AUDIT MAGAZINE

INTERVIEWS | 1 FEBRUARI 2022

VERTROUWEN IS GOED, CONTROLE IS BETER

Auteur: Drs. Nicole Engel-de Groot - Fong-Chi Wai MSc RO
Beeld: Adobe Stock - Brett Jordan
Leestijd: 5 min

Vladimir Lenin richtte in 1921 de KGB op om mensen die niet recht in de leer waren op te sporen en uit te schakelen met de woorden 'vertrouwen is goed, controle is beter'. De tijden zijn veranderd, maar deze uitspraak is nog altijd relevant. Want fact checking is een belangrijke sleutel om oplichting tegen te gaan. Tanya Wijngaarde van Fraudehelpdesk.nl over oplichting in Nederland.

Wat doet de Fraudehelpdesk?

"Wij zijn het landelijk meldpunt voor horizontale fraude. Horizontale fraude gaat over fraude en oplichting in het private domein, het omvat niet de fraude tussen mensen en overheid. Het omvat wel oplichting c.q. fraude van particulieren en bedrijven. Wij zijn een eerste loket, geven een eerste advies aan mensen en verwijzen ze eventueel door naar de juiste instanties. Dit kan bijvoorbeeld de politie zijn om aangifte te doen, of de Autoriteit Consument & Markt (ACM) als het gaat om een consumentenklacht."

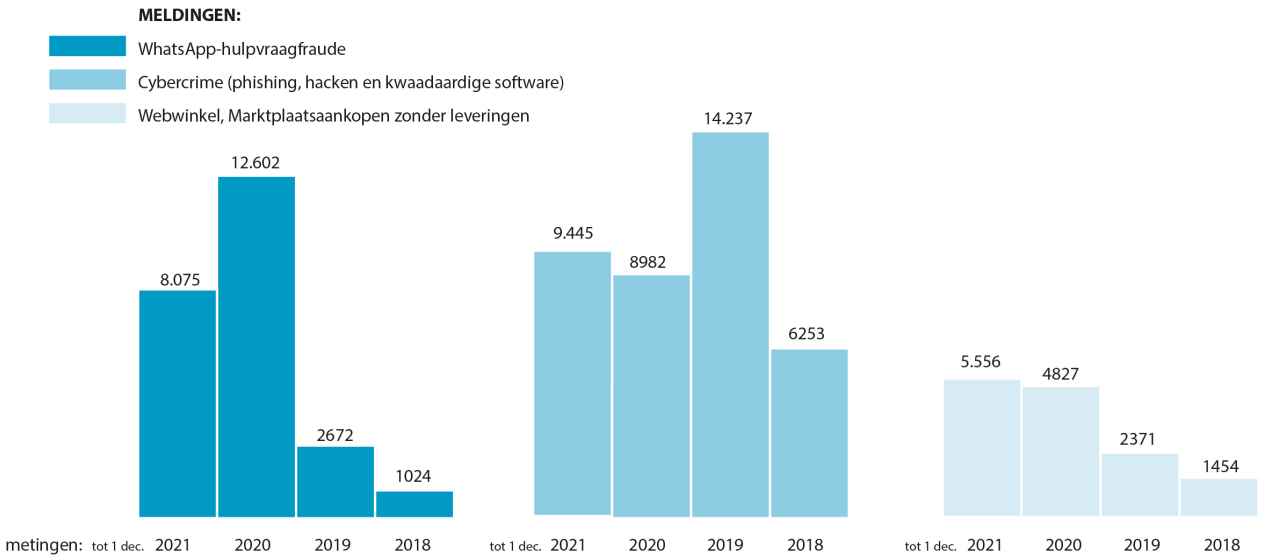
Tanya Wijngaarde (Fraudehelpdesk): “Oplichting vindt op een steeds geavanceerdere en geraffineerdere wijze plaats. Ieder nietsvermoedend bedrijf of persoon kan slachtoffer worden. Ook hoogopgeleide mensen”

Wat doen jullie met de meldingen?

