Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Ons kenmerk
3034406

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 9 oktober 2020
Onderwerp Cybercrime en gedigitaliseerde criminaliteit

Sinds vele jaren wordt de dreiging van cybercrime en digitale criminaliteit erkend. Sinds 2018 is er een integrale aanpak van cybercrime. Voor de opsporing zijn kwantitatieve doelstellingen in de Veiligheidsagenda 2019-2022 opgenomen, beschikt de politie op landelijk niveau over het specialistische Team High Tech Crime (THTC) en zijn met investeringen in het Regeerakkoord gespecialiseerde cybercrimeteams op regionaal niveau versterkt. De inzet op deze criminaliteitsvormen heeft tot verschillende beleidsinitiatieven en de nodige resultaten geleid. Over de voortgang van de integrale aanpak van cybercrime bent u geïnformeerd met de brief van 29 juni jl.[1] De urgentie die ik de afgelopen jaren richting uw kamer heb uitgedragen om online criminaliteit te bestrijden blijft onverminderd.[2] Met onze toegenomen digitale afhankelijkheid in de coronacrisis is deze digitale dreiging sterk toegenomen en is de online criminaliteit hard gegroeid. Een voorbeeld hiervan is hulpvraagfraude.

Met deze brief informeer ik u, mede namens de Minister voor Rechtsbescherming, nader over cybercrime en hulpvraagfraude (onder andere via whatsapp) tijdens de coronacrisis. Hiermee voldoe ik aan mijn toezegging van 16 juni jl. aan het Kamerlid Yeşilgöz-Zegerius over het aantal cybercrimemisdrijven en aan het verzoek van het Kamerlid Van Toorenburg over de handel in privégegevens van vijftigplussers voor whatsappfraude (kenmerk 2020Z12749). Eerst besteed ik kort aandacht aan enkele ontwikkelingen van de laatste maanden en de aanpak van jeugdige daders van cybercrime. Ik ga vervolgens meer uitgebreid in op hulpvraagfraude.

Online criminaliteit: cybercrime en gedigitaliseerde criminaliteit
De term 'cybercrime' wordt in het maatschappelijk debat vaak gebruikt als containerbegrip. In deze brief wordt onderscheid gemaakt tussen cybercrime en gedigitaliseerde criminaliteit. Vormen van criminaliteit die voorheen in de offline wereld plaatsvonden, maar nu online plaatsvinden, worden aangeduid met de term gedigitaliseerde criminaliteit. Het betreft bijvoorbeeld drugs- en wapenhandel via het darkweb en allerlei vormen van online fraude, waaronder hulpvraagfraude. Cybercrime (ook wel cybercrime in enge zin genoemd) betreft vormen van criminaliteit die ICT-systemen als doel hebben en derhalve niet

[1] Kamerstukken TK 2019/20, 26 643, nr. 696
[2] Kamerstukken TK 2019/20, 28 684, nr. 621; Kamerstukken TK 2017/18, 28 684, nr. 522; Kamerstukken TK 2018/19, 28 684, nr. 564;

mogelijk zijn zonder het bestaan van ICT-systemen. Het betreft bijvoorbeeld computervredebreuk, DDoS-aanvallen en de verspreiding van malware, waaronder ransomware. De term online criminaliteit wordt gebruikt om cybercrime en gedigitaliseerde criminaliteit samen aan te duiden.

Recente ontwikkelingen en wetenschappelijk onderzoek
In de brief van 29 juni jl. is reeds vermeld dat online criminaliteit tijdens de coronacrisis een stevige groei heeft doorgemaakt. De politie heeft deze groei nader geanalyseerd. Deze bleek vooral te zien bij de gedigitaliseerde criminaliteit, en dan vooral bij hulpvraagfraude. Cybercrime groeide ook door, maar deze paste meer in de groei die de politie in de afgelopen jaren reeds constateerde. Inmiddels lijkt de groei van online criminaliteit minder te zijn geworden, maar het huidige niveau ligt beduidend hoger dan voor de coronacrisis.

