Ministerie van Justitie en Veiligheid

Jaarbericht

2024

Integrale aanpak

online fraude

Online fraude is een groot maatschappelijk probleem waardoor jaarlijks meer dan twee miljoen Nederlanders te maken krijgen met pogingen tot digitale oplichting. Overheid en bedrijfsleven werken samen aan het verminderen van het aantal slachtoffers en de schade door online fraude. Dat doen ze in de integrale aanpak online fraude op terreinen als kennisagenda, gegevensdeling, interventies, opvolging door politie en openbaar ministerie, weerbaarheid, preventie en hulp aan slachtoffers. In dit jaarbericht blikken we terug op de integrale aanpak in 2024.

2024: veel actie, veel nieuwe partijen

Voor de integrale aanpak was 2024 het jaar van actie. Veel nieuwe partijen sloten daarbij aan. Hoe meer hoe beter, vindt programmamanager Léon Poffé: “We hebben alle partijen in de fraudeketen nodig.”

In 2023 werd het fundament voor de integrale aanpak gelegd. Per thema kwamen partners samen die elkaar vaak nog niet goed kenden. Zij leerden elkaars positie kennen, bouwden samen kennis op en ontwikkelden een gezamenlijke werkwijze. In 2024 leidde dit tot een reeks acties in alle zes de thema’s. Die leidden ertoe dat de kring van partijen die betrokken is bij de integrale aanpak flink is uitgebreid.

Léon Poffé is daar blij mee: “In de fraudeketen spelen veel partijen een rol. Voor een effectieve aanpak heb je ze allemaal nodig. Die keten wisselt per vorm van online fraude: bij bankhelpdeskfraude spelen vervoerders bijvoorbeeld geen rol, maar bij aan- en verkoopfraude wel. Per fraudesoort kijken we welke partijen we nodig hebben om interventies te ontwikkelen. Het is fijn dat steeds meer partijen meedoen.”

Het afgelopen jaar zijn er bijvoorbeeld veel interventies ontwikkeld om bankhelpdeskfraude aan te pakken. Hebben die effect?

“Ja, het aantal gevallen van bankhelpdeskfraude daalt. Daardoor zoeken criminelen naar andere manieren om mensen geld af te troggelen. Het wordt steeds eenvoudiger om online fraude te plegen. Alles wat je aan informatie nodig hebt om fraude te plegen, wordt op het dark web aangeboden. Ook maken criminelen steeds beter gebruik van technologie. Denk aan spraakberichtjes met een stem die dankzij AI exact lijkt op die van je dochter. In de aanpak lopen we per definitie achter de feiten aan. De uitdaging is om die tijd zo kort mogelijk te houden. Waar we goed weten te interveniëren, zien we dat criminelen het voor gezien houden. Het is hun altijd om geld te doen en als geld verdienen met online fraude te moeilijk wordt, is dat niet meer interessant.”

Belemmeringen voor gegevensdeling vormen een knelpunt in de aanpak. Hoe kijk je daar tegenaan?

“Het is een ingewikkeld probleem. Stel dat je als bedrijf een mogelijke fraudeur belet om gebruik te maken van jouw producten en die persoon blijkt geen fraudeur te zijn, dan pleeg je een onrechtmatige daad. En als het over het delen van gegevens hebben, hebben verschillende partijen het dan over dezelfde gegevens? In de werkwijze die we binnen de integrale aanpak hebben ontwikkeld, analyseren we eerst

welke beletsels in de praktijk gegevensdeling tussen partijen in de weg staan. Vervolgens bepalen we: stel nu dat we in die situatie wél gegevens kunnen uitwisselen, draagt dat dan bij aan het voorkomen van online fraude? Die vraag moet je op grond van het proportionaliteitsbeginsel in de wet altijd stellen. En dan is de volgende vraag welke wettelijke kaders er gelden voor uitwisseling.”

Wat was eind 2024 de stand van zaken?

“We zijn van start gegaan met een wetenschappelijke proeftuin om samen met partners uit te vinden of gegevensuitwisseling iets oplevert en of het volgens de wet kan. In zo’n setting is er experimenteerruimte. Het is alleen lastig om partners uit het bedrijfsleven bereid te vinden om mee te doen. Sommige partijen geven aan dat het moeilijk is om

data uit hun systemen te ontsluiten en denken ook dat ze deze data ook in een proeftuinsetting niet mogen delen. Mijn indruk is dat er juridisch meer kan dan vaak wordt aangenomen. En door het te proberen, wordt vanzelf duidelijk tegen welke grenzen je aanloopt."

Is aanpassing van de wet het uiterste middel om meer gegevensdeling mogelijk te maken?

"Onze werkwijze in de integrale aanpak richt zich ook op de vraag of nieuwe wetgeving nodig is. Maar in de juiste volgorde: eerst aantonen dat het nodig is. Goed om te vermelden dat ons onderzoek naar zogenoemde suspicious devices eraan heeft bijgedragen dat de minister van Economische Zaken en Klimaat gestart is met een wetgevingstraject om de Telecomwet aan te passen. Doel is om meer verkeersgegevens te kunnen delen. Je kunt dan bijvoorbeeld zien of er met een bepaald telefoonnummer heel veel sms'jes zijn verstuurd."

Inmiddels is het 2025. Wat zijn de doelen voor dit jaar?

"We blijven samenwerken op de zes thema's, met de focus op de thema's gegevensdeling en technische barrières. In proeftuinen willen we nieuwe concrete maatregelen ontwikkelen. Verder gaan we scherper monitoren of eerder gemaakte afspraken over de inzet van partners worden nagekomen. En tot slot willen we nog meer partners bij de integrale aanpak betrekken. Over de periode na 2025 kan ik zeggen dat de integrale aanpak zeker doorgaat. De Tweede Kamer is heel tevreden over de aanpak en heeft de motie Michon-Derkzen aangenomen waarin de regering wordt gevraagd deze door te ontwikkelen. Ons actieplan voor 2025 legt daar de basis voor."

