Van de hacker tot de casher: zo ontfutselen jonge criminelen tienduizenden euro's van goedgelovige bejaarden

De hacker, het callcenter, de kaartophaler de casher,... Maak kennis met de zogenaamde helpdeskfraude, een organisatie onder leiding van geharde criminelen die jongeren -zelfs minderjarigen - rekruteren om via een ingenieus systeem bejaarden van hun spaargeld te beroven.

De federale gerechtelijke politie (FGP) Limburg, het parket van Limburg en lokale politiezones zetten extra in op de bestrijding van de toenemende helpdeskfraude. Met team DOT is een nieuw Digitaal Opsporingsteam met gespecialiseerde speurders opgericht. Ze zijn fulltime bezig met de nieuwe oplichtingsmethodes en hebben vandaag een goed beeld van de fraudeurs.

Soldaten

De mensen die het vuile werk in het veld moeten opknappen, worden door de politiediensten soldaten genoemd. De rekrutering gebeurt online via bij jongeren populaire sociale media als Telegram of Snapchat. De medewerkers in de onderbouw van de organisatie zijn dan ook vaak net meerderjarig of zelfs minderjarig. "Jongeren stappen naïef mee in een verhaal waarvan ze de impact vaak onderschatten", zeggen FGP en parket. "Ze komen vaker uit een kwetsbaar milieu en hebben het financieel minder goed, maar we zien ook jongeren uit zeer gegoede families."
(lees verder onder de explainer)
De gemiddelde leeftijd van de rekruten ligt tussen 18 en 25 jaar, maar de jongste verdachte die de onderzoekers zijn tegengekomen, was amper 15 jaar. Opvallende vaststelling: de verhouding jongens en meisjes is 50/50. "Dat jongedames gegeerd zijn door de organisatie heeft een logische reden: ze ogen betrouwbaar en volwassen als ze netjes gekleed en geschminkt op pad gaan. Ook wordt verwacht dat ze beleefd zijn en een mooi taalgebruik hanteren."

Bedreigd

Eenmaal gerekruteerd, is het moeilijk om uit de organisatie te stappen. Wanneer rekruten wroeging of schrik krijgen en willen terugkrabbelen, worden ze bedreigd door de opdrachtgevers. Bij de rekrutering moeten de jongeren een kopie van hun paspoort en een digitale pasfoto afgeven. Daarmee worden valse pasjes gemaakt die moeten bewijzen dat ze voor een bank werken. Maar ze kunnen ook worden gebruikt als drukmiddel tegen de rekruten zelf. Jongeren die eruit willen stappen, krijgen dan te horen dat hun identiteitsgegevens zullen worden doorgespeeld aan de politie.

Maar het kan nog erger. “We hebben al aanslagen gehad zoals we ze in het drugsmilieu zien, waarbij onder meer brandbommen als signaal bij de twijfelaars worden achtergelaten.”

De soldaten zijn dan ook niet meer dan kanonnenvlees. “Wanneer een team of dader gevat wordt, is dat voor de organisatie slechts een kleine tegenslag. Zelf blijven ze buiten schot en de volgende ploeg staat al klaar om over te nemen.”

De mensen in het veld kunnen – al dan niet gecombineerd - verschillende rollen vervullen: die van medewerker in het callcenter, chauffeur, kaartophaler of casher.

De hacker

Alles begint bij hacking door cybercriminelen. Zij behoren niét tot de organisatie van de helpdeskfraudeurs, maar verkopen hen wel lijsten met tal van persoonsgegevens en identiteiten uit het hele land. Deze informatie vinden ze door in te breken in bijvoorbeeld de online opslag van overheidsinstanties. Denk maar aan de cyberaanval op Limburg.net in 2023 toen hackers de gegevens van bijna 230.000 gezinshoofden te pakken kregen. De lijsten bevatten naast de naam ook informatie als geboortejaar, woonplaats, burgerlijke staat, of bij welke bank iemand is aangesloten.

De lijsten circuleren op het dark web, het verborgen internet waar handel wordt gedreven die het daglicht niet mag zien. Maar ook applicaties als Telegram hebben verborgen groepen waarin persoonlijke data worden aangeboden.

Het is de gespecialiseerde Regional Computer Crime Unit (RCCU) van de federale politie die dit soort computercriminaliteit onderzoekt. Zij werken samen met het Digitaal Opsporingsteam (DOT).