“Wij registreren de fraudemeldingen en houden hierdoor zicht op de ontwikkelingen. We gebruiken de informatie uit de meldingen om campagnes op te zetten om mensen bewust te maken van fraude. Vaak doen wij dat samen met andere partijen, zoals het Openbaar Ministerie (OM), de Autoriteit Financiële Markten (AFM) of het Europees Consumenten Centrum (ECC). Wij rapporteren de cijfers aan het ministerie van Justitie en Veiligheid en deze zijn ook beschikbaar voor media, studenten en onderzoekers. Wij zijn een onafhankelijke private partij die subsidie ontvangt van de overheid om haar taak uit te voeren.”

Hoeveel meldingen krijgen jullie binnen?

“In 2020 hadden we 350.000 meldingen.”



Figuur 1. Top-3 meldingen

Zien jullie ook bepaalde trends?

“Ja. Je ziet in bepaalde perioden dat bepaalde fraudes pieken. Zo waren er in het begin van corona veel meer mensen actief met aankopen op websites en was er veel social-mediaverkeer. Toen zag je een toename in aan- en verkoopfraude en in WhatsAppfraude. Dat laatste valt onder de identiteitsfraude die sinds 2019 significant toenam.”

“Bedrijven denken soms dat zij niet interessant zijn voor oplichting. Maar dat is niet waar. Oplichters maken geen onderscheid”

Wat zijn zorgwekkende ontwikkelingen?

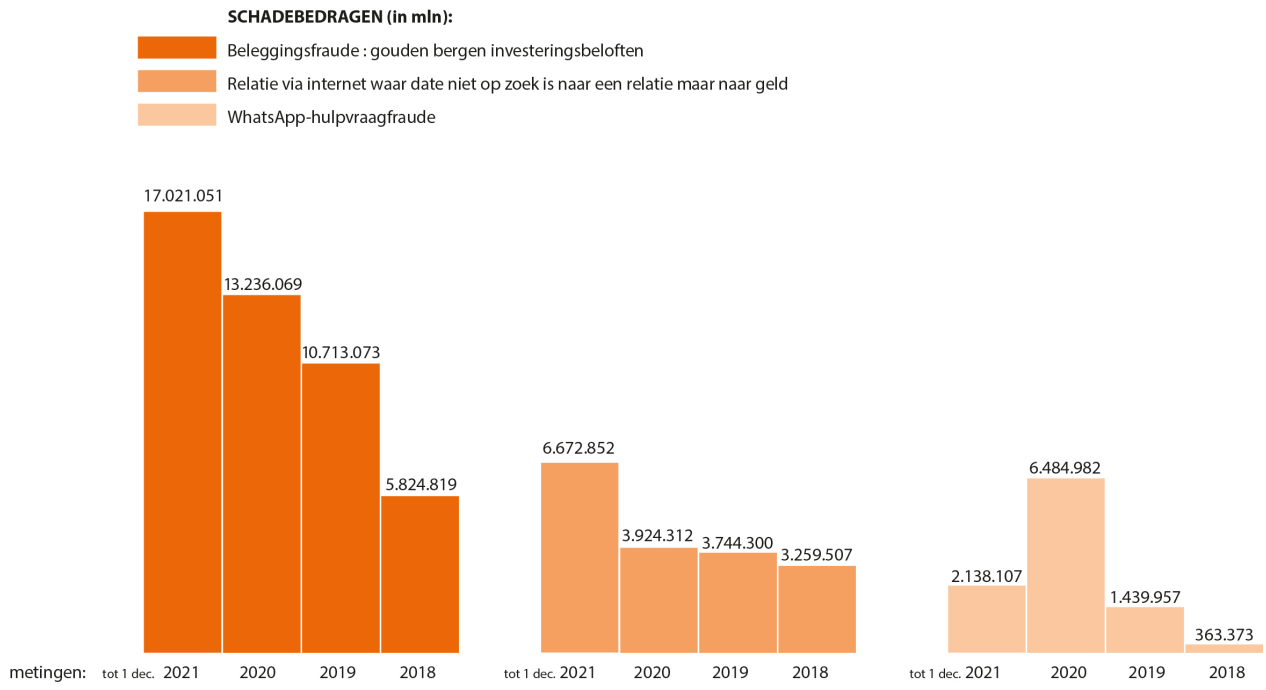
“De techniek wordt steeds beter en geavanceerder, en tegelijkertijd ook betaalbaarder en beter bereikbaar voor een grotere groep kwaadwillenden. Kant-en-klare pakketten met onder meer software én handleidingen om mensen op te lichten (waaronder scripts met wanneer je wat kunt zeggen) zijn online te koop. Je hoeft zelf niet per se technische kennis te hebben. En deep-faketechnologie bijvoorbeeld wordt steeds goedkoper en beter.”

