Co-funded by the European Union

FIGHT AGAINST LOVE SCAM

2023-1-DE02-KA210-VET-000151265

Abstract

Fight Against Love Scam (FALS) is een Europees initiatief dat is opgericht om volwassenen van 50 jaar en ouder te beschermen tegen online liefdesfraude en hen in staat te stellen zich hiertegen te verzetten. Het project brengt partners uit Duitsland, Nederland en Italië samen om het bewustzijn te vergroten en volwassenenopleiders, senioren en hun families te voorzien van de kennis en instrumenten om liefdesfraude te herkennen, te voorkomen en erop te reageren.

FALS bevordert online veiligheid, emotioneel welzijn en actief ouder worden door middel van een digitale handleiding, praktische tests en een online cursus. Het project stimuleert tevens de samenwerking tussen docenten, maatschappelijk werkers en gemeenschappen om sterkere ondersteuningssystemen voor ouderen op te bouwen.
Door educatie, preventie en empathie te combineren, streeft FALS ernaar de digitale wereld veiliger te maken voor iedereen.

Projectpartners

EUTH WONDERS E.V

IGOR VITALE INTERNATIONAL

ECREC European Center for Researching, Education and Consulting

Co-funded by the European Union

Gefinancierd door de Europese Unie. De geuite standpunten en meningen zijn echter uitsluitend die van de auteur(s) en weerspiegelen niet noodzakelijkerwijs die van de Europese Unie of het Europees Uitvoerend Agentschap voor Onderwijs en Cultuur (EACEA). Noch de Europese Unie, noch het EACEA kunnen hiervoor aansprakelijk worden gesteld.

Inhoudsopgave

Co-funded by
the European Union

Een boodschap van de projectpartners

Beste lezer,

Wij heten u van harte welkom bij deze gids, die voortkomt uit onze gezamenlijke inzet in Duitsland, Nederland en Italië om een van de meest kwetsbare groepen in onze samenleving ouderen die zich in de digitale wereld begeven – te ondersteunen en te helpen.

Fight Against Love Scam (FALS) is ontstaan vanuit een simpele maar dringende behoefte: het voorkomen van de emotionele en financiële schade die romantische oplichting veroorzaakt, en het bieden van hulpmiddelen aan volwassenenonderwijzers, gezinnen en senioren om online veilig te blijven. Te veel mensen zijn in stilte slachtoffer geworden en wij geloven dat het tijd is om kennis, zorg en gemeenschap in de schijnwerpers te zetten.
Dit boekje is meer dan een educatief hulpmiddel; het is een gebaar van solidariteit en respect. Het biedt inzichten, praktische richtlijnen en gedeelde ervaringen om waarschuwingssignalen te herkennen, digitale weerbaarheid te versterken en elkaar te ondersteunen bij het omgaan met online relaties.

We hopen dat u troost, duidelijkheid en vertrouwen vindt in deze pagina's.

Hartelijke groeten,

Het FALS-team: EUW (Duitsland),
EC (Nederland), IVI (Italië)

Handleiding overzicht

Inhoud van de handleiding

De handleiding bestaat uit 3 hoofdstukken die de inhoud van de methodologiehandleiding uiteenzetten:

1. Achter het masker: inzicht in liefdesfraude. Zorgvuldige
2. ondersteuning: goede praktijken voor docenten. Digitale
3. verdediging: basisprincipes van cyberbeveiliging voor
4. beginners. Kennis en groei: zelfevaluatie.

Kernelementen van de hoofdstukken

Hoofdstuk 1: Een overzicht van wat liefdesfraude is, hoe het gebeurt en hoe je het kunt herkennen en voorkomen.

Hoofdstuk 2: Praktische richtlijnen voor volwassenenonderwijzers over hoe ze ouderen kunnen ondersteunen, psychische kwetsbaarheid kunnen herkennen en kunnen reageren op oplichtingspraktijken.

Hoofdstuk 3: Inleiding tot online veiligheid, phishingdetectie en platformbewustzijn voor gebruikers zonder technische kennis.

Hoofdstuk 4: Een reeks korte tests om het begrip van liefdesfraude, emotioneel bewustzijn en digitale veiligheid te evalueren. Inclusief analyse aan de hand van infographics.

Over FALS

Co-funded by
the European Union

Invoering

De digitale wereld heeft talloze mogelijkheden voor verbinding gecreëerd, maar met die mogelijkheden komen ook nieuwe risico's. Een van de meest emotioneel schadelijke bedreigingen voor ouderen is tegenwoordig de zogenaamde 'liefdesoplichting', een vorm van online fraude die misbruik maakt van kwetsbaarheid en vertrouwen.

Het project Fight Against Love Scam (FALS) is een Europese samenwerking tussen partners in Duitsland, Nederland en Italië met een gedeelde missie: het beschermen, informeren en ondersteunen van mensen van 50 jaar en ouder, en hun naasten. Met deze handleiding willen we volwassenenonderwijzers de kennis en instrumenten bieden die nodig zijn om de signalen van online romantische oplichting te herkennen, psychologische en sociale ondersteuning te bieden en basisprincipes van cybersecurity op een toegankelijke en empathische manier aan te leren.

Deze gids is niet zomaar een handleiding, het is een oproep tot actie. Door het bewustzijn te vergroten en de capaciteit van docenten en zorgverleners te versterken, kunnen we schade voorkomen, herstel ondersteunen en de waardigheid en veiligheid van ouderen in digitale omgevingen bevorderen.

We nodigen u uit om de volgende hoofdstukken te lezen. Elk hoofdstuk is ontworpen om u te helpen een sterkere voorvechter, beschermer en voorlichter te worden in de strijd tegen liefdesfraude.

