VOORWOORD

De laatste strohalm, dat ben je vaak als iemand de moeite neemt om een journalist een e-mail te sturen. Ze doen het zelden om hun verhaal gepubliceerd te krijgen, maar omdat ze in wanhoop hopen dat tenminste iemand wil helpen. Het zijn getuigenissen vol ongeloof en paniek, vaak van mensen die nergens anders met hun verhaal terechtkunnen en hopen dat je er nog 'iets aan kunt doen'. Want of het nu om enkele honderden euro's aan cryptomunten gaat of een volledige spaarrekening die werd leeggehaald, het laat diepe sporen na. Emotioneel en financieel.

Ik word geconfronteerd met verhalen over uitgekiende oplichtingspraktijken: de vrouw die in de waan verkeerde dat ze een duurzame relatie opbouwde en nu achterblijft in een emotionele ruïne, de gepensioneerde bankier die, na een overtuigend telefoongesprek, zijn vermogen zag verdampen nadat oplichters aan de deur zijn bankkaarten, smartphone en zelfs iPad kwamen ophalen. Mensen die maandenlang beleggen op een platform dat niet bestaat. Jongeren die hun identiteit gestolen zien.

Deze verhalen zijn geen uitzonderingen. Ze zijn integendeel representatief voor een verraderlijk virus waartegen niemand immuun is, en dat zich, in tegenstelling tot wat vaak wordt gedacht, absoluut niet tot ouderen beperkt.

Wat veel slachtoffers wél gemeen hebben, is een blinde vlek in de perceptie van risico's. We beveiligen onze fysieke leefwereld met hekken, sloten en alarminstallaties. We zijn argwanend als een verkoper in een winkel ons iets probeert aan te smeren. We realiseren ons echter onvoldoende dat de meest reële dreiging vandaag niet via de oprit nadert of fysiek voor ons staat, maar via één enkele kabel onze woning binnenkomt.

De vraag die in nagenoeg elke getuigenis terugkeert, is dan ook: 'Hoe kon ik zo naïef zijn?' Het antwoord is even eenvoudig als complex: het is geen kwestie van intelligentie, maar van menselijkheid. De modus operandi van de hedendaagse crimineel is fundamenteel anders dan die van zijn analoge voorganger. De digitale zakkenroller 2.0 richt zijn pijlen niet enkel op technologische lekken in een systeem, maar op de psychologische kwetsbaarheden van de mens.

Zijn voornaamste instrumenten zijn onze eigen emoties: angst, hebzucht, vertrouwen of het verlangen naar sociaal contact. Door manipulatie wordt ons kritische beoordelingsvermogen ondermijnd of zelfs volledig uitgeschakeld. De technologie is een hefboom, onze psyche is de motor.

Het is precies deze kwetsbaarheid die de noodzaak van dit boek onderstreept. De meest efficiënte beveiliging tegen dit soort criminaliteit is niet technologisch, maar menselijk van aard. De oplichter faalt op het moment dat de eerste, cruciale schakel in de keten, u en ik, de strategie doorprikt en juist reageert.

Dit boek helpt om die eerste verdedigingslinie te versterken. Het biedt een heldere analyse van de mechanismen die oplichters misbruiken, brengt de technieken in kaart en reikt tips aan om jezelf en je omgeving te beschermen. Niet om angst te cultiveren, maar om je waakzaamheid en weerbaarheid te bevorderen.

In de strijd tegen de cybercrimineel, of die nu op een zolderkamer in je stad opereert of vanuit een ver land waar onze politie machteloos staat, is kennis ontegensprekelijk het krachtigste schild. Dit boek reikt die kennis aan, met de ambitie om van elke lezer een alerte en geïnformeerde burger te maken in een steeds complexere digitale wereld.

Kenneth Dée

Inleiding

Met een vleugje nostalgie denken we soms terug aan een eenvoudigere tijd. Een tijd waarin een deur simpelweg een voordeur was, je identiteit bestond uit niet meer dan een voor- en een achternaam, en je adres slechts een straatnaam, huisnummer en gemeente omvatte. Maar de wereld om ons heen is ingrijpend veranderd.

Alles werd digitaal en online: betalingen, verzekeringen, shoppen en zelfs je dagboek, maar lang niet iedereen is mee. Van kinderen over (jong)volwassenen tot senioren; iedereen heeft moeite om het tempo bij te houden. In jouw poging om up-to-date te blijven, heb je waarschijnlijk intussen ook al behoorlijk wat accounts. De verzameling van al je persoonlijke profielen op apps of websites bevat een schat aan gegevens: toegangscodes, logingegevens (gebruikersnaam/e-mailadres en wachtwoord), adres, wachtwoorden, rekeningnummers, digitale sleutels …