Onlangs heeft het WODC het rapport opgeleverd van het onderzoek naar de aard en omvang van cybercrime en gedigitaliseerde criminaliteit.[3] Uit dat onderzoek blijkt dat veel databronnen om de aard en omvang nader te kunnen duiden een lastig te interpreteren beeld opleveren. Kwantitatieve schattingen en wetenschappelijke conclusies zijn op basis van de huidige beschikbare gegevens daarom weinig precies. Ten behoeve van de beleidsvorming zijn dergelijke inzichten echter wel gewenst. Daarom wordt samen met het CBS inmiddels gewerkt aan de herziening van de tweejaarlijkse Veiligheidsmonitor. Daarin wordt meer aandacht besteed aan het slachtofferschap van cybercrime en online fraude. In 2021 wordt bovendien de rapportage van de vijfjaarlijkse Monitor Jeugdcriminaliteit verwacht. Ook in deze monitor zal meer aandacht worden besteed aan daderschap van cybercrime en gedigitaliseerde criminaliteit. Daarnaast wijst het recente rapport op het belang van voldoende expertise in de strafrechtketen. Dat belang onderken ik. In de afgelopen jaren is daarom geïnvesteerd in de capaciteit en expertise van de politie en het OM. Verderop in deze brief ga ik daar op in.

Cybercrime
Een overzicht van de aanpak van cybercrime vindt u in de brief van 29 juni jl. In de aanpak werken de ministeries van J&V en EZK nauw samen. In de brief is onder meer het aantal veroordelingen van cybercrimedelicten gemeld zoals gevraagd door het Kamerlid Yeşilgöz-Zegerius. Ter volledigheid noem ik opnieuw kort de aantallen. In 2017 zijn 69 meerderjarigen en 9 minderjarigen na hoger beroep veroordeeld. In 2018 ging het om 91 meerderjarigen en 15 minderjarigen, in 2019 betrof het 118 meerderjarigen en 10 minderjarigen.

In het kader van de aanpak vindt een veelheid aan preventieve en repressieve activiteiten plaats, waarbij actief wordt samengewerkt met private partijen en medeoverheden. Voor een totaaloverzicht verwijs ik naar mijn brief van 29 juni. Voor bepaalde doelgroepen worden specifieke preventieactiviteiten uitgevoerd. Zo worden diverse maatregelen uitgevoerd om daderschap en recidive van cybercrime onder de jeugd te voorkómen. Het betreft onder meer de campagnes "je bent maar één klik verwijderd van cybercrime" en "GameChangers" van de politie, het aanvullen van het risicotaxatie- en diagnose-instrumentarium (LIJ) en het interventiepalet, en de pilot Hack Right van de politie en het OM waarbij jeugdige cyberdaders op het rechte pad worden gebracht. Daarnaast ontwikkelt

[3] https://wodc.nl/onderzoeksdatabase/2921a-aard-en-omvang-cyber-en-gedigitaliseerde-criminaliteit.aspx

HALT een module om jongeren op scholen voorlichting te geven om zowel daderschap als slachtofferschap onder jongeren te voorkómen. De module is naar verwachting begin 2021 gereed.

In diverse gemeenten worden projecten ondersteund voor het tegengaan van cybercrime bij jongeren, ouderen, laaggeletterden en ondernemers. Formalisering van de samenwerking hiervan in een City Deal is voorzien in oktober. Mijn ministerie heeft daarnaast meegewerkt aan een project van het Ministerie van BZK en de gemeente Den Haag om een module over veilig internetten te maken voor www.oefenen.nl, gericht op (digitaal) laaggeletterden en senioren. Dit project is op 9 oktober afgerond. Mensen kunnen dan thuis en in bibliotheken oefenen met hun digitale vaardigheden en hun bewustzijn over online veiligheid vergroten. In deze module wordt met name aandacht besteed aan veilig online gedrag.