DOELSTELLINGEN VAN FALS

- Vergroot het bewustzijn onder ouderen (50+) over de risico's en tactieken van online romantische oplichting, zodat ze waarschuwingssignalen kunnen herkennen en emotionele en financiële schade kunnen voorkomen.
- Geef volwassenenonderwijzers de middelen, instrumenten en methoden om senioren in digitale omgevingen te ondersteunen en vroegtijdige signalen van psychische kwetsbaarheid te herkennen.
- Bied ondersteuning aan gezinnen en mantelzorgers door praktische richtlijnen te geven waarmee ze waarschuwingssignalen kunnen herkennen, met hun dierbaren kunnen communiceren en adequaat kunnen reageren op vermoedelijke oplichting.
- Bevorder digitale veiligheid door basiskennis over cyberbeveiliging te introduceren, zodat senioren veiliger online platforms kunnen gebruiken en risicovolle interacties kunnen vermijden.
- Ontwikkel een duurzaam educatief hulpmiddel door middel van een uitgebreide handleiding, zelfevaluatietoetsen en een digitale videocursus die gebruikt kan worden door centra voor volwassenenonderwijs, maatschappelijk werkers en familieleden in heel Europa.
- Stimuleer actief ouder worden en veerkracht door digitale geletterdheid en emotioneel welzijn te bevorderen, zodat ouderen betrokken, zelfstandig en veilig online kunnen blijven.

Doelgroep

01 Primaire doelgroep: Ouderen (50 jaar en ouder):

- De belangrijkste begunstigden van het project. Deze groep is steeds actiever online, maar mist vaak de digitale geletterdheid of emotionele steun om zichzelf te beschermen tegen romantische oplichting en andere vormen van online fraude. Het project is specifiek gericht op het versterken van hun bewustzijn, weerbaarheid en digitale veiligheid.

02 Docenten en trainers voor volwassenen

- Professionals werkzaam in het volwassenenonderwijs, buurthuizen of programma's voor digitale geletterdheid zullen worden getraind en uitgerust met instrumenten om oplichting via sociale media onder oudere cursisten te herkennen, te voorkomen en aan te pakken.

03 Familieleden en verzorgers

- Familieleden en naasten van ouderen zijn vaak de eersten die gedragsveranderingen opmerken en kunnen emotionele of praktische steun bieden in geval van een vermoedelijke oplichting.

04 Gezondheidszorg, maatschappelijk werkers, buurtcentra, ngo's en instellingen voor volwassenenonderwijs

- Professionals die mogelijk werken met ouderen die psychische problemen ondervinden als gevolg van oplichting of kwetsbaarheid voor online manipulatie.
- Organisaties die het handboek, de trainingsmaterialen en de digitale cursus van FALS kunnen integreren in hun educatieve of bewustmakingsactiviteiten.

Achter het masker: Liefdesfraude begrijpen

Co-funded by
the European Union

Agnese Federica Gobbi

Agnese Federica Gobbi, geboren in Slovenië, heeft een bachelordiploma in psychologische wetenschappen en technieken en volgt momenteel een masteropleiding psychologie aan de Guglielmo Marconi Universiteit in Rome. Sinds 2022 is ze een gewaardeerde medewerker bij Igor Vitale International s.r.l., waar ze zich specialiseert in audio- en videoproductie, fotografie, het schrijven van teksten en het ontwerpen van websites. Agnese heeft actief bijgedragen aan meer dan 15 projecten in uiteenlopende vakgebieden zoals de horeca, ambachten, ecologie en psychologie. Haar werk bracht haar naar verschillende delen van Europa, de overzeese Caribische gebieden, Frans-Polynesië, Groenland, de Zuid-Pacific en regio's in Zuid- en Oost-Azië, waarmee ze haar mondiale perspectief en multidisciplinaire expertise demonstreerde.

1 INLEIDING TOT DE LIEFDESOPLICHTING

De zogenaamde 'love scam', ook wel bekend als de romantische oplichting, is een vorm van online fraude waarbij oplichters emotionele banden misbruiken om mensen financieel te bedriegen. Geworteld in historische oplichtingstactieken, zoals de 'Spaanse gevangenen'-oplichting uit de 16e eeuw, blijven moderne romantische oplichtingspraktijken slachtoffers manipuleren door valse relaties en geïdealiseerde persona's te creëren. De opkomst van digitale communicatieplatformen heeft een vruchtbare bodem gecreëerd voor deze praktijken, waardoor oplichters anoniem kunnen opereren en hun bereik wereldwijd kunnen uitbreiden. Slachtoffers worden vaak gelokt door zorgvuldig opgestelde profielen en overtuigende verhalen, wat leidt tot aanzienlijke emotionele en financiële schade (Cemmi, n.d.; Coluccia et al., 2020; Europol, 2023). De laatste jaren is de liefdesoplichting steeds geavanceerder geworden, waarbij oplichters diverse psychologische tactieken gebruiken om controle over slachtoffers te krijgen en hen tot medewerking te dwingen. Inzicht in de mechanismen en gevolgen van liefdesoplichting, evenals het herkennen van vroege waarschuwingssignalen, is essentieel voor de bestrijding van deze frauduleuze activiteiten.

1.1 Wat is een liefdesoplichting?

De zogenaamde 'love scam', internationaal bekend als romantische oplichting, is een vorm van digitale fraude waarbij oplichters slachtoffers manipuleren om geld te verkrijgen door middel van valse liefdesbeloftes via internet. Volgens een uitspraak van het Italiaanse Hooggerechtshof (nr. 25165/2019) zijn personen die romantische interesse veinzen met als enig doel economisch of materieel voordeel te behalen, strafbaar op grond van artikel 640 van het Italiaanse Wetboek van Strafrecht (Coluccia et al., 2020 in Cemmi, n.d.). Het wijdverbreide gebruik van technologie heeft de opkomst en evolutie van deze vormen van oplichting vergemakkelijkt. Een onderzoek in Italië wees uit dat 3% van de bevolking slachtoffer is geworden van romantische oplichting, met een hogere incidentie onder vrouwen tussen de 40 en 60 jaar. Deze groep heeft de neiging relaties te idealiseren en intense emoties te zoeken, waardoor ze kwetsbaarder zijn. Slachtofferschap kan echter ook professionele succesfiguren treffen, zoals managers en docenten (Cemmi, n.d.; Commissariato di PS, n.d.). Hoewel romantische oplichting tegenwoordig voornamelijk via digitale platforms plaatsvindt, heeft het een lange geschiedenis. Een vroeg voorbeeld is de 'Spaanse gevangenenzwendel' uit de 16e eeuw, waarbij rijke individuen het doelwit waren. Bij deze oplichter deed hij zich voor als een onterecht gevangen Spaanse edelman met een verborgen fortuin. Hij veinsde wanhoop en vroeg om geld voor zijn vrijlating, in ruil voor een deel van zijn fortuin.

