Ministerie van Justitie en Veiligheid

Verslag van de dag

Informatiebijeenkomst
22 november 2023

Integrale aanpak
online fraude

Online fraude is een groeiend maatschappelijk probleem. In het project Integrale Aanpak Online Fraude werkt het Ministerie van JenV samen met partners aan effectieve oplossingen. Tijdens een online informatiebijeenkomst werd onder leiding van gespreksleider Anouschka Laheij nader ingezoomd op dit fenomeen. Waar hebben we het precies over bij online fraude? Hoe groot is de impact op de samenleving? En welke kennis is nodig om het succesvol te kunnen bestrijden? In drie artikelen blikken we terug op deze bijeenkomst.

Online criminaliteit kan óók high-impact crime zijn

De impact van online criminaliteit op slachtoffers is vergelijkbaar met die van traditionele criminaliteit. Soms is die zelfs groter, concludeert cybercrime-expert Jildau Borwell. Moet dit volgens haar gevolgen hebben voor de werkwijze van de politie? “Misschien is er te veel focus op efficiëntie.”

Opgebeld worden door een ‘medewerker van de bank’ die waarschuwt dat jouw geld niet veilig is en graag helpt om het over te maken naar een ‘veilige rekening’. Via Marktplaats betalen voor een Playstation die nooit geleverd wordt. Whatsappfraude, online bedreiging, gijzelsoftware, sextortion... Het spectrum van online criminaliteit is breed en dijt uit. En de impact op slachtoffers kan groot zijn, zag Jildau Borwell in haar werk als cybercrime-analist bij de politie-eenheid Noord-Nederland. Zo was al bekend dat slachtoffers van een vergrijp als sextortion (iemand dreigt seksueel getinte foto’s van een slachtoffer te verspreiden) niet zelden zelfmoordgedachten krijgen. In aangiften van online fraude, zoals bankhelpdeskfraude, Whatsappfraude of marktplaatsfraude, las zij terug dat ook de gevolgen daarvan ingrijpend kunnen zijn.”

Jildau Borwell

Borwell besloot met haar promotieonderzoek vanuit de Open Universiteit nader onderzoek te doen naar de impact van online criminaliteit: “Ik was benieuwd hoe die impact zich verhoudt tot die van traditionele criminaliteit. Van bijvoorbeeld een woninginbraak weten we dat die impact heel groot kan zijn. Het is high-impact-criminaliteit. Online criminaliteit wordt nooit zo gezien.”

Delictparen vergeleken

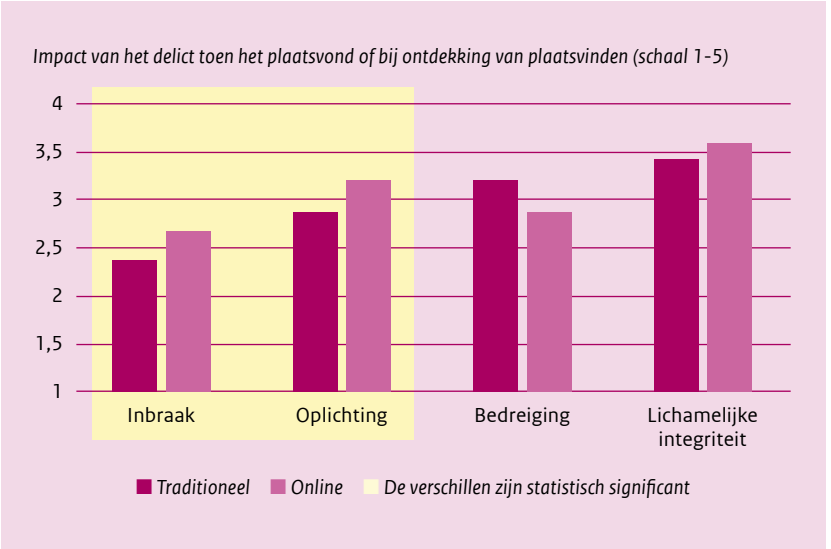
Ten onrechte, zo komt naar voren uit haar onderzoek. Daarin vergeleek ze ‘delictparen’; traditionele en online delicten die gelijkenissen vertonen, bijvoorbeeld woninginbraak versus hacken van een bankaccount, en een babbeltruc aan de deur versus bankhelpdeskfraude. De twee andere paren waren offline en online bedreiging en aanranding en beeldgerelateerd seksueel misbruik. Die vergelijkingen leverden opvallende resultaten op. Zo bleek de impact van online inbraak op het moment van ontdekking zelfs groter te zijn dan van een woninginbraak. Volgens Borwell kunnen daar verschillende verklaringen voor zijn: “Het heeft er misschien mee te maken dat mensen zich dom voelen; ze hebben toch op een phishing-link geklikt. Of misschien snappen ze niet goed wat

