Europees Netwerk inzake Criminaliteitspreventie

EUCPN Toolbox Series

Nr. 13

Preventie van individuele oplichting

Samenvatting

De 13e Toolbox van het EUCPN-secretariaat gaat over de preventie van *individuele oplichting.* Het Bulgaarse voorzitterschap (eerste helft van 2018) besliste om de focus te leggen op:

"[...] *fraudegerelateerde zaken, met name oplichting via de telefoon. Deze vorm van criminaliteit is de laatste jaren een winstgevende activiteit geworden, die zich zowel nationaal als over de grenzen heen ontwikkelt. Criminele groepen die zich op deze activiteit toeleggen, ontwikkelen zich op een dynamische manier en nemen steeds meer verschillende soorten slachtoffers in het vizier. Door de actieve deelname van slachtoffers, hun betrokkenheid bij criminele scenario's en het traumatiserende psychologische effect bij slachtoffers, moeten er grote preventieve inspanningen worden geleverd, rekening houdend met de specifieke kenmerken op lokaal, nationaal en grensoverschrijdend niveau"*

Individuele oplichting is een vorm van oplichting waarbij individuele burgers het doelwit zijn van criminelen. Slachtoffers worden overtuigd om mee te werken en worden vervolgens opgelicht. Ons huidige beeld van dit soort oplichting wordt vooral gevormd door de hedendaagse vormen ervan, met phishing als bekendste voorbeeld. We mogen echter niet vergeten dat individuele oplichting al eeuwenlang meegaat. Door de technologische ontwikkelingen van de laatste decennia hebben deze vormen van oplichting zich op veel grotere schaal kunnen ontwikkelen dan ooit voor mogelijk werd gehouden. Wie heeft er immers nog nooit een phishingmail ontvangen?

Zoals de *motivering* van het Bulgaarse voorzitterschap duidelijk maakt, nemen slachtoffers actief deel aan hun victimisatie. De dader wil het geld van het slachtoffer, maar kan er enkel met de hulp van het slachtoffer aan geraken. Die essentiële tactiek om het slachtoffer zover te krijgen, wordt **social engineering** genoemd. De dader wint zo het vertrouwen van het slachtoffer dat nodig is om de oplichting te laten lukken. De sociale psychologie biedt ons een beter begrip van dit fenomeen. Door te appelleren aan alledaagse sociale principes en deze 'menselijke zwakte' uit te buiten, slagen daders erin om de zogenaamde tweede route tot overreding te activeren. Voor de eerste route is veel denkwerk en cognitieve inspanning nodig. Maar de tweede route vereist minder inspanning en reageert haast onbewust. Door zich bijvoorbeeld voor te doen als een gezaghebbend figuur, zoals een politieagent, kunnen daders hun slachtoffers makkelijk tot een bepaalde mate van gehoorzaamheid dwingen. Deze sociale en cognitieve vuistregels hebben hun dagelijks nut, maar daders misbruiken ze in hun eigen voordeel.

Deze bedrieglijke tactieken worden voor een groot aantal **vormen van oplichting** toegepast. *Nigeriaanse oplichting, oma-oplichting, romantische oplichting, CEO-oplichting, ...* de mogelijkheden zijn even oneindig als de creativiteit van de oplichters. Doordat er zoveel verschillende vormen zijn, kunnen daders ervoor kiezen om in één keer op een zeer groot doelpubliek te mikken of om gerichter te werk te gaan. De laatste lijkt steeds meer voor te komen. Oplichters zijn zich gaan realiseren dat hun 'rendement' groter wordt als ze zich op een slimme manier tot hun slachtoffers richten. Phishingmails worden steeds geavanceerder en worden naar een specifiek gekozen doelwit of doelgroep verzonden. De verrassende laatste stap in deze evolutie is een combinatie van nieuwe en oudere technologie: de telefoon. Vishing, of 'voice phishing', combineert de voordelen van het internet en de telefoon. Online bellen kost haast niks, is moeilijker te traceren en kan geautomatiseerd worden. Het gebruik van de telefoon biedt extra voordelen: mensen hebben er meer vertrouwen in, en door de intiemere setting worden slachtoffers sneller overhaald. Tekenend voor het feit dat alles gesofisticeerder wordt: daders huren zelfs mensen in die de moedertaal spreken om de telefoongesprekken zo realistisch mogelijk te maken.

Momenteel weten we echter nog niet zoveel over individuele oplichting. Deze vorm van criminaliteit heeft een heel groot **dark number**, omdat van veel zaken geen aangifte wordt gedaan. Slachtoffers weten niet dat ze slachtoffer zijn geworden, vinden het niet ernstig genoeg, denken niet dat aangifte doen zal helpen of weten gewoon niet eens waar ze moeten zijn voor een aangifte. Bovendien zorgt de actieve rol die slachtoffers spelen ervoor dat ze

zichzelf de schuld geven en zich schamen, waardoor ze met hun verhaal niet naar buiten durven te treden. Er zijn zelfs vormen van oplichting met een "ingebouwd" antimeldingsmechanisme, waarbij slachtoffers illegale handelingen verrichten, waardoor ze zichzelf in een lastig parket brengen. Als ze dan naar de politie stappen, geven ze zichzelf als het ware aan.

Door het dark number is ook de **mythe** ontstaan dat vooral ouderen het slachtoffer zijn van deze vorm van oplichting, aangezien zij een makkelijke prooi vormen. Enkele studies hebben die mythe ontkracht, maar door hun beperkte aantal moeten we een slag om de arm houden. Toch zouden jongeren en mensen van middelbare leeftijd vatbaarder zijn voor oplichting. Een andere mythe is dat slachtoffers meestal worden afgeschilderd als ongeschoold of financieel analfabeet, maar het tegendeel blijkt waar te zijn. Een mogelijke verklaring is de 'knowing-doing gap': men herkent de signalen van oplichting wel, maar slaagt er niet in om die kennis op de eigen situatie toe te passen.