Om het plan aantrekkelijker te maken, noemde de oplichter een mooie, ongehuwde dochter en gebruikte hij romantische en familiale argumenten om empathie en emotionele betrokkenheid bij zijn slachtoffers op te wekken (Beek, 2016 in Cunha, n.d.; Gillespie, 2017 in Cunha, n.d.). De analyse van de Spaanse gevangenenfraude biedt inzicht in de basis van de moderne romantische oplichting. Ondanks de eeuwen die zijn verstreken, berust de kern van de fraude nog steeds op emotionele manipulatie. Hoewel methoden en technologieën zijn geëvolueerd, blijft het plan in essentie onveranderd: de oplichter bouwt een vertrouwensrelatie op, maakt gebruik van beloftes van liefde en een toekomst samen, en verleidt het slachtoffer ertoe geld en bezittingen af te staan (Cunha, n.d.). Deze vorm van fraude, een van de meest ingenieuze en succesvolle van zijn tijd, vereiste coördinatie tussen verschillende landen, waardoor het moeilijk was de oplichters te identificeren en te arresteren. De samenwerking tussen verschillende rechtsgebieden en de logistieke complexiteit stelden deze fraudeurs in staat om met een zekere mate van straffeloosheid te opereren, gebruikmakend van de beperkte communicatie- en handhavingsmogelijkheden van die tijd (Gregory & Nikiforova, 2012 in Cunha, n.d.).

Online fraude, waaronder zogenaamde 'romance scams', omvat een breed scala aan illegale activiteiten en maakt gebruik van digitale technologieën, zoals sociale media en datingapps, om slachtoffers te lokken en te misleiden. Oplichters gebruiken digitale tools zoals VPN's en RAT's om anoniem te blijven en toegang te krijgen tot de persoonlijke en financiële gegevens van slachtoffers, met als doel emotionele afhankelijkheid te creëren en voortdurend geld te eisen (EUROPOL, 2023; Wang, 2022).

Bij romantische oplichting volgt de oplichter doorgaans een patroon waarbij hij een emotionele band met het slachtoffer opbouwt door middel van geïdealiseerde profielen en tragische verhalen. Dit proces kan maanden duren, waardoor het slachtoffer een sterke emotionele band met de virtuele oplichter ontwikkelt. Deze dynamiek veroorzaakt, naast financieel verlies, aanzienlijke psychische schade (Whitty, 2015, 2012, 2018, 2013 in Wang, 2022; Dodge, 2016 in Wang, 2022).

1.2 Hoe herken je waarschuwingssignalen en hoe voorkom je ze?

Bij romantische oplichting worden geavanceerde psychologische manipulatietactieken gebruikt om emotionele en financiële controle over slachtoffers te verkrijgen. Hoewel romantische oplichting een relatief moderne vorm van cybercriminaliteit is, berust het op een reeks goed onderzochte tactieken die gericht zijn op het uitbuiten van emotionele kwetsbaarheden voor financieel gewin.

Studies hebben terugkerende strategieën geïdentificeerd die mensen kunnen helpen romantische oplichting te herkennen en te voorkomen dat ze er slachtoffer van worden. Een opmerkelijk raamwerk dat deze fasen beschrijft, is ontwikkeld door Whitty (in Cemmi, n.d.), die in kaart bracht hoe romantische oplichting zich doorgaans ontwikkelt in vijf fasen. Deze fasen, waaronder profilering, voorbereiding, uitbuiting, seksueel misbruik en onthulling, tonen de doelbewuste structuur en manipulatieve kracht die ten grondslag liggen aan romantische oplichting.

De eerste fase (profileringsfase) van een romantische oplichting bestaat uit het creëren van een valse identiteit die direct aantrekkelijk is voor het slachtoffer. Dit proces begint vaak met het verzamelen van persoonlijke gegevens van de sociale media-profielen en online aanwezigheid van het slachtoffer, zoals hobby's, interesses, levensdoelen en persoonlijke waarden.
Met behulp van deze informatie creëren oplichters persona's die de persoonlijkheid en ambities van het slachtoffer weerspiegelen. Op die manier wekken ze een indruk van compatibiliteit en gedeelde interesses, waardoor ze snel de gunst van het slachtoffer winnen. Oplichters beweren soms ook in de buurt te wonen, maar tijdelijk niet in staat te zijn af te spreken vanwege werk, vaak met een beroep dat internationale reizen vereist, zoals militaire dienst of hoge functies in het bedrijfsleven. Deze valse, maar herkenbare nabijheid creëert een gevoel van vertrouwen en gemeenschappelijkheid, waardoor de oplichter zijn band met het slachtoffer kan versterken en tegelijkertijd een handig excuus heeft voor zijn afwezigheid (Whitty, 2015, in Wang, 2022).

Zodra het eerste contact is gelegd, gaat de oplichter over naar een fase van emotionele verdieping (de voorbereidingsfase). Dit gaat verder dan oppervlakkige uitwisselingen; de oplichter begint een ogenschijnlijk intens liefdevolle en betrokken relatie met het slachtoffer op te bouwen. Ze gebruiken tactieken die vaak worden geassocieerd met 'love bombing', waarbij de oplichter het slachtoffer overlaadt met complimenten, uitingen van genegenheid, beloftes van een gezamenlijke toekomst en voortdurende aandacht. Deze tactiek is zeer effectief, omdat ze inspeelt op de menselijke behoefte aan verbinding en erbij horen. Oplichters kunnen bewerkte foto's, romantische berichten en zelfs gedichten sturen, allemaal bedoeld om de emotionele band te versterken. Na verloop van tijd verzamelen ze persoonlijke inzichten van het slachtoffer en identificeren ze eventuele lacunes in diens emotionele leven die kunnen worden gemanipuleerd. Een slachtoffer dat zich bijvoorbeeld ondergewaardeerd voelt, kan gevleid worden door de bewondering van de oplichter, terwijl iemand die zich eenzaam voelt snel afhankelijk kan worden van de constante aandacht.

