criminaliteit waarbij slachtoffers worden misleid om te investeren in zogenaamde goudprojecten. Oplichters beloven hoge rendementen en combineren vaak deze fraude met datingfraude (Abubakari & Amponsah, 2024). In de studie van Abubakari en Amponsah (2024) wordt een voorbeeld uit 2013 aangehaald, waarin twee Ghanezen Amerikaanse investeerders wisten te overtuigen om geld over te maken voor de aanschaf van goud in Ghana, met de belofte van winst na verkoop in de VS. De oplichters nodigden de slachtoffers uit naar Ghana en lieten hen bankrekeningen openen om vertrouwen te wekken en hen te overtuigen tot grotere investeringen (Abubakari & Amponsah, 2024). Zodra grotere bedragen door de investeerders werden overgemaakt, verdween het geld en werd het beloofde goud nooit geleverd (Abubakari & Amponsah, 2024). Volgens de auteurs laat dit voorbeeld zien dat fraudeurs gebruik maken psychologische manipulatie en vertrouwenstechnieken om slachtoffers te overtuigen van de legitimiteit van de investering (Abubakari & Amponsah, 2024).

Geldezels (witwassen). Uit de studie van Abubakari en Amponsah (2024) blijkt dat diasporaleden betrokken zijn bij witwassen. In Ghana lokken lokale oplichters slachtoffers, terwijl diaspora-actoren vaak als money mules optreden (Abubakari & Amponsah, 2024). Ze faciliteren de overdracht van illegaal verkregen geld naar medeplichtigen in Ghana en andere landen.

Impersonatie (computer). Uit het onderzoek van Lee en collega's (2023) blijkt dat oplichting (gerelateerd aan nepverkopen) in 57,58% van de strafzaken voorkwam. Cybercriminelen doen

zich voor als verkopers en lichten slachtoffers op door betaling te accepteren voor goederen of diensten die nooit worden geleverd (Lee et al., 2023). Dit vindt vaak plaats op online tweedehands handelssites waar de verdachten hun identiteit kunnen verbergen en vermijden ze direct contact met slachtoffers (Lee et al., 2023). Daarnaast kwam diefstal van persoonlijke informatie (gerelateerd aan cyberfinanciële criminaliteit) in 42,42% van gevallen voor. Verdachten stelen persoonlijke informatie om microbetalingen te doen of producten te kopen (bijv. cadeaubonnen, game-items). Dit vindt met name plaats via mobiele telefoongegevens, SNS-ID's en wachtwoorden (Lee et al., 2023). Ook vindt oplichting plaatst via valse online game-sites plaats, waarbij verdachten zich voordoen als sitebeheerders en slachtoffers misleiden om gevoelige gegevens, zoals telefoonnummers en authenticatiecodes, te verstrekken (Lee et al., 2023).

Publieke verspreiding (content). Het lijkt erop dat valse of beledigende informatie op online platforms worden geplaatst. Uit de studie van Lee en collega's (2023) blijkt dat in 66,13% van de gevallen verdachten valse of beledigende informatie plaatsen op openbare fora of sociale netwerksites, zoals openbare bulletinboards (82,93%) of SNS-sites (17,7%) (Lee et al., 2023).

Samenwerking handlangers (BEC). Uit de studie van Abubakari en Amponsah (2024) blijkt dat Ghanese netwerken vaak samenwerken met handlangers in de VS om bedrijven en individuen te misleiden.

Verschillende strategieën (witwassen). In de studie wordt besproken dat diaspora-oplichters verschillende witwasstrategieën gebruiken, zoals (1) het openen van bankrekeningen met gestolen identiteiten, (2) het oprichten van schijnbedrijven voor frauduleuze overboekingen, (3) het omleiden van fondsen naar persoonlijke rekeningen in Ghana (3) en het kopen en verschepen van voertuigen naar Ghana (Abubakari & Amponsah, 2024).

Trends

Bewustzijn (computer). Het lijkt erop dat criminelen van computer-gerelateerde cybercriminaliteit inspelen op het gebrek aan bewustzijn van gebruikers over beveiligingsmaatregelen (Lee et al., 2023). Veel gebruikers zijn zich namelijk niet bewust van de noodzakelijke beveiligingsmaatregelen of missen de technische kennis om hun gegevens adequaat te beschermen (Lee et al., 2023).

Gemakkelijke toegang tot persoonsgegevens (computer). Het lijkt erop dat bij computer-gerelateerde cybercriminaliteit criminelen gemakkelijk toegang hebben tot persoonsgegevens. Zo bleek uit de studie van Lee en collega's (2023) naar voren dat 27,27% van de verdachten van computer-gerelateerde cybercriminaliteit gemakkelijk toegang konden krijgen tot persoonsgegevens. Dit heeft volgens de auteurs ermee te maken dat slachtoffers onvoldoende hun gegevens beveiligen (Lee et al., 2023). Verdachten kunnen namelijk misbruik maken van slecht beveiligde gegevens, zoals onbeschermde telefoons of ontbrekende wachtwoorden (Lee et al., 2023). Veel verdachten verklaarden eerst persoonlijke informatie te stelen en deze vervolgens te gebruiken voor cybertransacties en do cyber-gefinancierde misdaden (Lee et al., 2023).

Gemakkelijke toegang tot persoonsgegevens (content). Het lijkt erop dat bij content-gerelateerde cybercriminaliteit criminelen gemakkelijk toegang hebben tot persoonsgegevens. De studie van Lee en collega's (2023) laat zien dat 66,13% van de verdachten van content-gerelateerde cybercriminaliteit gemakkelijk toegang konden krijgen tot persoonsgegevens, bijvoorbeeld op persoonlijke blogs of openbare fora. In 4,84% konden verdachten toegang krijgen tot de contactinformatie of SNS-accounts van het slachtoffer (Lee et al., 2023).

Relatie tot het slachtoffer (computer). Het lijkt erop dat de meeste daders van computer-gerelateerde cybercriminaliteit geen relatie hebben met het slachtoffer. Zo blijkt uit het onderzoek van Lee en collega's (2023) dat 81,82% van de verdachten het slachtoffer niet persoonlijk kenden, in 6,06% van de gevallen waren de dader en het slachtoffer vrienden van elkaar (Lee et al., 2023). In minder gevallen betrof het slachtoffer school alumnus (3,03%), een buur (3,03%), een zakelijke relatie (3,57%) of familie (3,03%) (Lee et al., 2023).

Relatie tot het slachtoffer (content). Het lijkt erop dat ongeveer de helft van daders van content-gerelateerde cybercriminaliteit geen relatie heeft met het slachtoffer. Zo blijkt uit het onderzoek van Lee en collega's (2023) dat 53,23% van de verdachten geen relatie had met het slachtoffer, in 8,06% van de gevallen betrof het slachtoffer een dienstverlener of schoolalumni. In minder gevallen waren het slachtoffer een minnaar (4,84%) of waren ze lid van dezelfde club (4,84%) (Lee et al., 2023).

Interventies/trainingen

Slachtoffergericht

Authenticatie- en registratiesystemen (computer). Ter bestrijding van computer-gerelateerde cybercriminaliteit kunnen technische maatregelen worden versterkt, zoals verbeterde authenticatie- en registratiesystemen om identiteitsdiefstal te voorkomen (Lee et al., 2023).

