Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2628

Vragen van lid **Mutluer** (GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid over *het bericht «Schrikbarende toename van online oplichting in Nederland»* (ingezonden 16 april 2025).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 4 juli 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 2117.

Vraag 1
Bent u bekend met het artikel getiteld «Online oplichting in Nederland stijgt schrikbarend: 2,4 miljoen slachtoffers»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat het feit dat het aantal slachtoffers van online oplichting in Nederland is gestegen tot maar liefst 2,4 miljoen schrikbarend is? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 2
Ieder slachtoffer van online fraude is er één te veel. Ik betreur het feit dat het aantal slachtoffers van online oplichting in 2024 ten opzichte van 2022 is gestegen.[2] De maatschappelijke impact van online fraude is groot en het zorgt voor zowel financiële als mentale problemen bij slachtoffers. Mijn ministerie werkt daarom al enkele jaren gezamenlijk met publieke en private partners aan een integrale aanpak van online fraude.

Vraag 3
Kunt u verklaren hoe het komt dat vooral jongeren hierbij vaker getroffen worden dan ouderen: 20 procent van de 15- tot 25-jarigen, tegenover 10 procent van de 65-plussers?

---

[1] De Telegraaf, 13 april 2025, Online oplichting in Nederland stijgt schrikbarend: 2,4 miljoen slachtoffers (https://www.telegraaf.nl/nieuws/159248149/online-oplichting-in-nederland-stijgt-schrikbarend-2-4-miljoen-slachtoffers).

[2] Centraal Bureau voor de Statistiek (2024), *Online Veiligheid en Criminaliteit* (https://www.cbs.nl/nl-nl/longread/rapportages/2025/online-veiligheid-en-criminaliteit-2024).

ah-tk-20242025-2628
ISSN 0921 - 7398
's-Gravenhage 2025

Antwoord 3
Een groot deel van de 15–25-jarigen brengt veel tijd door op het internet. Ze maken dagelijks gebruik van apps, sociale media en websites waardoor zij meer risico lopen dan anderen. Criminelen die zich schuldig maken aan online fraudevormen maken hier handig gebruik van en richten zich in sommige situaties juist op deze groep potentiële slachtoffers. Zo plaatsen zij veelvuldig «te mooi om waar te zijn»-aanbiedingen op sociale media waarbij specifieke goederen die aantrekkelijk zijn voor jongeren worden aangeboden. Het Centrum voor Criminaliteitspreventie en Veiligheid werkt sinds enkele jaren samen met scholieren.com aan een preventiecampagne specifiek gericht op jongeren. Uit recent onderzoek is gebleken dat er nog veel winst te behalen valt met campagnes gericht op beveiligingsmaatregelingen die jongeren zelf kunnen treffen om hun kans op slachtofferschap te verkleinen.[3] Dit is ook één van de zaken waar de pijler preventie en weerbaarheid van de integrale aanpak zich op richt.
Er zijn dan ook de nodige campagnes door de overheid ontwikkeld om burgers weerbaarder tegen gevaren online te maken, waaronder online fraude, zoals met *social engineering* campagnes, campagnes van veiliginternetten.nl etc.

Vraag 4
Kunt concreet aangeven welke concrete maatregelen er de afgelopen twee jaar genomen zijn om online oplichting tegen te gaan? Kunt u per maatregel aangeven wat het effect daarvan had moeten zijn op het tegengaan van die oplichting en wat het effect in de praktijk was?

Antwoord 4
Het kabinet investeert dit jaar 52,6 miljoen euro in de politie en de strafrechtketen voor de aanpak van cybercrime en gedigitaliseerde criminaliteit, waar online fraude een belangrijk onderdeel van uitmaakt. In de laatste Veiligheidsagenda zijn streefnormen van de politie opgenomen voor de aanpak. Dit bevat de streefnorm voor het minimumaantal verdachten, het aantal onderzoeken voor criminele samenwerkingsverbanden maar ook het percentage voor alternatieve afdoeningen. Over de behaalde resultaten wordt uw Kamer jaarlijks geïnformeerd in de voortgangsrapportage. Deze wordt op korte termijn aan uw Kamer toegestuurd.
Strafrecht alleen gaat online fraude niet oplossen, daarom is het van groot belang dat ook private partijen en het bedrijfsleven in het bijzonder online oplichting zo breed, effectief en efficiënt mogelijk aanpakken, om slachtofferschap te voorkomen. Sinds 2023 werkt mijn ministerie samen met het Ministerie van Economische Zaken, het Ministerie van Financiën, de politie, het Openbaar Ministerie, VNO-NCW/MKB Nederland, de Consumentenbond, de Nederlandse Vereniging van Banken (NVB), de Fraudehelpdesk en andere meldpunten, Slachtofferhulp Nederland, COIN, en Thuiswinkel.org in een integrale aanpak online fraude. Binnen de aanpak werken deze en andere partijen samen om het online oplichters zo moeilijk mogelijk te maken en slachtofferschap van burgers en ondernemers te voorkomen. Binnen de integrale aanpak wordt gewerkt langs vijf pijlers, waaronder barrières en interventies, preventie en weerbaarheid, en hulp aan slachtoffers. Zo wordt er geïnvesteerd in campagnes en het weerbaarder maken van burgers en bedrijven tegen online fraude en oplichting. In samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid zijn er folders met zogenoemde vuistregels en een specifieke tool ontwikkeld die burgers en bedrijven informeren over online oplichting en hen handvatten biedt om snel en efficiënt hulp te zoeken. Daarnaast werken de partners uit de integrale aanpak samen om de teksten op hun websites eenduidig te maken en hun dienstverlening zo goed mogelijk op elkaar af te stemmen. De politie heeft met Operatie Centurion de afgelopen jaren repressief ingezet en de inzet versterkt op het thema online criminaliteit. Deze projectmatige inzet wordt de komende jaren structureel geborgd.
Tot slot wil ik u wijzen op één van de vele initiatieven die publieke en private partners ondernemen: het initiatief «Bank voor de klas» waarbij banken in