Door geleidelijk aan deze emotionele kwetsbaarheden te leren kennen, positioneert de oplichter zichzelf als de oplossing voor de onvervulde behoeften van het slachtoffer, waardoor een afhankelijkheid ontstaat die moeilijk te doorbreken is. Deze fase kan langdurig zijn, weken of zelfs maanden duren, waarin de oplichter een emotionele band opbouwt en ervoor zorgt dat het slachtoffer zich betrokken voelt bij de relatie. Het uiteindelijke doel is het creëren van emotionele afhankelijkheid, waarbij het slachtoffer zich sterk aan de oplichter hecht en steeds meer bereid is om aan diens verzoeken te voldoen, in de overtuiging dat deze essentieel zijn voor het welzijn van de ander (Commissariato di PS, n.d.).

De oplichter gaat nu over van het opbouwen van vertrouwen naar het afpersen van geld (uitbuitingsfase). Nadat er al een sterke emotionele band is opgebouwd, begint de oplichter de situatie af te tasten door kleine gunsten te vragen, vaak gepresenteerd als dringende behoeften. De eerste verzoeken lijken misschien triviaal of redelijk, zoals het dekken van een kleine nooduitgave, en worden op een manier gepresenteerd die aansluit bij de empathische reactie van het slachtoffer op iemand om wie ze geven. Deze techniek staat bekend als de 'voet tussen de deur'-methode, waarbij kleine verzoeken geleidelijk leiden tot grotere financiële eisen. Zodra de oplichter geld heeft ontvangen, blijft hij zijn verzoeken opvoeren. In sommige gevallen presenteren oplichters een uitgebreide 'crisis', zoals een plotselinge medische noodsituatie of oplichting door een zakenpartner, waarvoor een aanzienlijk bedrag nodig is. Een andere tactiek, de 'deur in het gezicht'-methode, houdt in dat er eerst om een groot, onrealistisch bedrag wordt gevraagd en dat vervolgens wordt teruggebracht tot een kleiner bedrag.

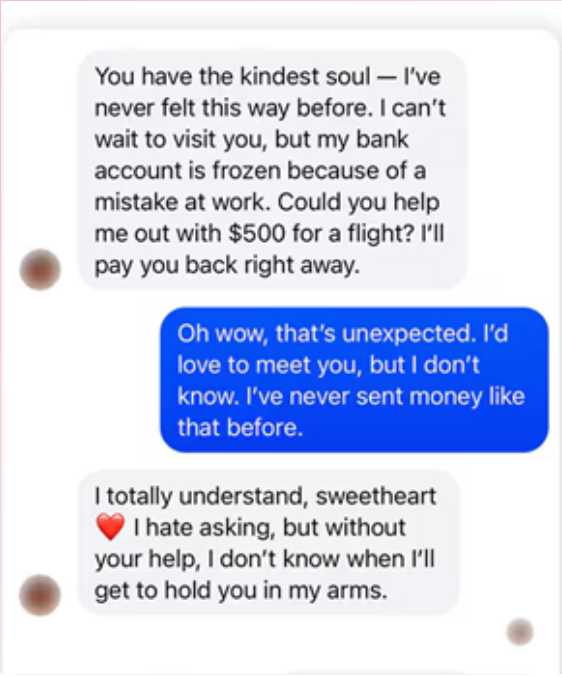
Deze aanpak maakt gebruik van de menselijke neiging om in te stemmen met een verzoek nadat een veeleisender verzoek is afgewezen. Oplichters kunnen ook gebruikmaken van voortdurende, kleine verzoeken voor alledaagse uitgaven, wat vaak voorkomt bij mannelijke slachtoffers. Hierbij vraagt de oplichter steeds om kleinere bedragen onder het mom van routinebehoeften, zoals energierekeningen of huur, en houdt zo de illusie in stand van een relatie die zal uitmonden in een echte ontmoeting (Cemmi, n.d.; Whitty & Buchanan, 2012 in Wang, 2022).

Hoewel dit niet in alle gevallen voorkomt, gaan sommige oplichters nog een stap verder door een seksueel element toe te voegen. In deze gevallen, zodra een aanzienlijk geldbedrag is verkregen, zet de oplichter het slachtoffer onder druk om seksuele handelingen via een webcam te verrichten, die vaak zonder medeweten van het slachtoffer worden opgenomen.

De oplichter kan deze opnames vervolgens gebruiken om het slachtoffer te chanteren, door te dreigen ze openbaar te maken tenzij er meer geld wordt betaald. Deze tactiek veroorzaakt psychische nood en vernedering bij het slachtoffer, waardoor de emotionele schade die door de financiële uitbuiting is veroorzaakt, nog groter wordt. Het laat ook zien hoe ver oplichters gaan om controle over hun slachtoffers uit te oefenen en hun financiële winst te maximaliseren (Whitty & Buchanan, 2012 in Wang, 2022). Wanneer de oplichter besluit dat hij of zij zoveel mogelijk uit de relatie heeft gehaald, verbreekt hij of zij abrupt alle contact met het slachtoffer, waardoor deze vaak in een staat van shock en verwarring achterblijft (onthullings- en verlatingsfase). Dit plotselinge vertrek dwingt het slachtoffer om de pijnlijke realiteit van het bedrog onder ogen te zien. Het verlies is niet alleen financieel, maar ook diep emotioneel, omdat veel slachtoffers het gevoel hebben een echte relatie te hebben verloren. De nasleep gaat vaak gepaard met gevoelens van schaamte, vernedering en verraad. Slachtoffers doorlopen een rouwproces dat vergelijkbaar is met het verlies van een geliefde, en de psychologische impact kan ingrijpend zijn, met onder andere depressie, angst en vertrouwensproblemen. Het besef dat de relatie gebaseerd was op manipulatie, zorgt ervoor dat veel slachtoffers hun eigen oordeel en gevoel van eigenwaarde in twijfel trekken, wat de emotionele impact van de oplichting vergroot (Whitty & Buchanan, 2012 in Wang, 2022).