Beheersysteem (content). Voor het bestrijden van content-gerelateerde cybercriminaliteit kunnen beheersystemen worden opgezet om schadelijke reacties en illegale inhoud te beheren en te rapporteren (Lee et al., 2023). Ook het verplicht stellen van echte namen voor gebruikers-ID's kan helpen om de identiteitsauthenticatie te versterken (Lee et al., 2023).

Detectie (content). Om content-gerelateerde cybercriminaliteit te bestrijden, kunnen filtersystemen worden geïmplementeerd die kwaadaardige tekst en afbeeldingen detecteren (Lee et al., 2023). Daarnaast moeten systemen regelmatig worden bijgewerkt om te kunnen inspelen op nieuwe vormen van cybercriminaliteit (Lee et al., 2023). Sites kunnen gebruikers die schadelijke inhoud verspreiden volgen en identificeren (Lee et al., 2023).

Gebruikerscontrole (content). In het onderzoek van Lee en collega's (2023) wordt er gesteld Sitebeheerders zouden een sociale verantwoordelijkheid hebben om gebruikers te informeren over cybercriminaliteit en de veiligheidsmaatregelen op hun platform (Lee et al., 2023). Ze kunnen gebruikers meer controle geven over hun persoonlijke gegevens, bijvoorbeeld door de optie te bieden om inhoud te verbergen of te verwijderen (Lee et al., 2023). Daarnaast kunnen zelfbevestigingsfuncties worden toegevoegd, zodat gebruikers hun geplaatste berichten kunnen herzien voordat ze definitief worden gepubliceerd (Lee et al., 2023).

Gebruikersidentificatie en notificatiefuncties (computer). De integratie van gebruikersidentificatie en notificatiefuncties, zoals meldingen bij inloggen vanaf een nieuw apparaat of bij langdurige inactiviteit, kan de veiligheid verhogen (Lee et al., 2023).

Regulering en aansprakelijkheid (computer). Lee en collega's (2023) stellen voor om de schaarste van game-items te reguleren om hacking te beperken en platforms die illegale handel mogelijk maken civielrechtelijk aansprakelijk te stellen. Ook kunnen online vergaderingen of verplichte regels helpen bij het opbouwen van vertrouwen tussen kopers en verkopers bij online transacties (Lee et al., 2023).

Schadelijk inhoud blokkeren (content). In de studie van Lee en collega's (2023) wordt er gesteld dat het belangrijk is om accounts en schadelijke inhoud direct te blokkeren, zodra cybercriminaliteit wordt geconstateerd, om verdere schade te voorkomen.

Tabel 38. Samenvatting resultaten van de literatuur over Business Email Compromise (BEC)-fraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ Trainingen (slachtoffer / dader)
-	-	-	-	-	-	Fases Samenwerking handlangers	-	-	-
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		*Grijs = neutrale factor*	

Tabel 39. Samenvatting resultaten van de literatuur over computer-gerelateerde cybercriminaliteit.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ Trainingen (slachtoffer / dader)
Geslacht (man)	Recidive	-	-	-	Financieel gewin	E-mail en mobile messenger	Bewustzijn Gemakkelijke toegang tot persoonsgegevens	-	Authenticatie- en registratiesystemen
Leeftijd	Strafblad					Impersonatie			Gebruikers-identificatie en notificatiefuncties Regulering en aansprakelijkheid

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

Tabel 40. Samenvatting resultaten van de literatuur over content-gerelateerde cybercriminaliteit.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ Trainingen (slachtoffer / dader)
Burgerlijke staat	Recidive	-	-	-	Persoonlijke veroordeling	Anonimiteit	Gemakkelijke toegang tot persoonsgegevens	-	Beheersysteem
Geslacht	Strafblad				Plezier en verveling	Contact via berichten of telefonisch	Relatie tot het slachtoffer		Detectie
Leeftijd					Slechte ervaringen	Publieke verspreiding			Gebruikers-controle
					Solidariteit met pestkop				Schadelijk inhoud blokkeren
					Woede				

Legenda ***Groen*** *= positieve relatie* ***Rood*** *= negatieve relatie* ***Blauw*** *= ambigue relatie* ***Grijs*** *= neutrale factor*

Tabel 41. Samenvatting resultaten van de literatuur over goudhandelfraude.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ Trainingen (slachtoffer / dader)
-	-	-	-	-	-	Fases	-	-	-
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		*Grijs = neutrale factor*	

Tabel 42. Samenvatting resultaten van de literatuur over witwassen.

Demografische kenmerken	Intrinsieke en persoonlijkheid kenmerken /mentaal / criminaliteit	Routine activiteiten	Sociale relaties	Macro-factoren	Neutralisatie Technieken / motieven	Modus operandi / misleidingstechnieken	Trends	Toekomstig onderzoek	Interventies/ Trainingen (slachtoffer / dader)
-	-	-	-	-	-	Geldezels Verschillende strategieën	-	-	-
	Legenda	***Groen** = positieve relatie*		***Rood** = negatieve relatie*		***Blauw** = ambigue relatie*		*Grijs = neutrale factor*	

4. Discussie

4.1. Samenvatting van de resultaten

Het doel van deze scoping review was het maken van een overzicht van uit wetenschappelijke bronnen, bekende risicofactoren voor daderschap van online criminaliteit en daarmee verbonden interventies, zodat professionals van de Nationale Politie en partnerorganisaties in korte tijd de inzichten over dit onderwerp te weten kunnen komen. De scoping review is uitgevoerd op basis van het (PRISMA-Scr) protocol van Leukfeldt en collega's (2022) waarin in zes online databases is gezocht naar studies gepubliceerd tussen 2021 en 2024. Dit resulteerde in 52 relevante studies van de bestaande literatuur (zie Bijlage C voor een volledig overzicht van de literatuur over daderschap).

De resultaten laten zien dat binnen gedigitaliseerde criminaliteit, met name bij online fraude, de studies **vooral aandacht besteden aan de modus operandi** van criminelen. Deze daders , **zowel specialisten als generalisten**, vaak onderdeel uitmaken van **grotere, criminele netwerken**. Deze netwerken helpen criminelen bij het herkennen en benutten van kansen om verschillende vormen van online criminaliteit te plegen. Cybercriminele **netwerken variëren sterk**, van losser georganiseerde groepen tot striktere clusters, met veel voorkomende typen zoals cyberfraude- en malware-netwerken. Binnen deze netwerken nemen criminelen met verschillende achtergronden uiteenlopende posities in om hun criminelen activiteiten te ontvouwen. **Online platforms** spelen hierin een belangrijke rol in het faciliteren van online criminaliteit. Deze ondergrondse platforms bieden een anonieme omgeving waar gebruikers criminelen tools, diensten en informatie met elkaar kunnen uitwisselen - vaak buiten het zicht van reguliere autoriteiten – wat leidt tot een professioneel ecosysteem. Het groeiende aanbod en beschikbaarheid van kant-en-klare criminele tools heeft ertoe geleid dat criminelen, zonder geavanceerde technische kennis, kunnen deelnemen aan (complexe vormen van) online criminaliteit. Voor wat betreft cybercrime in enge zin suggereert de literatuur dat van bijvoorbeeld hackers de twee hoofmethoden zijn diefstal en lekken van persoonlijke informatie, waarbij de belangrijkste kanalen die ze gebruiken zijn: (a) online sites (zoals portals), (b) interne systemen *van organisaties* (zoals provinciale kantoren) en (c) *bulletin boards* (zoals een bulletin board van een instelling).

