Geldezelproblematiek onder jongeren

Makkelijk snel geld verdienen

Hoe zorgen criminelen ervoor dat hun criminele geldspoor niet naar hen is toe te leiden? Door de inzet van geldezels. Geldezels, ook wel money mules of katvangers genoemd, vormen een cruciale schakel in criminele netwerken en zijn onlosmakelijk verbonden aan gedigitaliseerde criminaliteit.

Het zijn personen, vaak jongeren, die hun pinpas, crypto wallet (bij een crypto geldezel) of een ander betaalmiddel, al dan niet bewust, ter beschikking stellen voor het verplaatsen van crimineel vermogen. Criminelen gebruiken de bankrekening of crypto wallet van de geldezel om het geld van hun slachtoffers naar zichzelf door te sluizen. Met de inzet van geldezels wordt het spoor naar de crimineel onderbroken. Voor de geldezel betekent dit een pakkans van 100%.

Het onderzoek "***Recruiting co-offenders for financial cybercrime***" (Bekkers, Leukfeldt & Kleemans, 2024) analyseert hoe cybercriminelen medeplichtigen werven binnen financiële cybercriminele netwerken. Op basis van 15 politieonderzoeken in Nederland identificeert de studie drie typen medeplichtigen: professionele facilitators, gerekruteerde facilitators en geldezels.

Ernstige gevolgen

Bankrekeningen verstrekken die worden gebruikt bij de uitvoering van 'financieel gemotiveerde criminaliteit' beschouwt de wet als witwassen. Dit heeft ernstige gevolgen voor jongeren die zich hiervoor laten gebruiken. Denk hierbij aan: strafrechtelijke consequenties zoals een strafblad, gevangenis en hoge boetes. Maar ook banken nemen maatregelen door geen of minder hypotheek te verstrekken of een rekening te blokkeren.

Ook kan het gestolen geld via een deurwaarder op de geldezel worden verhaald. De geldezel is aansprakelijk. In het geval van minderjarige geldezels zijn de ouders aansprakelijk. Dit kan schrijnende gevolgen hebben voor het leven van een jongere en zijn naasten. Dienst doen als geldezel kan daarnaast een opstapje zijn naar een verdere criminele carrière waarbij een jongere betrokken raakt bij steeds zwaardere vormen van criminaliteit.

** Waar in de tekst 'hij/zijn' staat, wordt ook 'zij/haar' bedoeld.*

Om een beeld te krijgen van het "geldezelen" staan hieronder 3 voorbeelden.

Aan- en verkoopfraude: *een dader licht een slachtoffer op via een advertentiewebsite. Hij verkoopt iets zonder het product vervolgens op te sturen. Het crimineel verkregen geld wordt overgemaakt naar de bankrekening van de geldezel. Dit geld wordt contant opgenomen en de geldezel ontvangt zijn percentage van het gestolen geld. De geldezel is nu aansprakelijk.*

Afpersing via Snapchat: *via Snapchat ontvangen scholieren berichten dat ze een 'boete' moeten betalen, omdat ze iemand in de weg hebben gezeten. Deze boetes kunnen oplopen tot honderden euro's. Weigeren ze te betalen, dan worden zij en/of hun dierbaren bedreigd met de dood. Het blijkt dat jongeren ook vaak 'korting' op hun boete krijgen aangeboden. Daarvoor moeten ze namen doorgeven, zodat deze nieuwe slachtoffers weer kunnen worden afgeperst. Onder druk stelden geldezels hun bankrekening beschikbaar voor het overmaken van het gestolen geld.*

Phishing: *het slachtoffer ontvangt een phishing e-mail, die van een bank lijkt te komen. Er wordt gevraagd om een veiligheidsprobleem op te lossen en een onmiddellijke reactie is vereist. Het slachtoffer klikt door naar de neppagina van de bank en voert hier zijn inloggegevens in. Criminelen gebruiken de gegevens om vervolgens geld over te maken naar de geldezel. De geldezel neemt het geld zo snel mogelijk contant op.*

Het geldezelmechanisme uitgelegd

Ronselen

Het onderzoek van Bekkers et al. (2023) onder 3000 respondenten toont aan dat bijna 10% van de jongeren tussen 16 en 25 jaar benaderd werd door recruiters. Dit gebeurde voornamelijk via Snapchat en Instagram, maar ook via klasgenoten, vrienden of kennissen. Recruiters maken vaak misbruik van de kwetsbaarheid van een (aspirant) geldezel, waarbij sociale banden en de motivatie om snel geld te verdienen een belangrijke rol spelen. In veel gevallen worden jongeren meerdere keren per dag benaderd.