Voorbeelden van een chatgesprek in een zogenaamde liefdesoplichting

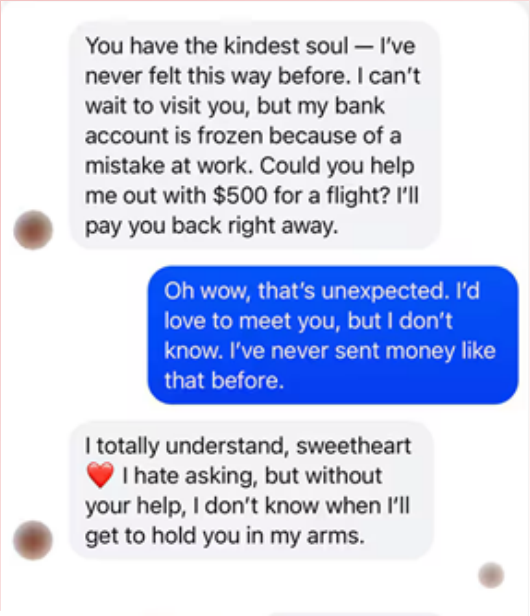
1- Militaire oplichting:



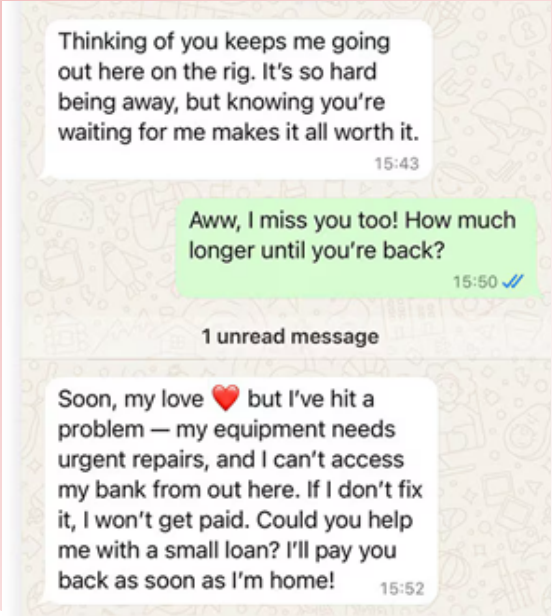
2- Nigeriaanse oplichting:

3. Crypto-romantiekoplichting

4. Oplichting via Facebook-romantiek

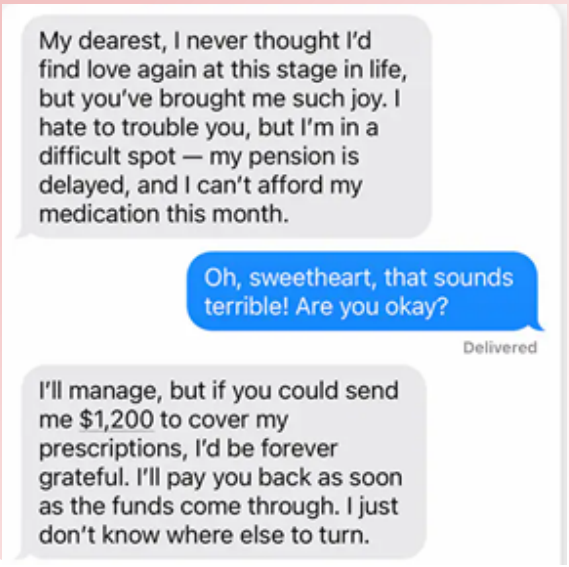


5. Oplichting met olieplatforms

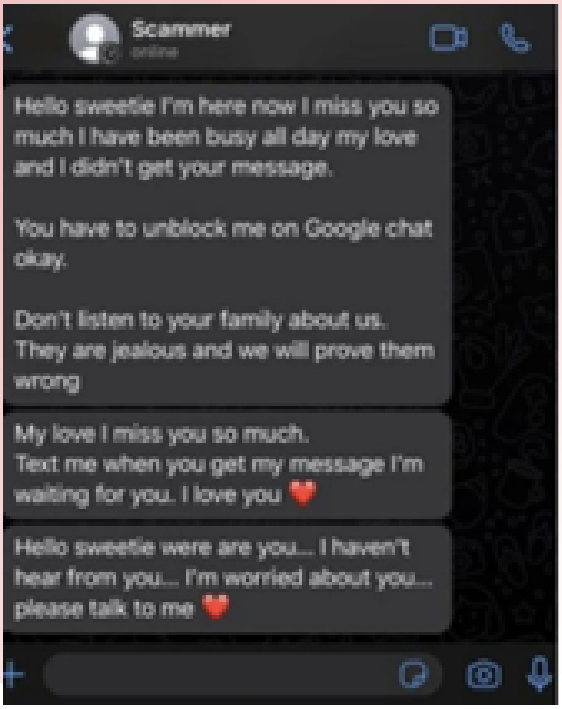


6. Romantische relaties met beroemdheden

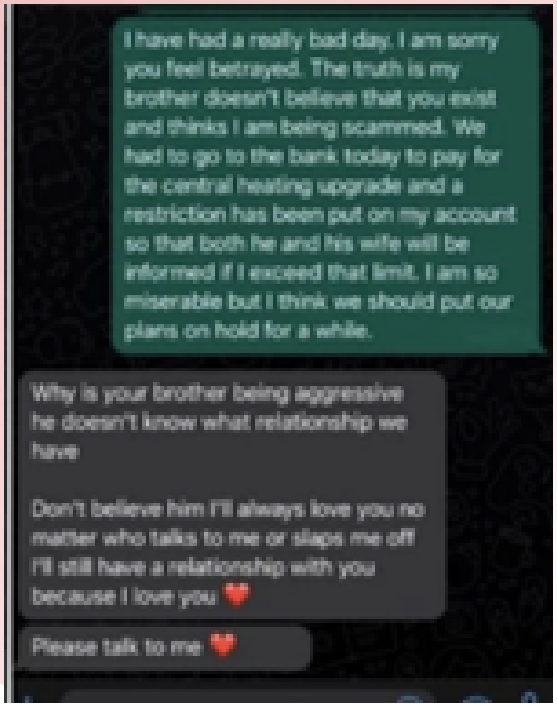
7. Oplichting met oudere mensen in romantische relaties