Helaas is het bestaan van zogenoemde '**sucker lists**' geen mythe. Telefoonoplichters kunnen hun slachtoffers willekeurig kiezen of openbare registers raadplegen, maar ze wisselen onderling ook lijsten uit met doelwitten die al eerder zijn opgelicht. Het gebruik van dergelijke lijsten geeft aan dat er veel gevallen zijn van herhaalde victimisatie. Sommige oplichters zullen bijvoorbeeld aanbieden om je te 'helpen' verloren bezittingen terug te krijgen...

Aangezien het bijzonder moeilijk is om deze vorm van criminaliteit te bestrijden, is preventie hoognodig. Er is echter weinig academisch en evaluatief onderzoek verricht naar individuele oplichting. Toch kunnen we enkele algemene bevindingen formuleren. De meest voorkomende vorm van preventie is het sensibiliseren van de bevolking. Dat kan gebeuren met een algemene sensibiliseringscampagne. Maar het is vooral in de vorm van een opleiding dat we een aantal positieve effecten zien. In feite proberen dergelijke opleidingen de eerder genoemde 'knowing-doing gap' te dichten. Een andere belangrijke methode is om met slachtoffers te werken. Wegens hun actieve rol en het risico op herhaalde victimisatie moeten slachtoffers ondersteund worden en op hun specifieke positie gewezen worden.

Tijdens het Bulgaarse voorzitterschap heeft het secretariaat een aantal **goede praktijken** rond dit onderwerp verzameld. Die kunnen ingedeeld worden op basis van hun doelgroep. Een eerste categorie is gericht op de hele bevolking. Het zijn sensibiliseringscampagnes, zoals de

voorbeelden uit België, Bulgarije of Zweden, of van Europol. Het gaat om radiospots, posters, flyers, gadgets,... die de bevolking nuttige informatie geven en tonen hoe men zichzelf kan beschermen. Een tweede reeks focust op ouderen. Hier worden meer interactieve methoden toegepast, zoals in Tsjechië. Ouderen nemen deel aan een interactief pedagogisch toneelstuk, waarin ze leren wat de meest voorkomende vormen van oplichting zijn en hoe ze daarop kunnen reageren. Die ervaring moet hen helpen om gepast te reageren als het echt gebeurt. Uit de evaluatie van dit project is gebleken dat dit ook zo was, aangezien de groep 2,5 keer meer nepdeals weigerde dan een controlegroep die het toneelstuk niet had gezien. Bij een laatste soort preventie ligt de focus op slachtoffers. Voorbeelden uit Australië, Canada en het Verenigd Koninkrijk hebben aangetoond dat dit soort preventie nodig is. Er zijn - zelfs wereldwijd - echter weinig ondersteunende diensten voor slachtoffers van individuele oplichting.

Tot slot heeft het EUCPN-secretariaat een workshop georganiseerd met verschillende deskundigen om een aantal **aanbevelingen** te formuleren om oplichting via de telefoon te voorkomen. Die zijn gestructureerd volgens de vijf strategieën van situationele criminaliteitspreventie. De eerste strategie is het vergroten van de inspanning die een dader moet leveren om de oplichting te laten lukken. Dat kan al bereikt worden door de publicatie van en toegang tot telefoonnummers te beperken. Een andere techniek kan zijn om het aantal telefoonnummers dat iemand mag hebben te beperken of op zijn minst te koppelen aan een bankrekening of paspoortnummer.

Een tweede strategie is het vergroten van de risico's. Daarvoor is informatie-uitwisseling essentieel. Die uitwisseling mag niet stoppen aan de grenzen van de publieke of particuliere sector, of op nationaal niveau. Alle partners hebben een belangrijk stuk van de informatiepuzzel in te vullen. Als men weet waar men mee te maken heeft, is de kans groter dat men het ook kan voorkomen. Uiteraard moet het eenvoudiger worden om aangifte te doen. Informatie moet verzameld worden voor ze kan worden gedeeld. Er werden ook aanbevelingen geformuleerd om de anonimiteit van de beller te beperken, door het bijna onmogelijk te maken om je locatie te vervalsen. Software voor stemherkenning kan in dit opzicht ook interessant zijn.

Het verkleinen van de beloning die deze vorm van criminaliteit kan opleveren, is een derde strategie om oplichting via de telefoon te voorkomen. De belangrijkste aanbeveling hier is dat illegaal verworven goederen in beslag genomen moeten worden. Daarvoor is het essentieel

dat geldstromen worden gemonitord om verdachte transacties op te sporen. Onze deskundigen raadden een EU-breed initiatief met de banksector aan om dit mogelijk te maken.

Een andere strategie is het beperken van uitlokking. Het is belangrijk om niet te veel informatie te delen over de manier waarop een oplichting effectief werd uitgevoerd, om copycats te vermijden. Daarnaast zou het kunnen helpen om bepaalde vormen van herhaalde victimisatie te voorkomen. De laatste strategie was het wegnemen van de voorwendselen. De focus hier ligt vooral op sensibilisering rond oplichting via de telefoon en over hoe men zichzelf kan beschermen. De eerder aangehaalde goede praktijken worden hier als belangrijke voorbeelden gegeven. Sensibiliseringscampagnes zouden dezelfde boodschap moeten verspreiden. Daarom moeten publiek-private partnerschappen en internationale samenwerkingsverbanden opgezet worden om zo consistent mogelijk te zijn: *zeg gewoon nee*.