Delictparen voor vergelijking

	Traditioneel	Online
Inbraak	Woninginbraak (N = 130)	Hacken account internetbankieren (N = 143)
Oplichting	Babbeltruc (N = 94)	Bankhelpdeskfraude (N = 212)
Bedreiging	Offline bedreiging (N = 52)	Online bedreiging (N = 56)
Lichamelijke integriteit	Aanranding (N = 138)	Beeldgerelateerd seksueel misbruik (N = 86)

Peritraumatische stress

(Impact tijdens delict/ontdekking) o.a. shock, ontkenning, hulpeloosheid.



er is gebeurd of zijn ze bang dat criminelen nog steeds in hun computer zitten. Maar het kan ook zijn dat slachtoffers niet goed weten wat ze moeten doen. Bij een woninginbraak is dat duidelijk: je schakelt de politie in. Bij online criminaliteit is het onduidelijker wat je moet doen, bijvoorbeeld als het gaat om herstelwerkzaamheden aan de computer of accounts."

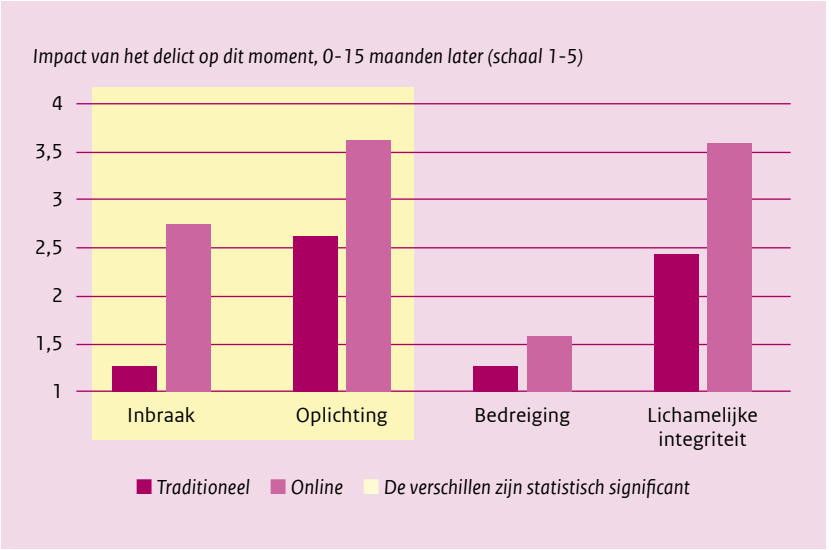
Zelfbeeld aangetast

Vaak blijkt het zelfbeeld van het slachtoffer flink te zijn aangetast: "Mensen nemen het zichzelf kwalijk en schamen zich ervoor. Bij de online varianten is dat gevoel veel erger. We weten dat bij aanranding het stigma bestaat dat slachtoffers ook zelf schuldig zijn. Bij de online variant komt victim blaming nog vaker voor. Bij sextortion krijgen slachtoffers vaak te horen: 'Je hebt die beelden toch zelf doorgestuurd? Maar ook bij andere fraudevarianten zie je dat terugkomen: 'Je weet toch dat je nooit op een link moet klikken?'"

We weten dat bij aanranding het stigma bestaat dat slachtoffers ook zelf schuldig zijn. Bij de online variant komt victim blaming nog vaker voor.

Aantasting zelfbeeld

Zelfverwijt en schaamte.



Meer erkenning

Wat moet de politie volgens haar doen met de bevindingen uit het onderzoek? Borwell noemt een paar zaken die volgens haar beter kunnen: "Veel slachtoffers willen graag erkenning voor wat ze hebben meegemaakt. Maar ze hebben ook meer praktische behoeften. Ze willen bijvoorbeeld weten waar ze moeten zijn om de problemen die zijn ontstaan op te lossen. Denk ook aan preventieadvies; veel slachtoffers zitten niet zo in de digitale wereld en hebben geen idee wat er precies is gebeurd en hoe ze dit in de toekomst kunnen voorkomen. In