Een positieve uitsmijter: "We zijn in 2024 echt toegekomen aan concrete acties waarmee online fraude wordt aangepakt. Dit levert zicht op wat goed werkt en waar er nog een tandje bij moet. Als programmamanager kan ik daar alleen maar tevreden mee zijn."

Kennisagenda

Breed onderzoek naar de civielrechtelijke aanpak van online fraude

Het civiel recht spreekt niet over daders en slachtoffers, maar over schuldeisers en debiteuren. Voor slachtoffers van online fraude kan dit een weg zijn om genoegdoening te krijgen. Susanne van 't Hoff-de Goede doet namens de Haagse Hogeschool onderzoek naar de civielrechtelijke afdoening van online fraude. In 2024-2025 werden drie projecten afgerond, vier projecten zijn in voorbereiding.

Een paar jaar geleden las Susanne een LinkedIn-bericht van een organisatie die slachtoffers van online fraude opriep contact op te nemen. Wij kunnen je helpen via het civiel recht je geld terug te krijgen, was de strekking. "Mijn eerste reactie was: fantastisch. Over het algemeen is het maar de vraag of slachtoffers van online criminaliteit genoegdoening krijgen. Slachtoffers van bankhelpdeskfraude kunnen proberen aan-

spraak te maken op een coulanceregeling van banken. Maar bij andere vormen van online fraude kon je je als slachtoffer vooral tot het strafrecht wenden. We weten dat maar een klein percentage van alle aangiften van online fraude uiteindelijk voor de rechter komt, waarbij voeging voor schadevergoeding mogelijk is. Bovendien geldt er voor dergelijke schadevergoeding dat de staat garant staat tot een maximum van vijfduizend euro, wat niet altijd de volledige schade dekt. En dan is het de vraag of de dader geld heeft om de rest van de schade terug te betalen."

Praktische uitvoering en juridische grondslag

Het LinkedIn-bericht riep ook vragen bij haar op. Die leidden tot een breed onderzoeksprogramma waarvan de eerste deelonderzoeken in 2024 werden afgerond. In het eerste werden de praktische uitvoering en de juridische grondslag van civielrechtelijke afdoening in kaart gebracht. Belangrijk, aldus Susanne, omdat dit voor online fraude nog niet was beschreven.

Een van de bevindingen was dat slachtoffers via verschillende routes een civielrechtelijke procedure kunnen starten door een rechtsvertegenwoordiger. Susanne: "Soms kennen ze de naam- en adresgegevens van degene aan wie ze geld hebben overgemaakt en wat achteraf fraude bleek te zijn. In andere gevallen verkrijgen slachtoffers deze gegevens via een procedure bij hun bank. Hiernaast loopt er nog een proef in drie politie-eenheden waarbij slachtoffers worden doorverwezen naar drie rechtsvertegenwoordigers die hieraan meedoen. Dat doorverwijzen gebeurt onder voorwaarden: als een vermeende fraudeur bijvoorbeeld onder toezicht is gesteld, vindt er geen doorverwijzing plaats."

Kennis en behoeften van slachtoffers

In een tweede deelonderzoek peilden Susanne en haar collega Merel van Leuken de kennis en behoeften van (potentiële) slachtoffers. Opvallende uitkomst: twee derde van alle ondervraagden wist niet van het bestaan van de civielrechtelijke route. Verder bleek er een kloof te zitten tussen intentie en gedrag: ondervraagden die nog geen slachtoffer waren, gaven vaker aan bereid te zijn een civielrechtelijke procedure te starten in het geval van online fraude dan slachtoffers. Mogelijk zien mensen meer barrières als ze eenmaal slachtoffer zijn geworden van online fraude."

Ervaringen van slachtoffers

In het derde deelonderzoek is onderzoek gedaan naar de ervaringen van slachtoffers met de civielrechtelijke procedure. Opvallende uitkomst was dat de beweegredenen om zo'n procedure te starten sterk uiteenlopen: "Lang niet alle geïnterviewden noemden financiële genoegdoening als reden. Er waren bijvoorbeeld veel slachtoffers die aangaven dat ze

wilden dat de fraudeur zou worden afgeschrikt. Of ze wilden voorkomen dat er nog meer slachtoffers zouden vallen."

Vier deelonderzoeken lopen nog. Eén daarvan bekijkt de civielrechtelijke procedure vanuit de dader: wat zijn vanuit dat perspectief de ervaringen? Volgens de planning wordt dit onderzoek eind 2025 afgerond. Dit geldt ook voor een onderzoek naar de gevolgen van de civiele route als deze op grote schaal toegepast gaat worden. Ook wordt onderzocht hoe de civielrechtelijke afdoening van online fraude tussen 2021 en 2023 is verlopen. De resultaten van het laatste deelonderzoek worden naar verwachting in maart 2026 bekend. Daarin worden handvatten voor slachtoffers en andere partijen ontwikkeld.