De opsporing en vervolging van diverse vormen van cybercrime is complex, onder meer door de mondiale architectuur van het internet en de afhankelijkheid van private partijen. Complexe rechtshulprelaties en belemmeringen voor rechtmatige toegang tot bewijsmateriaal, bijvoorbeeld door het gebruik van encryptie, VPN-servers en doorverhuurde serverruimte, maken succesvolle opsporing en vervolging van criminelen uitdagend. Voor de opsporing, vervolging en verstoring van cybercrime zijn kwantitatieve doelstellingen opgenomen in de Veiligheidsagenda. Met de investeringen uit het Regeerakkoord is bij de politie een uitbreiding van 145 fte gerealiseerd, die vooral worden ingezet ter versterking van de regionale cybercrimeteams. De werving van specialisten op dit gebied is niet eenvoudig, onder meer vanwege de schaarste van technisch experts op de arbeidsmarkt. Er is veelal sprake van zijinstroom, omdat met reguliere in- en doorstroom vaak niet in de benodigde expertise kan worden voorzien. De politie heeft daarom de wervingsinspanningen aangepast en gecentraliseerd. Ook is het wervingstraject voor cyberspecialisten in de tijd verkort. Inmiddels zijn de gewenste aantallen specialisten ingestroomd. Dat is een forse prestatie. De beschikbare capaciteit bij het OM blijft daarbij achter. Naast de opsporing besteden de politie en het OM aandacht aan preventie- en verstoringsmogelijkheden bij specifieke criminele werkwijzen of fenomenen. Daarmee wordt het criminelen zo lastig mogelijk gemaakt om hun activiteiten uit te voeren.

Hulpvraagfraude
Bij hulpvraagfraude is sprake van een delict waarbij een fraudeur zich via een berichtendienst voordoet als een familielid of bekende van een (potentieel) slachtoffer. Hij geeft aan in (geld)nood te zitten en bijvoorbeeld een factuur, die met spoed betaald moet worden, niet te kunnen betalen. Vervolgens vraagt de fraudeur om dat geld voor te schieten en over te boeken naar een bepaalde bankrekening of om in te gaan op een betaalverzoek. Het geld komt echter, vaak via diverse geldezels of buitenlandse bankrekeningen, bij de fraudeur terecht. Fraudeurs hanteren daarbij verschillende werkwijzen. Regelmatig benaderen fraudeurs hun potentiële slachtoffer vanaf een zogenaamd nieuw telefoonnummer en zeggen dat het ‘oude’, bekende telefoonnummer niet meer werkt. Daarbij wordt vaak de profielfoto, of zelfs de opgenomen stem gebruikt van degene voor wie de fraudeur zich voordoet. In andere gevallen wordt het account van een berichtendienst, bijvoorbeeld WhatsApp, van een persoon overgenomen door de fraudeur. Deze fraude wordt vaak gepleegd in georganiseerde verbanden.

Hulpvraagfraude is een sluwe en nare vorm van oplichting, waarvan vaak kwetsbare mensen slachtoffer worden. De coronacrisis maakt mensen soms extra kwetsbaar. Ze staan dikwijls minder in fysiek contact met hun naasten en communiceren meer op digitale wijze met elkaar. Criminelen misbruiken vervolgens de bereidheid van mensen om hun naasten in nood te helpen. Naast het lijden van financiële en emotionele schade worden behulpzaamheid en vertrouwen in elkaar erdoor ondergraven.

De politie en de Fraudehelpdesk geven aan dat het aantal aangiftes en meldingen van deze vorm van fraude sinds 2019 stijgt. Bij de Fraudehelpdesk zijn tot 1 augustus 2020 7.907 meldingen binnengekomen. In heel 2019 betrof het 2.663 meldingen. De politie meldt dat het aantal aangiftes vóór de coronacrisis op circa 120 tot 150 aangiftes per week lag. Sinds april van dit jaar is het mogelijk om digitaal aangifte te doen en komen er circa 100 aangiftes per dag binnen. De toename is waarschijnlijk deels veroorzaakt doordat het nu makkelijker is aangifte te doen en deels door een feitelijke toename. Deze kan mede zijn veroorzaakt doordat senioren tijdens de coronacrisis meer online actief zijn geworden, onder andere om contact te houden met familie en bekenden. Sinds april blijft het aantal aangiftes op het genoemde hoge niveau. Daarbij merkt de politie op dat het aantal gemelde pogingen tot hulpvraagfraude veel groter is dan vóór de invoering van de internetaangifte (40% tegenover minder dan 10%). Dit duidt erop dat de invoering van de internetaangifte de meldingsbereidheid vergroot en dat mensen mogelijk alerter zijn op deze vorm van fraude.