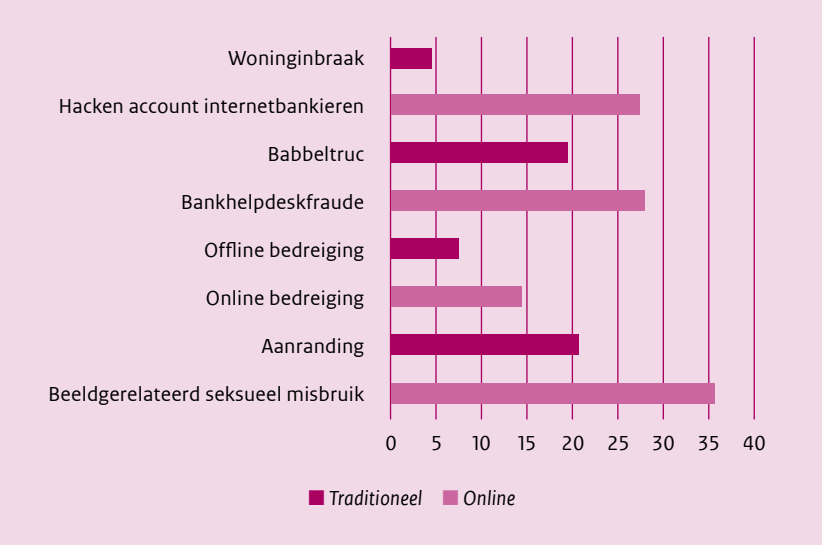
al dit soort gevallen kan de politie een rol spelen. Vooral om te voorkomen dat mensen niet angstig blijven en om uit te leggen welke stappen ze moeten zetten."

Menselijke kant onderbelicht

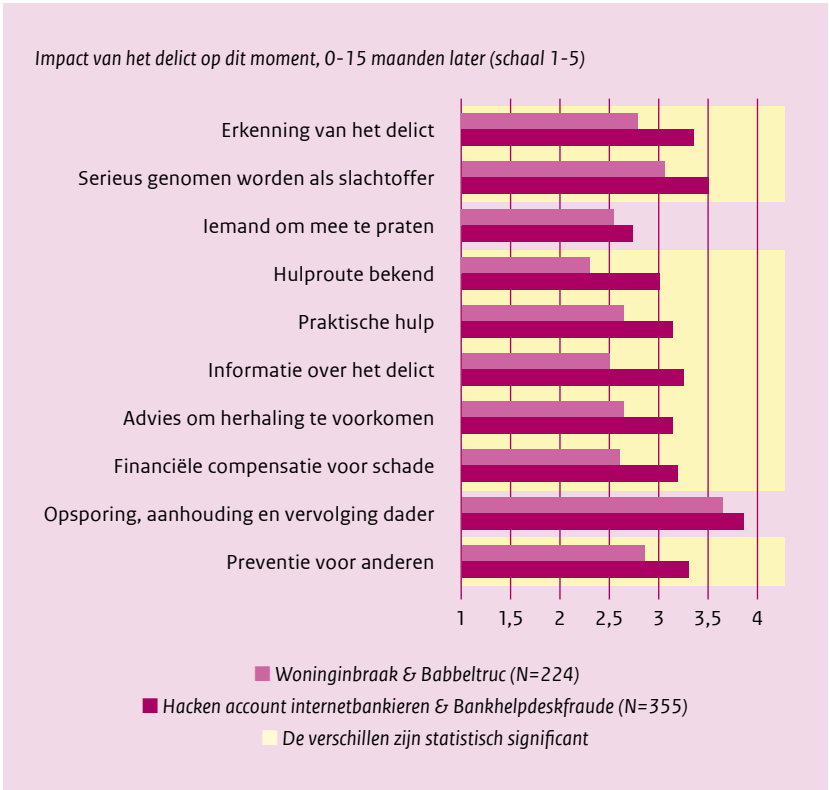
Initiatieven als Operatie Centurion om online criminaliteit effectiever aan te pakken, juicht Borwell toe. "Maar misschien is er wel te veel focus op efficiëntie en datagedreven werken. De menselijke kant blijft een beetje onderbelicht: doen we het goede voor slachtoffers?" Als voorbeeld van hoe het beter kan noemt ze dat de politie Oost-Nederland vanaf januari slachtoffers van online criminaliteit desgewenst thuis bezoekt. "Het is dan ook mogelijk dat de eerste opvang vanuit de politie in je eigen huiskamer gebeurt. Dat is toch anders dan wanneer je online aangifte moet doen. Slachtoffers moeten de mogelijkheid hebben een echt mens te kunnen spreken."

