

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

523

Vragen van de leden **Schut-Welkzijn, Moors** en **Van Oosten** (allen VVD) aan de Staatssecretaris van Sociale Zaken en Werkgelegenheid en de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over *het bericht «Tweetal steelt AOW via DigiD-fraude»* (ingezonden 17 oktober 2014).

Antwoord van Staatssecretaris **Klijnsma** (Sociale Zaken en Werkgelegenheid), mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Veiligheid en Justitie (ontvangen 11 november 2014)

Vraag 1

Kent u het bericht «Tweetal steelt AOW via DigiD-fraude»?¹

Antwoord 1

Ja.

Vraag 2

Klopt het dat de fraude heeft plaatsgevonden via «phishing»? Hoe ging dit in zijn werk?

Antwoord 2

De FIOD is onder leiding van het Functioneel Parket een strafrechtelijk onderzoek gestart. Hierin zijn aanwijzingen naar voren gekomen dat DigiD inloggegevens zijn verkregen via *phishing*. De *phishing* heeft vermoedelijk plaatsgevonden via mailverkeer dan wel via een telefonische benadering. In het onderzoek zijn ongeveer 5.000 DigiD's naar voren gekomen die mogelijk onbevoegd gebruikt zijn. Met circa 180 DigiD's zijn gegevens gewijzigd op websites van overheidsorganisaties. In veel gevallen kon de betrokken overheidsorganisatie op tijd ingrijpen en/of konden handelingen worden teruggedraaid. De betrokken burgers zijn direct geïnformeerd. De 5.000 gecompromitteerde DigiD's zijn verwijderd. In het onderzoek zijn tevens 70 verdachte bankrekeningen naar voren gekomen. Deze bankrekeningen zijn door de betreffende banken geblokkeerd.

¹ <http://nos.nl/artikel/710540-tweetal-steelt-aow-via-digidfraude.html>

Vraag 3

Deelt u de mening dat het stelen van uitkeringen door misbruik te maken van DigiD-gegevens van mensen die dit niet kunnen voorkomen bijdraagt aan het gevoel van onveiligheid van mensen en hun wantrouwen in ICT en de overheid voedt? Hoe gaat u dit wantrouwen wegnemen?

Antwoord 3

Het kabinet heeft continu aandacht voor veilige digitale dienstverlening middels DigiD. Burgers worden via diverse campagnes erop gewezen zorgvuldig met hun DigiD account om te gaan. De overheid zal nooit per email of telefoon persoonlijke gegevens vragen.

De Minister van Binnenlandse Zaken heeft u in de brief aan uw Kamer over aanhoudingen fraude met DigiD d.d. 16 oktober 2014 (Tweede Kamer, vergaderjaar 2014–2015, 26 643, nr. 329) toegezegd om uw Kamer op zo kort mogelijke termijn een overzicht te doen toekomen met de verschillende (mogelijke) maatregelen om het gebruik van DigiD nog veiliger te maken. Ik verwijs u in dat kader tevens graag door naar het antwoord op vraag 5.

Vraag 4

Zijn de gedupeerden schadeloos gesteld voor het gehele fraudebedrag? Wordt het fraudebedrag verhaald op de daders?

Antwoord 4

De schade is relatief beperkt gebleven vanwege de snelle waarneming van de fraude door de SVB en de effectieve samenwerking daarop van de gezamenlijke overheidsdiensten. In het kader van de Rijksbrede fraude aanpak en de daaruit ontstane geïntensiveerde samenwerking kon Logius samen met onder andere de SVB de omvang van de fraude snel detecteren. Daarna is alles in het werk gesteld om schade voor de slachtoffers te voorkomen en te minimaliseren. Alle gedupeerden hebben hun uitkering of toeslag alsnog ontvangen.

De totale omvang van de financiële schade wordt geschat op 50.000 euro. Deze zal waar mogelijk verhaald worden op de daders.

Vraag 5

Wat gaat u doen om phishing van DigiD's en deze soort fraude in de toekomst voorkomen?

Antwoord 5

Logius doet er alles aan om het gebruik van DigiD veilig te houden. Bij ontdekking van zogeheten *phishing* sites wordt contact opgenomen met het Nationaal Cyber Security Center (NCSC). Notice and TakeDown (NTD)-verzoeken worden daarbij ingezet om te bewerkstelligen dat deze websites niet langer voor *phishing*-doeleinden gebruikt worden. Gebruikers kunnen zelf ook meehelpen om het gebruik van DigiD veilig te houden. Op de website van DigiD wordt door Logius advies gegeven over het veilig omgaan met DigiD. Daarbij wordt onder meer gewezen op het belang dat de gebruiker controleert dat hij/zij daadwerkelijk inlogt op de echte inlogpagina van DigiD. Ook wordt gewaarschuwd voor valse e-mails waarin wordt gevraagd om inloggegevens in te vullen. Bovendien wordt uitgelegd hoe de gebruiker misbruik van zijn account kan herkennen en welke actie hij kan ondernemen bij geconstateerd misbruik. Tenslotte wordt verwezen naar de ondersteuning die kan worden geboden onder meer via de helpdesk van DigiD, het Centraal Meldpunt Identiteitsfraude en het Meldpunt Slachtoffers Fraude van de Belastingdienst.

Ook in de lopende Alert-Online-campagne wordt uitgebreid aandacht besteed aan veilig internetten, onder andere via de in deze periode gepresenteerde website www.veiliginternetten.nl.