Ambitie: langlopend onderzoek

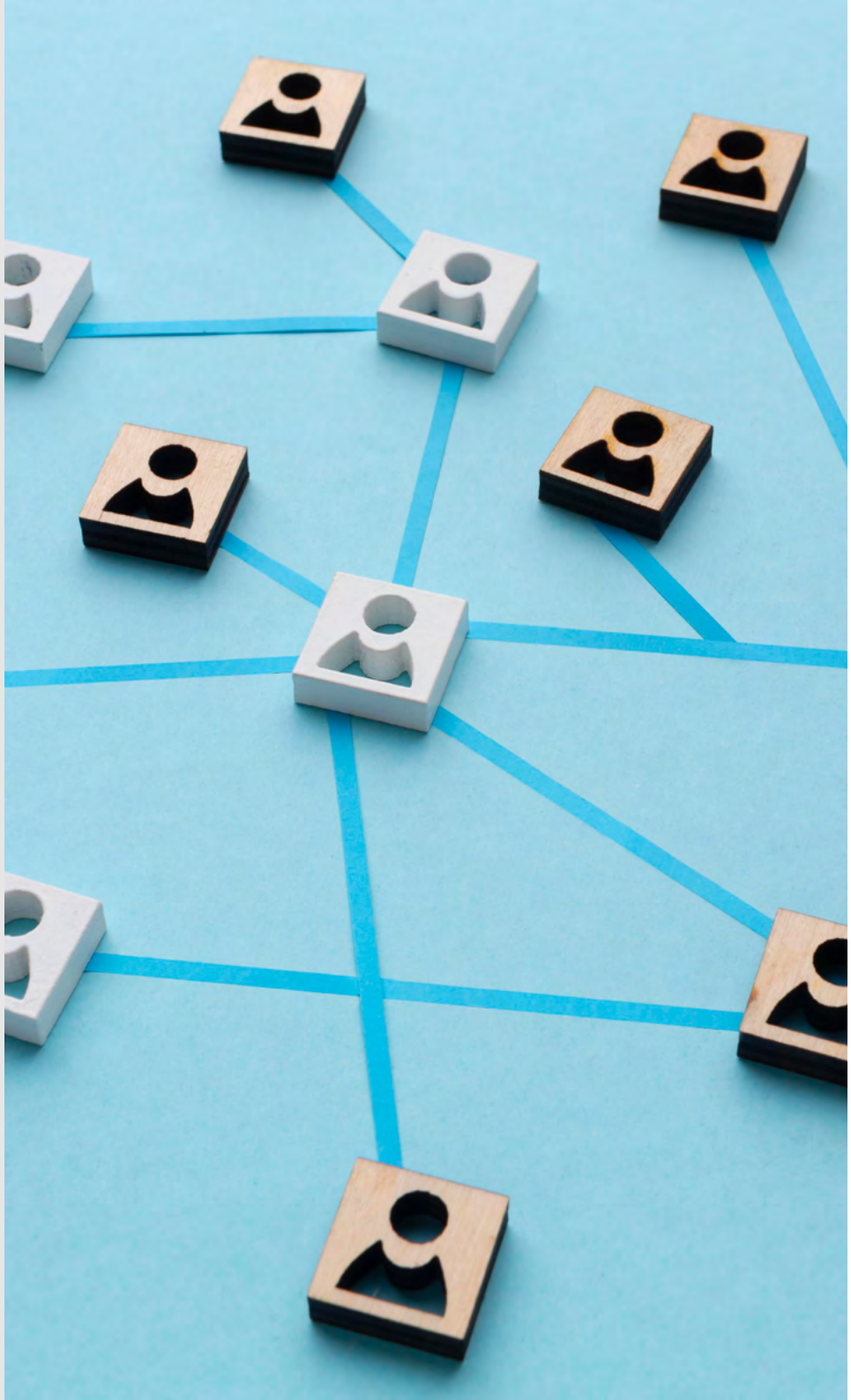
Ze heeft grote ambities: "Ik wil langlopend onderzoek gaan doen onder slachtoffers van online criminaliteit: "Welke 'reis in de tijd' maken ze door als slachtoffer en welke ervaringen doen ze gaandeweg op? En er is volgens haar onderzoek nodig naar victim blaming: "Nog veel te vaak krijgen slachtoffers van online criminaliteit de schuld van anderen, zelfs van hun partner of hun kinderen. Dit heeft niet alleen negatieve gevolgen voor het welzijn van slachtoffers, maar ook op hun hulpzoekgedrag. Dit moet echt anders. Ik wil begrip kweken voor het feit dat iedereen slachtoffer kan worden van online criminaliteit. Het is niet iets waar je 'intrapt', maar iets dat jou wordt aangedaan."

Gerealiseerd

- start 'Zicht op gedigitaliseerde criminaliteit' als dashboard voor informatie over online fraude in Nederland
- fenomeenbeeldanalyse online fraude Politie
- presentatie Integrale Aanpak Online Fraude bij Global Anti Scam Summit
- deelname partners Integrale Aanpak Online Fraude aan brainstorm 'van wetenschap naar praktische aanpakken' (Hogeschool Saxion)
- delen kennis andere landen tussen partners
- verdere uitbouw www.integraleaanpakonlinefraude.nl

Niet gerealiseerd

- onderzoek aard en omvang slachtofferschap online fraude in het bedrijfsleven (start Q1 2025)
- periodieke uitwisseling modus operandi (start Q1 2025)
- Nieuwsbrief (wel nieuwsberichten via het online platform)

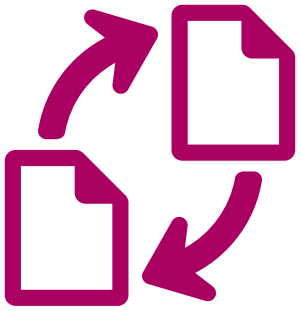


Gegevensdeling

Kijken naar wat wél kan

Partijen die te maken hebben met online fraude, kunnen niet zomaar persoonsgegevens met elkaar delen. Zeker voor gegevensdeling tussen sectoren zijn er veel mitsen en maren. Volgens Thijs Drouen - partner bij Hooghiemstra & Partners – overheerst daardoor het beeld dat delen vooral níet mag. Met zijn werkgroep analyseert hij wat nu al wél kan of wat er moet gebeuren om het mogelijk te maken.

In 2024 heeft de privacy-expertgroep flink wat betrokkenen geïnterviewd. “We wilden om te beginnen weten in welke fase partijen met online fraude te maken krijgen”, legt Drouen uit. “Hoe zit dat met een thuiswinkel, met een telecomprovider, met een bank? Wanneer komt de politie in beeld? We hebben in die interviews niet alleen besproken wat partijen doen als het misgaat, maar ook wat je preventief kunt doen om online fraude te voorkomen en in welke mate ketenpartners daarbij een rol spelen.”



‘Balans vinden tussen informatiebehoefte en bescherming van persoonlijke levenssfeer.’

Balans vinden

De balans vinden tussen de informatiebehoefte van partijen en de bescherming van de persoonlijke levenssfeer van mensen, dat is de uitdaging. “Er zitten flinke risico’s aan gegevensdeling”, beaamt Drouen. “Voorkomen moet worden dat mensen alleen maar op grond van een verdenking van fraude in een sociaal isolement terechtkomen.”

Partijen moeten daarom altijd de noodzaak van gegevensdeling kunnen aantonen, op basis van de grondslagen die daarvoor zijn. Drouen ziet dat dit leidt tot risicomijdend gedrag: ‘het zal wel niet mogen’. Los daarvan zijn er volgens hem ook andere motieven die gegevensdeling in de weg staan: “Sommige bedrijven vinden het geen goed idee om ervaringen met concurrenten te delen. Want dat zegt misschien iets over hun bedrijfsmodel.”

Multi-party computation

Obstakels genoeg, maar Drouen ziet interessante ontwikkelingen. Als voorbeeld noemt hij multi-party computation: “Met die technologie kun je voor een specifiek doel data ophalen bij partijen zonder dat die partijen elkaars data kunnen inzien. Uit de versleutelde data kun je waardevolle inzichten voor dat specifieke doel halen, maar de data zelf blijven bij de bron. Op basis van dit soort analyses kunnen ketenpartners bijvoorbeeld beter zicht krijgen op fraudevormen en het voorkomen daarvan”

De analyse van de werkgroep is nog niet klaar en Drouen wil nog niet op de resultaten vooruitlopen. Hij zegt wel dat de interviews een goed beeld hebben opgeleverd over wat qua gegevensdeling al wel kan en waar misschien aanpassing van wetgeving wenselijk is. Op casusniveau wordt daar komend jaar verder aan gewerkt. Drouen: “We spreken niet een bepaalde voorkeur uit. Je moet onze analyse zien als input voor beleidsmakers en bestuurders om beslissingen te nemen.”

Mogelijkheden zichtbaar maken

Met het Privacykader heeft de AP een tijdje geleden een analyse gegeven van waar cross-sectorale gegevensdeling aan moet voldoen. Met onze werkgroep proberen we zichtbaar te maken dat er in veel gevallen best mogelijkheden zijn om binnen die voorwaarden te blijven, waarbij niet wordt ontkend dat dat de conclusie kan zijn dat de wetgever aan zet is."

Hij is ervan overtuigd dat online fraude ook binnen het kader van het gegevensrecht effectiever kan worden aangepakt: "Het vergt een gezamenlijke investering in denkkracht, tijd en geld. Het is goed dat de overheid hier samen met de sectoren aan werkt. Ik zie ook graag dat de AP aansluit om samen met alle partners na te denken hoe verantwoorde gegevensdeling mogelijk is. Laten we alle lijnen bij elkaar brengen. Ik geloof dan ook in deze integrale aanpak."

Gerealiseerd

- advies over gegevensdeling ten aanzien van 'suspicious devices'
- overleg Autoriteit Persoonsgegevens (loopt door in 2025)
- quickscan delen strafrechtelijke gegevens in EU-landen (beperkt)

Niet gerealiseerd

- afronding TNO-onderzoek (Q2 2025)
- 'privacy kader' (afronding Q1/2 2025)
- uitwerking oplossingsrichtingen
- handleiding gegevensdeling

Barrières en interventies

Veilig bankieren makkelijker maken

Op de websites van alle banken vind je adviezen over veilig bankieren. Belangrijk, want door veilig te bankieren hebben criminelen minder kans om toe te slaan. De Rabobank constateerde dat er een kloof zit tussen wéten hoe je veilig je bankzaken regelt en het ook echt dóen. Door de app aan te passen, kunnen klanten nu veel makkelijker in actie komen, leggen Sven Troost (productmanager) en Chris van der Ven (design lead) uit.

Wat was precies het probleem?

Van der Ven: “De Rabobank biedt klanten meerdere oplossingen om hun veiligheid te vergroten. Op onze website legden we al heel goed uit wat je als klant kunt doen om veilig te bankieren en waarom dat belangrijk is. Uit onze data blijkt dat onze informatie over veilig bankieren veel wordt geraadpleegd. Maar we zagen ook dat mensen die deze informatie lezen, lang niet altijd in actie kwamen, omdat ze niet direct konden doorklikken naar de betreffende functionaliteit in de app. Daar kwam

Sven Troost

Chris van der Ven

bij dat de verschillende functionaliteiten om veilig te bankieren versnipperd in de app werden aangeboden. Dat heeft ermee te maken dat sommige functies ook bij een specifiek product horen. Denk aan het instellen van je limieten. Daardoor waren functionaliteiten slecht vindbaar voor de klant."

Welke oplossing hebben jullie ontwikkeld?

Troost: "We hebben alles over veilig bankieren in de app in één onderdeel samengebracht. Als klant lees je nu op één plek wat je allemaal kunt doen. Nieuw is ook dat je vanuit die informatie meteen kunt doorklikken om bijvoorbeeld je daglimiet aan te passen. Of om meteen in actie te komen als je slachtoffer van online fraude bent geworden. Voorheen kon dat niet, omdat de informatie op een webpagina buiten de app stond. De drempel is nu veel lager. En het werkt ook: behalve dat veel klanten op zoek zijn naar informatie, klikken ze nu ook veel door."

Hoe past de oplossing bij de integrale aanpak?

