DE CRIMINELE KOSTEN EN BATEN VAN ONLINE FRAUDE

Illustratie: Hans Sprangers

PRINT DIT ARTIKEL NAAR HOME

31 juli 2023

AUTEURS: SHANNA WEMMERS , JELMER BROUWER , BERT STULP

Online oplichting heeft een enorme impact op de slachtoffers en hun naasten. Interventies zijn veelal gericht op het weerbaar maken van potentiële slachtoffers of het bieden van ondersteuning na een fraudeactie. Bij dadergerichte interventies kunnen de door deze groep gepercipieerde baten juist lager en de verwachte kosten hoger worden voorgespiegeld.

Op sociale media worden continu foto's en video's gedeeld van internetoplichters. Een voorbeeld is een TikTok-filmpje van 2 tieners die bankhelpdeskfraude plegen. De ene telefoneert met een slachtoffer, de andere filmt het misdrijf. De beller vertelt het slachtoffer dat zijn bankgegevens opnieuw ingesteld moeten worden, tegen fraude. Hij heeft daar de persoonsgegevens voor nodig.

Hij weet niet dat hij op een gelekte gegevenslijst staat

Het slachtoffer, 92, vertrouwt het: tegenwoordig weet je het immers maar nooit met alle cybercrime. Hij deelt zijn gegevens met de overtuiging zijn bankgegevens goed te regelen. Hij weet niet dat hij op een gelekte gegevenslijst staat. Twintig minuten later wil hij naar de supermarkt, maar kan de boodschappen niet afrekenen. Zijn rekening is door de daders leeggetrokken.

"Gewoon € 30.000 verdiend in 3 minuten." – een tiener op TikTok over oplichting van een 92-jarige.

MODUS OPERANDI

De daders lichten een slachtoffer op met digitale middelen, vaak in samenwerkingsverband. Bij bankhelpdeskfraude doen de daders alsof zij een bankmedewerker zijn en het slachtoffer willen helpen met gegevensbeveiliging. Zij verzamelen de betalingsgegevens en laten, meestal via een omweg, geld overboeken naar zichzelf.

"Mijn pensioen is weg. Ik heb nog wat appels kunnen kopen." – 92-jarig slachtoffer van een TikTok-tiener.

Slachtoffers worden vaak in gelekte en gestolen data gevonden die worden verhandeld. In deze data hebben de daders inzichtelijk welke namen, telefoonnummers, adressen en geboortedata bij elkaar horen. De daders doorlopen vervolgens een kort selectieproces om de juiste slachtoffers te benaderen. Het gaat hierbij vooral om de hoogste leeftijd. Deze mensen staan bekend als minder digitaal vaardig, goed van vertrouwen en daardoor kwetsbaarder. Het wordt daders ook wel 'erg makkelijk gemaakt' (NOS, 2022).

"Nu de volgende." – een dader wijzend op een doelwit uit 1938.

De meeste daders plegen meerdere van deze misdrijven. Wanneer de daders het geld hebben wordt dit besteed aan bijvoorbeeld nieuwe merkkleding en sieraden. De 'buit' wordt soms gedeeld via socialemediakanalen, zoals Snapchat en TikTok. Op internet pochen rappers over hun succes in wat zij de F-game (fraudegame) noemen: het oplichten van mensen wordt beschouwd als een soort 'spel', met winnaars (de oplichters) en verliezers (de slachtoffers). Iedereen kan hierin meedoen en een specifieke rol spelen, afhankelijk van de beschikbare tijd en moeilijkheid (NOS, 2022).

IMPACT

De gevolgen van online en fysieke criminaliteit komen veelal overeen: psychische gevolgen, zoals angst, schuldgevoel en schaamte (Leukfeld, Malsch en Notté, 2019). Een vorm van fraude zoals hierboven beschreven gebeurt op afstand en kent meestal geen fysiek geweld. In tegenstelling tot bankpasfraude komt bij volledig op afstand gepleegde criminaliteit een dader niet binnen de fysieke persoonlijke leefomgeving van het slachtoffer.

rmijnt het ven van de ers in de appij

Toch zijn de impact op het slachtoffer en de maatschappij enorm. Naast de financiële schade (die overigens niet altijd vergoed wordt) schamen slachtoffers zich en durven soms niet meer naar buiten. Hun (zelf)vertrouwen krijgt een flinke kras en de pakkans van deze daders is relatief laag. Dit ondermijnt het vertrouwen van de slachtoffers (en hun naasten) in de maatschappij.

