Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

Aanhangsel van de Handelingen

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

75

Vragen van de leden **Kathmann** en **Mutluer** (beiden GroenLinks-PvdA) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Binnenlandse Zaken en Koninkrijkrijkrelaties over *de explosieve stijging van fraude met visa en phishing* (ingezonden 30 juli 2025).

Antwoord van Minister **Van Oosten** (Justitie en Veiligheid) (ontvangen 22 september 2025). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 2869.

Vraag 1
Bent u bekend met het bericht: «Fraude met visa explodeert, Nederlandse vakantiegangers al voor tienduizenden euro's opgelicht: hier moet je op letten»? (De Telegraaf, 23 juli)

Antwoord 1
Ja.

Vraag 2
Hoeveel meldingen van fraude bij visumaanvragen zijn er tot nu toe gedaan? In hoeveel gevallen ging dit om phishing?

Antwoord 2
Uit navraag bij de Fraudehelpdesk blijkt dat er in het jaar 2024 12 meldingen over fraude met visumaanvragen zijn geregistreerd. Deze meldingen hadden betrekking op valse websites waarop zogenaamd een visum aangeschaft kon worden. In de eerste helft van 2025 kreeg de Fraudehelpdesk 189 meldingen, waarvan 154 melders aangaven financieel te zijn gedupeerd. Ook het Centraal Meldpunt Identiteitsfraude (CMI) heeft meldingen met betrekking tot fraude met visumaanvragen ontvangen. In 2024 ging het om 89 meldingen en in 2025 tot en met juli om 353 meldingen. Zowel de Fraudehelpdesk als het CMI schrijven de toename van het aantal meldingen toe aan de invoering (sinds 2 april 2025) van de verplichte ETA voor het Verenigd Koninkrijk, hoewel er ook andere typen visa tussen de meldingen zitten.
Er is op dit moment geen duidelijk verband te leggen tussen het aantal meldingen en in hoeveel gevallen hier sprake is van phishing. Phishing is een werkwijze die wordt ingezet door criminelen om bijvoorbeeld oplichting en fraude te plegen. Daarnaast wordt in het geval van een melding niet altijd aangegeven of het om phishing gaat. Er zijn meldingen over (valse) websites waarbij tussenpartijen te veel geld vragen voor het verzorgen van (kosten-

ah-tk-20252026-75
ISSN 0921 - 7398
's-Gravenhage 2025

loze) visumaanvragen, maar vervolgens wel daadwerkelijk een geldig visum toesturen. Daarnaast zijn er meldingen waarbij melders denken dat zij een visumaanvraag doen en gegevens opgeven waarna er (soms meerdere keren) geld van hun creditcard wordt afgeschreven, maar er geen visum(aanvraag) wordt ontvangen.

Vraag 3
Hoe verhoudt het aantal gemelde gevallen via de Fraudehelpdesk zich tot officiële aangiften bij politie en meldingen bij visumverlenende instanties?

Antwoord 3
Er zijn op dit moment geen betrouwbare cijfers beschikbaar over het aantal aangiften over visumverstrekking bij de politie, noch over de verhouding van het aantal meldingen bij andere instanties dan de politie. Fraude met visa wordt net als phishing niet als aparte categorie geregistreerd en is daarmee niet eenvoudig uit het politiesysteem te halen. In de Veiligheidsagenda 2023–2026 zijn streefnormen voor de politie afgesproken omdat de groei van gedigitaliseerde criminaliteit moet worden geremd.[1] Hier valt ook de bestrijding van online fraude onder. Er is geen centrale registratie van meldingen van visumverlenende instanties (zoals ambassades). Als mensen met deze vorm van fraude geconfronteerd worden, roep ik hen op aangifte te doen bij de politie.

Vraag 4
Wat is de rol van reizigers-adviesportals en luchtvaartmaatschappijen in het informeren over officiële visumkanalen? Wordt er samengewerkt om nepwebsites actief te signaleren?

Antwoord 4
Op de website www.nederlandwereldwijd.nl kan men het reisadvies van het land van bestemming lezen ter voorbereiding op de reis. Op de landenpagina staat een kopje met «Hoe bereid ik mijn reis voor?». Onder dit kopje staat onder andere uitgelegd of een visum nodig is en waar deze aangevraagd kan worden (met een link naar een officiële website). Op www.nederlandwereldwijd.nl wordt op alle Schengenvisum aanvraagpagina's en inreisvisum aanvraagpagina's het volgende geadviseerd: *«Voorkom onnodige kosten en maak zelf uw afspraak. Maak geen afspraak bij een tussenpersoon.»*
Desgevraagd geeft het Ministerie van Buitenlandse Zaken aan dat op de aanvraagpagina's van sommige landen nog een extra waarschuwing staat. Als een ambassade bijvoorbeeld signaleert dat er veel fraude plaatsvindt in een bepaald land, dan wordt de informatie aangevuld. Zo is er onlangs door de ambassade in Turkije verzocht om toe te voegen dat de klant geen tolk via een tussenpersoon moet regelen.
Zo nu en dan plaatsen ook Nederlandse ambassades in diverse landen op eigen initiatief voorlichting of waarschuwingen op hun social mediakanalen. Zo heeft de Nederlandse ambassade in India onlangs op haar Instagram en Facebook account een waarschuwing geplaatst voor fraude met visa, alsook een verwijzing naar de officiële website.