8. Voorbeeld van een oplichter



9- Voorbeeld van een oplichter



1.2.1 Wat is 'sextortion' en hoe herken je het?

Sextortion is een vorm van seksuele afpersing, een cybercriminaliteit waarbij daders dreigen intieme beelden of video's te verspreiden als het slachtoffer niet aan hun eisen voldoet (Interpol, 2022; National Crime Agency, 2021 [NCA]; U.S. Immigration and Customs Enforcement [ICE], 2025). Bij deze praktijken gebruiken daders vaak romantiek of online intimiteit om compromitterend materiaal te verkrijgen, dat ze later gebruiken voor geld, seksuele gunsten of verdere uitbuiting (Wang, 2024).

Wat betreft liefdesfraude ontstaat afpersing doorgaans nadat online vertrouwen is opgebouwd: oplichters creëren valse identiteiten op datingsites of sociale media, bouwen een emotionele band op en moedigen vervolgens het delen van naaktfoto's of seksuele webcaminteracties aan, die soms stiekem worden opgenomen (Kloess et al., 2014). Eenmaal verkregen, worden deze materialen gebruikt als dwangmiddel, waarbij oplichters dreigen ze naar familie, vrienden of werkgevers te sturen, tenzij aan hun eisen wordt voldaan (Europol, 2017). In sommige gevallen gebruiken daders de dreiging van openbaarmaking als "impliciete chantage" om de controle over de slachtoffers te behouden (Whitty & Buchanan, 2012).

✦ Waarschuwingssignalen zijn onder andere:

• snelle escalatie naar seksuele gesprekken of eisen (Europol, 2017);
• weigering om deel te nemen aan normale videogesprekken terwijl er wel op wordt aangedrongen expliciet materiaal te ontvangen (Patchin & Hinduja, 2020);
• profielen met gestolen of tegenstrijdige foto's (Interpol, 2022);
• emotionele manipulatie of dreigingen met zelfbeschadiging (Wang, 2024);
• en slachtoffers aansporen om snel over te stappen van openbare platforms naar privékanalen (NCA, 2021).

Psychologisch gezien gebruiken daders manipulatiestrategieën, vaak met behulp van 'love bombing' of overdreven vleierij om de weerstand van slachtoffers te verlagen (Coluccia et al., 2020). Ze kunnen slachtoffers ook via sociale media onderzoeken om de dreiging te versterken en de indruk te wekken dat ontmaskering imminent is (Patchin & Hinduja, 2020). Belangrijk is dat sextortion gedijt op de schaamte en het zwijgen van slachtoffers; onderzoek

Uit onderzoek blijkt dat velen aarzelen om aangifte te doen uit angst voor stigmatisering (Cross, 2014; Pietilä & Korhonen, 2024). Door de signalen vroegtijdig te herkennen, kunnen mensen de moed vinden om contact te verbreken en professionele hulp of hulp van de politie te zoeken.

1.2.2 Casestudies over slachtoffers van liefdesfraude

Romantische oplichting is geëvolueerd van simpele online misleidingen tot complexe criminele netwerken met een wereldwijd bereik, zoals verschillende overtuigende voorbeelden illustreren. Deze voorbeelden laten zien hoe romantische oplichting zowel emotioneel verwoestend als financieel destructief kan zijn en hoe het zich richt op kwetsbare personen door middel van emotioneel manipulatieve tactieken.

Casestudie 1

In Italië richtte een zeer georganiseerd netwerk van zogenaamde 'romance scams' zich op oudere mannen, voornamelijk in de regio Calabrië. Dit netwerk bestond uit Roemeense staatsburgers die jonge vrouwen inschakelden om persoonlijke, vaak fysieke, relaties met hun slachtoffers op te bouwen. Door een diepe emotionele band te smeden, overtuigden deze vrouwen de oudere mannen ervan om aanzienlijke geldbedragen over te maken, zogenaamd voor noodgevallen in verband met familie of gezondheid. Deze zaak laat zien hoe sommige vormen van 'romance scams' verder gaan dan het online domein en ook face-to-face interacties omvatten, waardoor de impact van de oplichting op de slachtoffers wordt vergroot. Het netwerk opereerde in meerdere landen en maakte gebruik van geavanceerde witwaspraktijken, waarbij het van de slachtoffers verkregen geld via verschillende financiële kanalen werd verdeeld om opsporing te voorkomen. Deze operatie leverde meer dan een miljoen euro op, wat de aanzienlijke winsten onderstreept die georganiseerde 'romance scams' kunnen opleveren. De multinationale reikwijdte en de gestructureerde aard van deze oplichting tonen de uitdagingen aan waar autoriteiten voor staan bij het onderzoeken en vervolgen van dergelijke zaken, vooral omdat deze netwerken vaak grensoverschrijdend opereren (EUROPOL, 2022).

Casestudie 2

Een 53-jarige man, kwetsbaar na een recente scheiding, werd slachtoffer van romantische fraude toen hij via een datingsite nieuwe contacten zocht. Hij werd benaderd door een vrouw die beweerde uit Spanje te komen, maar in de Verenigde Staten woonde. De vrouw stuurde hem foto's, maar vermeed elk persoonlijk contact of videocontact. Ze communiceerde via telefoon, Skype en e-mail. Nadat er een band was ontstaan, begon ze om financiële hulp te vragen. Aanvankelijk beweerde ze dat ze geen eten kon betalen, later dat ze een paspoort nodig had om hem te bezoeken. In de loop der tijd maakte het slachtoffer meer dan £15.000 over naar zijn zogenaamde partner.