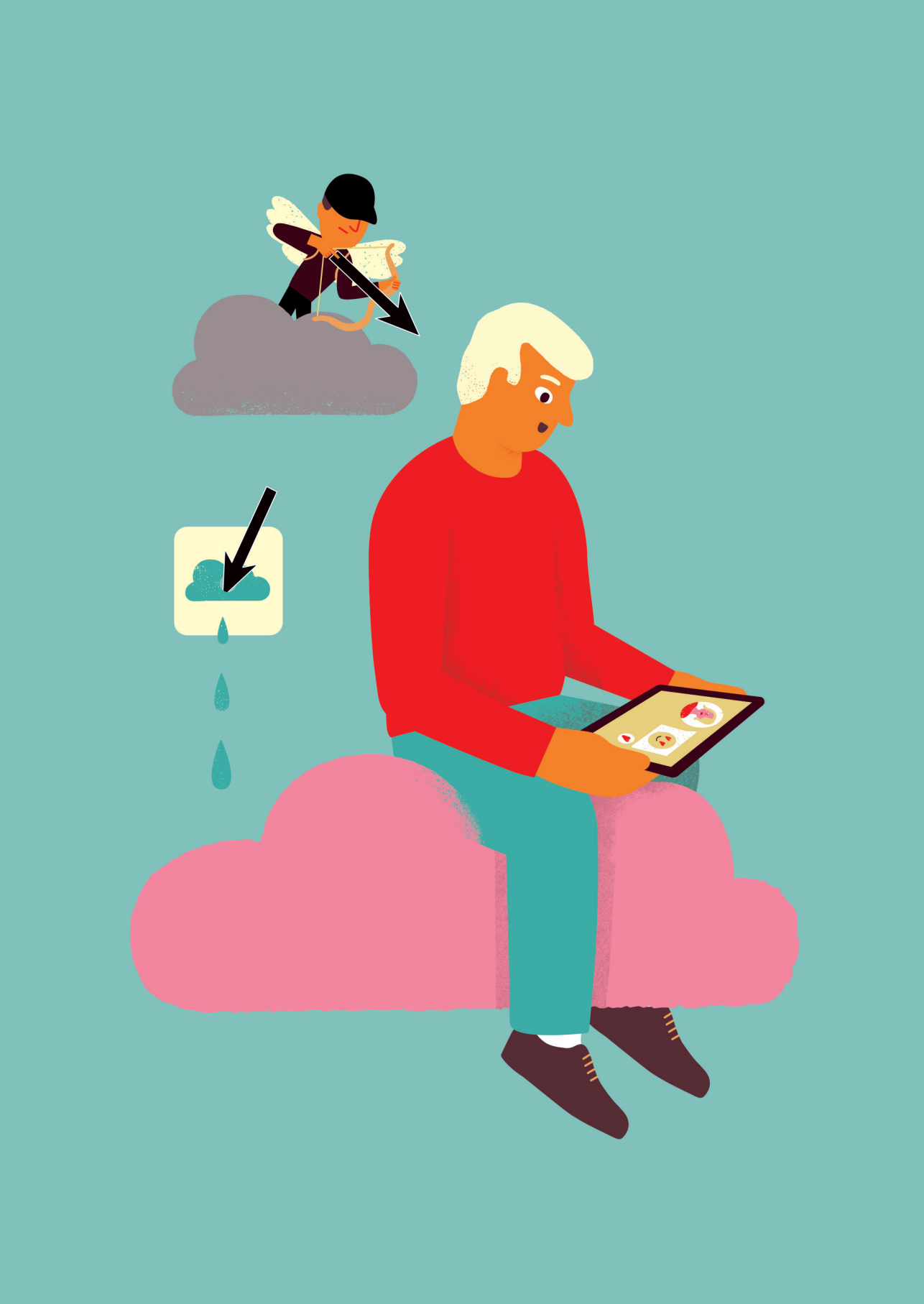
Helaas wijzen de cijfers over online oplichting uit dat we nog te weinig aandacht besteden aan deze nieuwe vorm van beveiliging. In ons streven naar innovatie en gemak hebben we wellicht de risico's onderschat die gepaard gaan met onze steeds verder gedigitaliseerde levens.

De gevaren kennen en actief stappen ondernemen is de eerstelijnsbescherming voor onszelf en de mensen rondom ons. Alleen zo kunnen we de vruchten plukken van technologische vooruitgang, zonder onnodig kwetsbaar te worden voor de risico's die ermee gepaard gaan.

In een wereld die steeds meer verweven raakt met technologie, is het belangrijk om onze digitale veiligheid met dezelfde zorg te behandelen als onze fysieke beveiliging. Deuren afsluiten wordt uitloggen, je sleutel veilig bewaren of niet delen geldt ook voor logingegevens en paswoorden.

De les die we als kind leerden dat we de deur niet mochten openen voor vreemden, vertaalt zich naadloos naar de digitale wereld: check eerst wie je een bericht stuurt voor je antwoordt! We moeten uiterst terughoudend zijn met het delen van onze persoonlijke gegevens. Het vrijgeven van deze informatie kan net zo desastreus zijn als je huissleutels aan een willekeurige voorbijganger geven.

In deze nieuwe digitale realiteit ligt de verantwoordelijkheid voor het vertrouwen van een persoon of dienst volledig bij onszelf. Je moet altijd kritisch en waakzaam blijven, ongeacht hoe overtuigend of ogenschijnlijk betrouwbaar een verzoek om informatie mag lijken.



1

FRAUDE EN OPLICHTERIJ

Het woord 'fraude' wordt gebruikt voor uiteenlopende misdrijven, waaronder oplichting, valsheid in geschrifte en bedrog. Het behoort tot de vermogensdelicten, waarvan ook diefstal deel uitmaakt. Bij fraude is altijd opzet in het spel en het gaat dus meestal om bedrog: het opzettelijk misleiden van een ander om onrechtmatig voordeel te verkrijgen. Bij fraude worden gegevens en informatie vervalst of aangepast om een illegaal voordeel te behalen.

Oplichting betekent meestal hetzelfde, alleen speelt dat zich vaker af in de persoonlijke sfeer. Hoewel het volgens de Belgische en Nederlandse wetgeving een misdrijf is, is het lastiger te vervolgen en te bewijzen door justitie.

Oplichting en fraude zijn vormen van misbruik van vertrouwen waarbij iemand je misleidt om er zelf financieel beter van te worden. Dit kan je boos of verdrietig maken. Misschien vertrouw je anderen minder snel? Als slachtoffer kan je je ook schamen en schuldig voelen. Je vraagt je misschien af waarom je het niet had zien aankomen en hoe je zo dom kon zijn. Dat is een volkomen normale reactie.

Helaas trekken fraude en oplichting een donkere draad door onze geschiedenis. De motieven – geld, wraak, informatie – blijven ook vandaag gelden, maar de spelregels zijn veranderd met de digitale opkomst vanaf de 20e eeuw. Oplichterij onderging een wereldwijde schaalvergroting en zo ook hadden de gevolgen en gevaren een veel grotere impact.

DE 'KUNST' VAN HET OPLICHTEN IS ZO OUD ALS DE MENSHEID

OPLICHTING 1.0

'Oplichter' is eigenlijk een modern woord voor 'charlatan'. De kwakzalvers uit de middeleeuwen werden bijvoorbeeld geclassificeerd als charlatans, maar ook zakkenrollers, beurzensnijders en kettingrukkers.