Om slachtoffers te misleiden, passen bij nagenoeg alle vormen van online criminaliteitcriminelen verschillende social engineeringtechnieken toetoewaarvan de meest gebruikte zijn: (a) autoriteit, (b) schaarste en (c) urgentie. – met betrekking tot de studies specifiek over cybercrime in enge zin is niet geheel duidelijk welke technieken het meest worden gebruikt. Zo doen daders zich voor als professionals, zoals bankmedewerkers of overheidsfunctionarissen, om vertrouwen te wekken bij slachtoffers (autoriteit). Een andere tactiek is het presenteren van een aanbod als uniek en tijdelijk, zodat slachtoffers zich onder druk gezet voelen om snel te beslissen zonder de gevolgen goed te overdenken of advies te vragen (schaarste). Cybercriminelen lijken ook een gevoel van tijdsdruk te creëren om slachtoffers te misleiden door te suggereren dat ze zo snel mogelijk geld nodig hebben vanwege een noodgeval. Daarbij is te constateren dat het succes van de oplichting mede wordt bepaald in hoeverre criminelen hun misleidingsstrategieën weten aan te passen als reactie op het gedrag en de achtergrond van hun slachtoffers.

Wat de literatuur verder laat zien is datcybercriminelen **neutralisatietechnieken gebruiken om hun daden goed te praten en morele schuld te verminderen**. De bestaande literatuur geeft een voorzichtige indicatie dat bij vooral gedigitaliseerde criminaliteit de drie meest gehanteerde rationalisatiestrategieën ‘ontkennen van verantwoordelijkheid’ ’ (d.w.z. de schuld wordt

afgeschoven op externe factoren), ‘ontkennen van schade’ (d.w.z. er wordt door de dader beweert dat niemand is benadeeld) en ‘ontkennen van slachtofferschap’ (d.w.z. de dader vindt dat het slachtoffer het heeft verdiend). Voor wat betreft de literatuur over cybercrime in enge zin spelen met name ‘ontkennen van slachtofferschap’ en ‘hogere morele principes’. Bij laatstgenoemde rechtvaardigen bijvoorbeeld hackers hun acties als bijdragen aan het algemeen belang, bijvoorbeeld door beveiligingslekken bloot te leggen of overheidsinformatie transparant te maken. In tegenstelling tot online fraude, lijkt vanuit de neutralisatietechniek ‘het ontkennen van letsel’ geen voorspellende factor uit te gaan.

Voor wat betreft het motief om betrokken te raken bij online criminaliteit, lijken gedigitaliseerde cybercriminelen **vooral gedreven** te worden **door financieel gewin**. Redenen hiervoor kunnen variëren van het voorzien in de eigen levensbehoeften tot aan het onderhouden van een gezin. In mindere mate lijken factoren als wraak, hebzucht of ideologische bevlogenheid een rol te spelen waarom mensen online criminaliteit plegen. Bij cybercrime in enge zin zien we dat bij hackers juist ideologische redenen opereren een belangrijk motief vormen bijvoorbeeld om een organisatie of bedrijf schade toe te brengen omdat die in hun ogen hen eerder schade heeft toegebracht of om corrupte overheden en wetshandhavingsinstanties te straffen. Daarnaast opereren ook een groot aandeel hackers ook vanuit impulsiviteit, nieuwsgierigheid of plezier.

Als er specifieker wordt gekeken naar de risicofactoren, dan blijkt dat bij online fraudemet name **economische en sociale invloeden** mensen ertoe aan te zetten om cyberdelicten te plegen. In vooral ontwikkelingslanden lijkt de heersende economische malaise, dat wil zeggen hoge werkeloosheid, armoede, slechte banenkansen, als katalysator te fungeren voor online criminaliteit; om toch in de eigen basisbehoeften te voorzien, zien velen zich genoodzaakt om een cyber criminele carrière te bewandelen. Bij zowel online fraude als cybercrime in enge zin is er mogelijk een verband te constateren tussen welvaart en de prevalentie van cyberdelicten; in rijke Westerse landen vinden de cyberdelicten plaats, doordat de hoge welvaart in deze landen lucratieve kansen bieden voor criminelen, en in arme landen worden deze aanvallen uitgevoerd – de zwakkere economische landen trekken immers de cybercriminelen aan.

Vanuit sociaal oogpunt lijken op de eerste plaatst bij meerdere vormen van online criminaliteit ***peers*** een belangrijke rol te spelen waarom mensen cyberdelicten plegen. Het hebben van deviante vrienden vergroot mogelijk de kans op betrokkenheid bij van cyberdelicten. De beïnvloeding door leeftijdsgenoten kan zowel in de offline als online wereld plaatsvinden. Ze worden gerekruteerd door vrienden, kennissen of anderen met kennis van illegale activiteiten. Sociale relaties fungeren in zekere zin als toegangspoorten tot wereld van online criminaliteit. In het verlengde hiervan speelt de gemeenschap waartoe een individu behoort hierin verder een rol. De wens om geaccepteerd te worden binnen online gemeenschappen, met name als gedrag als sociaal acceptabel wordt beschouwd, kunnen mensen aanzetten tot online criminaliteit.

Op individueel niveau is de literatuur betrekkelijk schaars: er nauwelijks onderzoek gedaan naar demografische en intrinsieke risicofactoren. Met laatstgenoemde in gedachte lijkt er een aanwijzing te zijn dat cyberdelicten voornamelijk door mannen worden gepleegd, hoewel het aandeel ervan zou kunnen afhangen van het type cyberdelict. Zo bestaan hackers met name uit mannen, terwijl vrouwen meer betrokken zijn bij datingfraude. Het wetenschappelijke discours is al meer ambigue over leeftijd, aangezien het onduidelijk of met name jongeren of ouderen online criminaliteit plegen. Dit zou eveneens kunnen afhangen van het type delict.

Tenslotte benadrukken de aangehaalde studies in sterke mate het **belang van voorlichting** om daders van het criminele pad af te houden. De literatuur suggereert dat het belangrijk is

dat mensen bewust zijn van de aanzienlijke financiële en emotionele schade die het kan hebben voor slachtoffers, maar zich ook realiseren wat de risico's zijn die gepaard gaan met het plegen van online criminaliteit. Het risico op hoge sancties en de kans om gepakt te worden, kunnen mensen ervan weerhouden om cyberdelicten te plegen, hoewel dit eveneens lijkt af te hangen van het motief van daders. Zo lijken bijvoorbeeld ideologisch gestuurde criminelen, zoals hackers, mogelijk moeilijker af te schrikken zijn dan criminelen die opereren vanuit een financieel motiefvanwege hun sterke drang om de 'missie' te voltooien. Bovenstaande illustreert meteen ook de complexiteit van online criminaliteit en dat een *one fits all benadering* niet bestaat, maar juist maatwerk geboden is, om effectief te zijn in het voorkomen van dader- en slachtofferschap. Daarbij is het van belang dat interventies niet alleen *evidence-based zijn*, maar dat deze ook deze regelmatig worden geëvalueerd en op basis daarvan al dan niet worden herziend, zodat deze effectief blijven in het licht van de voortdurend veranderde en evoluerende aard van online criminaliteit.

