Ministerie van Justitie en Veiligheid

Impressie van de eerste werkconferentie

Aan de oever van de Maarsseveense Plassen, in congreslocatie InnStyle, kwamen een paar honderd professionals bijeen voor de eerste werkconferentie van de Integrale aanpak online fraude. Na een welkom door programmamanager en dagvoorzitter Léon Poffé introduceert hij Lisette de Bie, plaatsvervangend directeur-generaal Rechtspleging en Rechtshandhaving bij het ministerie van Justitie en Veiligheid (JenV). Zij blikt terug op de start van het programma in 2022. “Sindsdien is de samenwerking flink gegroeid; nieuwe partijen sloten zich aan.” Een goede ontwikkeling volgens haar, “want online criminaliteit is de meest voorkomende vorm van criminaliteit. In 2024 werden ruim 1,4 miljoen Nederlanders slachtoffer.”

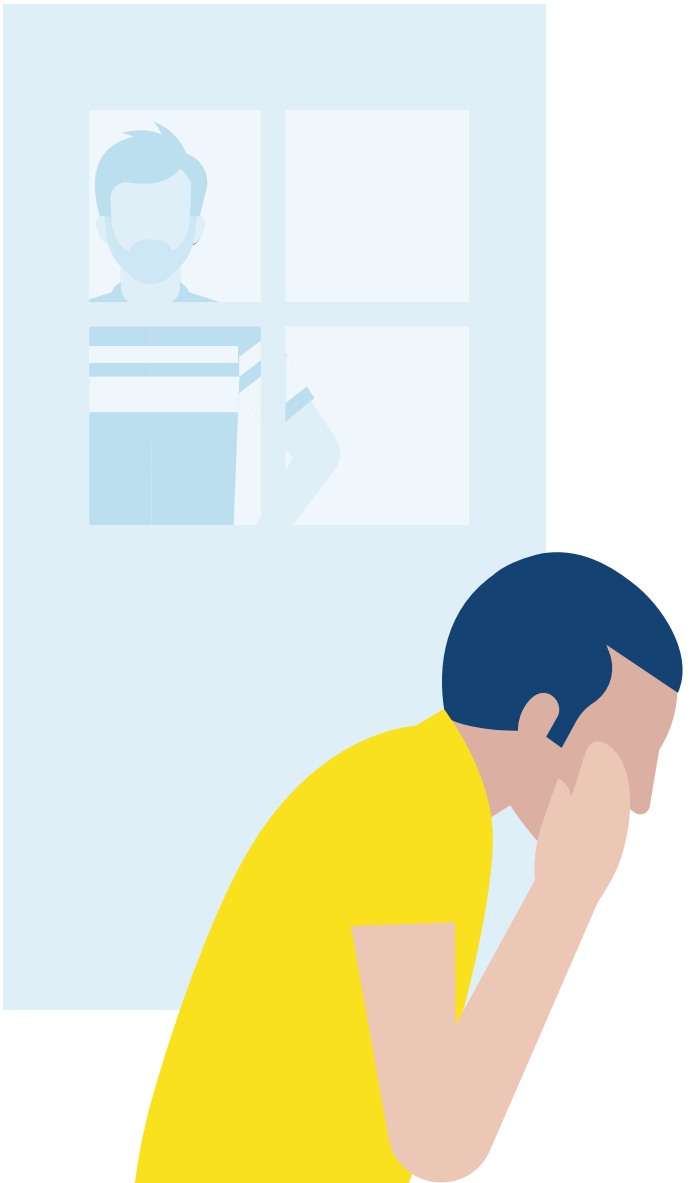
De Bie benadrukt dat de impact van online fraude groot is, niet alleen financieel maar zeker ook emotioneel. Mensen verliezen niet alleen geld, maar ook vertrouwen in digitale diensten en hun eigen oordeel. Juist daarom is het volgens haar zo belangrijk om ervaringen en inzichten te delen en criminelen samen een halt toe te roepen. Ze realiseert zich dat dit veel inzet vraagt van alle partners en belooft dat JenV een betrouwbare regiepartner blijft.

Na de gezamenlijke aftrap volgt een dag vol inhoudelijke sessies, waarin de deelnemers vanuit verschillende invalshoeken de aanpak van online fraude verder verdiepen. In dit verslag een impressie van deze verhalen.

Boven: Léon Poffé, onder: Lisette de Bie

Fraude met nepagenten: strafmaat sluit niet aan op ernst

In de themasessie over de jacht op nepagenten schetsen politierechercheur Jorn Buitenkant (Districtsrecherche IJsselland) en Shannon Mosterd (officier van justitie Oost-Nederland) een onthutsend beeld van deze vorm van oplichting. Die treft vooral oudere mensen. Via gegevensbestanden op het darkweb, overlijdensadvertenties en telefoongidsen op internet komen de slachtoffers op een lijst met 'leads' te staan. Criminelen bellen slachtoffers zogenaamd namens de politie of de bank en sturen vervolgens een 'agent' langs om kostbare spullen 'veilig te stellen'.



In een filmpje van een inval is te zien hoe weinig er nodig is om een dergelijk callcenter te runnen. Buitenkant: "Een studiootje met twee mensen op bed, vijf telefoons en that's it." Bekend is dat er ook vanuit auto's op een parkeerplaats of bankjes in een park wordt gebeld en aangestuurd. Buitenkant legt uit hoe een dadergroep is georganiseerd: achter de schermen zorgt een coördinator voor de lijst met namen, adressen en telefoonnummers. Een welbespraakte beller wint het vertrouwen van het slachtoffer en een ophaler met chauffeur staat binnen enkele minuten voor de deur. Ondertussen blijft de telefoonlijn bezet, zodat slachtoffers bij twijfel niemand anders kunnen bellen.

De gedeelde video- en geluidsfragmenten roepen verontwaardiging op. Zo is er een gesprek te horen met een vrouw wier man de dag daarvoor is overleden, maar die desondanks genadeloos de fuik in wordt gedreven: "Dit zijn gewetenloze mensen die over lijken gaan."

Enorme impact

De opnamen die Mosterd ook tijdens een requisitoir inbracht, blijkt hoe geraffineerd criminelen te werk gaan. De bellers, vaak vrouwen, zijn welbespraakt en weten slachtoffers zo te overrompelen met informatie dat deze geen tijd krijgen om helder na te denken.
De impact is enorm: slachtoffers schamen zich zo dat ze zich mentaal hebben laten overmeesteren dat ze vaak geen aangifte durven te doen. Ondertussen lopen

de cijfers op: in 2025 zijn al meer dan tienduizend meldingen van nepagenten gedaan. “Ander verhaal, zelfde script”, aldus Buitenkant: “Vaak zien we dat daders ook al bekend zijn van andere vormen van online fraude, zoals bankhelpdeskfraude. Ook de modus operandi komen overeen.”

Het verschil met bijvoorbeeld bankhelpdeskfraude is wel dat de drempel om in te stappen lager is. Mosterd legt uit: “Je hebt niet iemand nodig die genoeg bij de pinken is om in de bankomgeving van een slachtoffer te komen. Daarbij worden ook altijd digitale sporen achtergelaten. Het instaptarief van fraude met nepagenten is daardoor een stuk lager.”

Ook op politiemensen heeft fraude met nepagenten impact. Die merken dat deuren vaker gesloten blijven als er buurtonderzoek wordt gedaan. Want ben je nog wel te vertrouwen? Nepagenten hebben vaak ook een uniform aan en kunnen zich legitimeren met een identiteitsbewijs. Dat het vals is, maakt niet uit, legt Buitenkant uit: “De meeste mensen weten niet hoe een officiële politie-ID eruitziet.”

‘Waarom een taakstraf?’

Ook de aanpak in de strafrechtketen komt aan bod. In een onderzoek naar een callcenter wisten Buitenkant en Mosterd achttien zaken te koppelen aan één dadergroep. Mosterd: "Op dit moment zijn er geen (passende) richtlijnen/oriëntatiepunten voor deze vorm van criminaliteit. De ernst en impact van deze feiten laten zich het best vergelijken met een woninginbraak waarbij de inbreker wordt overlopen. Helaas zien we dat er soms nog taakstraffen worden opgelegd aan daders. Binnen het OM wordt er daarom gewerkt aan specifiek richtlijnen voor fraude met nepagenten.

> *“Dit zijn gewetenloze mensen die over lijken gaan.”*


VERSLAG VAN DE DAG
Integrale aanpak
online fraude
NEE

De psychologie achter online fraude en hoe ING daarop inspeelt

Tijdens een sessie over fraudepreventie lieten ING-fraude-experts Kim Gunnink en Lillian Katje zien hoe diep online oplichting inwerkt op het hoofd en het hart van slachtoffers. Ze bespraken onder meer beleggingsfraude, datingfraude en bankhelpdeskfraude, en vooral de vraag hoe je als bankmedewerker een klant kan laten inzien dat diegene is opgelicht.

Volgens Katje is er een verschil tussen kortdurende en langdurige fraude. Bij bankhelpdeskfraude wil de crimineel dreiging, urgentie en een gevoel van paniek overbrengen. Bij beleggingsfraude, datingfraude en hybride vormen daarvan draait het juist om fear of missing out, om het creëren van vertrouwen en emotionele verbondenheid.

Weerstand

Die emoties bepalen ook hoe slachtoffers reageren als de bank hen probeert te waarschuwen. Gunnink liet zien hoe drie vormen van weerstand steeds terugkomen: reluctance (‘Jij bepaalt niet voor mij’), scepsis (‘Jullie van ING zijn toch tegen crypto?’) en ego defense: (het willen vasthouden aan een positief zelfbeeld. Cognitieve dissonantie, bevestigingsbias en verliesaversie versterken dat nog eens. “Op het moment dat wij zeggen dat iemand wordt opgelicht, raakt dat direct iemands zelfbeeld. Dan gaat de weerstand omhoog: ‘Ik heb me echt wel goed ingelezen; ik ben niet over een nacht ijs gegaan.’”

Om klanten toch te bereiken, ontwikkelde ING gerichte interventies. Zo vertelt Katje dat bij bankhelpdeskfraude de standaardbetaallimiet is verlaagd en dat er een wachttijd van vier uur geldt voor het verhogen van die limiet. Er verschijnt dan ook een interactief waarschuwingssysteem in de app. Klanten moeten aangeven waarom zij hun limiet verhogen. “Met die vier uur wachttijd creëren we een mentale afkoelperiode: klopt dit verhaal eigenlijk wel? Sinds we deze interventie hebben ingevoerd, is de schade door bankhelpdeskfraude flink gedaald.”

Boven: Kim Gunnink, onder: Lillian Katje

Van Geldfit tot Check het gesprek

Voor datings- en beleggingsfraude werkt ING samen met Geldfit. Slachtoffers worden als zij dat willen ‘warm’ doorverwezen voor uitgebreide financiële en psychologische begeleiding. In 2024 werden 350 klanten doorgezet; 70 procent verbrak uiteindelijk het contact met de oplichter. De gemiddelde schade daalde met ongeveer 60 procent. Gunnink: “We kunnen niet altijd voorkomen dat mensen slachtoffer worden, maar we kunnen ze wel helpen om zelf tot inzicht te komen en weer grip te krijgen.”

Daarnaast is er de functie ‘check het gesprek’ in de betaalapp en sinds kort ook in Mijn ING. Als een klant tijdens een telefoongesprek geld probeert over te maken, licht er een knop op waarmee de klant op de achtergrond kan controleren of de bank daadwerkelijk belt. Maandelijks maken meer dan tienduizend klanten er gebruik van; het aantal zaken van bankhelpdeskfraude halveerde bijna.