- Nemen we even een duik in het verleden, met een paar voorbeelden. Al in 300 v.Chr. probeerden de Griekse kooplieden Hegestratos en Zenosthemis hun verzekering te bedotten door hun schip opzettelijk tot zinken te brengen. Maritieme fraude avant la lettre dus.
- In de 16e eeuw betaalden Europese vorsten vorstelijke bedragen voor hoorns van eenhoorns. De Deense koning Frederik III liet er zelfs een troon van maken, aangezien hij via Groenland onbeperkt aan 'eenhoornhoorns' kon komen. In werkelijkheid waren de hoorns afkomstig van de narwal en maakten ze handige Vikingen en Scandinavische handelaren schatrijk.

- Bedrog en voeding gaan ook vaak hand in hand. In de 19e eeuw kleurden oplichters groenten met koper om ze aantrekkelijker te maken en vermengden ze melk met smerig water en bloem om de hoeveelheid te vergroten.
- Sommige oplichters werden befaamd door hun bedrog. Denk aan Charles Ponzi, Bernard Madoff en Frank Abagnale (wiens leven werd verfilmd in *Catch Me If You Can*). Of neem Victor Lustig, de Tsjechische immigrant die de Eiffeltoren 'verkocht' aan nietsvermoedende schroothandelaren.
- Wist je trouwens dat de Ponzi-fraude al bestond voordat Charles Ponzi (1882-1949) er zijn naam aan verbond? De eer komt toe aan mevrouw Adelheid 'Adele' Spitzeder. Zij wist in 1869 wat armoede was en besloot dat haar dat nooit meer zou overkomen. Ze lokte slachtoffers met de belofte om hun geld met hoge rentes te beheren, betaalde oude slachtoffers met het geld van nieuwe en verrijkte zichzelf. Toen ze op 12 november 1872 werd gearresteerd, bleek er zo'n 38 miljoen gulden te ontbreken – nu ruim 400 miljoen euro. Het bankwezen was nog zo jong dat toezicht en wetten ontbraken, waardoor ze slechts vier jaar cel kreeg voor verduistering en gebrekkige boekhouding. Maar liefst 31.000 klanten waren geruïneerd; een tragische illustratie van de verwoestende gevolgen van ongebreidelde hebzucht.
- In 1911 betaalde de Argentijn Eduardo de Valfierno een medewerker van het Louvre om de Mona Lisa te stelen. Hij had het echte schilderij niet nodig; hij wilde alleen dat het verdween, zodat hij zijn vervalsingen aan illegale verzamelaars kon slijten. Of hoe fraudeurs profiteren van de menselijke ijdelheid en wens om iets exclusiefs te bezitten.

OPLICHTING 2.0

Al van bij in het begin van het digitale tijdperk waren de oplichters present. In de beginjaren van het internet – toen velen nog geen persoonlijk e-mailadres hadden – waren er slimme ondernemers die e-maildatabases samenstelden en verkochten aan marketeers, die er handig gebruik van maakten om hun reclame rond te sturen. Vandaag noemen we dat spam (ongewenste e-mails), maar toen was het een relatief nieuwe manier om reclame te maken. Phishing, of oplichterij via e-mail, zou voor het eerst hebben plaatsgevonden in het begin van de jaren zeventig, hoewel de term pas halverwege de jaren negentig bekend werd.

Sindsdien is online oplichterij enkel toegenomen, van valse e-mailadressen tot informatie afkomstig van enorme datalekken. Oude trucs – zoals Nigeriaanse Prins-fraude, waarbij grote geldbedragen beloofd worden in ruil voor kleine voorschotten – verschenen in e-mails in plaats van een envelop. Onze digitale wereld heeft simpelweg een nieuw speelveld gecreëerd voor oude en nieuwe oplichterspraktijken.

De opkomst van e-commerce, online bankieren en sociale media creëerde schatkamers vol geld en informatie met zwakke plekken waar cybercriminelen (de georganiseerde online misdaad) gretig op azen. Dankzij het web is het voor oplichters kinderspel geworden om zich voor te doen als een betrouwbare instantie of persoon. Met een paar muisklikken bereiken ze via nepmails, valse websites of fictieve social media-profielen talloze slachtoffers tegelijk. Deze digitale berichten waren en zijn vaak zo overtuigend dat het bijna onmogelijk is om de imitatie te doorzien, zeker nu de fraudeur onzichtbaar blijft. Met behulp van tekstverwerkers, grafische software en een schat aan online sjablonen maken ze in een handomdraai geloofwaardige nepdocumenten, die vervolgens razendsnel digitaal verspreid worden. Zo ontstaat een web van misleiding dat zich moeiteloos uitstrekt over landsgrenzen en tijdzones.

Het internet heeft het verzamelen van informatie over slachtoffers helemaal veranderd. Waar fraudeurs vroeger nog in vuilnisbakken moesten graven, moeten ze nu alleen maar je social media-profiel bekijken. Mensen delen immers vaak onbewust veel te veel over zichzelf. Door je gegevens te combineren met valse invulformulieren of misleidende enquêtes komen oplichters in korte tijd alles te weten wat ze nodig hebben. Jouw persoonlijke informatie wordt vervolgens ingezet voor nieuwe oplichtingspraktijken of simpelweg verkocht op digitale zwarte markten.

Onze technologische vooruitgang heeft social engineering (digitale emotionele manipulatie) naar een nieuw niveau getild. Een valse betalingsherinnering in je mailbox, een nepbericht van een zogenaamd familielid in nood of een anonieme reactie op sociale media: het zijn stuk voor stuk beproefde tactieken waarmee internetoplichters inspelen op je menselijke emoties. De menselijke psychologie blijft het zwakke punt bij uitstek in de digitale verdediging. Juist daarop weten fraudeurs feilloos in te spelen met geraffineerde manipulatietechnieken.

Daarnaast zijn er fraudetechnieken ontstaan die vóór het internettijdperk ondenkbaar waren. Malware, ransomware en hacking zijn allemaal vormen van digitale criminaliteit die je computer of data in gevaar brengen. Ze vormen de vaste onderdelen van grootschalige oplichtingspraktijken, mogelijk gemaakt door kwetsbaarheden in de software en apparaten die we dagelijks gebruiken.