Na tussenkomst van de politie en ondersteuning van slachtofferhulp stopte de man met het versturen van geld en begon hij emotionele en praktische hulp te ontvangen. Deze zaak illustreert hoe oplichters kwetsbare levenssituaties, zoals een scheiding, uitbuiten en hun eisen geleidelijk opvoeren, waarbij ze vertrouwen opbouwen door middel van consistent maar oppervlakkig contact (Surrey Police, n.d.).

Casestudie 3

Een 65-jarige weduwe werd slachtoffer van romantische oplichting nadat ze via Facebook contact had gelegd met een man die beweerde officier in het leger te zijn. Eenzaam na het overlijden van haar man zocht ze gezelschap en raakte al snel overtuigd van de oprechte bedoelingen van de man. De oplichter, die alleen via Facebook en telefoon met haar communiceerde, beweerde dat hij geld nodig had om het leger te verlaten en voor zijn zieke zoon te zorgen. Het slachtoffer, die wilde helpen, stuurde £7.500. Kort daarna vroeg de oplichter om nog eens £3.500 voor de medische kosten van zijn zoon. De bank greep echter in vóór de transactie en gaf een waarschuwing af volgens hun bankprotocol, waardoor verder verlies werd voorkomen. Deze interventie, samen met het daaropvolgende advies van de politie, hielp het slachtoffer inzien dat het om oplichting ging. Deze zaak benadrukt het belang van bankprotocollen en ondersteuningssystemen binnen de familie bij de bescherming van kwetsbare personen tegen oplichting (Surrey Police, n.d.).

Casestudie 4

Een 66-jarige gescheiden man die alleen woonde, werd het doelwit van meerdere romantische oplichtingspraktijken nadat hij zich had aangemeld bij verschillende online datingplatforms. Hij onderhield contact met verschillende vrouwen via e-mail, sms en telefoon en liet hen geloven dat hij hun levensonderhoud betaalde, inclusief huur en rekeningen, en zelfs vluchten voor bezoeken die nooit plaatsvonden. In vijf jaar tijd maakte hij meer dan £100.000 over naar verschillende oplichters. Zijn dochter maakte zich uiteindelijk zorgen bij de politie, die ingreep. Financiële instellingen blokkeerden vervolgens de toegang van de man tot geldovermakingsdiensten om verdere verliezen te voorkomen. Deze zaak illustreert hoe langdurige oplichting de financiële zekerheid kan ondermijnen en onderstreept het belang van betrokkenheid van familie en financieel toezicht bij het herkennen en stoppen van dergelijke oplichtingspraktijken (Surrey Police, n.d.).

Casestudie 5

Een onderzoek naar romantische oplichting afkomstig uit Nigeria heeft een gedetailleerd draaiboek aan het licht gebracht dat oplichters gebruiken om hun slachtoffers te misleiden. Dit draaiboek biedt een stapsgewijze aanpak.

Stapsgewijze richtlijnen voor het opbouwen van vertrouwen, het manipuleren van emoties en het geleidelijk opvoeren van financiële eisen. Oplichters in Nigeria richten zich vaak op vrouwen van middelbare leeftijd of ouder, die mogelijk alleenstaand zijn of recent weduwe zijn geworden, en profiteren van hun mogelijke eenzaamheid en behoefte aan verbinding. In de beginfase creëren oplichters profielen die er verfijnd en charmant uitzien, met flatterende foto's en ogenschijnlijk betekenisvolle gesprekken. Het draaiboek beschrijft tactieken voor het opbouwen van een 'stormachtige romance', een strategie die bedoeld is om de geïdealiseerde relaties na te bootsen die vaak in de media te zien zijn. Na verloop van tijd manipuleren oplichters het slachtoffer door haar te laten geloven in een gezamenlijke toekomst, terwijl ze steeds grotere financiële eisen stellen. Dit draaiboek belicht de systematische aanpak van deze oplichters en de berekende stappen die betrokken zijn bij romantische oplichting, waarbij de nadruk ligt op het professionele karakter van romantische fraude als criminele onderneming (DocumentCloud, n.d.).

Gezien de hardnekkigheid van romantische oplichting, zijn er bepaalde technologische hulpmiddelen beschikbaar om frauduleuze profielen te identificeren. Swindlerbuster Face Search, bijvoorbeeld, stelt gebruikers in staat om een omgekeerde beeldzoekactie uit te voeren op foto's die in datingprofielen worden gebruikt. Door te achterhalen of een afbeelding aan meerdere namen of locaties is gekoppeld, kunnen mensen de authenticiteit van online profielen beter controleren.

1.3 Statistieken

De post- en communicatiepolitie houdt het internet dagelijks actief in de gaten. Gespecialiseerd personeel houdt toezicht op online ruimtes, met name sociale mediaplatformen, om crimineel gedrag te voorkomen en te bestrijden. Deze gespecialiseerde afdeling werkt gecoördineerd op nationaal en internationaal niveau en maakt gebruik van kantoren in het hele land om incidenten met betrekking tot cybercriminaliteit te beheren en te onderzoeken. Een van de problemen die worden aangepakt, is de zogenaamde 'romance scam', oftewel romantische fraude, die in 2021 een duizelingwekkende stijging van 118% liet zien ten opzichte van de zaken die in 2020 werden behandeld. Hoewel mannen over het algemeen minder vaak het slachtoffer worden van deze vorm van oplichting, zijn talloze Italiaanse mannen misleid door daders die zich voordoen als buitenlandse vrouwen en sociale media-accounts gebruiken met provocerende afbeeldingen, vaak als modellen of rijke erfgenamen. Deze oplichting kan leiden tot aanzienlijke financiële verliezen, waarbij individuele gevallen soms oplopen tot honderdduizenden euro's. Alleen al in 2021...