Tot slot investeert ING in de kunst van het klantgesprek: diepgaande trainingen voor collega’s over psychologie, weerstanden, tone-of-voice en gespreksvoering, ondersteund door een digitaal ‘weerstandswiel’. In combinatie met een case tracker en empathische vervolggesprekken moet dat ervoor zorgen dat klanten het gevoel hebben dat ze er niet alleen voor staan.

Bekijk de presentatie

Hulp aan slachtoffers: wegwijs in het meldpuntenlandschap

Na online te zijn opgelicht, begint voor slachtoffers vaak een complexe reis langs bank, politie en andere loketten. Mick Claessens (Centrum voor Criminaliteits-preventie en Veiligheid) en Miriam Pronk (Ministerie van JenV) laten in hun sessie zien hoe de Integrale Aanpak Online Fraude probeert orde te scheppen in de hulpreis. Hulp aan slachtoffers is namelijk een van de actielijnen in de integrale aanpak.

Claessens schetst eerst de omvang: online criminaliteit raakt een grote groep burgers en bijna iedereen kent wel iemand die ermee te maken heeft gehad. Toch weten slachtoffers vaak niet direct waar zij voor hulp moeten aankloppen. In de zaal klinkt: bank, politie, Fraudehelpdesk, maar ieder loket is er voor iets anders. “We zien dat professionals elkaar soms al niet kunnen vinden”, stelt Claessens. “Dan kun je van een slachtoffer helemaal niet verwachten dat die de weg weet.”

Factsheet en vuistregels

Claessens en Pronk maken deel uit van de werkgroep Hulp aan slachtoffers, binnen de Integrale Aanpak Online Fraude. Banken, politie, Fraudehelpdesk, Slachtofferhulp Nederland, onderzoeksinstellingen en private partijen zijn aangesloten. Een eerste stap was het opstellen van een factsheet die duidelijk laat zien wie wat doet, wat alleen een bank kan, wat juist alleen Slachtofferhulp, politie of een meldpunt. Vanuit die basis stelde de

Mick Claessens

werkgroep vijf vuistregels op. Deze werken als een globaal stappenplan dat voor de meeste slachtoffers werkt zonder te pretenderen dat er één ideale route is. “De ideale hulpverlener voor alle slachtoffers bestaat niet. Dit komt omdat slachtoffers verschillende behoeften hebben: de één zoekt een luisterend oor, de ander wil zijn schade verhalen en weer een ander wil voorkomen dat de dader door kan gaan met het plegen van online fraude”, benadrukt Pronk.

Online tool

De eerste stap is vaak de bank, om schade te beperken. Via aangifte bij de politie en financiële afwikkeling gaat de route naar psychosociale ondersteuning en naar specifieke meldpunten per fraudevorm. Net gelanceerd is een online tool (Hulp bij online criminaliteit) die een persoonlijker advies geeft op basis van de antwoorden die slachtoffers op vragen geven. Claessens zegt erbij dat de tool nog in ontwikkeling is en stap voor stap wordt aangepast op basis van inzichten uit de praktijk en uit onderzoek.

Buurthuis en bibliotheek

In de discussie wordt benadrukt dat slachtoffers ook in buurthuizen, bibliotheken en gemeenteloketten terecht moeten kunnen voor vragen en om warm doorverwezen te kunnen worden. Verder wordt duidelijk dat er binnen de politie steeds meer aandacht komt voor hulp aan slachtoffers. Zo gaat de politie

Bekijk de presentatie

sneller langs bij slachtoffers en zijn er in sommige regio’s hulplijnen voor collega’s aan de keukentafel die bij twijfel behoefte hebben aan het oordeel van een expert.

De oproep van Claessens en Pronk: denk mee, deel ervaringen en deskundigheid en help mee om de weg naar hulp voor slachtoffers zo eenvoudig mogelijk te maken.