Handel in gegevens van vijftigplussers voor hulpvraagfraude
RTL Nieuws heeft op 23 juni jl. over hulpvraagfraude bericht. In dat bericht wordt melding gemaakt van grootschalige handel in privégegevens van vijftigplussers ten behoeve van het plegen van hulpvraagfraude. Deze gegevens zouden afkomstig zijn van callcenters, waarbij medewerkers klantgegevens zouden doorverkopen aan criminelen. De callcenters gaven volgens het bericht van RTL Nieuws aan dat bij hen geen gevallen hiervan bekend zijn, dat er strikte protocollen worden gehanteerd als een medewerker wordt betrapt en dat zo nodig aangifte wordt gedaan. Bovendien zijn callcenters volgens de Algemene Verordening Gegevensbescherming (AVG) verplicht een melding te doen bij de Autoriteit Persoonsgegevens als een datalek heeft plaatsgevonden en dit waarschijnlijk leidt tot een risico voor de rechten en vrijheden van betrokkenen.

Uit aangiftes wordt vaak niet direct duidelijk hoe daders aan gegevens van slachtoffers zijn gekomen. In sommige gevallen is duidelijk dat de gegevens afkomstig zijn van bijvoorbeeld een datingsite of een online verkoopplatform. Wel is de politie in opsporingsonderzoeken incidenteel gestuit op de handel in gegevens zoals door RTL Nieuws bericht. Er zijn vooralsnog geen aangiftes gedaan door callcenters.

Opsporing van hulpvraagfraude
De politie en het OM nemen hulpvraagfraude zeer serieus. Online fraude is niet expliciet opgenomen in de laatste Veiligheidsagenda en er zijn derhalve geen kwantitatieve doelstellingen voor de opsporing vastgesteld. Gezien de forse stijging en de maatschappelijke impact van hulpvraagfraude tijdens de coronacrisis hebben de politie en het OM desalniettemin besloten aan dit specifieke fenomeen extra aandacht te besteden. De mogelijkheid om via internet aangifte van hulpvraagfraude te doen is versneld mogelijk gemaakt, en dat helpt bij de aanpak. Het geeft slachtoffers een laagdrempelige mogelijkheid om

aangifte te doen, zodat de politie meer inzicht krijgt in de omvang en de aard van deze vorm van criminaliteit. Daarnaast is de politie gestart met een landelijke aanpak om deze vorm van oplichting tegen te gaan. De aanpak van hulpvraagfraude wordt daarin centraal opgezet en gecoördineerd. Aangiftes worden landelijk gebundeld, zodat snel zicht ontstaat op zaken die kansrijk zijn en verbanden tussen zaken kunnen worden gesignaleerd. Bij de aanpak wordt nadrukkelijk gekeken naar geldezels en criminele samenwerkingsverbanden. De aanpak heeft inmiddels geleid tot een aantal succesvolle opsporingsonderzoeken en strafzaken. Een voorbeeld is de recente uitspraak van de Rechtbank Overijssel, die forse celstraffen bevat voor twee daders.[4]

Preventie van hulpvraagfraude
De meest effectieve manier om fraude te bestrijden blijft het voorkómen ervan. Dat geldt zeker voor hulpvraagfraude. Het is van groot belang dat mensen zich bewust zijn van, en alert zijn op, de berekenende werkwijze van criminelen. Ook is het van belang dat mensen voorzichtig zijn met het delen van persoonlijke informatie, bijvoorbeeld op sociale media. Die persoonlijke informatie wordt door fraudeurs gebruikt om geloofwaardiger over te komen. Ik span mij samen met diverse publieke en private partijen in om mensen te waarschuwen voor deze vorm van fraude. Daarbij richt ik me op specifieke doelgroepen, waaronder senioren, in nauwe samenwerking met de ouderenorganisaties. Zoals ik in mijn brief van 27 augustus jl. aangaf ben ik in september in samenwerking met de ouderenbonden een campagne gestart om senioren via voorlichtingsfilms en webinars meer bewust te maken van dit soort vormen van criminaliteit en hen handelingsperspectieven te bieden om te voorkomen dat ze slachtoffer worden. Deze campagne is de uitwerking van mijn toezegging naar aanleiding van de mondelinge vraag van het lid Van Toorenburg op 17 december jl. om publiekelijk aandacht te besteden aan fenomenen waar ouderen slachtoffer van worden, zoals babbeltrucs en gedigitaliseerde criminaliteit. Aan deze thema's is aandacht besteed in samenwerking met vele partijen, waaronder de ouderenbonden, de politie, het OM, Slachtofferhulp Nederland, de Fraudehelpdesk, het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), Veiliginternetten.nl, banken, supermarkten en de telecomsector. Ook hebben inmiddels meer dan 150 gemeenten zich bij de campagne gericht op senioren aangesloten. Naast hulpvraagfraude wordt er in deze campagne aandacht besteed aan babbeltrucs, meekijken bij pinnen en phishing.