4.2. Onderzoekslacunes en toekomstig onderzoek

Een nevendoelstelling van deze *scoping review* was het identificeren van onderzoekslacunes. Na het analyseren van de in aanmerking komende studies, identificeerden we verschillende onderzoekslacunes:

I. Ten eerste is er over de gehele linie bezien nog maar **weinig onderzoek gedaan naar risicofactoren**. Dit geldt met name voor demografische kenmerken (zoals leeftijd, geslacht en opleidingsniveau) en intrinsieke persoonlijkheidskenmerken (bijvoorbeeld zelfcontrole, verslaving en stoornissen). Het in kaart brengen van deze risicofactoren is zonder meer van belang voor vroegtijdige signalering, gerichte preventiemaatregelen en adequate rehabilitatieprogramma's. Hierbij zouden de risicofactoren niet afzonderlijk worden moeten onderzocht, maar in samenhang met elkaar, omdat er mogelijk interactieeffecten optreden.
II. Ten tweede is er gebrek aan onderzoek gericht op **evalueren van bestaande interventies** gericht. Het belangrijk is om preventieprogramma's te evalueren aan de hand van wetenschappelijke maatstaven om te beoordelen of ze succesvol en effectief zijn.
III. Ten derde is er bij veel vormen van online delicten (zoals hacking, malware endatingfraude) een **gebrek aan wetenschappelijk literatuur over *pathways***, ofwel de verschillende ontwikkelingspaden die leiden tot criminogeen gedrag. Kennis over pathways helpt om online criminaliteit beter te begrijpen, te voorspellen en voorkomen.
IV. Ten vierde zijn de meeste studies uit deze scoping review **gebaseerd op cross-sectionele onderzoeksmethoden**, dat wil zeggen gegevens die op één enkel moment in de tijd zijn verzameld. Doordat het een momentopname is, is het moeilijker om causale relaties vast te stellen. Daarom is er behoefte aan meer longitudinaal onderzoek, waardoor causaliteit kan worden gemeten en daarmee individuele verschillen zichtbaar worden.
V. Ten vijfde bestaat de behoefte uit de literatuur om dadergedrag te verklaren op basis van directe data, zoals via interviews, gedragsobservatie en zelfrapportage van de daders zelf, in plaats van onderzoek dat indirect dadergedrag meet, zoals via vrienden/familie van daders. Doordat deze gegevens afkomstig zijn van de dader zelf, in plaats van

bijvoorbeeld interpretaties van derden, kunnen motieven, gedachten en emoties die achter het criminogeen gedrag schuilgaan beter in kaart worden gebracht.

VI. Hoewel onderzoek voorzichtig uitwijst dat cybercriminelen **neutralisatietechnieken** hanteren om hun misdaden te rechtvaardigen, blijkt dat hier nog maar weinig onderzoek naar is gedaan. Toekomstig onderzoek zou zich hier dan ook bij een breed aantal delicten op kunnen richten. Vanuit praktisch opzicht kan het begrijpen van welke technieken verschillende soorten cybercriminelen gebruiken helpen bij het ontwikkelen van preventiestrategieën of het effectiever maken van reclasseringsprogramma's, maar ook bij recidivebeoordelingen.

VII. Meer in het algemeen is het belangrijk dat de genoemde lacunes worden onderzocht binnen een **zo breed mogelijke sociale context**. De literatuur suggereert dat het voorspellend vermogen van risicofactoren kan variëren afhankelijk van het onderzoekssubject, het type cyberdelict en de economische of politieke omstandigheden.

VIII. Meer dan twee derde van de geïncludeerde studies zijn uitgevoerd in Afrikaanse of Aziatische landen. Vanwege de sociale, economische, politieke en culturele verschillen tussen deze landen en westerse landen, zijn de resultaten mogelijk maar beperkt generaliseerbaar.

4.3. Beperkingen van het huidige onderzoek

Dit onderzoek kent een aantal beperkingen. Allereerst is er in deze studie alleen gezocht naar studies in databases, waardoor uitsluitend studies die openbaar toegankelijk en gepubliceerd zijn, zijn meegenomen. Ten tweede is het beoordelen van potentieel relevante studies uitgevoerd door één onderzoeker. Hoewel dit op een wetenschappelijk onderbouwde en systematische wijze is uitgevoerd, bestaat er de mogelijkheid dat potentieel relevante studies niet als zodanig zijn aangemerkt. Ten derde geldt hetzelfde voor betreft het extraheren, synthetiseren en analyseren van de data. Hierdoor is het risico op vertekeningen in de gesynthetiseerde data mogelijk groter dan wanneer het onderzoek was uitgevoerd door twee of meerdere onderzoekers. Ten vierde is er alleen gezocht in de databases, waardoor alleen studies die openbaar/gepubliceerd zijn, zijn meegenomen. Ten vijfde is er binnen de databases alleen gezocht op Engelstalige literatuur. Hierdoor zijn er mogelijk papers geschreven in andere talen niet geïdentificeerd. Wel is het zo dat Engels de gangbare taal van de wetenschappelijke wereld is en om die reden de meeste criminologisch gerelateerde literatuur in het Engels is gepubliceerd. Ten zesde is alleen de data verzameld die de studies in de tekst hebben opgeschreven. Hierdoor is wellicht relevante informatie die in andere artikelen voorkwamen niet meegenomen in deze studie. Daar komt bij dat in het geval dat aangehaalde studies door de auteurs verkeerd zijn geïnterpreteerd of overgenomen – dit zou dan het sterkst gelden voor de niet-systematische reviews – dat deze onjuistheden ook in dit onderzoek worden weerspiegeld.

Literatuur

Aborisade, R. A. (2023). Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of Parents' Disposition Towards Children's Involvement in Cybercrimes. *Deviant Behavior*, *44*(7), 1102-1120. Academic Search Ultimate.

Abubakari, Y. (2024). The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies. *Deviant Behavior*, *45*(5), 708-735. Scopus. https://doi.org/10.1080/01639625.2023.2263137

Abubakari, Y., & Amponsah, A. (2024). Economic cybercrime in the diaspora: Case of Ghanaian nationals in the USA. *JOURNAL OF MONEY LAUNDERING CONTROL*. https://doi.org/10.1108/JMLC-03-2024-0047

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). *Veiligheidsmonitor 2023*. https://www.rijksoverheid.nl/documenten/rapporten/2024/03/01/tk-bijlage-veiligheidsmonitor-2023

Alam, M. N. (2021). Three Essays on Socially Engineered Attacks: The Case of Online Romantic Scams [Ph.D., The University of North Carolina at Greensboro]. In *ProQuest Dissertations and Theses* (2620099834). ProQuest Dissertations & Theses Global. https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/dissertations-theses/three-essays-on-socially-engineered-attacks-case/docview/2620099834/se-2?accountid=12045

Alhasan, A. A. (2022). An Examination of Fraud from Three Perspectives: The Perpetrator, the Whistleblower, and the Examiner [Ph.D., West Virginia University]. In *ProQuest Dissertations and Theses* (2714895873). ProQuest Dissertations & Theses Global. https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/dissertations-theses/examination-fraud-three-perspectives-perpetrator/docview/2714895873/se-2?accountid=12045

Apantaku, P. O. (2021). Cybercrime: Motivations, Modes, and Emerging Trends, with Nigeria as a Case Study [Ph.D., University of Portsmouth (United Kingdom)]. In *PQDT - UK & Ireland* (2636129759). ProQuest Dissertations & Theses Global. https://login.ezproxy.leidenuniv.nl/login??url=https://www.proquest.com/dissertations-theses/cybercrime-motivations-modes-emerging-trends-with/docview/2636129759/se-2?accountid=12045

Baethge, C., Goldbeck-Wood, S., & Mertens, S. (2019). SANRA—a scale for the quality assessment of narrative review articles. *Research Integrity and Peer Review*, *4*(1), 5. https://doi.org/10.1186/s41073-019-0064-8

Balogun, N. A., Abdulrahaman, M. D., & Aka, K. (2024). EXPLORING THE PREVALENCE OF INTERNET CRIMES AMONG UNDERGRADUATE STUDENTS IN A NIGERIAN UNIVERSITY: A CASE STUDY OF THE UNIVERSITY OF ILORIN. *Nigerian Journal of Technology*, *43*(1), 71-79. Scopus. https://doi.org/10.4314/njt.v43i1.10

Bekkers, L. M. J., & Leukfeldt, E. R. (2023). Recruiting money mules on instagram: A qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior*, *44*(4), 603-619. Scopus. https://doi.org/10.1080/01639625.2022.2073298

Bijmans, H., Booij, T., Schwedersky, A., Nedgabat, A., & van Wegberg, R. (2021). Catching phishers by their bait: Investigating the Dutch phishing landscape through phishing kit detection. *Proc. USENIX Secur. Symp.*, 3757-3774. Scopus.

https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114475836&partnerID=40&md5=cd712ca8e3ec8aab48022ed652763434

Bossler, A. M. (2021). Neutralizing Cyber Attacks: Techniques of Neutralization and Willingness to Commit Cyber Attacks. *American Journal of Criminal Justice*, *46*(6), 911-934. Scopus. https://doi.org/10.1007/s12103-021-09654-5

Braithwaite, J., Herkes, J., Ludlow, K., Testa, L., & Lamprell, G. (2017). Association between organisational and workplace cultures, and patient outcomes: Systematic review. *BMJ Open*, *7*(11), e017708. https://doi.org/10.1136/bmjopen-2017-017708

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(S1), S47-S59. Scopus. https://doi.org/10.1080/14616696.2020.1804973

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, *159*. Scopus. https://doi.org/10.1016/j.exger.2021.111678

Chawki, M. (2021). Cybercrime in the Context of COVID-19. In Arai K. (Red.), *Lect. Notes Networks Syst.* (Vol. 285, pp. 986-1002). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-030-80129-8_65

Cole, T. (2022). Exploring Fraudsters Strategies to Defraud Users on Online Employment Databases. *International Journal of Cyber Criminology*, *16*(2), 61-86. Publicly Available Content Database. https://doi.org/10.5281/zenodo.4766567

Cretu-Adatte, C., Zbinden, R., Brunoni, L., Bunning, H., Azi, J. W., & Beaudet-Labrecque, O. (2024). How do Ivorian Cyberfraudsters Manage Their Criminal Proceeds? *European Journal on Criminal Policy and Research*, *30*(3), 359-378. Scopus. https://doi.org/10.1007/s10610-024-09597-7

Cross, C. (2022). Meeting the challenges of fraud in a digital world. In *The Handb. Of Secur.* (pp. 217-238). Springer; Scopus. https://doi.org/10.1007/978-3-030-91735-7_11

Dearden, T. E., & Gottschalk, P. (2024). Convenience Theory and Cybercrime Opportunity: An Analysis of Online Cyber Offending. *Deviant Behavior*, *45*(3), 348-360. Scopus. https://doi.org/10.1080/01639625.2023.2246626

Dickinson, T., & Wang, F. (2024). Neutralizations, Altercasting, and Online Romance Fraud Victimizations. *Deviant Behavior*, *45*(5), 736-751. Scopus. https://doi.org/10.1080/01639625.2023.2263610

Dickinson, T., Wang, F., & Maimon, D. (2023). What Money Can Do: Examining the Effects of Rewards on Online Romance Fraudsters' Deceptive Strategies. *Deviant Behavior*, *44*(9), 1386-1400. Academic Search Ultimate.

Eseadi, C., Ogbonna, C. S., Otu, M. S., & Ede, M. O. (2021). Hello pretty, hello handsome!: Exploring the menace of online dating and romance scam in Africa. In *Crime, Ment. Health and the Crim. Justice Syst. In Afr.: A Psycho-Criminol. Perspect.* (pp. 63-87). Springer International Publishing; Scopus. https://doi.org/10.1007/978-3-030-71024-8_4

Faqir, R. S. A., & Arfaoui, D. (2024). Psychological Insights into the Behavior of Cybercriminals: A Theoretical Perspective. *Pakistan Journal of Criminology*, *16*(2), 263-276. Scopus. https://doi.org/10.62271/pjc.16.2.263.276

Goyal, N., Mamidi, R., Sachdeva, N., & Kumaraguru, P. (2023). Warning: It's a scam!! Towards understanding the Employment Scams using Knowledge Graphs. *Proceedings of the 6th*

Joint International Conference on Data Science & Management of Data (10th ACM IKDD CODS and 28th COMAD), 303-304. https://doi.org/10.1145/3570991.3571053

Hawker, S., Payne, S., Kerr, C., Hardey, M., & Powell, J. (2002). Appraising the Evidence: Reviewing Disparate Data Systematically. *Qualitative Health Research*, *12*(9), 1284-1299. https://doi.org/10.1177/1049732302238251

Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers and Security*, *128*. Scopus. https://doi.org/10.1016/j.cose.2023.103158

Jiang, Y., Wen, X., & Qian, X. (2024). Impact of gain-loss framing on online scam susceptibility: The role of scam frames, warning frames, and risk perception. *BEHAVIOUR & INFORMATION TECHNOLOGY*. https://doi.org/10.1080/0144929X.2024.2378883

Johnson, S. D. (2024). Identifying and preventing future forms of crimes using situational crime prevention. *Security Journal*, *37*(3), 515-534. Scopus. https://doi.org/10.1057/s41284-024-00441-5

Johnson, S. D., & Nikolovska, M. (2024). The Effect of COVID-19 Restrictions on Routine Activities and Online Crime. *Journal of Quantitative Criminology*, *40*(1), 131-150. Academic Search Ultimate.

Khweiled, R., Jazzar, M., & Eleyan, D. (2021). Cybercrimes during COVID -19 Pandemic. *International Journal of Information Engineering and Electronic Business*, *13*(2), 1. Coronavirus Research Database; Publicly Available Content Database. https://doi.org/10.5815/ijieeb.2021.02.01

Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime, Law and Social Change*, *76*(2), 109-130. Scopus. https://doi.org/10.1007/s10611-021-09957-y

Kikerpill, K., & Siibak, A. (2021). MAZEPHISHING: THE COVID-19 PANDEMIC AS CREDIBLE SOCIAL CONTEXT FOR SOCIAL ENGINEERING ATTACKS. *TRAMES: A Journal of the Humanities & Social Sciences*, *25*(4), 371-393. Academic Search Ultimate.