Sneller malafide webshops blokkeren, aangiften stimuleren

Hoe krijgen we meer aangiften van mensen die slachtoffer zijn geworden van aankoopfraude? Deze vraag staat centraal in de sessie van Lennaert Steendam (Achmea) en Rick van der Rest (deurwaarderskantoor LAVG). Zij nemen de deelnemers stap voor stap mee door de oplossing.

Na een korte introductie over hun eigen rol in de dagelijkse strijd tegen online fraude, starten Steendam en Van der Rest met een praktijkvoorbeeld: de webshop simpelwerkt.nl die in een paar weken tijd voor tonnen verkoopt zonder te leveren. In groepjes bespreken deelnemers hoe zo'n site zoveel schade kan aanrichten en ook zo lang online kan blijven. Reclame via Google Ads, scherpe prijzen en nepreviews worden genoemd.

Steendam benoemt de kern van het probleem: het duurt simpelweg te lang voordat er genoeg aangiften zijn gedaan om een patroon te herkennen. Zolang er geen stapel aangiften ligt, kan de crimineel achter een malafide webshop slachtoffers blijven maken. "Het allerbelangrijkste is dat we die nepwebshops zo snel mogelijk uit de lucht krijgen", benadrukt hij.

LMIO als *trusted flagger* van SIDN

De tweede vraag die de deelnemers wordt gesteld, is hoe je een malafide .nl-webshop offline krijgt en welke partijen daarvoor moeten samenwerken. Dit leidt naar Gijs van der Linden, van het Landelijk Meldpunt Internetoplichting (LMIO). Aangiften van online oplichting komen bij het LMIO binnen. Van der Linden legt uit hoe een algoritme bepaalt welke webwinkels het eerst bekeken worden en hoe het LMIO vervolgens hosting providers en SIDN (registreert .nl-domeinen) informeert. Hij heeft goed nieuws: "Het LMIO kan op zeer korte termijn als trusted flagger zorgen dat SIDN malafide .nl-webshops na onze melding direct ontkoppelt. Dat is een stevige verstoring."

Beslisboom

Maar dan moet de stroom aangiften wél sneller op gang komen, zodat die benodigde stapel aangiften er snel is.

Lennaert Steendam

In een volgende ronde bespreken deelnemers wat daarbij kan helpen. Daarop presenteren Steendam en Van der Rest de kern van hun interventie: een online beslisboom op de website van de Fraudehelpdesk, die door een grote groep slachtoffers van online fraude wordt bezocht. De interventie, die op het punt staat technisch uitgerold te worden, begint bij het onderbuikgevoel van het slachtoffer. Binnen enkele minuten helpt de beslisboom te bepalen of er waarschijnlijk sprake is van oplichting. Valt de uitkomt negatief uit, dan volgt direct de route naar online aangifte én naar civiele mogelijkheden om geld terug te krijgen.

Drempels weghalen

Van der Rest benadrukt dat de tool meer biedt dan alleen een duwtje richting politie: “Je eindigt altijd met een handelingsperspectief: wat kan ik bij mijn bank, bij de politie en zélf doen?” Bij het ontwerp zijn ook inzichten van het onderzoek van Jildau Borwell (politie) naar de beleving van slachtoffers meegenomen. De toon van de tool is bewust waarderend en ondersteunend en slachtoffers wordt duidelijk gemaakt dat zij niet alleen zichzelf helpen, maar ook toekomstige slachtoffers. Volgens Steendam is dat essentieel: “Als we drempels weghalen en mensen laten voelen dat hun melding ertoe doet, verwachten we minder slachtoffers, meer daders in beeld en meer geld dat terugvloeit naar de rechtmatige eigenaar.”

Rick van der Rest

Bekijk de presentatie

Inzicht in de modus operandi anno 2025

Wat gebeurt er nu precies tussen fraudeur, bank en klant en waarom is het voor banken zo lastig om in te grijpen bij online fraude? Boudewijn van der Valk en Tom Luiten van ING nemen de deelnemers mee in de modus operandi van online criminelen.