Troost: "Vanuit de integrale aanpak is voor banken de interventie 'veiligheidspagina' gekozen. Dit naar aanleiding van de criminal journey bankhelpdeskfraude. Dit sloot heel goed aan op onze ideeën voor veilig bankieren. Het gaf ons een boost om onze ideeën ook echt te realiseren."
Van der Ven: "En natuurlijk zijn we er trots op dat we de interventie als eerste bank gerealiseerd hebben."

Wat staat er nog op het wensenlijstje?

Troost: “We zijn met van alles bezig. Om een voorbeeld te noemen: “We willen een sterkere connectie tussen ouder en kind via de app. Kinderen zijn een kwetsbare groep en we willen ouders graag meer mogelijkheden bieden om kun kind te begeleiden als onderdeel van de financiële opvoeding.”
Van der Ven: “We stappen ook af van onze one-si-ze-fits-all-benadering van klanten. Jongeren moet je anders aanspreken dan ouderen. Iedere doelgroep vraagt om een andere toon en om andere functionaliteiten. In ontwerpses-sies met de doelgroep willen we doorgronden hoe we onze content kunnen laten aansluiten op de realiteit van die groep. Daar willen we de komende tijd een flinke stap in zetten.”

‘Het gaf een boost om onze ideeën ook echt te realiseren.’

Gerealiseerd

- ‘criminal journeys’ en barrièremodellen bank-helpdeskfraude en aan- en verkoopfraude
- ontwikkelen en uitvoeren interventies bank-helpdeskfraude en aan- en verkoopfraude (deels doorlopend in 2025)
- contactpersonenlijsten organisaties in ‘fraudeketen’

Niet gerealiseerd

- ‘criminal journey’ beleggingsfraude (Q1 2025)
- herijking ‘criminal, journeys’ en barrièremodellen bankhelpdeskfraude en aankoop- en verkoopfraude (2025)
- start proeftuin ‘suspicious devices’
- onderzoek mogelijkheden afspraken per sector (2025)

Opvolging door politie en OM

Net als de crimineel heeft ook de Politie zich naar het internet verplaatst

Aad Lensen werd een paar jaar geleden betrokken bij een grote zaak rond valse webshops. De dader werd opgepakt en sindsdien wordt hij steeds vaker bij zaken van online fraude betrokken. Digitale criminaliteit móet je met partners aanpakken, weet hij.

Van kauwgomballendief tot moordenaar. In de 33 jaar dat Aad Lensen bij de Politie werkt, heeft hij bijna elk type dader wel langs zien komen. De laatste jaren ziet hij dat criminelen zich van de straat naar de computer verplaatsen: “Criminelen hebben al jaren geleden het internet ontdekt. Als Politie kunnen we niet zeggen: daar zijn we niet van. We zijn er zelfs honderd procent wél van, net als van de klassieke autokraak en de woninginbraak.”

Maar waar een klassieke inbreker op een dag, zoals Lensen het zegt, ‘maximaal een pandje of vier kan doen’, kan een crimineel in dezelfde tijd honderden, misschien wel duizenden

slachtoffers hebben gemaakt. Dat maakt de bestrijding ervan uitdagend. Daar komt bij dat online criminaliteit niet aan een locatie gebonden is. De politie-eenheden zijn dat wel. In de landelijke aanpak Operatie Centurion werken de Politie en het OM daarom aan een betere structuur om online criminaliteit effectiever op te kunnen volgen. Lensen: “We moeten ons daar echt nog wel meer in ontwikkelen, maar we hebben al wel mooie stappen gemaakt.”

Datagedreven werken

Als voorbeeld noemt hij het datagedreven weken: “Rond verkoopfraude werken we al langer zo. Daarbij herkent het systeem bepaalde fenomenen. Stel dat een bepaald bankrekeningnummer aan een aantal aangiften van online fraude hangt en ons systeem ziet dit rekeningnummer ook terugkomen in aangiften in Limburg en Friesland, dan worden deze aangiften automatisch geclusterd en pakken we de zaak met prioriteit op.”

Voor een effectieve aanpak van online fraude is samenwerking met andere partijen een must, stelt Lensen. “Telecombedrijven, techbedrijven, vervoerders, banken; ze beschikken allemaal over onmisbare puzzelstukjes aan informatie.” Hij noemt de Electronic Crime Task Force als voorbeeld. Deze expertgroep van Politie, OM, banken en een creditcardmaatschappij maken samen analyses waarmee de opsporing verder kan. “Aan de hand van hun analyses kwam de dader van een grote zaak van bankhelpdeskfraude bijvoorbeeld in beeld.”

Zaken moeten dan wel worden opgevolgd. In Operatie Centurion is proefgedraaid met een landelijk coördinatieteam dat als verdeelstation naar de regionale politie-eenheden werkt. Die aanpak werkt zo goed dat die nu verder wordt ontwikkeld rond analyse, coördinatie en interventie. “Met die landelijke werkwijze willen we bijvoorbeeld voorkomen dat er in Limburg en Groningen collega’s bezig zijn met dezelfde dadergroep, zonder dat zij dat van elkaar weten.”

Impact is groot

Hij benadrukt dat de impact van online criminaliteit op slachtoffers groot kan zijn: “Jildau Borwell, cybercrimespecialist bij de politie, heeft hier onderzoek naar laten uitvoeren. Uit haar onderzoek blijkt zelfs dat online fraude soms meer impact heeft op slachtoffers dan vergelijkbare reguliere delicten.” Hij is blij met het initiatief van collega’s in Oost-Nederland die slachtoffers van online criminaliteit thuis bezoeken: “Alleen al om mensen hun verhaal te laten vertellen en ze met raad en daad bij te kunnen staan. Het mooie is dat de pakkans daardoor soms wordt vergroot. Stel dat iemand zijn bankpas heeft afgegeven, waarna zijn rekening is leeggehaald. Dan blijkt bijvoorbeeld dat de buren een slimme

deurbel hebben hangen of een kenteken van een verdacht iemand hebben genoteerd. Dat biedt mooie kansen voor de opsporing."