De leider

Bij de FGP en het parket weten ze het zeker: de leidinggevenden binnen het organogram van helpdeskfraude zijn doorwinterde criminelen die meer op hun kerfstok hebben dan alleen oplichting en diefstal. “Ze hebben hun sporen al verdiend. Het is grof geschut. Ze kunnen leunen op het netwerk dat ze in het verleden al uitbouwden en deinzen er niet voor terug om geweld te gebruiken. Ze rekruteren, maar uiten ook dreigementen aan het adres van de mensen die voor hen werken.”
De kopstukken zijn vooralsnog geen Belgen, maar komen vooral uit Nederland. Hen opsporen en arresteren is een echte uitdaging voor gerecht en politie.

Het callcenter

De onderzoekers hebben sterke vermoedens dat de mensen van het callcenter zeer dicht bij de leidinggevenden staan en fysiek zelfs in dezelfde ruimte werken. Zo anticiperen ze enorm snel en worden ze nauw aangestuurd in netelige situaties. “Hun profiel is doorheen de jaren veranderd. In de beginperiode waren het Engelstaligen. Daarna werden het Nederlanders, maar intussen merken we dat de Vlamingen het hebben overgenomen. Dat versterkt hun geloofwaardigheid.”

De medewerkers beschikken over een gedetailleerd draaiboek met tal van scenario’s over hoe ze in elke situatie moeten reageren. “Ze weten precies wat ze moeten doen. Met de info van het potentiële slachtoffer als leidraad winnen ze op een slinkse manier het vertrouwen.”
De mensen van het callcenter vertellen details waarvan het slachtoffer denkt dat alleen de bank over die informatie kan beschikken. Zo worden ze meegezogen in het verhaal. Als de valse bankmedewerker vertelt dat iemand de bankrekening van het slachtoffer aan het plunderen is, is de val gezet. Dat de daders (hoog)bejaarde slachtoffers viseren is geen toeval. “Zij zijn een makkelijk doelwit. Soms hangen de slachtoffers een uur aan de telefoon met de beller. Ze vertellen letterlijk hun hele levensverhaal en voelen zich gehoord aan de andere kant van de lijn. De daders zijn eigenlijk halve psychologen.”

De kaartophaler

“We hebben een vis aan die lijn.” Die woorden vanuit het callcenter zijn het signaal voor de bende om de klus in het veld af te maken. Teams van twee personen rijden op elk moment van de dag rond in de regio waar het callcenter op dat moment slachtoffers zoekt. Ze staan live in contact met het callcenter.
Die nabijheid bij is zeer belangrijk, ‘de vis’ mag immers geen tijd krijgen om na te denken. Het callcenter staat ook nog altijd telefonisch in contact met het slachtoffer. “Als het goed is belt mijn collega nu aan”, weerklinkt aan de andere kant van de lijn. Om te bewijzen dat alles veilig verloopt, moet de ‘bankmedewerker’ die aanbelt een cijfercode zeggen. Zo is het vertrouwen meteen gewonnen.
Een andere strategie is dat het callcenter zegt dat de politie eraan komt. Dan transformeert de bankmedewerker in een politieagent in burger.
Vanaf dan gaat het bliksemsnel. Terwijl het slachtoffer instructies krijgt van de beller neemt de kaartophaler over. De lijn blijft wel open zodat de leidinggevenden horen wat er gebeurt. Het slachtoffer moet eerst een stappenplan volgen waarbij de pincode wordt ingetypt terwijl de kaartophaler meekijkt. Daarna wordt de bankkaart afgegeven met de belofte dat deze wordt vernietigd. Soms wordt de kaart zelfs doorgeknipt, maar dat gebeurt op zo’n manier dat deze daarna bruikbaar blijft.
Het slachtoffer wordt overstelpt met informatie en de dader zal ook proberen om kostbare items als juwelen vast te krijgen, met de belofte dat deze veilig in een bankkluisje worden ondergebracht. Tot slot krijgt het slachtoffer de vraag om het toestel waarmee hij of zij bankzaken verricht, af te staan. De daders sluiten af met de geruststellende mededeling dat de nieuwe bankkaarten een dag later met de post toekomen. “Als de slachtoffers toch argwaan krijgen, kunnen ze online voorlopig niets meer controleren”, verduidelijken politie en parket.
Alsmaar vaker wordt de job van kaartophaler door meisjes en jonge vrouwen uitgevoerd. Zij verdienen tot 300 euro per dag. Wie tien dagen in de maand op pad gaat heeft dus 3.000 euro, wat voor een minderjarige veel geld is.

Chauffeur

De kaartophalers hebben ook een chauffeur. Vaak stelt de organisatie een mooie wagen met tankkaart ter beschikking. Wat ze moeten doen, klinkt simpel. Terwijl ze live volgen wat het callcenter doet, moet de chauffeur er voor zorgen dat de kaartophalers op tijd ter plaatse zijn als een slachtoffer in de val is getrapt. Voor één dag gratis rondrijden met de kaartophaler verdienen ze minstens 100 euro.