Wat is deep fake?

“Met deep fake kun je op basis van een foto bewegend beeld van iemand maken, of op basis van enkele woorden iemands stemgeluid nabootsen. Daardoor lijkt het levensecht. Een paar jaar geleden was dat nog ver weg, nu is oplichting met gebruik van deep fake echt een reëel risico.”

Welke ontwikkelingen zien jullie nog meer?

“Ook phishing mails zijn steeds meer geavanceerd. Voorheen was het bijvoorbeeld een mail met veel spelfouten en met de aanhef ‘beste bankklant’. Tegenwoordig zien de mails een stuk professioneler uit en weten ze, waarschijnlijk door informatie uit datalekken, vaak je naam en word je persoonlijk aangesproken. Of trucs worden gecombineerd, bijvoorbeeld een nep-mail met daarin een link die al toegang geeft tot je bankgegevens, waarna je gebeld wordt met de kennis van je naam en toenaam en al je bankgegevens. Op zo’n moment klinkt het alsof je echt door de bank gebeld wordt. Ze weten immers ze al je gegevens. Als daarna wordt gevraagd om een overboeking te doen, zijn mensen geneigd hieraan gehoor te geven. In december 2019 kwamen de eerste meldingen binnen over deze oplichting. In 2020 was de totale schade van deze vorm van oplichting 4 miljoen euro.”



Figuur 2. Top-3 schadebedragen fraude

Wat betekent dit?

“Al dit soort ontwikkelingen en technieken zijn zorgwekkend. Als er sprake is van WhatsAppfraude, waarbij iemand via WhatsApp door zogenaamd een bekende benaderd wordt om geld over te maken, dan is deel van het standaard advies: bel die bekende. Zo kun je controleren of je te maken hebt met een oplichter. Maar wat als er sprake is van deep fake en je echt iemand ziet en hoort zoals je hem kent? Probeer dan maar eens echt van vals te onderscheiden.”

“Kant-en-klare pakketten met onder meer software én handleidingen om mensen op te lichten (waaronder scripts met wanneer je wat kunt zeggen) zijn online te koop”

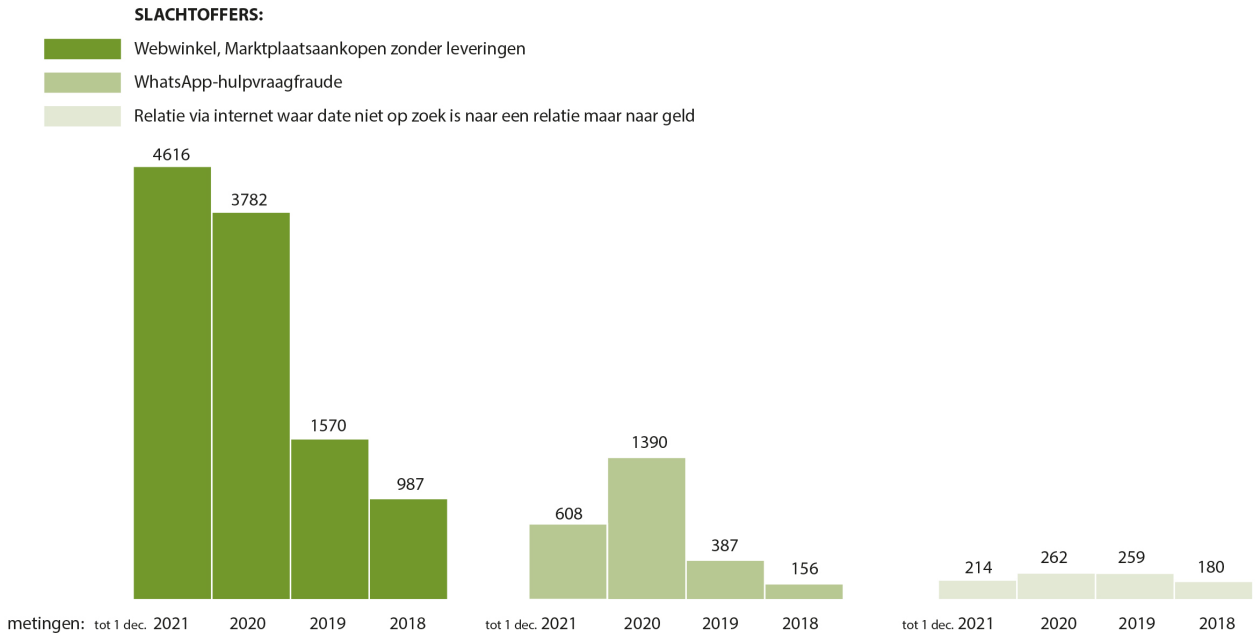
Wat wordt gedaan met fraudemeldingen?