"Vroeger heb ik mijn land verdedigd, nu ben ik zelfs bang om de deur open te doen." – 92-jarig slachtoffer.

CRIMINOLOGISCH KADER

Voorwaarden om bankfraude (zoals spoofing) goed te kunnen toepassen zijn het hebben van een geschikt doelwit (slachtoffer), de afwezigheid van effectief toezicht en een gemotiveerde dader (hier de uitbuiter) (Cohen en Felson, 1979). Criminelen wegen hierbij kosten en baten tegenover elkaar af. Dit is een economische overweging waarbij niet alleen kwantitatieve factoren een rol spelen, zoals tijd en geld, maar ook 'immateriële' overwegingen, zoals emotionele en sociale factoren (Van Velthoven, 2012): De baten zijn bijvoorbeeld geld, hiermee te kopen goederen en status. De kosten zijn bijvoorbeeld investering in tijd en geld, maar ook pakkans, risico op economische schade (zoals een strafblad), sociale schade (zoals uitsluiting) en wroeging. Hoe de crimineel de kosten en baten afweegt ligt aan de mogelijkheden die de situatie biedt, maar ook in hoeverre zij hun capaciteiten inschatten om die te benutten.

Om online fraude goed te kunnen bestrijden is het dus van belang om holistisch naar gepercipieerde criminele kosten en baten te kijken in relatie tot doelwit, toezicht en motivatie. De hoeveelheid

online fraude en schade groeit (NOS, 2022). Dit betekent dat de kosten-batenafweging nog als positief wordt ervaren door de criminelen. Dit leidt tot de volgende overwegingen:

- Het *doelwit* is nog steeds aantrekkelijk voor de dader. Hoewel verschillende bewustzijnsinterventies bestaan voor dergelijke fraudevormen bij potentiële slachtoffers kan niet verwacht worden dat deze 100 procent effectief zijn en dat frauduleuze situaties altijd herkend worden. Daarbij verandert de modus operandi van oplichters continu.
- Het *toezicht* blijkt onvoldoende opgewassen tegen de hoeveelheid oplichting. De pakkans is laag, waardoor ruimte wordt ervaren door (potentiële) criminelen om te frauderen.
- De *motivatie* om bankfraude en spoofing te plegen blijft hoog. Wat betreft de baten kan voldoende verdiend worden ten opzichte van de kosten: Het gaat hierbij om (tien)duizenden euro's per slachtoffer, die worden uitgegeven aan statusverhogende spullen (NOS, 2022). De kosten worden onder andere bepaald door de vereiste voorbereiding, benodigde vaardigheden, pakkans en afstand tot het slachtoffer. Deze kosten dalen als de criminele daad in georganiseerd verband wordt uitgevoerd, waarbij individuele leden een specifieke functie vervullen. De 'mentale kosten', zoals wroeging, worden opgevangen door schade te ontkennen met neutralisatietechnieken (Sykes en Matza, 1958). Een voorbeeld is het excuus dat de financiële schade gecompenseerd wordt (meestal niet). Ook zou plegen 'op afstand' de drempel verlagen (NOS, 2022).

AANBEVELINGEN

Om de criminele kosten-batenafweging duurzaam te verlagen en deze vorm van criminaliteit effectief te beperken worden de volgende (bij voorkeur in samenhang uit te voeren) aanbevelingen voorgesteld.

en vinden
nieuwe
heden om
te omzeilen

Wat betreft het *doelwit*, (potentiële) slachtoffers, blijft actueel bewustzijn van belang, onderzoek naar mogelijkheden om hun weerbaarheid te vergroten en 'aantrekkingskracht' als doelwit continu te verminderen. Criminelen vinden continu nieuwe mogelijkheden om toezicht te omzeilen. Hiervoor dient voorlichting te blijven bestaan. Trainingen kunnen daarnaast gericht worden op het bespreekbaar maken van het onderwerp, het bewustmaken van digitale financiële mogelijkheden voor criminelen en het bieden van handvatten voor herkenning van en handelen bij oplichting. Een training kan dus betrekking hebben op (1) preventie, zoals vermogen veiligstellen, (2) het moment tijdens een fraudeactie, zoals herkenning, sturen van een alarmsignaal of een directe hulpvraag en (3) de periode na afloop, zoals het veiligstellen van sporen en doen van aangifte (zie bijvoorbeeld ook De Vries en Wemmers, 2022: p. 26-27).

Het is niet realistisch te verwachten dat de politie voldoende capaciteit kan inzetten voor voldoende toezicht op dit soort bankfraude (Boekhoorn, 2020). Ook banken hebben maatregelen ontwikkeld tegen fraude en voeren continu onderzoek voor het voorkomen en opsporen van bankfraudes, maar criminelen blijven deze maatregelen omzeilen. Er is meer heil te verwachten van het weerbaarder maken van slachtoffers (zoals hierboven beschreven) en de inzet van technologie daarbij. (Potentiële) slachtoffers kunnen ondersteund worden met technologische hulpmiddelen voor verhoogd toezicht en een toegenomen pakkans, zoals (deur)belcameratoezicht en audio-opnamemiddelen (bijvoorbeeld De Vries en Wemmers, 2022). Daarnaast kunnen laagdrempelige alarmopties worden ontwikkeld voor verdachte situaties. Dit kan bijvoorbeeld via een

knop in de bank-app, maar ook een alarm: zoals het huidige senioren- of 'valalarm' kan een dergelijke melding ook eerst richting familie of buren, zodat deze direct hulp kunnen bieden (bijvoorbeeld door deel te kunnen nemen aan het telefoongesprek). Bij dergelijke toezichtversterking is het van belang dat deze opties niet omzeild kunnen worden door oplichters.

Ten opzichte van de *daders* is het van belang de baten te verlagen in verhouding tot de kosten. Hiervoor dienen interventies gericht te worden op het verlagen van de (gepercipieerde) opbrengst, zoals geld, spullen en status. Bewustzijnscampagnes voor (potentiële) daders waarin de sociale winsten lager en de sociale risico's hoger worden voorgesteld, kunnen de motivatie verlagen. Het gaat hierbij om een soort paradigmashift van materiële naar meer duurzame maatschappelijke normen en waarden, waarin het geen respect verdient om kwetsbaarheden uit te buiten. De monetaire waarde is vrij objectief te bepalen, maar om de criminele motivatie te verlagen dient ook op beleving gefocust te worden.

schap moet
iet geen
erdient om
arheden uit te

Tegelijkertijd dienen de kosten voor de dader verhoogd te worden. Nu ligt de focus vooral op het financieel gewin, de materiële spullen die je hiermee kunt kopen en die leiden tot een idee van 'succesvol zijn', terwijl de slachtoffers en economische risico's voor de dader worden weggecijferd. Zolang bankhelpdeskfraude en andere vormen van cybercrime nog als een spel ('F-game') worden beschouwd dat status oplevert, kunnen daders dit gebruiken om verantwoordelijkheid af te schuiven. De boodschap moet echter zijn dat het geen respect verdient om kwetsbaarheden uit te buiten. Sterker nog, het gedrag moet gezien worden zoals het is: een oneerlijke wedstrijd. Ofwel: valsspelen in de F-game.

Een dergelijke gedragsbeïnvloeding is complex en het verdient daarom aanbeveling gedegen onderzoek uit te voeren naar de relevante factoren die ten grondslag liggen aan de fraude, zowel op het gebied van slachtoffer, dader als toezicht. Op basis van een systemisch inzicht in de samenhang en dynamiek van dergelijke factoren kunnen interventies worden ontwikkeld voor dergelijke jongeren. Die zouden een niet-criminele invulling van behoeften gericht op onder andere geld, status en tijdsbesteding tot doel moeten hebben. <<

Shanna Wemmers is werkzaam bij TNO, Jelmer Brouwer en Bert Stulp zijn werkzaam bij de Politie Fryslân.
Dit artikel is geschreven in samenwerking met Digitaal platform Fryslân van de politie. De fenomeen- en (fictieve) casusinformatie is gebaseerd op hun kennis en expertise, op basis van echte casuïstiek.
Shanna Wemmers is bereikbaar voor vragen en discussies via e-mail: shanna.wemmers(at)tno.nl.