Daarnaast heb ik onlangs samen met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en Scholieren.com een campagne gehouden om jongeren te stimuleren om hun eigen (groot)ouders te waarschuwen voor hulpvraagfraude en met hen de afspraak te maken om altijd eerst met elkaar te bellen voordat er geld wordt overgemaakt ('Niet gebeld, geen geld'). Het streven is om de crimineel voor te zijn door (klein)kinderen zelf hun (groot)ouders te laten voorlichten. Deze campagne is inmiddels breed gedeeld via sociale media. In 2019 heb ik samen met mijn collega van Economische Zaken en Klimaat (EZK) de preventiecampagne 'Eerst checken dan klikken' uitgevoerd. De boodschap van deze campagne is behulpzaam tegen veel vormen van gedigitaliseerde

[4] ECLI:NL:RBOVE:2020:2959 d.d. 10 september 2020, zie ook www.nu.nl/tech/6076576/twee-mannen-uit-deventer-krijgen-tot-drie-jaar-cel-voor-whatsapp-fraude.html

criminaliteit, waaronder hulpvraagfraude, en cybercrime. Via de site www.veiliginternetten.nl, die ik samen met het ministerie van EZK en het ECP (Platform voor de informatiesamenleving) vormgeef, kunnen mensen informatie vinden over hoe men onder andere hulpvraagfraude en phishing kan voorkómen. Ook andere publieke en private partijen, zoals de politie, de Fraudehelpdesk, banken, de Consumentenbond en Slachtofferhulp Nederland bieden veel informatie over hulpvraagfraude en het voorkomen daarvan.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
DRC / C&V

Datum
9 oktober 2020

Ons kenmerk
3034406

De Fraudehelpdesk is recent gestart met een campagne 'Laat je niet neppen tijdens het appen!.' De politie is via sociale media en de eigen kanalen een online campagne gestart gericht op 50-plussers en hun (klein)kinderen. Slachtofferhulp Nederland (SHN) biedt slachtoffers van hulpvraagfraude kosteloos juridische, praktische en emotionele ondersteuning, en online lotgenotencontact. De WhatsApp-dienst van Facebook kent een waarschuwingsscherm op het moment dat een persoon door een nieuwe gebruiker wordt benaderd, zodat die persoon extra alert is. WhatsApp kent een twee-staps-verificatiesysteem om te voorkomen dat een account wordt overgenomen. Ik roep mensen op om zoveel mogelijk van dit soort beveiligingsmogelijkheden gebruik te maken. Banken hebben hun fraudedetectie aangescherpt en proberen via hun eigen kanalen zoveel mogelijk mensen te waarschuwen.

Tot slot
De toenemende digitalisering van ons maatschappelijk, economisch en financieel verkeer heeft goede kanten, maar ook een keerzijde: ook criminelen maken hier gebruik van. Bij de aanpak spelen vele partijen een rol, zowel bij de preventie als bij de inzet van het strafrecht. De meest effectieve bijdrage kunnen mensen zelf leveren door goed op te blijven letten. De overheid ondersteunt mensen daarin en probeert de criminelen aan te pakken als zij toch slachtoffers hebben gemaakt. Helaas is het niet te verwachten dat criminelen de digitale wereld in de toekomst niet blijven misbruiken. Ik blijf daarom inzetten op een stevige aanpak.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus