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

822

Vragen van het lid **Six Dijkstra** (Nieuw Sociaal Contract) aan de Minister van Justitie en Veiligheid over *het bericht «Criminelen ontdekken een nieuwe oplichtingstruc: phishing via QR-codes»* (ingezonden 12 november 2024).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 16 december 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 717.

Vraag 1
Heeft u kennisgenomen van het bericht «Criminelen ontdekken een nieuwe oplichtingstruc: phishing via QR-codes»?[1]

Antwoord 1
Ja.

Vraag 2
Heeft u een beeld van de mate waarin phishing via QR-codes in Nederland plaatsvindt op dit moment?

Antwoord 2
Betrouwbare schattingen van de mate waarin phishing via QR-codes plaatsvindt zijn moeilijk te maken omdat deze gevallen niet apart worden geregistreerd door de politie of de Fraudehelpdesk.
De Fraudehelpdesk heeft tot op heden nog geen meldingen ontvangen over fraude door middel van QR-codes bij laadpalen, parkeerautomaten of restaurants, zoals genoemd in het artikel. De politie heeft het beeld dat de vormen van oplichting met QR-codes genoemd in het nieuwsbericht nog nauwelijks voorkomen in Nederland.
Misbruik van QR-codes in e-mails komt de politie wel vaker tegen. Het gaat hierbij vooral om bankhelpdeskfraude en andere vormen van fraude met bankgegevens, beleggingsfraude en creditcardfraude. Phishing (per e-mail of per post), telefonische fraude en online op handelssites waarbij de (ver)koper een QR-code moet scannen om de betaling te bevestigen, zijn de meest voorkomende fraudevormen waar QR-codes bij betrokken zijn. De Fraude-

[1] Nu.nl, 11 november 2024, Criminelen ontdekken een nieuwe oplichtingstruc: phishing via QR-codes, (https://www.nu.nl/tech/6334596/criminelen-ontdekken-een-nieuwe-oplichtingstruc-phishing-via-qr-codes.html).

ah-tk-20242025-822
ISSN 0921 - 7398
's-Gravenhage 2024

helpdesk ontving in 2024 ongeveer 20 meldingen van phishing met QR-codes, waarbij de schade geschat wordt op ongeveer € 160.000. Daarnaast ontvangt de Fraudehelpdesk jaarlijks ongeveer 600.000 e-mails via de geautomatiseerde e-mailcheck. De schatting van de Fraudehelpdesk is dat ongeveer 20% tot 25% van de ingestuurde valse mails een QR-code bevat. Het aantal registraties waarin sprake is van phishing via QR-codes per mail lijkt gestegen.

Vraag 3
Heeft u een beeld sinds wanneer deze modus operandi door criminelen toegepast wordt?

Antwoord 3
De Fraudehelpdesk is sinds 2018 bekend met phishing via QR-codes. Het Openbaar Ministerie (OM) heeft deze vorm van oplichting voor het eerst genoemd in de Fraudemonitor 2019 en 2020.[2]

Vraag 4
Hoeveel gevallen van phishing via QR-codes zijn er het afgelopen jaar bij de politie gemeld?

Antwoord 4
De politie houdt geen aparte registraties bij van het aantal gevallen van phishing via QR-codes.

Vraag 5
Besteedt de politie aandacht aan deze nieuwe vorm van oplichting? Zo ja, op welke manier? Zo nee, waarom niet?

Antwoord 5
Als er een aangifte van deze nieuwe vorm van oplichting wordt gedaan, wordt de zaak in behandeling genomen en geprioriteerd conform de daarvoor geldende kaders. De politie probeert altijd alert te zijn op nieuwe fenomenen.

Vraag 6
Welke uitdagingen en belemmeringen ondervinden de politie en het Openbaar Ministerie (OM) bij de opsporing en vervolging van criminelen die deze vorm van oplichting inzetten?

Antwoord 6
Gedigitaliseerde criminaliteit in het algemeen heeft het vermogen om snel te veranderen en heeft vaak een internationale component. Een ander onderscheidend kenmerk is dat personen die zich bezighouden met deze vormen van criminaliteit zoveel mogelijk uit het zicht van de opsporing proberen te blijven door hun identiteit af te schermen.
Daarnaast is er sprake van een hefboomeffect waarmee een crimineel in korte tijd veel slachtoffers kan maken. De vrij openlijke handel in buitgemaakte gegevens op sociale media faciliteert deze online criminaliteit. Verder vloeit geld steeds vaker naar buitenlandse rekeningen waardoor interveniëren moeilijker wordt.

Vraag 7
Welke maatregelen treft u om burgers te informeren over de risico's van phishing via QR-codes?

Antwoord 7
Er worden vanuit verschillende publieke en private organisaties campagnes gevoerd gericht op de preventie van gedigitaliseerde criminaliteit als geheel en om te informeren over de risico's van phishing met behulp van QR-codes. Het kabinet investeert in het vergroten van de digitale weerbaarheid van burgers en bedrijven en steunt voorlichtingscampagnes, die al dan niet in samenwerking met (private) partijen worden vormgegeven. Zo publiceert de Fraudehelpdesk op haar site dagelijks een selectie van de naar hen doorge-

[2] Kamerstukken II 2021/22, 17 050, nr. 600.

stuurde valse e-mails, ook die met een QR-code. Bedrijven van wie de naam wordt misbruikt in de mails die door de Fraudehelpdesk worden gepubliceerd, worden hiervan op de hoogte gesteld. Op de website en op sociale media worden tevens regelmatig waarschuwingen voor nieuwe of toenemende fraudevormen gepubliceerd.
Daarnaast worden er op initiatief van de politie, de banken, de Fraudehelpdesk, veiliginternetten.nl, de Betaalvereniging Nederland, het Digital Trustcenter en de Consumentenbond ook regelmatig campagnes georganiseerd om burgers en bedrijven weerbaarder te maken tegen deze vorm van gedigitaliseerde criminaliteit. In oktober 2024 is de Nationale Cursus Digitale Weerbaarheid met financiële steun van het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) gelanceerd. In de cursus is een module opgenomen over phishing, waarin phishing door middel van QR-codes ook aan bod komt. De website voorkomfraude.nl van de Nederlandse Vereniging van Banken (NVB) en de initiatieven vanuit de integrale aanpak van online fraude spelen een belangrijke rol in het versterken van de digitale weerbaarheid van kwetsbare groepen. Gelet op de steeds veranderende modus operandi, zijn deze initiatieven blijvend van belang.

Vraag 8
Heeft u contact met bedrijven wiens QR-codes door criminelen gespoofd worden en bent u in gesprek met deze bedrijven om fraude zoveel mogelijk tegen te gaan?

Antwoord op 8

Voor een gerichte en effectieve aanpak is het van groot belang dat bedrijven aangifte doen indien ze te maken krijgen met spoofing. Ze kunnen hier melding van doen bij de politie of dit (anoniem) melden bij Meld Misdaad Anoniem.
Mijn beleid is gericht op het bevorderen van weerbaarheid en op preventie. Het doel hiervan is om zoveel mogelijk schade en slachtoffers aan de voorkant te voorkomen.
Daarom faciliteer ik de voorlichting rondom deze vorm van criminaliteit door de mogelijkheden waarmee criminelen fraude kunnen plegen onder de aandacht te brengen bij zowel burgers als bedrijven. Vanuit mijn ministerie en de Rijksoverheid in den brede zijn er diverse activiteiten en trajecten om de (cyber-)weerbaarheid van zowel burgers als bedrijven te verhogen. Binnen de integrale aanpak van cybercrime worden ook door de deelnemende partners trends en fenomenen met elkaar uitgewisseld en waar nodig worden deze gedeeld met de getroffen branches. De strafrechtelijke aanpak van fraude is belegd bij opsporings- en vervolgingsinstanties.

Vraag 9
Anticipeert u op nieuwe vormen van oplichting waarbij digitale technologieën worden ingezet? Zo ja, welke zijn dit?

Antwoord 9
Digitale technologieën worden vandaag de dag helaas veelvuldig ingezet door criminelen om strafbare feiten mee te plegen. In een steeds meer gedigitaliseerde maatschappij kan dus ook niet worden uitgesloten dat er (nieuwe) digitale technologieën worden ingezet voor criminele doeleinden zoals oplichting.
Daarom is het groot van belang om continu te anticiperen op nieuwe vormen van fraude. De Financial Intelligence Unit – Nederland (FIU-NL), het Financial Advanced Cyber Team (FACT) van de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) en de Electronic Crimes Task Force (ECTF) zetten zich onder andere in om deze nieuwe fraudefenomenen op te sporen. Van welke aard nieuwe criminaliteitsvormen zullen zijn en welke werkwijze hiermee gepaard gaat, is niet altijd van tevoren te voorspellen. Op 23 mei jl. is uw Kamer bijvoorbeeld door de Minister van Financiën geïnformeerd over de mogelijk-

heden tot fraude met betaalproducten met behulp van deepfakes/kunstmatige intelligentie.[3] Deze nieuwe vormen hebben dan ook de aandacht van het kabinet.

Vraag 10
Kunt u deze vragen afzonderlijk van elkaar beantwoorden?

Antwoord 10
Ja.

[3] Aanhangsel Handeling II 2023/24, nr. 1820.