De digitale oplichters vormen het hele jaar door een bedreiging, maar ze zijn extra actief rond grote evenementen en feestdagen, zoals populaire concerten, festivals, Black Friday, Kerstmis of de koopjesperiode.

Waargebeurd

2020 leek een topjaar te worden voor fraudeurs, met grote sport- en cultuurevenementen, zoals het EK, de Copa Ameréca en de Olympische Spelen op de agenda. Maar het lot besliste anders: de COVID-19-pandemie gooide roet in het eten. Tegelijk bood dit nieuwe kansen voor oplichters. Want ze deinzen er niet voor terug om een internationale crisis uit te buiten. De pandemie bracht uitdagingen én kansen voor online bedrijven. Streamingdiensten, bezorgapps, datingplatforms en marktplaatsen floreerden, maar hun groeipijnen maakten hen ook het doelwit van fraude. De online bedrijven waren niet voorbereid op het groeiende aantal gebruikers en waren niet klaar om daarvoor de nodige bijkomende veiligheidsmaatregelen in te bouwen. Velen wisten dat het gebruik van het populaire vergaderplatform Zoom[1] niet zonder risico's was. Stel je voor: je logt in voor een zakelijke meeting, iedereen stelt zich netjes voor, tot plots een onbekende, schreeuwende vrouw het scherm overneemt. Toch bleef iedereen, uit noodzaak, deze diensten gebruiken.

Het gebruik van digitale diensten bleek financieel aantrekkelijk, maar de pandemie bracht ook ingrijpende gedragsveranderingen met zich mee. Frauduleus gedrag past zich moeiteloos aan elke situatie aan. In het Verenigd Koninkrijk bleek uit onderzoek dat meer dan een derde van de mensen tijdens de lockdown werd benaderd door oplichters, terwijl bijna twee derde vreesde dat iemand uit hun omgeving slachtoffer zou worden.

De meest recente groeisprong in oplichterij wordt toegeschreven aan de opkomst van artificiële intelligentie (AI). AI is slimme software die taken uitvoert zoals een mens. Die software wordt 'slim' genoemd, omdat ze niet alleen vaste opdrachten uitvoert, maar ook zelf kan bijleren van voorbeelden, fouten of nieuwe situaties, en daardoor steeds beter wordt in de taak. Bijvoorbeeld: met AI kunnen criminelen zich via gemanipuleerde foto's en video's op ingenieuze wijze voordoen als iemand anders. Zo kunnen ze beveiligingssystemen omzeilen die een beroep doen op gelaatsherkenning.

Het gemak waarmee online fraude gepleegd kan worden, is vandaag een van de grootste problemen. Hackers blijven hun vaardigheden ontwikkelen, in lijn met de technologische vooruitgang. Het aantal websites, marktplaatsen en platforms met door gebruikers gemaakte content – teksten, foto's, video's die hun leven beschrijven – blijft stijgen, en het is zelfs niet zo moeilijk om die systemen te gaan misbruiken. De geschiedenis bewijst dat de creativiteit van oplichters ver gaat. In de voortdurende wedloop tussen beveiliging en bedrog lijkt de vindingrijkheid van de fraudeur telkens weer een stap voor te liggen. Wees daarom waakzaam, kritisch en goed geïnformeerd als verdediging tegen een wereld waarin technologie en sociale manipulatie hand in hand gaan.

FRAUDE IN CIJFERS

Als we naar de cijfers kijken, dan wordt de omvang van digitale fraude pas echt duidelijk. Fraude is uitgegroeid tot een hoogtechnologische miljardenindustrie. Alleen al in de VS liep de schade voor de federale overheid in 2024 op tot meer dan 500 miljard dollar. Ook in Europa zijn de bedragen duizelingwekkend: volgens het rapport *Nasdaq Verafin: Financial Crime Insights: Europe*[2] stroomde er in 2023 naar schatting 750,2 miljard dollar aan witwasgeld en illegale fondsen door het Europese financiële systeem, goed voor 2,3% van het totale bbp. Daarvan kwam 103,6 miljard dollar voort uit fraude: van identiteitsdiefstal en cyberaanvallen tot bank- en kredietkaartfraude.

Fraudecijfers 2023 Nasdaq Verafin: Nederland en rest EU (waartoe België in het onderzoek is gerekend).

Nederland

Categorie	Waarde in dollar (2023)	Waarde in euro (2023)
Totaal fraudeverlies	$ 8.500.000.000	€ 7.854.000.000
Totaal bankfraudeverlies	$ 8.100.000.000	€ 7.484.400.000
Totaal consumenten- en bedrijvenfraude	$ 384.000.000	€ 354.816.000
Betaalfraude	$ 8.100.000.000	€ 7.484.400.000
Voorschotfraude	$ 219.000.000	€ 202.356.000
Cybergerelateerde fraude	$ 93.000.000	€ 85.932.000
Kredietkaartfraude	$ 63.000.000	€ 58.212.000
Fraude door zich anders voor te doen	$ 43.000.000	€ 39.732.000
Vertrouwensfraude	$ 15.000.000	€ 13.860.000
Fraude met werkgelegenheid	$ 14.000.000	€ 12.936.000
Chequefraude	$ 1.000.000	€ 924.000