[3] Online oplichting en jongeren: een inkijk in hun ervaringen, juni 2024 (https://hetccv.nl/app/uploads/2024/09/RAPPOR1.pdf).

samenwerking met de politie in 2024 voorlichting hebben gegeven aan ruim 53.000 leerlingen in het basisonderwijs, het voortgezet onderwijs en het middelbaar beroepsonderwijs.[4] Jongeren werden met dit initiatief wegwijs gemaakt met het herkennen en voorkomen van online fraude.
De effecten van de maatregelen die worden getroffen om online fraude tegen te gaan zijn moeilijk te meten. Pas op lange termijn zijn directe effecten van campagnes merkbaar. Daarnaast is het thema online fraude voortdurend aan verandering onderhevig en worden er steeds weer nieuwe vormen van online oplichting en fraude waargenomen.

Vraag 5
Is het waar dat slachtoffers van online oplichting zich vaak onvoldoende geholpen voelen door politie en justitie? Zo ja, hoe komt dat en wat wordt er gedaan om dit vertrouwen te herstellen? Zo nee, wat is er dan niet waar?

Antwoord 5
Politie en justitie pakken niet alle oplichtingszaken strafrechtelijk op, dat kan ook niet omdat daar niet genoeg capaciteit voor is. De politie en het Openbaar Ministerie kunnen niet aan alle strafbare feiten prioriteit geven en een strafrechtelijke opvolging is niet altijd mogelijk. Ook worden er wel eens fouten gemaakt, bijvoorbeeld bij het opnemen van een aangifte. De afgelopen periode zijn er maatregelen getroffen om de ondersteuning van mensen die te maken krijgen die te maken krijgen met online fraude te verbeteren.
De politie en het OM hebben samen met andere partijen de afgelopen jaren geïnvesteerd in een verbetering van de integrale aanpak van online fraude. Zo heeft de politie meerdere initiatieven gestart om de dienstverlening aan slachtoffers van online criminaliteit te verbeteren. Met het project digitale meldkamer gaat de politie bij online criminaliteit die net heeft plaatsgevonden of anderszins urgent is, direct ter plaatse voor het veiligstellen van sporen, het opnemen van de aangifte en het geven van slachtofferhulp. Uit evaluatie komt naar voren dat slachtoffers tevreden zijn over deze mogelijkheid. Dit project is onlangs in werking getreden in alle eenheden waardoor deze werkwijze tot standaard is verheven.[5]
Daarnaast hebben verschillende partners uit de integrale aanpak vuistregels ontwikkeld voor slachtoffers van online criminaliteit waardoor de informatievoorziening aan slachtoffers is verbeterd. Slachtoffers van aan- en verkoopfraude die online aangifte doen en wiens zaak niet strafrechtelijk wordt opgepakt, worden gewezen op de mogelijkheden die ze zelf kunnen ondernemen, waaronder het verhalen van de schade op de oplichter. Alle slachtoffers die aangifte doen worden gewezen op de mogelijkheid van slachtofferhulp. Indien zij dat aangeven, vindt doorverwijzing plaats naar Slachtofferhulp Nederland.
Verder investeert dit kabinet fors in de aanpak van gedigitaliseerde criminaliteit, waaronder online fraude, door de politie. De politie gaat een centrale voorziening voor gedigitaliseerde criminaliteit inrichten ten behoeve van de regionale eenheden en de Eenheid Landelijke Opsporing en Interventies. Bovendien zal de politie met de beschikbaar gestelde middelen de uitvoeringscapaciteit voor de aanpak van gedigitaliseerde criminaliteit in de eenheden vergroten. De kennis en vaardigheden van digitale opsporing gaat politie ook vergroten met de toegekende gelden. Bovendien heeft de politie aandacht voor de impact van online oplichting op slachtoffers en past haar werkwijzen daarop aan.[6] De politie stimuleert de aangiftebereidheid en meldingsbereidheid van online fraude, maar wijst (mogelijke) slachtoffers ook op manieren of instanties voor het verkrijgen van (gedeeltelijke) genoegdoening, zoals civiel schadeverhaal, het verwijderen van online berichten of emotionele hulp.