De sessie begint met uitleg over een belangrijk onderscheid: fraude in de bankomgeving versus fraude in de klantomgeving. In het eerste geval logt de fraudeur in op de rekening van de klant en maakt zelf geld over. Bij de tweede vorm wordt de klant opgelicht, maar maakt deze uiteindelijk zelf geld over. Dat verschil is juridisch cruciaal: Als iemand anders de transactie doet, vergoedt de bank te schade tenzij de klant grove nalatigheid kan worden verweten. Maar als de klant betaalt, is er geen directe vergoedingsplicht, terwijl de impact vaak net zo groot is."

Zwaartepunt verschoven

Waar klassieke bancaire fraude (phishingmails, nagemaakte inlogsites, gestolen passen) tot een paar jaar geleden domineerde, ziet ING dat het zwaartepunt is verschoven naar oplichtingsvormen waarin de klant langdurig wordt 'bewerkt' door de crimineel. Eerst wordt het vertrouwen gewonnen, dan wordt urgentie gecreëerd en pas dan wordt geld buitgemaakt.

In het traditionele stroomschema kon de bank nog op meerdere fronten ingrijpen: bij een verdachte inlog, een onbekend apparaat of een afwijkend betaalpatroon kon de bank blokkeren, bellen en controleren. Bij fraude in de klantomgeving ligt dat anders. De klant is dan allang misleid, buiten het zicht van de bank. Het eerste signaal is vaak pas een ongebruikelijke transactie. "Dat is het allereerste moment waarop wij überhaupt iets zien. En omdat de klant zelf betaalt, moeten we het hebben van dat ene signaal én van het gesprek dat volgt."

'Lek op de fraudeafdeling'

Die gesprekken zijn niet makkelijk, laten Van der Valk en Luiten horen aan de hand van geluidsfragmenten van bankhelpdeskfraude. In een van deze fragmenten is een klant te horen die door de fraudeur 'gescript' is: ze krijgen precies ingeprent wat ze moeten zeggen als de bank belt. Vaak krijgen ze te horen dat er een lek is op de fraudeafdeling van de bank. Doordat klanten door de oplichters worden gescript om een verzonnen verhaal te vertellen als verklaring voor de transacties die zij willen doen, worden zelfs ervaren medewerkers aan het twijfelen gebracht.

Boudewijn van der Valk

In dit soort gevallen doet ING er alles aan de klant tot inkeer te laten komen, door te vragen of er een familielid of wijkagent kan meekijken of om de klant uit te nodigen op kantoor. Maar zomaar gegevens delen met een ander, mag niet. Nieuwe ideeën worden op hun haalbaarheid

Tom Luiten

onderzocht, zoals een koppeling met telecomproviders om te zien of een klant tijdens een verdachte transactie aan het bellen is.

(Romantische) investeringsfraude

Vervolgens wordt ingezoomd op investeringsfraude, relationele fraude en hybride vormen daartussen. Vaak hebben fraudeur en klant al maanden of jaren een relatie. Slachtoffers worden via sociale media en chatgroepen met juichverhalen gelokt. Sommige online romances veranderen geleidelijk in een investeringsadvies. “Het grootste probleem is dat de klant de fraudeur vertrouwt. Die belt al een jaar elke dag, terwijl wij in vijf minuten moeten uitleggen dat iemand wordt opgelicht.”

In de sessie komen een reeks andere modus operandi aan bod, van voorschotfraude (er ligt een flinke erfenis voor je klaar, maar om dat geld te ontvangen moet je eerst een dure advocaat betalen), abonnementsfraude en 'vriend-in-noodfraude' ('Hoi pap, ik heb een nieuw nummer en ik moet mijn nieuwe badkamer nog aanbetalen') tot een nieuwe vorm van malware, waarbij een ogenschijnlijke simkaartupdate in werkelijkheid ervoor zorgt dat de fraudeur het scherm van de klant op afstand kan bedienen, en door het scherm heel donker te maken de klant niet ziet dat de fraudeur toegang krijgt tot de bankieren-app van de klant en daarmee geld overmaakt. Ook de rol van technologie

Bekijk de presentatie

komt voorbij: deepfakes lijken nog beperkt toegepast te worden door fraudeurs, maar AI en robotstemmen maken het wel makkelijker om op grote schaal contact op afstand te automatiseren. Tegelijkertijd proberen banken hun klanten weerbaarder te maken, zoals met de campagne Check het gesprek van ING.

Banken worden steeds beter in het technisch opsporen van verdachte transacties. Deze sessie laat zien dat de echte strijd zich afspeelt in het hoofd en het hart van de klant. Zonder vertrouwen in de waarschuwende bank blijft de bank in sommige gevallen machteloos.

Kirstin de Jong

Van criminal journey naar interventies

Online fraude groeit mee met de digitalisering en laat een forse schadelast achter. In 2023 lag die in Nederland naar schatting op 109 miljoen euro terwijl slechts een op de vijf slachtoffers aangifte doen. Tegen die achtergrond schetsen Kirstin de Jong (Nederlandse Vereniging van Banken) en Philo Warmerdam (AFM) in hun sessie hoe de Integrale aanpak online fraude werkt en wat die oplevert.

Centraal in de presentatie staat de criminal journey: een stap-voor-stap beschrijving van hoe online fraudeurs werken. In deep-dives, begeleid door EY, brengen experts per fraudevorm (aan- en verkoopfraude, bank-helpdeskfraude en beleggingsfraude) de ‘reis’ van de crimineel en een bijbehorend barrièremodel in kaart. Per fraudevorm hebben de deelnemers aan de deep-dives zestig tot negentig mogelijke barrières bedacht. Met de meest haalbare gaan de partners van het programma aan de slag.

De criminal journey bij bankhelpdeskfraude telt zes fasen: oriëntatie (informatie over potentiële slachtoffers verzamelen), voorbereiding, benadering (contact leggen), overtuiging (social engineering tooling), geldoverboeking (vaak via geldezels) en besteding van het verduisterde geld. Belangrijk inzicht: vaak kunnen partijen al in de eerste drie fasen ingrijpen om te voorkomen dat er slachtoffers worden gemaakt.

Interventies

Het programma heeft al veelbelovende interventies opgeleverd:

- Veiligheidspagina in bankapps: een centrale plek waar klanten veiligheidsinstellingen beheren (limieten, machtigingen, apparaten beheren). Rabobank ging er in juli 2024 als eerste bank live mee. ABN-AMRO en ING volgden.
- Line Busy: het plan om vanuit de banken bij telecom-aanbieders te checken of een klant telefonisch in gesprek is tijdens het overboeken van geld. Dat wijst vaak op fraude. Als die gebeurt, moet de bank de betaling kunnen blokkeren. Hiervoor moet de wet worden aangepast. In navolging van een Kamermotie werkt het Ministerie van Economische Zaken aan een wetsvoorstel.
- Waarschuwingsboodschappen op Telegram: in groepen waar 'handige lijstjes' circuleren, plaatst de Politie boodschappen om potentiële fraudeurs af te schrikken.
- Sneller ingrijpen bij beleggingsfraude: samenwerking tussen AFM, banken en een cryptoaanbieder om vermoedelijke boiler rooms sneller op te sporen en offline te krijgen.
- Aankoopfraude: het Landelijk Meldpunt Internetoplichting (LMIO) is nu trusted flagger voor .nl-domeinen bij SIDN, waardoor frauduleuze websites sneller op zwart gaan.
- Voorlichting op beurzen, via de campagne Laat je niet interneppen en tijdens rondetafelgesprekken met Kamerleden.

Philo Warmerdam

Bekijk de presentatie

De vrolijke emoji's in de harde straattaal van jongeren

Aan het eind van de dag zorgen Barbara van Croonenborgh (operationeel specialist jeugd en digitaal) en digitaal wijkagent Pip van den Herik van de Politie Eenheid Rotterdam voor een energieke en soms confronterende afsluiting. Met humor, straattaal en schokkende voorbeelden nemen ze de zaal mee in de digitale leefwereld van jongeren op of over het randje van de criminaliteit: van Tik-Tok en Telegram tot drillrap.