Bekkers et al. (2024) benadrukken dat wervingsstrategieën variëren van het aanbieden van makkelijke verdiensten, zoals 'verdien €500 in een dag', tot manipulatie en misleiding, waarbij geldezels wordt voorgesteld dat het om een legitieme financiële dienst gaat. In sommige gevallen worden jongeren onder druk gezet of zelfs bedreigd om hun bankrekening af te staan. Geldezels ontvangen meestal een percentage van het illegaal verkregen geld.

Functie van de geldezel

Geldezels spelen een belangrijke rol in criminele netwerken. Ze worden gebruikt om luxe aankopen te doen, geld te innen, te verplaatsen of wit te wassen.

Een verontrustende ontwikkeling is dat geldezels niet alleen hun bankrekening moeten afstaan, maar ook hun identiteitskaart of paspoort. Hiermee openen criminelen online bankrekeningen en crypto wallets op naam van de geldezel, zonder dat deze doorheeft hoeveel transacties er via zijn identiteit lopen. In sommige gevallen worden binnen criminele netwerken zelfs identiteitsbewijzen doorverkocht.

Criminele netwerken kennen ook andere rollen:

- Ronselaar: benadert aspirant-geldezels in de buurt of via sociale media (Snapchat, Instagram).
- Gooier: verplaatst buitgemaakt geld tussen geldezelrekeningen.
- Prepper: bereidt rekeningen voor om de beveiliging van banken en betaalplatformen te omzeilen.

Verklaringen deelname

Waarom laten geldezels hun bankgegevens eigenlijk misbruiken? Vanuit de literatuur zijn hier deze verklaringen voor gevonden: een luxe levensstijl, normaliseren van het gedrag, lage risicoperceptie, misleiding en dwang.

Een luxe levensstijl en normaliseren van het geldezelen

Bepaalde groepen jongeren houden er een luxe levensstijl op na (zoals designer kleding of dure auto's) en maken frauduleuze activiteiten normaal. Dit is een heersende subcultuur. Recruiters kiezen financieel kwetsbare jongeren uit. Gedrag van anderen binnen de subcultuur en het zien dat vrienden makkelijk snel geld verdienen door als geldezel op te treden, kan kwetsbare jongeren beïnvloeden dit ook te doen.

Het toepassen van neutralisatietechnieken

Een groep maakt excuses voor hun criminele gedrag door neutralisatietechnieken. Ze geven bijvoorbeeld aan niet door te hebben gehad dat het ging om frauduleuze activiteiten. Of ze zeggen dat het slachtoffer zelf schuldig is, omdat deze zich niet beter had beveiligd. Ook zijn er geldezels die beweren zelf slachtoffer te zijn. Dit kan natuurlijk als de geldezel werd gemanipuleerd en/of niet in staat was om een bewuste risicoafweging te maken.

Lage risicoperceptie

Aan de rol van geldezel hangt een pakkans van 100%. Dit staat dan ook niet in verhouding tot de kleine beloning die een geldezel voor zijn diensten ontvangt. Uit onderzoek blijkt dat geldezels zich vaak niet bewust zijn van de risico's die kleven aan het geldezelen. Ze onderschatten de risico's en consequenties of weten niet wat geldezelen eigenlijk inhoudt. Het aanbod om makkelijk snel geld te verdienen, lijkt dan aantrekkelijk.

Misleiding en dwang

De deelname gebeurt ook door misleiding en dwang. Wanneer een jongere instemt, wordt hij gevraagd de bankpas en pincode af te geven of zelf geld over te maken naar een derde partij. In eerste instantie krijgen ze soms een kleine vergoeding, wat hen het gevoel geeft dat er weinig risico aan is verbonden. Alleen worden ze al snel onder druk gezet om vaker hun rekening en identiteitsgegevens ter beschikking te stellen, vaak met dreigementen of valse beloftes van grotere bedragen.