% Victim blaming

('Mijn omgeving geeft mij de schuld van het delict')



Behoeftes na delict (vermogenscriminaliteit)








Beter inzicht in het spinnenweb rond online fraude

Wat drijft iemand tot online fraude? TNO onderzocht hoe daders tot hun gedrag komen en hoe zich dat in de tijd ontwikkelt. Die kennis is volgens onderzoekers Guido Veldhuis en Naomi Keja nodig om tot een goed onderbouwde, integrale aanpak van online fraude te komen.

Een fenomeenanalyse, zo heet de analyse die TNO van online fraude heeft opgesteld. Veldhuis legt uit wat die precies inhoudt: “We zijn met alle betrokkenen die een rol spelen in de aanpak van online fraude om de tafel gaan zitten. Samen hebben we gekeken wie welke kennis heeft. Online fraude is een ontzettend complex probleem. Het ontstaat uit een heleboel onderdelen die allemaal met elkaar interacteren. Als je bijvoorbeeld kijkt naar welke personen een rol spelen, dan heb je natuurlijk allereerst de daders. Die variëren van de buurjongen of het buurmeisje tot professionele organisaties met callcenters die vanuit het buitenland opereren. Beide soorten daders kunnen overigens grote schade aanrichten, hebben we gezien. Naast de daders zijn er de facilitators. Fraude wordt vaak gepleegd via platforms, zoals een berichtendienst of een veilingsite. Ook banken spelen een rol als schakel in het betalingsverkeer. Partijen als de Politie en het OM willen fraude opsporen en ertegen optreden En het slachtoffer is de speelbal in het midden. Dat kan een individu zijn, maar ook een bedrijf.”

Al die partijen zijn constant in beweging, stelt Veldhuis: “Daders passen zich aan op wat wij bijvoorbeeld aan maatregelen bedenken. Consumenten eisen betaalgemak, maar ook veiligheid. De manier waarop de politie en het OM

Naomi Keja en Guido Veldhuis

kunnen en mogen opsporen, varieert. Dat levert een enorm spinnenweb op met allerlei interacties tussen partijen."

1.000 adressen voor 125 euro

Dat online fraude moeilijk aan te pakken is, komt volgens Naomi Keja onder andere doordat daders eenvoudig aan kennis en benodigdheden komen. "Via de berichtendienst Telegram kunnen gebruikers anoniem criminele advertenties in chatgroepen plaatsen. In die groepen wordt ook om producten en diensten gevraagd. Denk aan lijsten met gegevens van potentiële slachtoffers, zoals naam, geslacht, leeftijd, e-mailadres en telefoonnummers. Soms staan er zelfs foto's en berichten van potentiële slachtoffers op social media bij. Voor 125 euro heb je binnen 2, 3 minuten een lijst met 1.000 adressen binnen."

Fraudebijbel

Keja laat zien dat er ook complete belscripts worden verkocht om personen telefonisch op te lichten. Ze toont verder een plaatje van een advertentie waarin een 'fraudebijbel' wordt aangeboden. "Daarin staan allerlei methoden om mensen op te lichten. Criminelen maken ook gebruik van social engineering; technieken om het slachtoffer psychologisch te manipuleren. Bijvoorbeeld door iemand onder druk te zetten. Of door een vertrouwensband op te bouwen. Denk bijvoorbeeld

aan Whatsappfraude: de zoon die waarschijnlijk ook echt op vakantie is, is zijn telefoon of portemonnee kwijtgeraakt en de politie kan niet helpen. Of moeder alsjeblieft snel even geld kan overmaken."
Slachtoffers voelen zich vaak schuldig en schamen zich. Dat is schadelijk, stelt Keja: "Er moet daarom heel voorzichtig met slachtoffers worden omgesprongen. En iedereen kan erin trappen. Criminelen gaan steeds geraffineerder te werk; echt en nep zijn nauwelijks meer van elkaar te onderscheiden."

We vinden het maar wat fijn om met een Tikkie aan elkaar te betalen voor een drankje of even snel wat geld aan je kind over te kunnen maken. Maar dat zijn nu juist die mechanismen waar fraudeurs meteen gebruik van maken.