Vraag 5
Wat doet u om online fraude via phishing te voorkomen en te bestrijden, onder andere bij visumaanvragen? Zijn deze maatregelen effectief gebleken?

Antwoord 5
In oktober 2024 zijn de Ministeries van Justitie en Veiligheid en van Binnenlandse zaken en Koninkrijksrelaties gestart met de meerjarige publiekscampagne «Laat je niet interneppen», om Nederlanders te wapenen tegen verschillende vormen van online oplichting, waaronder phishing. In de campagne komen de diverse signalen en overtuigingstechnieken aan bod, die online criminelen gebruiken en krijgen mensen handelingsperspectief mee om online oplichting te kunnen herkennen. Uit het meest recente campagne-effectonderzoek blijkt onder meer dat mensen zich meer waakzaam voelen als gevolg van de campagne en dat Nederlanders het belangrijk vinden dat de

[1] Veiligheidsagenda 2023-2026

Rijksoverheid op dit onderwerp campagne voert, maar dat (nog) niet meer mensen zich beter in staat voelen de signalen en overtuigingstechnieken te herkennen.[2] De aanbevelingen uit het campagne-effectonderzoek zullen worden meegenomen bij de volgende *flight* van de campagne in september 2025.
Naast bewustwordingscampagnes werkt de Nederlandse overheid aan de doorontwikkeling van het Register Internetdomeinen overheid zodat burgers in dat register bij twijfel een snelle check kunnen doen of websites van de Nederlandse overheid zijn of niet. Het Register is te raadplegen via https://organisaties.overheid.nl/domeinen. Bij twijfel over de echtheid van websites kan bovendien contact worden opgenomen met de gratis Digihulplijn (Bereikbaar via telefoon en chat op 0800 - 1508). Ook loopt een impactonderzoek naar de haalbaarheid van invoering van een uniforme domeinnaamextensie voor websites van de overheid, te beginnen bij de Rijksoverheid. Een uniforme domeinnaamextensie zoals .gov.nl of .overheid.nl maakt in één keer duidelijk dat de overheid afzender is van een website en is, mits consequent toegepast, makkelijk te communiceren richting het publiek.
Daarnaast voert mijn ministerie de regie op de integrale aanpak van online fraude.[3] De integrale aanpak online fraude heeft als doel om meerjarig gezamenlijk de krachten te bundelen, de onderlinge informatiepositie te verstevigen, het kennisniveau te verhogen, te weten en te doen wat werkt om sneller, flexibeler en effectiever op te kunnen treden tegen online fraude teneinde het aantal slachtoffers te verminderen. Partners in deze publiek-private samenwerking zijn onder andere de politie, het Openbaar Ministerie, VNO-NCW/MKB Nederland, de Consumentenbond, de Nederlandse Vereniging van Banken (NVB), COIN, Thuiswinkel.org, de Vereniging Nederlandse Gemeenten (VNG), het Ministerie van Economische Zaken enhet Ministerie van Financiën. Het jaarbericht en het actieplan voor 2025 zijn in juni jl. door mijn ambtsvoorganger aan uw Kamer toegezonden.[4]

Vraag 6
Hoeveel gevallen van phishing zijn er jaarlijks in Nederland? Welk aandeel van de gevallen van online oplichting betreft phishing?

Antwoord 6
Bij de politie wordt phishing niet als een apart delict geregistreerd en daarom zijn hier geen precieze cijfers over te delen. Dit komt omdat phishing vaak een middel is om verschillende soorten criminaliteit te kunnen plegen.
Wel blijkt uit de Veiligheidsmonitor 2024 van het Centraal Bureau voor de Statistiek dat krap 1 procent van de mensen in 2024 zich slachtoffer noemt van phishing. Bij 17 procent van de slachtoffers ging het om wangirifraude: de dader probeert het slachtoffer te laten terugbellen naar (dure) betaalnummers. Verder kreeg 12 procent te maken met beleggingsfraude en eenzelfde deel werd slachtoffer van bankspoofing, waarbij de oplichter zich voordoet als een bankmedewerker. Nepboetes of nepfacturen werden door 11 procent van de slachtoffers genoemd. Vriend-in-nood-fraude, waarbij iemand geld betaalde aan een zogenaamde bekende (via een nepbericht of voice cloning), en nepacties troffen respectievelijk 9 en 6 procent van de slachtoffers. De andere vormen van phishing werden door 4 procent of minder genoemd.[5]

Vraag 7
Bent u bekend met Belgische phishing-schild, het BAPS-Systeem, waarmee in 2024 zo'n 1,6 miljoen verdachte links zijn gedetecteerd en omzeild op basis van meldingen van burgers?[6]

Antwoord 7
Ja.