Waarschuwingssignalen

- Anderen hebben de bankrekening van de jongere nodig om geld op te nemen.
- Een jongere heeft meerdere bank-passen, KVK inschrijvingen en/of rekeningen.
- Hij heeft dure kleding dat niet in verhouding staat tot zijn inkomsten.
- Er is geen legale economische verklaring voor zijn inkomsten.
- Hij heeft grote hoeveelheden contante bedragen op zak.
- De jongere heeft veel contact met personen met criminele antecedenten.
- Hij heeft veel online chatcontact en gebruikt versluierde taal.

Aanpak

Vanuit de City Deal 'Lokale Weerbaarheid Cyber crime' werkt het CCV voor vier Preventie met Gezag gemeenten een aanpak Geldezels uit. Binnen deze pilots wordt een uitwerking gemaakt op de volgende vier thema's:

- Planvorming en samenwerking met partners zoals politie, OM, schuldhulpverlening, onderwijs, jongerenwerk e.d.
- Algemene voorlichting om bewustzijn en risicoperceptie te vergroten en gedragsverandering te bereiken; offline (op scholen) en online (via campagnes) gericht op jongeren in de leeftijd van 12 tot 23 jaar.
- First offender aanpak: een geldezel zonder criminele antecedenten ervan doordringen dat zijn misstap niet moet leiden tot verder crimineel gedrag, nagaan wat ertoe leidde om als geldezel op te treden en die oorzaak proberen weg te nemen.
- Veelpleger aanpak: een geldezel met criminele antecedenten laten stoppen met zijn criminele gedrag en zorg aanbieden.

De resultaten van de vier geldezelpilots worden in 2025 verwacht. Het CCV begeleidt deze pilots in de opstart, uitvoering en evaluatie.

Meer informatie

Wil je meer weten over de aanpak van geldezels? Neem contact op met: CCV-adviseur Siènne Stoker.
Email: sienne.stoker@hetccv.nl
Telefoonnummer: (06) 11 921 363

Bronnen

Online fraude in beeld: Fenomeenbeeld Online fraude 2024. Politie, Eenheid Landelijke Opsporing en Interventies & Eenheid Landelijke Expertise en Operaties. https://hetccv.nl/app/uploads/2024/11/OnlineFraudeFenomeenbeeld2024.November2024.pdf

Bekkers, L., Leukfeldt, R., & Kleemans, E. (2024). *Recruiting co-offenders for financial cybercrime: An analysis of police investigations into cybercriminal networks.* Trends in Organized Crime. https://doi.org/10.1007/s12117-024-09556-y

Artikel Parool: *Tientallen scholieren van middelbare scholen in Amsterdam-Zuid afgeperst via Snapchat* https://www.parool.nl/nederland/tientallen-scholieren-van-middelbare-scholen-in-amsterdam-zuid-afgeperst-via-snapchat~b977b33a

Anti Money Laundring Centre. (2021). *Witwasindicatoren*. https://www.amlc.nl/wp-content/uploads/2020/04/witwasindicatoren-april-2020-1.pdf

Bekkers, L., Van Houten, Y., Spithoven, R., & Leukfeldt, E. R. (2023). Money Mules and Cybercrime Involvement Mechanisms: Exploring the Experiences and Perceptions of Young People in the Netherlands. *Deviant Behavior*, 1-18.

Bekkers, L. & Leukfeldt, E.R, (2022) Recruiting money mules on Instagram: A qualitative examination of online involvement mechanisms into cybercrime. *Deviant Behaviour.* DOI:10.1080/01639625.2022.2073298

Bekkers, L., Leukfeldt, E.R., Van 't Hoff- de Goede, S., Misana-ter Huurne, E., Van Houten, Y., Spithoven, R. (2022). *Cyberweerbaarheid: Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime. Een interventie tegen geldezels*.

Bekkers, L., Moneva, A., & Leukfeldt, E.R. (2022) *Understanding cybercrime involvement: a quasi experiment on engagement with money mule recruitment ads on Instagram. Journal of Experimental Criminology.* DOI:10.1007/s11292-022-09537-7

Europol. (2021). *Money Muling.* https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and- prevention-guides/money-muling.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, 42(5), 569-581.

Stichting het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) draagt bij aan de maatschappelijke veiligheid door het stimuleren van publiek-private samenwerking, actieve kennisdeling van de veiligheidspraktijk en kwaliteitsontwikkeling van instrumenten en regelingen.

Vormgeving: CO3, Woltera Niemeijer **Fotografie:** Shutterstock.