Op een andere manier kijken

Hoe kan de fenomeenanalyse nu helpen om meer grip te krijgen op online fraude? Veldhuis benadrukt dat dit ingewikkeld is. “Dat komt ook doordat de neiging bestaat om meer van hetzelfde te doen: meer fte’s, nog meer euro’s op een bepaalde manier inzetten. Maar het is juist belangrijk om op een andere manier naar de problematiek te kijken. De manier waarop bijvoorbeeld met slachtoffers wordt omgegaan, is zo’n punt waar echt een andere draai aan het systeem kan worden gegeven. Als er meer met slachtoffers gepraat wordt, kan dat helpen in de verwerking. Maar het levert ook betere informatie op. Je kunt ook denken aan een andere manier van communiceren met potentiële jonge daders. Zijn onze kinderen op de hoogte dat online fraude een serieus misdrijf is waarvoor je gevangenisstraf kunt krijgen. En waarmee je echte mensen echte schade toebrengt?”

Guido Veldhuis

Verslaafd aan gebruiksgemak

Een van de grote dilemma’s in de bestrijding van online fraude blijft de vraag hoeveel veiligheid willen we als samenleving en hoeveel privacy zijn we bereid daarvoor op te geven? Veldhuis: “In de opsporing is veel mogelijk, maar privacy is een groot goed en er is niet voor niets wetgeving die daar kaders aan stelt. Daarbij komt dat wij als consumenten verslaafd zijn geraakt aan gebruiksgemak. We vinden het maar wat fijn om met een Tikkie aan elkaar te betalen voor een drankje of even snel wat geld aan je kind over te kunnen maken. Maar dat zijn nu juist die mechanismen waar fraudeurs meteen gebruik van maken.”

Maar wat is het nut van de fenomeenanalyse als het fenomeen zo snel verandert? “Goede vraag”, vindt Veldhuis. “Zeker, de uitingsvormen van online fraude veranderen. Misschien wordt Whatsappfraude de komende jaren wel wat kleiner. Maar de vaste patronen veranderen niet. Het is goed om daar zicht op te houden. Veiligheid komt niet vanzelf, daar moeten we constant aan werken, ook omdat de mensen die ons geld afhandig willen maken dat ook doen.”

Hoe een rapper tegen de lamp liep met zijn webshops

Onder de naam Operatie Centurion werken de Nationale Politie en het OM samen met ketenpartners aan het verstoren van gedigitaliseerde criminaliteit. Die aanpak is succesvol, stellen Jacqueline Bonnes (OM) en Aad Lensen (politie-eenheid Rotterdam). Een mooi voorbeeld is de zaak tegen een Rotterdamse rapper annex online oplichter.

In 2018 en 2019 verkocht de man dure merkkleding online. De zaak kreeg veel media-aandacht, onder meer in het tv-programma Opgelicht. Dit leidde tot veel meldingen bij het Landelijk Meldpunt Internetoplichting (LMIO). Op basis hiervan startte het OM samen met de politie een onderzoek. Uiteindelijk werd de man in 2023 veroordeeld. “Het was een complexe zaak”, aldus officier van justitie Bonnes, die gespecialiseerd is in cybercriminaliteit. “De man heeft zo’n 200 mensen opgelicht. We denken dat hij daarmee meer dan 120.000 euro aan schade veroorzaakt. Dat het zolang duurde voordat hij werd veroordeeld, komt doordat het lastig rechercheren was. Hij bouwde webshops om zijn spullen aan te bieden, soms onder zijn eigen naam en soms met een andere persoon samen. Meestal leverde hij de spullen niet. Maar af en toe wel. Als er te veel klachten tegen die webshop

Jacqueline Bonnes

Aad Lensen

kwamen, dan werd die webshop gesloten. Maar dan opende hij gelijk weer een nieuwe. Daar trapten dan weer veel mensen in en zo kon het verder gaan."

Wetswijziging hielp mee

Op een gegeven moment kwam de zaak bij de politie in Rotterdam binnen via het LMIO. Lensen vertelt hoe het balletje toen is gaan rollen: "We dachten meteen: dit is wel iets. Toen hebben we een integraal team geformeerd met mensen met financiële kennis, digitaal experts, maar ook de reguliere tactische rechercheurs."
Een wetswijziging die per 1 maart 2019 inging, hielp volgens Bonnes mee: "Er is toen een nieuw artikel toegevoegd in het Wetboek van Strafrecht over online handelsfraude. Die is precies voor dit soort zaken bedoeld: mensen die onder hun eigen naam een webshop beginnen, maar dan toch niet leveren en daar een beroep of gewoonte van maken."
"In het verleden kwam deze meneer daarmee weg", vult Lensen aan: "Dan zei hij dat hij zijn spullen gewoon onder zijn eigen naam verkocht en dus niks verkeerds deed."