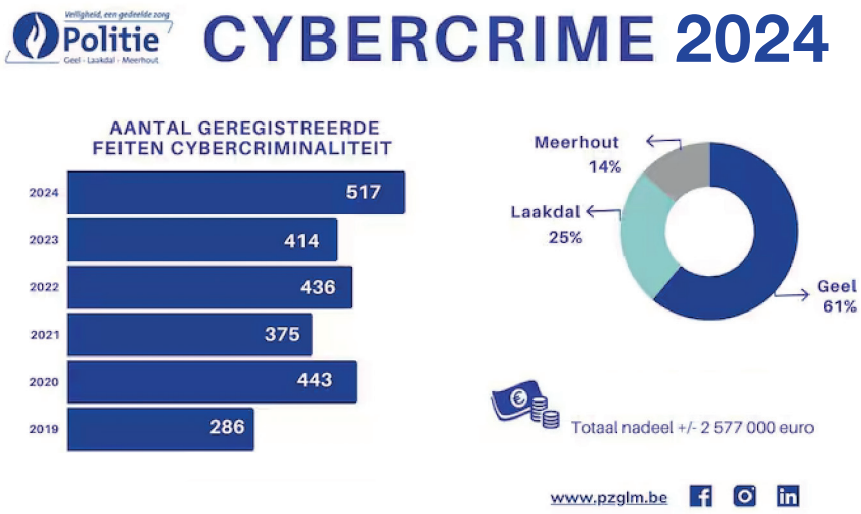
Rest van de EU (Oostenrijk, België, Bulgarije, Kroatië, Cyprus, Tsjechië, Estland, Griekenland, Hongarije, Ierland, Letland, Litouwen, Luxemburg, Malta, Polen, Portugal, Roemenië, Slowakije, Slovenië)

Categorie	Waarde in dollar (2023)	Waarde in euro (2023)
Totaal fraudeverlies	$ 2.200.000.000	€ 2.032.800.000
Totaal consumenten- en bedrijvenfraude	$ 1.300.000.000	€ 1.201.200.000
Totaal bankfraudeverlies	$ 844.000.000	€ 779.856.000
Voorschotfraude	$ 934.000.000	€ 863.016.000
Betaalfraude	$ 814.000.000	€ 752.136.000
Cybergerelateerde fraude	$ 272.000.000	€ 251.328.000
Fraude door zich anders voor te doen	$ 121.000.000	€ 111.804.000
Chequefraude	$ 19.000.000	€ 17.556.000
Kredietkaartfraude	$ 11.000.000	€ 10.164.000
Vertrouwensfraude	$ 10.000.000	€ 9.240.000
Fraude met werkgelegenheid	$ 3.000.000	€ 2.772.000

Wisselkoersen: 2023 (1 USD = 0,924 EUR); juli 2025 (1 USD = 0,854 EUR).

Dat cyberfraude allang geen 'ver van mijn bed'-show meer is, tonen de recente cijfers van de Belgische politiezone Geel-Laakdal-Meerhout. In een interview gaf korpschef Dirk Van Aerschot (HLN)[3] aan dat het aantal gevallen van cybercriminaliteit in 2024 met 22% gestegen was ten opzichte van 2023. Informaticafraude (54%) had daarin het grootste aandeel, met vooral phishing via mail, WhatsApp en sms. De politie registreerde hiervan 277 aangiftes, een stijging van 25%.

Overzicht van cybercriminaliteit in de Belgische politiezone Geel-Laakdal-Meerhout.



Cijfers van cybercrime in 2024. © Politiezone Geel-Laakdal-Meerhout

De categorie 'oplichting met het internet' omvat 32% van de geregistreerde feiten, goed voor 168 gevallen, waaronder fraude bij online kopen en verkopen, en vriendschapsfraude (zogezegde 'vrienden' die jou geld willen aftroggelen). Ook hier was er een stijging van 19% ten opzichte van het jaar ervoor. Daarnaast werden er 44 feiten van hacking vastgesteld, 24 feiten van valsheid in informatica en 4 gevallen van sabotage van een computersysteem.

Het financiële nadeel per aangifte varieert van enkele euro's tot tienduizenden euro's. In totaal liep het verlies in 2024 op tot ongeveer 2.577.000 euro. Dit cijfer ligt in werkelijkheid waarschijnlijk veel hoger, want uit de veiligheidsmonitor van 2021 blijkt dat in deze zone slechts 8% van de slachtoffers van phishing en 10% van internetoplichting daadwerkelijk aangifte deed. Volgens korpschef Van Aerschot zijn dit de belangrijkste redenen om geen aangifte te doen: het verlies was niet groot, men dacht er niet aan of men dacht dat de politie toch niets kon doen.

Dat benadrukt een bekend probleem: de werkelijke omvang van cyberfraude blijft onderschat, omdat veel slachtoffers geen aangifte doen uit schaamte, onwetendheid of om andere redenen. De echte cijfers liggen dus mogelijk tien keer hoger.

Op nationaal niveau is het beeld even alarmerend. Volgens het Belgische Febelfin[4] werd in 2023 bijna 40 miljoen euro gestolen via phishing, hoewel de banken 75% van de frauduleuze overschrijvingen hebben geblokkeerd of teruggevorderd. Computerfraude is veruit de meest voorkomende vorm van cybercriminaliteit in België (bijna 85% van de gevallen in 2023), gevolgd door hacking (8,41%) en computervervalsing (6,48%). Sabotage blijft marginaal met minder dan 1%.

Maar de bewustwording blijft achter: 9% van de Belgen heeft nog nooit van phishing gehoord, en bijna een derde van de 12- tot 25-jarigen kent de term niet. Uit onderzoek van Febelfin en Indiville blijkt dat 55% van de Belgen in 2023 minstens één phishingbericht kreeg, en 8% werd ooit slachtoffer. Jongeren zijn extra kwetsbaar: 10% werd slachtoffer van phishing, en 19% kent iemand die het overkwam.

Ook in Nederland zijn de cijfers zorgwekkend. Volgens de nationale veiligheidsmonitor 2023[5] werd 16% van de bevolking slachtoffer van een online delict. Online oplichting en fraude kwamen het vaakst voor (9%), gevolgd door hacking (6%) en online bedreiging/intimidatie (3%). Twee op de drie Nederlanders van 15 jaar of ouder kregen in 2023 minstens één verdacht bericht, 2% trapte erin en 0,8% verloor daadwerkelijk geld. Bijna 20% van de phishingslachtoffers werd opgelicht door bankhelpdeskfraude, waarbij een slachtoffer geld betaalde aan een oplichter die zich voordeed als een medewerker van de bank.

'Slechts' 0,8% van de Nederlands bevolking werd daadwerkelijk slachtoffer van phishing – dat klinkt misschien niet indrukwekkend, tot je het even doortrekt naar de wereldbevolking. Dan zie je meteen hoe gigantisch en winstgevend deze criminele handel is.

En jouw persoonlijke risico? Dat stijgt elk jaar. Naarmate je ouder wordt, deel je steeds meer gegevens online, je spaart en bouwt vermogen op, en ondertussen worden cybercriminelen steeds slimmer en geraffineerder. Je bent, zonder het te beseffen, een steeds aantrekkelijker doelwit.

DE WERELD IS HET SPEELVELD VAN OPLICHTERS GEWORDEN

Het beroep van zakkenroller is moeiteloos meegegroeid met zijn tijd: de wereld is nu de digitale speeltuin van de zakkenroller 2.0. Waar cybercriminaliteit rond 2010 nog een relatief kleine industrie was, explodeerde het fenomeen tussen 2010 en 2020 tot een miljardenbusiness. In dat decennium gingen er wereldwijd biljoenen dollars verloren door cyberaanvallen. Ransomware maakte zijn opmars, mede dankzij de opkomst van digitale valuta als de bitcoin, de snelle digitalisering van bedrijven en de wildgroei aan mobiele apparaten, nieuwe besturingssystemen en het dark web. Voor oplichters liggen de kansen voor het oprapen.

De jaren 2010 was het decennium waarin cybercriminaliteit voet aan de grond kreeg, maar in de jaren 2020 is de criminele wereld pas echt geprofessionaliseerd. Twee krachten versterken elkaar: enerzijds de wereldwijde toename van cybercrime – aangejaagd door technologische vooruitgang en sociaaleconomische ontwikkelingen, vooral in Oost-Europa en Azië – en anderzijds de razendsnelle digitalisering van bedrijven, die massaal overstappen naar de cloud en internationale groei nastreven, vaak sneller dan hun beveiliging kan volgen.

Info

De **cloud** is een plek op het internet waar je bestanden en programma's kan bewaren en gebruiken zonder dat ze op je eigen computer staan.

Een **botnet** is een netwerk van computers en apparaten die ongemerkt zijn besmet met malware en op afstand worden bestuurd door een cybercrimineel.

Machine learning is een techniek waarbij computers zelf leren van voorbeelden, in plaats van alleen vaste instructies te volgen.

Enkele gevolgen[6] op een rij:

- Cybercriminaliteit is wereldwijd het grootste bedrijfsrisico geworden.
- De gemiddelde kosten van een datalek liggen nu op 4,45 miljoen dollar.
- 82% van de datalekken vindt plaats in de cloud.
- De gezondheidszorg is vandaag de meest aangevallen sector.
- Phishing en gestolen inloggegevens zijn de populairste aanvalsmethoden.
- Ransomware was in 2023 verantwoordelijk voor 24% van alle aanvallen.

Oplichters werken tegenwoordig samen in organisaties, bendes en zelfs door staten gesteunde groepen, zoals in China en Rusland. Cybercriminelen zijn er in verschillende soorten:

- Hobbyisten: hacken uit nieuwsgierigheid of voor de lol.
- Hyperhackers: bieden hun diensten aan voor geld of status.
- Cyberhuurlingen: werken uit ideologie of loyaliteit voor overheden of bedrijven.
- Cyberterroristen: gebruiken het internet voor propaganda, rekrutering of om chaos te zaaien.
- Cybercrime als business: goed georganiseerde, winstgedreven criminele ondernemingen die wereldwijd opereren en zich richten op sectoren als financiën, gezondheidszorg en kritieke infrastructuur.

Bekende cybergroepen zijn onder meer REvil, DarkSide en Conti (ransomware), Joker's Stash en Genesis Market (kredietkaartfraude), Silk Road en AlphaBay (darkweb-marktplaatsen) en Emotet, Mirai en TrickBot (botnets).

Cybercriminaliteit evolueert razendsnel. Terwijl cybersecurity voortdurend verbetert, blijft het een kat-en-muisspel tussen overbelaste beveiligingsteams en steeds slimmere criminelen. De technologieën die onze digitale wereld moeten beschermen – zoals machine learning en AI – worden net zo hard ingezet door cybercriminelen. Het is een voortdurende strijd om de aanvallers voor te blijven.

Hoewel overheden en bedrijven steeds betere beveiliging inzetten – van GDPR-wetgeving tot geavanceerde antivirussoftware – blijft de wereldwijde schade door cybercriminaliteit hardnekkig stijgen. Volgens prognoses van het statistiekenbureau Statista[7] zullen de wereldwijde jaarlijkse kosten in 2029 naar verwachting oplopen tot 15,63 biljoen dollar (of 13,76 miljard euro), een stijging van bijna 70% ten opzichte van 2024[8].

FRAUDEURS ZIJN GEWETENLOOS

GEWETENLOZE LIEFDE

Romantische fraude, vriendschapsfraude, datingfraude, romance scam, pig butchering … Het zijn allemaal namen voor een vorm van oplichting waarbij criminelen hun slachtoffers eerst weten te charmeren. Het recept is telkens hetzelfde: oplichters bouwen via datingsites en apps als Tinder, Bumble, Feeld of HER een vertrouwensband op, vaak met valse profielen die er perfect uitzien. Zodra het vertrouwen is gewonnen, slaan ze toe en wordt het slachtoffer financieel uitgekleed.

Waargebeurd

Een schrijnend voorbeeld laat zien hoe geraffineerd deze oplichters te werk gaan. Een slachtoffer leert via een datingsite een oosterse vrouw kennen. Al snel verhuizen de gesprekken naar WhatsApp, waar ze maandenlang intensief contact hebben. Ze toont oprechte interesse, vraagt naar zijn familie, luistert naar zijn zorgen – alles om zijn vertrouwen te winnen. Na een jaar dagelijkse gesprekken komt ze met een 'gouden tip': haar makelaar heeft haar flink laten verdienen met investeringen, onder meer in cryptomunten. Ze wil haar 'beste online vriend' deze kans niet ontnemen. Vol vertrouwen stort hij een flink bedrag, maar de makelaar blijkt nep te zijn en het slachtoffer verliest 10.000 euro. De financiële klap is groot, maar de emotionele schade is minstens zo heftig: ongeloof, woede, schuld en schaamte.

Romantische fraude draait om het bespelen van menselijke verlangens: vriendschap, liefde, aandacht, soms gewoon een luisterend oor of zelfs een concertticket. Wie zijn eenzaamheid of verlangen online deelt, loopt extra risico. Oplichters jagen zonder scrupules op wanhoop en menselijke behoeften, zonder enig geweten.

Deze fraude situeert zich allang niet meer op het domein van eenlingen. Er bestaan inmiddels criminele organisaties die zich specialiseren in fraude zoals romance scams. Ze zetten talloze valse profielen in en hebben personeel nodig om alle slachtoffers te bedienen. Om dat 'personeelstekort' op te lossen, maken ze zelfs gebruik van moderne slavernij.

ONLINE SLAVERNIJ

Cyberslavernij is een groeiende criminele industrie. De meeste cyberslavernij tref je aan in Zuidoost-Azië, en dan vooral Cambodja, Laos, Myanmar en in toenemende mate ook de Filipijnen[9].

Duizenden mensen uit China, Thailand, Vietnam, India en andere landen worden onder voorwendselen naar Cambodja gelokt. Hen wordt een gouden toekomst beloofd, maar ze belanden opgesloten in zwaarbewaakte cyberscamcomplexen, vaak gevestigd in casino's of resorts. Indiase technici worden massaal geronseld voor goedbetaalde banen, maar eenmaal aangekomen worden ze tot cyberfraude gedwongen, soms tot zestien uur per dag, in erbarmelijke omstandigheden. Vluchten is vrijwel onmogelijk: tralies, prikkeldraad en gewapende bewakers houden iedereen binnen. Mishandeling, bedreiging, marteling en afpersing zijn dagelijkse kost. Familieleden van slachtoffers worden onder druk gezet voor losgeld.

Waargebeurd

In augustus 2022 bracht Al Jazeera het schokkende verhaal *Meet Cambodia's cyber slaves*[10], waarin het lot van Lu Xiangri centraal stond. Ooit was hij financieel analist in China, maar in 2020 strandde hij in Cambodja, op zoek naar een nieuwe start. Door de coronapandemie verloor hij zijn baan en zat hij zonder geld vast in Phnom Penh. Toen hem een goedbetaalde job werd aangeboden, werd hij in werkelijkheid verkocht aan een oplichtersbende. Lu werd gedwongen te werken in een scamfabriek, waaruit hij pas vrij zou kunnen komen als hij zijn 'aankoopbedrag' van 12.000 dollar had terugverdiend.

De schaal van deze industrie is enorm: naar schatting werken tot 150.000 mensen onder dwang in deze scamcentra, die miljarden dollars opleveren voor criminele netwerken. Vooral in het Cambodjaanse Sihanoukville, het epicentrum van de cyberslavernij, zijn de omstandigheden schrijnend. Er zijn zelfs meldingen van seksueel geweld, bloed- en orgaanhandel[11].

Ondanks internationale druk en enkele politieacties blijft de handel bloeien, mede dankzij de bescherming van machtige figuren en corrupte elites. De Cambodjaanse overheid kondigde begin 2025 weliswaar een taskforce aan om online scamoperaties te bestrijden, maar mensenrechtenorganisaties zijn sceptisch over de effectiviteit daarvan.

Cyberslavernij is daarmee uitgegroeid tot een van de meest schrijnende vormen van moderne mensenhandel in onze tijd, een industrie die draait op wanhoop, misleiding en brute uitbuiting.

Info

Bekijk de documentaire op **YouTube: Behind Asia's cyber slavery DW Documentary, 29 jan 2024**

De documentaire onthult een systeem van moderne slavernij, waarbij internationale criminelen migranten dwingen tot oplichting, en waarvan de opbrengst circuleert via grensoverschrijdende criminele netwerken in Zuidoost-Azië.

HOE AANTREKKELIJK ZIJN MIJN GEGEVENS?

Je denkt misschien dat jouw vertrouwde bank of favoriete winkelier alles op orde heeft, maar de realiteit is weerbarstiger. Financiële instellingen en bedrijven hebben niet altijd de middelen of de wil om optimale cyberveiligheid te garanderen. Daardoor ben je vaak minder beschermd dan je zou hopen.

VERTROUW NIET BLINDELINGS OP JE FAVORIETE INSTELLING

Tijdens de Pay360-conferentie in april 2025[12] waarschuwde Carolin Gardner van de Europese Bankautoriteit (EBA) voor het lakse gebruik van technologie bij financiële instellingen. Volgens haar is er een duidelijke toename van ernstige handhavingszaken tegen instellingen die technologie ondoordacht inzetten, wat de kans op financiële criminaliteit vergroot.

Ook De Nederlandsche Bank (DNB) luidt de noodklok. Zowel banken als consumenten moeten voorbereid zijn op het scenario waarbij het elektronische betalingsverkeer na een grote cyberaanval enkele dagen volledig stilvalt. Bij een cyberaanval breken hackers in op de computers met uiteenlopende slechte bedoelingen (hacking). Een noodvoorraad contant geld, zoals een biljet van vijftig euro, is dan geen overbodige luxe. DNB waarschuwt bovendien in haar rapport 'Overzicht Financiële Stabiliteit, najaar 2024'[13] dat de snelle digitalisering en geopolitieke spanningen – denk aan de oorlog tussen Oekraïne en Rusland, handelsoorlogen en andere diplomatieke conflicten – de risico's voor de financiële sector fors vergroten. Cybercriminelen maken steeds gerichter gebruik van artificiële intelligentie om banken, verzekeraars en andere instellingen aan te vallen. De sector is extra kwetsbaar door de afhankelijkheid van externe partijen, zoals clouddienstverleners en telecombedrijven. Als zij worden gehackt, voelen banken en consumenten dat meteen.

Zelfs bedrijven met een sterke reputatie en goede beveiliging zijn niet immuun voor cybercriminaliteit. De schade beperkt zich niet tot directe financiële verliezen. Reputatieschade door fraude kan tot honderd keer groter zijn dan het oorspronkelijke verlies. Bedrijven krijgen te maken met negatieve publiciteit, verlies van vertrouwen, dalende aandelenkoersen en problemen bij het aantrekken van personeel.

Waargebeurd

In april 2025 werd Ahold Delhaize, moederbedrijf van Delhaize en Albert Heijn, getroffen door een ransomware-aanval[14]. Het Russische hackerscollectief INC Ransom stal 6 terabyte aan gevoelige data, waaronder identiteitsbewijzen en vertrouwelijke documenten. De hackersgroep meldde de aanval zelf op het zogenoemde dark web en deelde daar ook enkele documenten waar het de hand op kon leggen. Daarop waren onder meer oude gegevens te vinden, zoals een geheimhoudingsverklaring van iemand die een locatie van Ahold Delhaize bezocht. Ook identiteitsbewijzen van personen werden vrijgegeven.

Cryptobeurs Bybit, met beveiliging op militair niveau, werd op 22 februari 2025 gehackt[15]. Daarbij verdween voor 1,5 miljard dollar aan cryptomunten – mogelijk de grootste cryptodiefstal ooit. De Noord-Koreaanse hackersgroep Lazarus wist een groot deel van deze buit onherroepelijk weg te sluizen.

WELKE SOORTEN DATA ZIJN POPULAIR BIJ HACKERS?

In de EU was in 2025 bijna 20% van de cyberaanvallen gericht op organisaties in het openbaar bestuur. Daarna volgden transport (11%), financiën (9%), digitale infrastructuur (9%), zakelijke dienstverlening (8%), algemene overheid (8%) en de maakindustrie (6%)[16].

De cijfers laten zien dat geen enkele sector immuun is, maar dat vooral organisaties met gevoelige data of een sleutelrol in de samenleving het vaakst worden getroffen.

Volgens het Amerikaanse cybersecuritybedrijf Syteca[17] lopen vooral financiële instellingen, de gezondheidszorg, bedrijven met intellectueel eigendom en overheidsorganisaties het grootste risico op datadiefstal. Dit bepaalt welke sectoren het meest kwetsbaar zijn voor cyberaanvallen.

De tabel toont de zeven meest aangevallen sectoren in 2024, zoals beveiligingsbedrijf IBM Security[18] die op een rij gezet heeft (al is er wel discussie over de precieze volgorde).

Sectoren die het meest slachtoffer zijn van cyberaanvallen (2024, IBM Security).

Rang	Sector	Percentage incidenten (2024)
1	Industrie/maakindustrie	26%
2	Financiële dienstverlening en verzekeraars	23%
3	Professionele, zakelijke en consumentendiensten	18%
4	Overheid en openbaar bestuur	13%
5	Transportdiensten	7%
6	Detailhandel	5%
7	Gezondheidszorg	n.v.t. (maar structureel hoog)

Andere sectoren, zoals landbouw, bouw, management, dienstverlening, media en entertainment, technologie, software, transport, horeca en communicatie, lopen eveneens risico. Zowel interne medewerkers als externe aanvallers kunnen gevoelige data buitmaken.

- De grootste oorzaak van datalekken in de detailhandel is het lage beveiligingsniveau. Veel winkeliers vertrouwen op externe partijen voor beveiliging of laten het onderwerp zelfs volledig links liggen. In de overheidssector zijn cyberaanvallen vaak gericht op financieel gewin of spionage.
- Energie- en nutsbedrijven zijn door hun cruciale rol extra kwetsbaar voor ransomware, zeker nu digitale en klassieke technologieën steeds meer verweven raken.
- De gezondheidszorg werd in 2023 het hardst getroffen door datalekken. Hackers zijn vooral uit op financieel gewin, maar misbruiken gestolen gegevens ook voor toegang tot medische dossiers of voor het verkrijgen van medicatie op naam van slachtoffers.
- Onderwijsinstellingen zijn door hun afhankelijkheid van digitale platforms een aantrekkelijk doelwit voor aanvallers die uit zijn op persoonsgegevens, financiële data en onderzoeksresultaten.

Ook jouw gegevens op social media-accounts, zoals Facebook, Twitter, Snapchat en Instagram, zijn erg gegeerd door criminelen. De grote bedrijven achter de sociale media zijn moeilijker te bedotten. Daarom richten ze hun pijlen op de individuele gebruiker, door zich te vermommen onder een nepprofiel en jou zo te lokken om gegevens vrij te geven, of – zelfs erger – je financieel uit te schudden. Elk detail van je leven zullen ze dankbaar aanvaarden om uit te buiten tegen jou of iemand anders.

Waargebeurd

In mei 2025 waren op Facebook en X reclames te zien waarin Belgisch premier Bart De Wever en minister-president Matthias Diependaele beleggingsplatformen aanraadden, met de boodschap dat je er snel rijk mee kon worden. Deze ad werd begeleid door een nepvideo (deepfake), waarbij het lijkt alsof De Wever aan Diependaele vraagt of hij al heeft meegedaan aan het 'project'.[19] De video ziet er echt uit, maar alles is nep en enkel bedoeld om mensen op te lichten.

De Franse Anne (53 jaar) raakte via Instagram maandenlang verstrikt in een oplichtingszaak: oplichters deden zich voor als Brad Pitt en vroegen haar om geld, onder meer voor luxecadeaus, invoerrechten en een kankerbehandeling. Ze maakte in totaal 830.000 euro over, ze verloor daarbij haar huis en ondernam drie zelfmoordpogingen. Haar verhaal verscheen begin 2025 op de Franse televisie, maar leidde tot spot en pesterijen op sociale media, zelfs door bedrijven als Netflix en voetbalclub Toulouse, die later hun excuses aanboden. Anne benadrukte dat ze niet verliefd werd op Brad Pitt, maar vooral gehoor gaf aan zijn urgente verhaal over ziekte en geldproblemen. Oplichters gebruikten AI-gegenereerde foto's en valse nieuwsberichten om haar te misleiden, zelfs nadat roddelbladen het echte koppel Brad Pitt en Ines de Ramon toonden[20].


INMELDEN