---

[4] Bank voor de klas bereikt 53.000 leerlingen met voorlichting over online fraude.
[5] Kamerstukken II, 2024–2025, 29 628, nr. 1253.
[6] Nationale Politie, *Online fraude in beeld, Fenomeenbeeld online fraude 2024* (https://hetccv.nl/app/uploads/2024/11/OnlineFraudeFenomeenbeeld2024.November2024.pdf).

Vraag 6
Wordt er vanuit de justitiële autoriteiten effectief samengewerkt met banken, online platforms en telecomaanbieders om oplichting te voorkomen en snel op te treden bij signalen van fraude? Waar bestaat die samenwerking concreet uit en waaruit blijkt dat die samenwerking effectief is? Acht u het nodig die samenwerking te intensiveren en op welke wijze gaat u dat doen?

Antwoord 6
In het kader van de integrale aanpak online fraude werken de politie en het Openbaar Ministerie regelmatig samen met banken en telecomaanbieders. Deze samenwerking heeft onder andere geleid tot het sluiten van bankrekeningen van meerdere stelselmatige fraudeurs. Daarnaast wordt onder meer gewerkt aan de knelpunten bij gegevensdeling die worden ervaren in de samenwerking met banken, telecomaanbieders en online platformen. In de volgende voortgangsbrief over de integrale aanpak van online fraude zal ik u hier nader over informeren. Begin dit jaar heeft de Minister van Economische Zaken u geïnformeerd voornemens te zijn een voorstel in te dienen om de Telecommunicatiewet aan te passen om het misbruik van telecommunicatievoorzieningen te bestrijden ten behoeve van de aanpak van online fraude.[7]
In aanvulling op het antwoord op vraag 4 verwijs ik naar de verschillende samenwerkingsvormen zoals het Landelijk Meldpunt Internetoplichting (LMIO) en Electronic Crimes Taskforce (ECTF). Het LMIO is een samenwerking tussen de politie, banken, het Openbaar Ministerie, Marktplaats en internetserviceproviders. Het doel van LMIO is om internetoplichting, vooral in online handelsomgevingen, te verminderen door aangiftes te behandelen, te analyseren en te veredelen, en door samen te werken aan het signaleren en aanpakken van oplichters. Het ECTF is in 2011 opgericht met als doel om in publiek-privaat verband digitale criminaliteit te bestrijden. Deze samenwerkingen zijn waardevol, aangezien gedigitaliseerde criminaliteit een complex maatschappelijk probleem is en dit niet alleen met het strafrecht is op te lossen.

Vraag 7
Hoe vaak hebben slachtoffers van online oplichting in 2024 een verzoek gedaan bij de banken om via de PNBF-regeling terugbetaling te vorderen van hun oplichters? En hoe vaak hebben zij bij weigering hiervan de NAW-gegevens van hun oplichters opgevraagd en gekregen?

Antwoord 7
Zoals ik heb aangegeven in de beantwoording van eerdere vragen van het lid Mutluer, bevestigt de Betaalvereniging Nederland dat de toepassing niet centraal wordt geregistreerd en dat dit een aangelegenheid is van individuele banken in hun hulp aan slachtoffers en de wederkerige bereidheid van twee banken om primair buitengerechtelijke bemiddeling mogelijk te maken tussen hun beider rekeninghouders.[8] Het is daardoor niet mogelijk om een overzicht te verkrijgen van het aantal verzoeken in het kader van de PNBF-regeling (de Procedure NAW-gegevens Begunstigde bij niet-bancaire Fraude).

Vraag 8
Kunt u aangeven hoe gevolg is gegeven aan motie-Mutluer[9] waarbij is gevraagd om in samenspraak met Betaalvereniging Nederland en de Nederlandse Vereniging van Banken de PNBF-regeling bekender te maken en uit te bereiden naar paymentserviceproviders?