'Meesterschetser'

Uiteindelijk is het nog best een intensief onderzoek geweest. Lensen: "Je moet bijvoorbeeld bankgegevens vorderen bij banken en daar moeten we dan op wachten. Om meer bewijs

tegen hem te vergaderen hebben we ook een tap geplaatst. Uit telefoongesprekken bleek dat hij nog volop bezig was met zijn praktijken. Dat moesten we allemaal vastleggen in het proces-verbaal. Jacqueline moest dit vervolgens aanbieden bij de rechtbank. En we hadden natuurlijk aangiftes nodig. We hadden er al veel, maar gedurende het onderzoek bleek dat er ook nog veel slachtoffers waren die geen aangifte hadden gedaan. Die hebben toen alsnog aangifte gedaan."
Het belang om deze man aan te pakken, was volgens Lensen groot: "Juist omdat hij zo bekend was en veel mensen hem adoreerden. Hij pronkte er ook mee, voelde zich onaantastbaar. Hij had ook shirts laten maken met de tekst 'meesterschetser', oftewel meesteroplichter."

De uitdaging zat hem vooral in het massale aantal slachtoffers. Het vraagt nogal wat om met zoveel slachtoffers een goed dossier op te bouwen.

Jacqueline Bonnes en Aad Lensen in gesprek met gespreksleider Anouschka Laheij.

Unieke zaak

In 2023 werd de man veroordeeld tot 2 jaar cel en een schadevergoeding van ongeveer 20.000 euro. Minder dan de eis van Bonnes van 6 jaar cel en 120.000 euro schadevergoeding. “De rechter heeft de man voor een deel vrijgesproken, omdat het verschil tussen een slechte ondernemer en een echte oplichter soms lastig te bewijzen is. Al met al was het een unieke zaak. Dat geldt zeker voor de uitleg van de rechter over het verschil tussen een slechte ondernemer en een oplichter. Maar ook het grote aantal slachtoffers en hoe die in het onderzoek konden worden opgespoord, maakt deze zaak bijzonder. En natuurlijk de populariteit van de man in zijn community.”

Het blijft voor Bonnes moeilijk te begrijpen hoe het kan dat iemand die de ene na de andere dag webshops opent en weer sluit toch lange tijd buiten schot kan blijven: “In de offline wereld kan dat niet, dan word je ergens geregistreerd. We moeten voor de online wereld barrières tegen dit soort praktijken opwerpen. Ook tegen het gebruik van geldezels, die we ook in deze zaak tegenkwamen.”

Partners

De zaak is volgens Lensen een mooi voorbeeld waartoe een integrale aanpak kan leiden. “De uitdaging zat hem vooral in het massale aantal slachtoffers. Het vraagt nogal wat om met zoveel slachtoffers een goed dossier op te bouwen. Sommige aangiftes werden ook teruggetrokken. Dan vertelde hij mensen: ‘Als je jouw aangifte intrekt, zorg ik ervoor dat je alsnog je spullen geleverd krijgt.’ Voor de politie is dit een zeer leerzame zaak geweest. We hebben zoveel expertise goed weten te bundelen: financieel, tactisch, digitaal. En we hebben heel goed samengewerkt met onze partners. Die hebben we gewoon nodig. Banken hebben bijvoorbeeld veel eerder in de gaten dat er iets niet goed gaat dan wij.”

“Help ons”

Hebben de twee nog een laatste tip? Lensen: “Zoek je partners vooral op als je ergens tegenaan loopt. Wat kun je voor elkaar betekenen zodat we het gezamenlijk belang kunnen dienen?

Bonnes is het daarmee eens: “Natuurlijk heeft de politie beperkte capaciteit. Dat betekent dat we samen dit soort problemen te lijf moeten gaan. Samen met de financiële sector, bijvoorbeeld. Dat gebeurt ook al. Dan geven ze op basis van hun analyses bijvoorbeeld aan: ‘We denken dat deze 20 slachtoffers door 1 verdachte of groep verdachten zijn gedupeerd’. Telecombedrijven kunnen dit soort analyses ook maken, net als bedrijven in de technische infrastructuur. Dus help ons!”

HIER KUNT U DE ONLINE INFORMATIEBIJEENKOMST TERUGKIJKEN ↗

Integrale aanpak

online fraude