“De Fraudehelpdesk rapporteert aan de overheid en zet campagnes op gebaseerd op het beeld dat ontstaat uit alle meldingen. De Fraudehelpdesk heeft geen opsporingsbevoegdheid. Eerder gaven we ook aan de politie meldingen door, maar sinds de AVG-wet mag dat niet meer. Dat is heel jammer, want juist door in een vroeg stadium te melden over pogingen tot oplichting kan veel ellende voorkomen worden. Mensen stappen meestal pas naar de politie als er echt schade is.”

Kun je je wel beschermen tegen fraude?

“Elementaire zaken zijn belangrijk. Bijvoorbeeld eerst checken en dan klikken. Fact checking dus: controleer de afzender die je appt of belt. Preventie zit ook in unieke en sterke wachtwoorden. Gebruik dus niet hetzelfde wachtwoord voor verschillende accounts en maak wachtwoorden ingewikkeld. Je kunt ze noteren in een wachtwoordmanager. En maak back-upbestanden van je harde schijf en bewaar die losgekoppeld van de computer, zodat bij malware niet hele IT-processen platliggen en gegevens onbereikbaar zijn.”

“Dit geldt trouwens zowel voor bedrijven als particulieren. Voor bedrijven is het nog belangrijker om ook je domein voldoende te beschermen. Bedrijven denken soms dat zij niet interessant zijn voor oplichting. Maar dat is niet waar. Iedereen kan doelwit zijn en oplichters maken geen onderscheid. Bewustwording is belangrijk maar niet voldoende. Het is moeilijk om mensen te bewegen tot handelen.”



Figuur 3. Top-3 slachtoffers fraude

Hoe kwetsbaar is Nederland voor een destabiliserende fraude?

“Best kwetsbaar, want alles wordt steeds digitaler en is met elkaar verbonden. Met name de groep mensen die digitaal niet onderlegd is, is kwetsbaar. En tegelijkertijd kan het iedereen het overkomen. Oplichting vindt op een steeds geavanceerdere en geraffineerdere wijze plaats. Door de alsmaar meer voorkomende datalekken weten oplichters ook steeds meer. Ieder nietsvermoedend bedrijf of persoon kan slachtoffer worden. Ook hoogopgeleide mensen.”

Bent u zelf ooit slachtoffer geweest van oplichting?

“Nee, maar dat is ook omdat ik hier werk. Daardoor ben ik me heel erg bewust van alle risico’s. Als dat niet het geval zou zijn, durf ik mijn hand er niet voor in het vuur te steken dat het me niet zou overkomen.”

Over
Tanya Wijngaarde is woordvoerder/voorlichter van Fraudehelpdesk.nl.

Tags: Fake news, informatiebeveiliging

Bron url: https://auditmagazine.nl/interviews/vertrouwen-is-goed-controle-is-beter/