Hij is blij met de samenwerking met kennisinstellingen, waaronder de Haagse Hogeschool, Saxion Hogeschool en de Universiteit Leiden. "Ik vind dat een goede ontwikkeling dat onderzoekers steeds meer diepgaand onderzoek naar online criminaliteit doen. Dit levert ons waardevolle inzichten op over hoe het fenomeen in elkaar steekt en welke interventies effectief kunnen zijn. We doen hier ook zelf onderzoek naar. Een van de producten die dit heeft opgeleverd, is een fenomeenanalyse van de tien meest voorkomende vormen van gedigitaliseerde criminaliteit."

'Te gek voor woorden'

En ja, soms zit privacywetgeving in de weg, omdat partijen cruciale opsporingsgegevens niet met elkaar kunnen delen. Lensen noemt het 'te gek voor woorden' dat een verdachte die via een online verkoopplatform tientallen mensen heeft opgelicht vervolgens gewoon bij een ander platform zijn gang kan gaan. Simpelweg omdat het ene platform niets mag delen, al is het maar alleen een red flag. "Het kan niet zo zijn dat privacywetgeving alleen de verdachte beschermt. Gelukkig gaat het stapje voor stapje beter, maar we lopen steeds nog tegen obstakels aan."

Gerealiseerd

- periodieke informatiedeling bij opsporing en vervolging
- tussentijdse presentaties uitkomsten onderzoek naar criminele netwerken achter 'geldezels'
- tussentijds presentaties uitkomsten onderzoek naar civiel schadeverhaal

Niet gerealiseerd

- besluit inrichting online aangifteloket bedrijfsleven (2025)

Weerbaarheid en preventie

Be!eef Beurs schoolvoorbeeld van integraal werken

Esther Mieremet (Veiliginternetten) merkt dat partijen in de integrale aanpak heel nieuwsgierig zijn naar wat er allemaal al gebeurt rond preventie en weerbaarheid. Wat elders goed werkt, kan zo worden gekopieerd. Als het tenminste maar bijdraagt aan het grotere geheel.

Veiliginternetten.nl is de toepasselijke naam voor de website die burgers al meer dan tien jaar adviezen geeft over hoe zij veilig kunnen internetten. Esther Mieremet is namens het onafhankelijke platform ECP verantwoordelijk voor de inhoud van de website en het netwerk van alle partijen die eraan bijdragen. Sinds 1 januari is zij ook projectleider van de actielijn Preventie en weerbaarheid binnen de integrale aanpak online fraude. Die rol past haar goed, want veel van de partijen die aan de integrale aanpak meedoen, zitten ook in het netwerk achter veiliginternetten.nl: “Samen met publieke en private

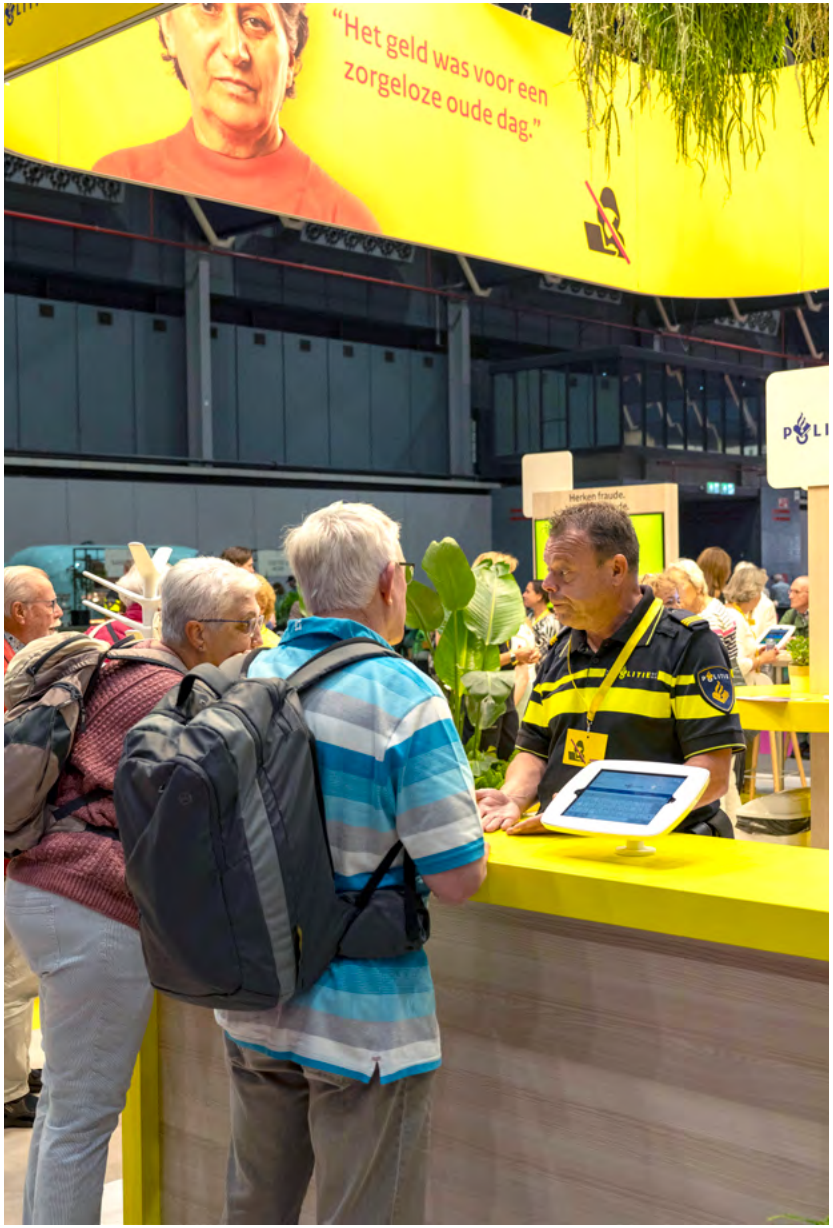
partners bedenken we ideeën voor de inhoud van de website en ontwikkelen we bijvoorbeeld publiekscampagnes. Samen willen we voor een veiliger internet zorgen. Dat hoeft niet allemaal onder één paraplu. Als bijvoorbeeld KPN iets slims bedenkt voor zijn klanten, dan communiceren ze dat via hun eigen kanalen."

De stichting ECP ontstond zo'n 25 jaar geleden toen het mogelijk werd om met pin in winkels af te rekenen. Om te voorkomen dat iedere bank een eigen pinapparaat op de toonbank zou zetten, moest er één systeem komen. Het plan daarvoor ontstond aan de tafel van ECP. Al snel groeide het platform uit tot de plek waar publieke en private partijen samen oplossingen bedenken voor uitdagingen rond digitalisering. "We zijn al jaren een schakel in preventie en weerbaarheid", aldus Mieremet. "En nu zijn we ook onderdeel van het projectteam van de integrale aanpak."

Wat is er rond preventie en weerbaarheid gebeurd binnen de integrale aanpak?

"Blikvangers waren de beurs Be!eef, voorheen de 50Plus-Beurs, en de Senioren Expo. Die laatste vond begin 2025 plaats, maar we zijn natuurlijk al eerder begonnen met de voorbereidingen. We waren op beide beurzen in één stand aanwezig met de Politie, Slachtofferhulp Nederland, de Fraudehelpdesk en de NVB. Voor mij is het een mooi voorbeeld van integraal werken om samen de doelgroep aan te spreken en te helpen. Mensen kwamen langs voor advies, maar lieten ons soms ook hun schrijnende verhaal horen. Anderen vertelden dat zich prima digitaal redden, maar wilden toch weten of ze bepaalde zaken rond digitale veiligheid goed begrepen hebben. Tijdens beide beurzen verzorgde de Politie ook sessies over wat je als burger aan preventie kunt doen."

'Inzichten en ervaringen nog beter met elkaar delen.'



Hoe verloopt de samenwerking tussen de partijen?

"Goed. Alle afzonderlijke partijen doen veel aan preventie en weerbaarheid. De intrinsieke motivatie is groot; het is geen doel dat van hogerhand wordt opgelegd. De uitdaging is om te zorgen voor integraliteit. We zoeken samen altijd naar een gemeenschappelijk belang in de aanpak. Binnen onze actielijn komen we ongeveer een keer in de zes weken samen. De groep die dan samenkomt, is groter dan alleen maar de kernpartners van de integrale aanpak. Afhankelijk van de agenda kijken we welke partijen we graag willen laten aansluiten. Denk aan een partij als het Centrum voor Criminaliteitspreventie en Veiligheid, dat bijvoorbeeld filmpjes voor senioren heeft ontwikkeld waarmee ze buurthuizen en bibliotheken bezoeken. We willen natuurlijk dat andere partijen van hun inzichten en expertise kunnen profiteren. Denk ook aan de Veiligheidsalliantie Rotterdam en de regionale aanpak van de Politie Oost-Nederland, gericht op bestrijding van online criminaliteit. Er gebeurt al heel veel en met de integrale aanpak willen we inzichten en ervaringen nog beter met elkaar delen."

Senioren zijn een belangrijke doelgroep. Jongeren ook?

"Zeker. Niet alleen omdat ze vaak slachtoffer zijn, maar ook omdat kwetsbare jongeren vaak als geldezel worden ingezet. In preventieve zin is er veel meer nodig dan dat ze tegen ze

zegt: Pas op, je hebt nu een strafblad. Want het kan nog altijd heel lucratief zijn om je pinpas uit te lenen. Om legaal net zo veel te verdienen, moet je volgens mij een halfjaar bij de supermarkt werken. Kernvraag is: wat moeten we als samenleving doen om ervoor te zorgen dat zij niet voor het snelle geld kiezen?"

Wat staat er op de agenda voor 2025?

"Allereerst wil ik graag nog meer structuur aanbrengen in hoe we werken. Wat doen we wel en wat is niet reëel? Het actieprogramma dat we hebben opgesteld, is daarvoor leidend. Integraal werken betekent ook dat we elkaar moeten blijven opzoeken en zorgen dat we interventies niet allemaal op hetzelfde moment doen. Dus bijvoorbeeld niet alle activiteiten gericht op senioren organiseren in april en mei, waarna er voor die groep de rest van het jaar niets meer wordt gedaan. 2025 wordt ook het jaar waarin we willen zorgen dat de samenwerking ook de komende jaren doorgaat. De overheid moet bezuinigen, maar ziet de urgentie om online fraude tegen te gaan ook. Misschien moeten we het anders gaan organiseren. Verder wil ik graag aan de buitenwereld nog beter laten zien dat de integrale aanpak van preventie en weerbaarheid werkt. Als burger voel je je toch veiliger als je weet dat allerlei partners samenwerken aan digitale veiligheid."

Gerealiseerd

- Veiliginternetten.nl verzorgt de centrale regie / coördinatie
- partners stemmen onderling campagnes af en werken ook samen
- bij Beleef! en seniorenbeurs hebben partners gezamenlijk de integrale aanpak gepresenteerd

Niet gerealiseerd

- campagnekalender (2025)
- preventiestrategie
- eigen preventieve maatregelen

Hulp aan slachtoffers

‘Je hebt elkaar nodig om de juiste dingen te doen’

Online fraude veroorzaakt veel ellende bij slachtoffers. Voor praktische, juridische, preventieve en psychosociale hulp kunnen zij bij verschillende meldpunten terecht. Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) ontwikkelde samen met de werkgroep Hulp aan slachtoffers handige hulpmiddelen voor medewerkers van meldpunten en voor slachtoffers zelf. Daardoor weten slachtoffers beter welke stappen ze moeten zetten om de juiste hulp te krijgen.