---

[2] Campagne-effectonderzoek Laat je niet interneppen | Rapport | Rijksoverheid.nl
[3] Integrale aanpak online fraude
[4] Kamerbrief met 2e voortgangsrapportage Integrale Aanpak Online | Kamerstuk | Rijksoverheid.nl
[5] 4. Online oplichting en fraude | CBS
[6] Center voor cybersecurity Belgium, 13 maart 2025, 44% van de Belgen stuurt phishingberichten door naar verdacht@safeonweb.be (ccb.belgium.be/nl/recent-news-tips-and-warning/44-van-de-belgen-stuurt-phishingberichten-door-naar).

Vraag 8
Kunt u nader toelichten wat het doel en de reikwijdte is van de pilot met een Anti-Phishing Shield (APS) die u heeft aangekondigd in deze zomer?[7] Welke partijen zijn hier bij betrokken?

Antwoord 8
Het doel van de pilot is de effectiviteit van het Anti-Phishing Shield (APS) in kaart brengen. Op basis van de resultaten van de pilot wordt beoordeeld of een structureel APS in Nederland wenselijk is.
De pilot wordt uitgevoerd door het Nationaal Cyber Security Center in samenwerking met KPN en is gericht op een beperkte klantengroep van KPN. Deze groep heeft zich op vrijwillige basis via opt-in aangemeld voor de dienst *Veilig browsen* van KPN. Dit is een malwarefilter dat ervoor zorgt dat apparaten veilig online gaan. De denial list (een lijst van bronnen die als onveilig of verdacht zijn aangemerkt) uit deze APS-pilot wordt hierin verwerkt. Hiermee sluit de pilot aan bij de maatregelen die KPN al neemt binnen de bestaande, versterkte beveiliging voor KPN-klanten. De pilot wordt op een later moment mogelijk uitgebreid met meerdere partijen uit de telecomsector.

Vraag 9
Wanneer verwacht u de uitkomsten van deze pilot? Koppelt u deze terug aan de Kamer met een voorstel voor vervolgstappen?

Antwoord 9
De pilot is eind juli 2025 gestart en duurt zes maanden. De pilot wordt tussentijds en na afloop geëvalueerd. Op basis hiervan wordt een advies voor een eventuele landelijke uitrol uitgebracht. U wordt in de volgende Kamerbrief over de integrale aanpak van cybercrime geïnformeerd over het vervolg van het APS.

Vraag 10
Op welke manier is de Autoriteit Consument & Markt als toezichthouder betrokken bij de pilot? Hoe gaat u tegemoetkomen aan zorgen over netneutraliteit?

Antwoord 10
De Autoriteit Consument & Markt (ACM) is als onafhankelijke toezichthouder niet actief betrokken bij de pilot. In een eerder stadium is het APS met de ACM besproken. De pilot vindt plaats binnen de geldende wettelijke kaders. Uitgangspunt bij netneutraliteit is dat de internetaanbieder de toegang tot het internet niet mag beperken, vanwege het recht op open toegang tot het internet. Hierbij gelden in het kader van de Europese netneutraliteitsverordening enkele uitzonderingsmogelijkheden. Zo mag een internet serviceprovider wél beperkingen opleggen indien – en slechts zolang – dit nodig is om de integriteit en de veiligheid van het netwerk van de eindgebruikers te beschermen. Er dient daarbij een afweging gemaakt te worden over wanneer en onder welke omstandigheden dergelijke beperkingen noodzakelijk zijn. Binnen de pilot is het aan de deelnemende partijen om na te gaan of hun werkwijze in lijn is met de regels inzake netneutraliteit. Zie ook het antwoord op vraag 8.

Vraag 11
Wat doet u nog meer om slachtoffers van phishing te voorkomen? Hoe stimuleert u commerciële oplossingen om verdachte websites te blokkeren, met respect voor netneutraliteit?

Antwoord 11
Binnen de integrale aanpak cybercrime bestaan er meerdere initiatieven en worden in samenwerking met de Ministeries van Binnenlandse Zaken en Koninkrijkrelaties, en Economische Zaken voorlichtingscampagnes gehouden om ervoor te zorgen dat mensen zich kunnen beschermen tegen phishing. Enkele voorbeelden hiervan zijn de campagnes «Laat je niet interneppen»

[7] Kamerstuk 26 643, nr. 1357

over online oplichting, «Dubbel beveiligd is dubbel zo veilig» over tweefactorauthenticatie, en «Doe je updates» over het uitvoeren van updates op slimme apparaten. Hierover bent u in de afgelopen Kamerbrief integrale aanpak cybercrime geïnformeerd.
Ik sta in beginsel positief tegenover commerciële oplossingen die mensen tegen online criminaliteit beschermen. Ook dergelijke oplossingen dienen te worden uitgevoerd binnen de geldende wet- en regelgeving.

Vraag 12
Kunt u deze vragen afzonderlijk van elkaar beantwoorden?

Antwoord 12
Ja.