Antwoord 8
Mijn ministerie is aan het begin van dit jaar in gesprek gegaan met de Betaalvereniging Nederland over de PNBF-regeling. De Betaalvereniging Nederland (BVN) heeft in dit gesprek bevestigd dat er met de *aangesloten* Nederlandse banken, leden en Nederlandse Payment Service Providers een regeling hieromtrent is afgesproken. Deze regeling ziet op het volgende: de bank van het slachtoffer informeert de eigen rekeninghouder over de

[7] Kamerstukken II, 2024–2025, 29 911, nr. 456.
[8] Kamerstukken II, Aanhangsel van de Handelingen, 2024–2025, nr. 370.
[9] Kamerstuk 26 643, nr. 1248.

mogelijkheid van het indienen van een terugbetalingsverzoek en in een latere fase onder voorwaarden een verzoek tot verstrekking van NAW-gegevens. Deze afgesproken regeling betreft een interbancaire voorziening die de leden op vrijwillige basis aanbieden. Aangezien een bank – van ogenschijnlijk betrouwbare transacties – niet kan zien dat een betaalopdracht werd gegeven onder invloed van een strafbaar feit, is van belang te vermelden dat de gedupeerde rekeninghouder wel zelf contact met de bank zoekt alvorens de bank de rekeninghouder over deze optie kan informeren. Ook de bij de BVN aangesloten Payment Service Providers kunnen deze regeling reeds toepassen.
Ten aanzien van de bekendheid van de PNBF kan ik bevestigen dat BVN en NVB onderschrijven dat informatieverstrekking vanuit banken over de PNBF actief gebeurt, zoals ook via de website www.veiligbankieren.nl.
Tot slot blijft de inzet van PNBF beperkt omdat toepassing hiervan beperkt is tot wegsluizen van frauduleuze gelden van Nederlandse rekeningnummers naar NL IBAN-nummers. Criminelen zoeken manieren om geld weg te sluizen waar de pakkans het kleinst is. De Nederlandsche Vereniging van banken geeft aan te zien dat het merendeel van de frauduleuze gelden nu rechtstreeks richting buitenland gaat, gepind wordt, in crypto worden omgezet, of via (internationale) Payment Service Providers weggesluisd wordt.

Vraag 9
Deelt u de mening dat de bestrijding van online oplichting meer prioriteit zou moeten krijgen binnen het justitie- en veiligheidsdomein? Zo ja, worden er in dat licht meer capaciteit en middelen vrij gemaakt voor de opsporing en vervolging van digitale fraude en online oplichting? Zo nee, waarom niet?

Antwoord 9
Online oplichting is één van de grootste criminaliteitsvormen en is schaalbaar, internationaal en daarom een hardnekkig fenomeen dat bestreden moet worden. Zoals ik in antwoord op vraag 4 heb toegelicht investeert dit kabinet 52,6 miljoen euro in de politie en de strafrechtketen voor de aanpak van cybercrime en gedigitaliseerde criminaliteit, waar online fraude een belangrijk onderdeel van uitmaakt. Ook de politie spant zich conform de Veiligheidsagenda in voor de bestrijding van gedigitaliseerde criminaliteit. De verwachting is dat dit een belangrijk thema blijft voor de komende jaren. Zoals ook toegelicht is de rol van alleen het strafrecht onvoldoende. Daarom is er ook geïnvesteerd in een integrale samenwerking met publieke en private partijen. In dit kader wijs ik u op mijn antwoord op vraag 5.

Vraag 10
Welke rol ziet u voor het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC) en andere instanties in de aanpak van deze problematiek?

Antwoord 10
Ik zie in het geval van online oplichting maar een beperkte rol weggelegd voor het Nationaal Cyber Security Centrum (NCSC). Online oplichting is een vorm van gedigitaliseerde criminaliteit, daar waar het NCSC zich richt op de cybersecurity van Nederland en de bescherming van de digitale infrastructuur. Het NCSC signaleert algemene trends op het gebied van cybersecurity, deelt dreigingsinformatie en ontwikkelt handreikingen, handelingsperspectieven en praktische richtlijnen om organisaties en burgers te ondersteunen bij het versterken van hun digitale weerbaarheid. Daarnaast publiceert het beveiligingsadviezen en -rapporten en werkt het intensief samen met verschillende veiligheidsinstanties.
Het Digital Trust Center (DTC) is een belangrijke partner in de bestrijding van online fraude. Het DTC informeert ondernemers hoe zij veilig digitaal kunnen ondernemen, bijvoorbeeld door het aanbieden van de *Basisscan Cyberweerbaarheid* en de *CyberVeilig Check* voor zzp en mkb. Ook biedt de organisatie een praktische actielijst aan met behulpzame activiteiten en tips om ondernemingen digitaal weerbaar te maken. Daarnaast hebben het NCSC en DTC recent vijf basisprincipes van digitale weerbaarheid opgesteld, die organisaties handvatten bieden voor het ontwikkelen van een gezonde en degelijke cyberbeveiligingsstrategie.