De casher

De kaartophaler en casher zijn meestal dezelfde persoon. Nadat met succes de bankkaarten van het slachtoffer werden ontfutseld, volgt het leegroven van de rekening(en).
Via bankautomaten halen ze cash af. Deze som is begrensd vanwege het dagtarief. Daarnaast worden online zoveel mogelijk bestellingen geplaatst. Behalve luxemerken gaat het over spullen die jongeren aanspreken: geluidsboxen, iPhones, spelconsoles, VR-brillen, drones of

cadeaukaarten. Maar de speurders zien ook stofzuigers van Dyson op de lijst passeren. “Het zijn allemaal zaken die gemakkelijk en anoniem terug verkocht kunnen worden.”
De cashers rijden met de chauffeur mee naar Nederland. “Daar overhandigen ze alles aan een tussenpersoon van de leidinggevenden. We hebben op dit moment sterke vermoedens dat de organisatie via buitenlandse vennootschappen de goederen terug op de reguliere markt aan de man brengt”, besluiten politie en justitie.

Hoe Nicole (89) tienduizenden euro’s verloor

** Dit is een fictieve reconstructie*

De 89-jarige Nicole uit Hasselt krijgt op een vrijdagochtend telefoon van een medewerker van ING. De vriendelijke man, die zich voorstelt als Bert, vertelt dat hij een verdachte betaling van 1.000 euro naar een rekening in Rusland ziet en vraagt of Nicole iets besteld heeft. Zij schiet meteen in paniek, maar tijdens het gesprek stelt Bert de hoogbejaarde gerust: Hij kan de fraude voorkomen, maar dan moet er snel gehandeld worden. Bert vraagt of een medewerker mag langskomen om alles in orde te brengen en de fraudegevoelige kaarten op te pikken. Bert zegt dat Nicole de medewerker moet vragen achter de veiligheidscode van vier cijfers. De code is 4987.
Die medewerkster (16) is een kompaan van oplichter Bert die op dat moment al in de buurt is en in een mum van tijd bij het slachtoffer aanbelt. Dan gaat het snel. Het jonge meisje, met mantelpakje, toont vluchtig haar pasje dat bewijst dat ze voor ING werkt. Ze stelt zich voor als Sara en antwoordt Nicole dat de code 4987 is. Sara gaat met Nicole naar binnen. Nicole hangt nog steeds met Bert aan de lijn. Hij vertelt haar dat ze nog een aantal handelingen moet verrichten en Sara haar hiermee zal helpen. Met het toestelletje voor online bankieren moet Nicole het stappenplan volgen en onder meer de geheime code van de bankkaarten indrukken. Op dat moment kijkt kaartophaler Sara stiekem mee en onthoudt de pincodes. Daarna vraagt Sara met een geruststellende glimlach om alle bankkaarten mee te geven. Bert zegt intussen dat hij goed nieuws heeft: “Goed gedaan Nicole, het is gelukt. We hebben de betaling naar Rusland geblokkeerd. De nieuwe bankkaarten zullen morgen met de post worden opgestuurd.” Bert neemt afscheid van Nicole en haakt in terwijl Sara al afscheid heeft genomen.
Sara en haar chauffeur Ivan (19) rijden met de bankkaarten en codes naar geldterminals en halen daar 2.500 euro cash af. Dan is de daglimiet bereikt. Intussen worden de bankkaarten ook gebruikt voor online aankopen. Sara en Ivan bestellen twaalf spelconsoles, tien iPhones, vier VR-brillen, twee drones en een aanzienlijk aantal giftcards van 500 euro per stuk. Dat herhalen ze tot de rekening leeg is. Het gaat alles samen om bijna 37.000 euro. De aangekochte goederen worden opgehaald in de elektrowinkels en naar een onbekende tussenpersoon gebracht die de aankopen voor de organisatie in ontvangst neemt. Vervolgens verkopen zij alles weer in het buitenland.
Wanneer de twijfel bij Nicole toeslaat en ze haar rekeningen wil controleren, is het geld al verdwenen. Bert, Nicole en Ivan hebben vaak genoeg aan een halve dag om voor tienduizenden euro’s te stelen.

Winkeliers kunnen helpen: opgelet voor grote bestellingen

Politie en parket waarschuwen niet alleen de bevolking voor helpdeskfraude, ook de verkopers van elektronica en luxemerken worden opgeroepen om alert te zijn. “Als iemand vijf smartphones of tien Gopro’s bestelt en deze door een jongere worden uitgehaald, wees dan waakzaam en bel eerst de politie alvorens de goederen mee te geven. Hetzelfde met grote bedragen die op een prepaidkaart of cadeaubon worden gezet.”

HBVL 30/5/25
Phillip Pergens