Lakhani, S. (2021). Perspectives on Internet-Based Crimes. In *Criminal Psychology and the Criminal Justice System in India and Beyond* (pp. 145-153). Springer Nature; Scopus. https://doi.org/10.1007/978-981-16-4570-9_9

Lee, C. S. (2022). How Online Fraud Victims are Targeted in China: A Crime Script Analysis of Baidu Tieba C2C Fraud. *Crime and Delinquency*, *68*(13-14), 2529-2553. Scopus. https://doi.org/10.1177/00111287211029862

Lee, S.-H., Kang, I., & Kim, H.-W. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*. Scopus. https://doi.org/10.1016/j.techsoc.2023.102361

Leong, W. Y., Leong, Y. Z., & Leong, W. S. (2024). The Intersection of Scammers and Artificial Intelligence. *IEEE Int. Conf. Consum. Electron. - Taiwan, ICCE-Taiwan*, 539-540. Scopus. https://doi.org/10.1109/ICCE-Taiwan62264.2024.10674334

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

Leukfeldt, E. R., Loggen, J., & Moneva, A. (2022). *Protocol—A Systematic Narrative Review of Pathways into and out of Cyber-Dependent and Financially Motivated Cyber-enabled Crime*. OSF Registries. https://doi.org/10.17605/OSF.IO/MJZEA

Levi, M., & Smith, R. G. (2022). Fraud and pandemics. *Journal of Financial Crime*, *29*(2), 413-432. Scopus. https://doi.org/10.1108/JFC-06-2021-0137

Loggen, J., Moneva, A., & Leukfeldt, R. (2024a). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review*, *52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

Loggen, J., Moneva, A., & Leukfeldt, R. (2024b). Pathways Into, Desistance From, and Risk Factors Related to Cyber-Dependent Crime: A Systematic Narrative Review. *Victims & Offenders*, 1-32. https://doi.org/10.1080/15564886.2024.2370295

Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, *27*(3), 364-387. Academic Search Ultimate.

McGuire, M., & Dowling, S. (2013a). Chapter 1: Cyber-dependent crimes Home Office Research Report 75. In *Cyber crime: A review of the evidence*. Home office. https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf

McGuire, M., & Dowling, S. (2013b). Chapter 2: Cyber-enabled crimes—Fraud and theft Home Office Research Report 75. In *Cyber crime: A review of the evidence*. Home office. https://assets.publishing.service.gov.uk/media/5a755a94e5274a59fa7177f7/horr75-chap2.pdf

NCTV. (2024). *Cybersecuritybeeld Nederland 2024*. https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024

Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: Transnational computer fraud in Vietnam. *Journal of Crime and Justice*, *44*(4), 419-440. Scopus. https://doi.org/10.1080/0735648X.2020.1818605

Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2022). How Do Individuals Justify and Rationalize their Criminal Behaviors in Online Romance Fraud? *Information Systems Frontiers*, *24*(2), 475-491. Scopus. https://doi.org/10.1007/s10796-020-10051-2

Ojolo, T. L., & Singh, S. B. (2023). The transnational dimension of organised crime: An investigation into the operational structure of cybercrime in Nigeria. *EUREKA: Social and Humanities*, *6*, 87-98. Coronavirus Research Database; Publicly Available Content Database. https://doi.org/10.21303/2504-5571.2023.003263

Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, *30*(6), 1653-1663. Scopus. https://doi.org/10.1108/JFC-08-2022-0185

Orjiakor, C. T., Ndiwe, C. G., Anwanabasi, P., & Onyekachi, B. N. (2022). How do internet fraudsters think? A qualitative examination of pro-criminal attitudes and cognitions among internet fraudsters in Nigeria. *Journal of Forensic Psychiatry & Psychology*, *33*(3), 428-444. Psychology and Behavioral Sciences Collection.

Othman, R., & Ameer, R. (2022). In employees we Trust: Employee fraud in small businesses. *Journal of Management Control*, *33*(2), 189-213. Scopus. https://doi.org/10.1007/s00187-022-00335-w

Petticrew, M., & Roberts, H. (2006). *Systematic Reviews in the Social Sciences: A Practical Guide* (1ste dr.). Wiley. https://doi.org/10.1002/9780470754887

Politie. (2021). *'Investeer in aanpaak cybercrime'*. https://www.politie.nl/nieuws/2021/april/15/investeer-in-aanpak-cybercrime.html

Pollock, D., Evans, C., Menghao Jia, R., Alexander, L., Pieper, D., Brandão De Moraes, É., Peters, M. D. J., Tricco, A. C., Khalil, H., Godfrey, C. M., Saran, A., Campbell, F., & Munn, Z. (2024).

"How-to": Scoping review? *Journal of Clinical Epidemiology*, *176*, 111572. https://doi.org/10.1016/j.jclinepi.2024.111572

Puchkov, D. (2021). International Cyber Crime: Main Trends. *REVISTA SAN GREGORIO*, *44*, 8-13. https://doi.org/10.36097/rsan.v1i44.1580

Rachh, A. (2024). Spatial and temporal analysis of cyber-crime cases in India. *Letters in Spatial and Resource Sciences*, *17*(1). Scopus. https://doi.org/10.1007/s12076-023-00360-w

Ridho, W. F. (2024). Unmasking online fake job group financial scams: A thematic examination of victim exploitation from perspective of financial behavior. *Journal of Financial Crime*, *31*(3), 748-758. Scopus. https://doi.org/10.1108/JFC-05-2023-0124

Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology*, *13*. Scopus. https://doi.org/10.3389/fpsyg.2022.912242

Steinmetz, K., Pimentel, A., & Goe, W. (2021). Performing social engineering: A qualitative study of information security deceptions. *COMPUTERS IN HUMAN BEHAVIOR*, *124*. https://doi.org/10.1016/j.chb.2021.106930

Sun, Z., Oest, A., Zhang, P., Rubio-Medrano, C., Bao, T., Wang, R., Zhao, Z., Shoshitaishvili, Y., Doupé, A., & Ahn, G.-J. (2021). Having your cake and eating it: An analysis of concession-abuse-as-a-service. *Proc. USENIX Secur. Symp.*, 4169-4186. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104014091&partnerID=40&md5=d4e71f6b88a3c399cc71db556c1ac6dd

Tambe Ebot, A. (2023). Advance fee fraud scammers' criminal expertise and deceptive strategies: A qualitative case study. *Information and Computer Security*, *31*(4), 478-503. Scopus. https://doi.org/10.1108/ICS-01-2022-0007

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., … Straus, S. E. (2018). PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation. *Annals of Internal Medicine*, *169*(7), 467-473. https://doi.org/10.7326/M18-0850

Van De Schoot, R., De Bruin, J., Schram, R., Zahedi, P., De Boer, J., Weijdema, F., Kramer, B., Huijts, M., Hoogerwerf, M., Ferdinands, G., Harkema, A., Willemsen, J., Ma, Y., Fang, Q., Hindriks, S., Tummers, L., & Oberski, D. L. (2021). An open source machine learning framework for efficient and transparent systematic reviews. *Nature Machine Intelligence*, *3*(2), 125-133. https://doi.org/10.1038/s42256-020-00287-7

Van Nguyen, T. (2022). The modus operandi of transnational computer fraud: A crime script analysis in Vietnam. *Trends in Organized Crime*, *25*(2), 226-247. Academic Search Ultimate.