In 2023 ontwikkelde het CCV al een handige factsheet die medewerkers van meldpunten helpt om slachtoffers van online fraude naar het juiste punt te verwijzen. Deze factsheet kreeg in 2024 een vervolg, legt Claessens uit: “Het ontbrak nog aan een compleet beeld van wat je als slachtoffer kunt doen. Daarom hebben we vijf vuistregels opgesteld. De eerste stap is meestal dat je melding doet bij je bank en vervolgens bij de politie. Wil je schade verhalen, dan kun je dat ook op verschillende manieren doen. En als je behoefte hebt

aan psychosociale hulp, dan kun je je melden bij Slachtofferhulp Nederland. De laatste stap die je kunt zetten, is vooral bedoeld om meer slachtoffers te voorkomen. Ook daar zijn meldpunten voor."

Deze vijf vuistregels zijn eerst opgesteld voor de meldpunten zelf. In de tweede helft van 2024 is er ook een flyer gemaakt bestemd voor de slachtoffers zelf. "We hebben deze flyer bewust gelanceerd bij de politie", legt Claessens uit. "De politie gaat steeds vaker langs bij slachtoffers van online fraude, maar politiemensen hebben dan niet alle tijd van de wereld. Ze kunnen in ieder geval de flyer achterlaten zodat het slachtoffer weet wat hij of zij kan doen."

Hulp bundelen

Claessens geeft toe dat het 'meldpuntenlandschap' er ook voor hem als professional best ingewikkeld uitziet. Zou het niet beter zijn als er één meldpunt komt? "Dat zou heel mooi zijn. Maar dat moet organisatorisch ook kunnen en zover is het nog niet. Sommige organisaties hebben bepaalde bevoegdheden die andere niet hebben. En dan zijn er ook nog allerlei beperkingen die gegevensdeling in de weg staan. Mijn hoop is wel dat we met de integrale aanpak de hulp aan slachtoffers iets kunnen bundelen. Zodat je als slachtoffer minder stappen hoeft te zetten."

Ondertussen is het CCV ook bezig met de ontwikkeling van een zelfhulptool voor slachtoffers. "Die is niet alleen bedoeld voor slachtoffers van online fraude, maar ook van hacken en online geweld. Het idee is dat slachtoffers na het invullen van een korte vragenlijst advies op maat krijgen. Bij de ene vorm van fraude is het bijvoorbeeld belangrijk om je bank te bellen. Bij identiteitsfraude moet je ook contact opnemen met het Centraal Meldpunt Identiteitsfraude. Dat hoeft bij andere vormen weer niet. Die tool neemt slachtoffers aan de hand en de uitkomst is afhankelijk van wat jou is overkomen."

'Elkaar kennis en expertise gebruiken'

Twee jaar geleden wisten medewerkers van meldpunten soms niet van het bestaan van andere meldpunten af. Dat is nu wel anders, zegt Claessens: "We weten veel beter van elkaar wie we zijn, wat we doen en hoe we slachtoffers van online fraude snel kunnen doorverwijzen. Bij het opstellen van de vijf vuistregels merkte ik hoe belangrijk het is om gebruik te kunnen maken van elkaars kennis en expertise. Slachtofferhulp Nederland kan bijvoorbeeld precies aangeven welke toon je in de tekst moet aanslaan. Je hebt elkaar nodig om de goede dingen te doen."

Wat staat er op zijn wensenlijstje? "Een betere koppeling tussen wetenschap en praktijk. Er wordt gelukkig steeds meer wetenschappelijk onderzoek gedaan. Tot nu toe sloot er inci-

denteel wel eens een wetenschapper aan bij een bijeenkomst van onze werkgroep. Vanaf nu gebeurt dat structureel. Er is steeds meer bekend over hoe slachtoffers delicten ervaren en aan welke hulp zij behoefte hebben. Laatst volgde ik een presentatie over civielrechtelijk schadeverhaal. Uit onderzoek van de Haagse Hogeschool blijkt dat de meeste slachtoffers niet weten dat die mogelijkheid er is, terwijl het wel belangrijk voor hen kan zijn. Op basis van het onderzoek verkennen we nu hoe we de civielrechtelijke optie beter bekend kunnen maken”

Aandacht voor herhaald slachtofferschap

Claessens wil daarnaast meer aandacht voor herhaald slachtofferschap. “Er is een groep kwetsbare mensen die meerdere malen slachtoffer wordt van online fraude. Uit onderzoek blijkt dat de kans dat slachtoffers van online fraude binnen één jaar opnieuw slachtoffer worden van online fraude bijna vier keer zo groot is als diezelfde kans voor niet-slachtoffers van online fraude. Als deze slachtoffers zich melden bij één van de meldpunten kunnen hier specifieke interventies voor ontwikkeld worden. Daar liggen nog heel veel kansen.”

Gerealiseerd

- technische ondersteuning en advisering slachtoffers bij verschillende informatiepunten digitale Overheid
- vuistregels voor intake door meldpunten
- folder hulpaanbod slachtoffers bij meldpunten

Niet gerealiseerd

- halfjaarlijkse slachtofferpanels (2025)
- ontwikkeling ‘tool’ voor verwijzing naar juiste aanspreekpunt (2025)
- integratie meld- en hulpvoorzieningen in www.mijnslachtofferzaak.nl (2025)
- vergroten bekendheid mogelijkheden civiel schadeverhaal (2025)

Voor meer informatie:

integraleaanpakonlinefraude@minjenv.nl

integraleaanpakonlinefraude.nl

Integrale aanpak

online fraude