Van Croonenborgh begint met een disclaimer: wat zij laten zien, gaat over een klein deel van de jeugd. Het overgrote deel gamet en scrolt door filmpjes zonder zich met criminaliteit in te laten. "Onze doelgroep bestaat niet uit kinderen die netjes hun huiswerk maken."

De extremen die voorbijkomen, zijn heftig. De zaal ziet filmpjes van jongeren die worden uitgekleed, geslagen, geschopt en vernederd: shaming als online chantagemiddel. Niet alles wordt online gezet, benadrukt van den Herik, maar wat te zien is, komt binnen. Van Croonenborgh vraag de zaal om anders te kijken naar daders in online fraudezaken: "Die jongen die als nepagent voor de deur staat, is soms net zo goed slachtoffer."

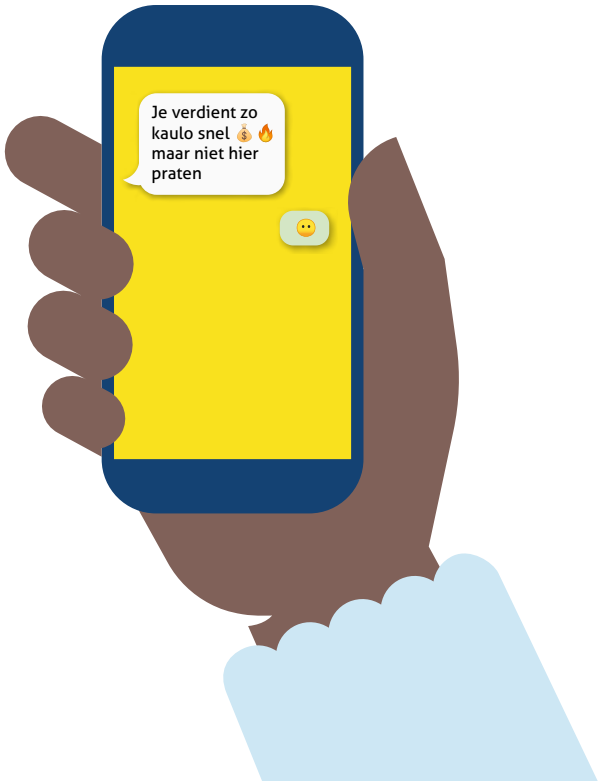
Snelweg naar criminele uitbuiting

Duidelijk wordt hoe de online omgeving van jongeren kan fungeren als snelweg richting criminele uitbuiting. Jongeren zien drillraps vol geld en status. In telegramgroepen kun je terecht voor drugs, wapens, uithalers in de haven of een klus als pinner. Op Spotify zijn playlists met muziek die scammen/F-gaming aanprijzen of idealiseren. Voor jongeren in een instabiele thuissituatie kan dat aantrekkelijk zijn.

Daar bovenop komt generatieve AI. Van Croonenborgh laat zien hoe met één foto en een gekloonde stem een rapvideo wordt gemaakt waarin een echte jongen dingen 'doet' die hij nooit gedaan heeft. "Straks krijg je niet alleen een appje van je 'dochter' bij Whatsappfraude, maar zie en hoor je haar."

Emoji-quiz

Toch blijft de sessie niet hangen in somberheid. Als uitsmijter doet de zaal mee met een emoji-quiz. Met rode en groene kaarten in plaats van 'petje op, petje af' mag iedereen raden welke emoji's staan voor drugs, wapens, banken, havenuithalers en geldezels. De quiz maakt luchtig én pijnlijk duidelijk wat er achter de verborgen beeldtaal zit. Uiteindelijk blijft er een winnaar over die deze subtaal het best begrijpt.



integraleaanpakonlinefraude.nl

Integrale aanpak

online fraude