Wang, F. (2024). Victim-offender overlap: The identity transformations experienced by trafficked Chinese workers escaping from pig-butchering scam syndicate. *Trends in Organized Crime*, 1-32. Academic Search Ultimate.

Wang, F., & Dickinson, T. (2024). Hyperpersonal feedback and online romance fraud: An empirical examination. *JOURNAL OF CRIME & JUSTICE*. https://doi.org/10.1080/0735648X.2024.2376700

Wang, F., Howell, C. J., Maimon, D., & Jacques, S. (2021). The Restrictive Deterrent Effect of Warning Messages Sent to Active Romance Fraudsters: An Experimental Approach. *International Journal of Cyber Criminology*, *15*(1), 1-16. Publicly Available Content Database. https://doi.org/10.5281/zenodo.4766529

Yar, M. (2006). *Cybercrime and Society*. SAGE Publications Ltd. https://doi.org/10.4135/9781446212196

Zhou, Y., Liu, W., Lee, C., Xu, B., & Sun, I. (2024). Traditional social learning predicts cyber deviance? Exploring the offending versatility thesis in social learning theory. *Behavioral Sciences and the Law*, *42*(4), 417-434. Scopus. https://doi.org/10.1002/bsl.2664

Bijlage A. Abstract screening tool

Abstract screening

1. Wordt er Engels gebruikt in de titel?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

2. Geeft de titel aan dat dit GEEN correctie, erratum of opgehaald artikel is?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

3. Geeft de abstract aan dat dit document één enkel artikel bevat?
a. Ja of onduidelijk: doorgaan met screenen
b. Nee: stoppen met screenen

4. Geeft de abstract aan dat het hoofdgebied van het onderzoek cybercriminaliteit of (financieel gemotiveerde) gedigitaliseerde criminaliteit?
a. Ja of onduidelijk: doorgaan met screenen
b. Nee: stoppen met screenen

5. Geeft de abstract aan dat het artikel gaat over risicofactoren, interventies/trainingen, modus operandi, overtuigings- en neutralisatietechnieken, rechtvaardigheidsstrategieën, motieven en/of trends die gericht zijn op daderschap?
a. Ja of onduidelijk: doorgaan met screenen
b. Nee: stoppen met screenen

6. Geeft de abstract aan dat de studie empirisch is of een review?
a. Ja of onduidelijk: doorgaan met screenen
b. Nee: stoppen met screenen

Besluit: Moet dit artikel worden opgenomen?
– Ja, alle 6 screeningvragen beantwoord met "Ja" of "Onduidelijk"
– Nee, minstens 1 screeningvraag beantwoord met "Nee

Bijlage B. Full tekst screening tool

Volledige tekst

1. Wordt er in de volledige tekst Engels gebruikt?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

2. Geeft de volledige tekst aan dat het GEEN correctie, erratum of opgehaald artikel is?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

3. Geeft de volledige tekst aan dat het een tijdschriftartikel, boek, hoofdstuk in een boek, conferentie-/proceedingpaper, technisch rapport, dissertatie/thesis of een overheidsdocument is?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

4. Geeft de volledige tekst aan dat het specifiek ingaat op ten minste één vorm van cybercriminaliteit of gedigitaliseerde criminaliteit?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

5. Geeft de volledige tekst aan dat het artikel gaat over risicofactoren, interventies/trainingen, modus operandi, overtuigings- en neutralisatietechnieken, rechtvaardigheidsstrategieën, motieven en/of trends die gericht zijn op daderschap?
a. Ja of onduidelijk: doorgaan met screenen
b. Nee: stoppen met screenen

6. Geeft de volledige tekst aan dat het een empirische studie of review is?
a. Ja: doorgaan met screenen
b. Nee: stoppen met screenen

Besluit: Moet dit artikel worden opgenomen voor volledige beoordeling?
– Ja, alle 6 screeningvragen beantwoord met "Ja"
– Nee, minstens 1 screeningvraag beantwoord met "Nee"

Bijlage C. Overzicht van de bevindingen

Relatie	**Type criminaliteit**[8]						
	Online criminaliteit	Cybercriminaliteit[9]	Phishing/vishing	Online fraude[10]	Geldezels	Social engineering	Bitcoin gerelateerde online criminaliteit
Positieve relatie	• Afpersing • AI-technologie • Anonimiteit • Armoede • Avengers • Bewustzijn • Cognitieve bias (2x) • Cognitieve gedragstheorie • Context en landen • Corporate crimes • Cryptocurrency • Cultuur • Cyberoorlog en normalisatie • Daderperspectief • DarkNet • Dehunmanisering • Detectie • Digitaal bewijs	• Bewustzijn schade • Blokkeren van toegang • Chatrooms en sociale media • Frequentie • Game-items • Gebruikte kanalen • Geslacht en leeftijd • Internetgebruikers • Koopbaarheid van persoonsgegevens • Monitoren • Multilevel model • Neutralisatietechnieken	• Adequaat handelen • Algemene termen in e-mails • Autoriteit (2x) • Behulpzaamheid • Bewustwording (2x) • Decoy-pagina's • Detectiemethoden • Disproportioneel aandel • Dreiging • Financieel gewin • Frequentie • Interactie • Misdaadscripts (2x) • Monitoren	• Aankopen bankkaartgegevens • Aanpakken van neutralisaties en rationalisaties • Account Abuse Detection Principles (AADP) • Achtergrondinformatie werknemer • Afschrikking (2x) • Afwezigheid capabele bewaker • Altercasting • Anonimiteit • Anticiperen • Armoedebestrijding	• Accounts blokkeren • Anonimiteit verminderen • Bewustwording • Misbruik financiële problemen • Gesloten netwerken • Instagram • Monitoren en waarschuwingen • Neutralisatie- en normalisatietechnieken • Peer pressure en subculturele normen	• Authenticiteit • Autoriteit • Beloning en behulpzaam zijn • Demografische factoren • Gedrag afstemmen • Modus operandi en detectie-mechanismen • Motivatie • Normaal overkomen • Overtuigend profiel • Psychologische en sociale mechanismen	• Bewustwording • Concentratie criminaliteit • Detectie

[8] Het 'keer (x)- teken' met daarvoor een getal geeft het aantal aan waarin de betreffende factor in verschillende delicten binnen deze categorie/kolom wordt benoemd.
[9] Onder de categorie 'cybercriminaliteit' vallen de delicten hacking (3.1.2.) en malware (3.1.3).
[10] Onder de categorie 'Online fraude' vallen de delictenonline fraude (algemeen) (3.1.4), online romantisch fraude (3.1.7), pig-butchering scam (3.1.8), advance fee fraud (3.1.9), e-commerce fraude (3.1.10), concession-Abuse-as-a-Service (CAaaS)-fraude (3.1.11), online werkgelegenheidsfraude (3.1.12), online werknemersfraude (3.1.13), online bankpasfraude (3.1.14).

- Digitale ruimte (ethische filter)
- Disrespect
- Economische rechtvaardiging
- Ethisch gedrag
- Evaluatie
- Extravagante levensstijl
- Faciliterende factoren
- Financieel gewin
- Financiële problemen
- Frequentie
- Gebruik van persoonsgegevens
- Gemeenschap
- Geslacht (man)
- Groeiende dreiging
- Groepsdruk
- Hogere loyaliteiten
- Innovatieve methodes
- Intimidatie
- IT-kennis
- Kant-en-klare tools
- Koloniaal verleden
- Maatschappelijke eisen
- Neutralisatietechnieken (algemeen)
- Ontkennen van slachtofferschap
- Peers
- Persoonlijke informatie
- Plezier en impulsiviteit
- Rechtvaardigingsclaim
- Social engineering
- Steekproef
- Strafblad en recidive
- Veroordelaars veroordelen
- Verspreiding van schuld
- Verspreiding via download of bijlages in e-mails
- Woede
- Motivatie oplichter
- Onder druk zetten
- Phishingkits
- repository
- Rekrutering
- Samenwerking
- Sociale context
- Sociale contexten
- Sociale manipulatie
- Vergelijkend onderzoek
- VoIP-technologie
- Wetshandhaving
- Attitudes
- Audits
- Autoriteit (2x)
- Begeerlijk
- Beleefde toon
- Beleefdheid
- Beloning
- Betaalbaarheid
- Betrokkenheid bij niet-oplichters-praktijken
- Bewustwording (2x)
- Bewustwording (dader)
- Bewustzijn (2x)
- Blokkeren communicatie
- Certificering van datingsites
- Culturele normen veranderen
- Detectie (2x)
- Monitoren
- Diaspora
- Digitale omgeving
- Documenteren aard en
- Presenteren als reguliere bedrijven
- Privé-chats
- Regionale gerichtheid
- Subcultuur
- Voorlichting
- van slachtoffers
- Realistisch scenario schetsen
- Snel en eenvoudig
- Sociale norm
- Timing
- Urgentie en druk

• Meervoudige dader • Migratie • Migratiestatus • Monitoren • Ondersteuning slachtoffer • Ongelijkheid • Online platforms • Ontkennen van schade • Ontkennen van slachtofferschap • Ontkennen van verantwoordelijkheid • Peers • Psychoanalytische Theorie • Risico van AI • Risicobeoordeling • Risicogedrag • Samenwerking • Seksuele uitbuiting • Sociaal leertheorie • Sociaalgerichte interventies • Socio-economisch interventie • Space Transition theorie • Steekproef				omvang fraude • Economische marginalisatie • Effectiviteit van verlies-geframede waarschuwingen • E-mail • Empathieniveau • Evaluatie maatregelen • Externe validiteit • Financieel gewin (2x) • Focus op niet-technologisch beroep • Fraudebestrijdingsplan toekomstige crisis • Frequentie • Gecompromitteerde accounts • Gedeelde banden en gemeenschappelijke affiliaties			

			• Stress • Traditioneel en online sociaal leren • Verdienmodel • Veroordelen van de veroordelaars • Wetgeving (2x) • wetshandhaving • Wisselende MO • Wraak • Zelfbeschermingsmaatregelen		• Gedrag aanpassen en imitatie • Geestelijke gezondheid • Geldezels • Geloofwaardig overkomen • Genderdiscours • Generaliseerbaarheid en diversiteit • Geslacht (man) • Gesprek voortzetten op ander platform • Gevoel van controle en zelfvertrouwen • Gezins- en sociale omgeving • Groepsinteractie (2x) • Hebzucht • Heersende norm • Herhaaldelijke verzoeken	

					• Herstel en re-integratie • Het vier-ogen-principe • Hybride inter-actie • Impact ver-kleinen bij slachtoffers • Inschakelen handlangers • Internetge-bruik • Kwetsbaar-heid demo-grafische groepen • Liegen over eerdere ge-sprekken • Longitudinaal onderzoek • Maatschap-pelijke impact • Maatschap-pelijke norm • Medelijden en urgentie • Meerdere lan-den (2x) • Meldingsge-drag • Meldingspunt voor slachtof-fers		

- Menselijk gedrag
- Mentorschap (2x)
- Merchant Operation Protocol (MER-OP)
- Misbruik door familie
- Misbruik retourbeleid
- Misleiding
- Mixed method
- Modus operandi (3x)
- Monitoren
- Morele en juridische gevolgen
- Netwerk
- Neutralisatie bij ouders van fraudeurs
- Normalisatie
- Ondersteunende rol vrouw
- Ondersteuning slachtoffers
- Onderwijs en bewustwording
- Ondeugd

					• Ongebruikelijke gedrag • Ongecontroleerde toegang • Ontkennen van slachtofferschap • Opvolgberichten • Opvragen persoonlijke informatie • Ouders (2x) • Passend profiel • Patriarchale normen • Persoonlijke verhalen • Platform (2x) • Politieke en economische klimaat • Profiel • Psychologische kenmerken en gevolgen • Psychologische mechanismen • Rationalisaties • Real-time data			

- Rehabilitatie- en preventie-programma's
- Religieuze band
- Risico-identificatie
- Robin Hood
- Rol medeplichtigen
- Romantische band
- Routine-activiteiten theorie
- Salaris-tarieven manipuleren
- Samenwerking (4x)
- Samenwerking corrupte overheidsfunctionarissen
- Sancties
- Schaarste (2x)
- Screeningtools
- Sectorvergelijking
- Skimming
- Smurfen
- Social engineering

					• Social engineering-technieken • Sociale banden • Sociale bewijskracht • Sociale nabijheid • Software voor transacties • SQL-injectie • Steekproef • Strikte en onvermijdelijke straffen • Technologie • Telefoongesprekken • Timing waarschuwingsberichten • Toewijding • Urgentie (2x) • Verbergen identiteit • Verhogen van eisen • Verklaren dadergedrag • Verliesaversie (2x) • Verplichte vakanties en			

				functiewisse-lingen • Verschillende demografie • Vertrouwen opbouwen • Victim-bla-ming voorko-men • Vluchtgedrag • Voorlichting (2x) • Waarschu-wingsberich-ten • Wetgeving • Wettelijke voorschriften uitbuiten • Zelfbescher-mingsmaatre-gelen • Zoekmachi-nes			
Nega-tieve re-latie	• Empathie • Morele ontwikke-ling • Opleidingsniveau • Ouderschap • Religieuze over-tuigingen • Sociale banden • Zelfcontrole	• Persoonlijke rechtvaardiging • Relatie tot het slachtoffer • Welvaart	• Levensduur phishing-aanval	• Directe inter-actie • Leeftijd • Nepaccounts identificeren • SES en oplei-dingsniveau • Strafblad • Welvaart			

Ambigue relatie	• Altruïsme • Leeftijd	• Afschrikking • Chatrooms • Ontkennen van schade • Persoonlijke rechtvaardiging • Rechtvaardiging door vergelijking • Rechtvaardiging o.b.v. noodzaak • Verantwoordelijkheid ontkennen		• Geslacht en werkpositie • Leeftijd			
Descriptieve/ neutrale factoren	• Internet • Methode en data-analyse • Rol van staten • Versmelting van online criminaliteit		• Netwerk • Reverse phishing	• COVID-19 pandemie • Fases (6x) • Keuze slachtoffer • Methode en data-analyse • Mislukte oplichtingen • Netwerk (actoren) • Netwerk (structuur) • Obstakels voor opsporing en vervolging • Onderzoekssubject • Preventiemaatregelen en vertrouwen			• Methode en data-analyse

				• Tarieven service providers • Theoretische modellen • Veelvoorkomende methodes			