Er werd gerapporteerd dat er ongeveer € 4,5 miljoen verloren is gegaan door deze oplichtingspraktijken (Commissariato di Pubblica Sicurezza Online, n.d.). In Europa treft romantische oplichting tussen de 1% en 3% van de bevolking, waarbij de verliezen in verschillende landen aanzienlijke financiële gevolgen hebben. Zo meldden Finse politiegegevens uit 2020 210 incidenten met een totale schade van € 6,1 miljoen, wat in 2023 opliep tot € 10,4 miljoen, wat de toenemende prevalentie van deze misdrijven weerspiegelt (Pietilä & Korhonen, 2024). De financiële impact van romantische oplichting strekt zich uit over het hele continent, en het patroon van bedrog dat in deze incidenten wordt waargenomen, onderstreept het belang van publieke bewustwording en digitale geletterdheid in de strijd tegen online fraude.

Het platform CybSafe meldt dat ongeveer 20% van de mensen slachtoffer wordt van romantische oplichting, waarbij millennials (18%) en generatie Z (15%) het meest getroffen worden. Ondanks de hoge slachtoffercijfers doet slechts 55% van de slachtoffers aangifte van deze oplichting, en van degenen die dat wel doen, neemt 36% contact op met de autoriteiten. Deze statistieken benadrukken zowel de generatieverschillen in kwetsbaarheid als in het aangiftegedrag, en suggereren de noodzaak van gerichte preventieve strategieën en meer ondersteuning voor alle demografische groepen (CybSafe, 2023).

1.4 Slachtofferschap van liefdesfraude

1.4.1 Psychologische gevolgen voor slachtoffers van liefdesfraude

Slachtofferschap door cybercriminaliteit, zoals romantische oplichting, cyberstalking of fraude, leidt tot diepgaande psychologische gevolgen die vergelijkbaar zijn met die van soortgelijke offline misdrijven. Slachtoffers ervaren een scala aan emotionele, sociale en fysiologische effecten. Onderzoek toont bijvoorbeeld aan dat slachtoffers van cyberpesten vergelijkbare gevolgen ondervinden als slachtoffers van traditioneel pesten, waaronder sociale angst, depressie en een verminderd gevoel van veiligheid (Smith et al., 2008, in Open University, 2024).

Op vergelijkbare wijze weerspiegelt de angst die cyberstalking veroorzaakt die van stalking in persoon, waardoor slachtoffers te maken krijgen met hoge niveaus van angst, hyperwaakzaamheid en stress (Dreßing et al., 2014, in Open University, 2024). Hoewel de effecten van trolling minder onderzocht zijn, suggereert nieuw bewijs dat ook dit kan bijdragen aan aanzienlijke psychische schade, wat wijst op de noodzaak van verdere interventie.

Verder onderzoek naar de impact ervan op slachtoffers is nodig. Met name romantische oplichting heeft unieke en uitgebreide psychologische gevolgen vanwege de multidimensionale aard van de schade. Onderzoek toont aan dat slachtoffers van romantische oplichting te maken krijgen met wat Button et al. (2014) een "dubbele klap" noemen: het financiële verlies en de emotionele verwoesting die voortvloeit uit het vermeende uiteenvallen van een echte relatie. Studies benadrukken dat dit emotionele verraad vaak de financiële schade overschaduwt en diepgaand leed bij slachtoffers veroorzaakt. Button et al. (2014) stellen dat de combinatie van financieel verlies en emotioneel verraad door deze oplichting ertoe leidt dat veel slachtoffers ernstig emotioneel trauma oplopen. Het werk van Whitty en Buchanan (2012; 2016) bevestigt dit en laat zien dat slachtoffers vaak worstelen met schaamte, schuldgevoel en zelfverwijt, wat hen er vaak van weerhoudt hulp te zoeken. Dergelijke geïnternaliseerde schaamte kan worden versterkt door externe oordelen, aangezien slachtoffers soms door anderen als "naïef" of "goedgelovig" worden bestempeld (Buchanan & Whitty, 2014, in Open University, 2024).

De psychologische gevolgen van cybercriminaliteit zijn ingrijpend en vaak langdurig. Veel slachtoffers melden depressie, sociaal isolement, symptomen die lijken op posttraumatische stressstoornis (PTSS), dwanggedachten, een laag zelfbeeld en een diepgeworteld wantrouwen jegens anderen (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012; Bates, 2017, in Open University, 2024). Slachtoffers melden ook vaak fysieke symptomen, zoals aanhoudende hoofdpijn, spijsverteringsproblemen en slaapstoornissen, die hun emotionele belasting verder verergeren en het herstel bemoeilijken. Copingstrategieën neigen aanvankelijk naar onaangepaste mechanismen, waaronder middelengebruik en vermijdingsgedrag, voordat slachtoffers kunnen overschakelen naar positievere methoden zoals counseling of deelname aan belangenbehartiging. Herstel wordt echter vaak belemmerd door maatschappelijke opvattingen, met name het wijdverbreide probleem van slachtofferbeschuldiging. Slachtofferbeschuldiging vormt een cruciaal obstakel in het herstelproces, vooral voor slachtoffers van cybercriminaliteit. Victimologisch onderzoek, dat teruggaat tot Mendelsohns vroege typologieën uit de jaren 30, suggereerde dat slachtoffers een rol zouden kunnen spelen in hun slachtofferschap. De moderne victimologische theorie stelt daders echter over het algemeen verantwoordelijk en erkent dat factoren buiten de controle van het slachtoffer vaak bijdragen aan hun uitbuiting. Desondanks worden slachtoffers van cybercriminaliteit vaak beschuldigd van gedeeltelijke verantwoordelijkheid, vaak vanwege diepgewortelde overtuigingen over een 'rechtvaardige wereld' (Lerner, 1980, in Open University, 2024). Dit geloofssysteem suggereert dat de wereld functioneert volgens een principe van rechtvaardigheid, wat mensen ertoe aanzet om...

Men gelooft dat slachtoffers iets moeten hebben gedaan om het kwaad aan te trekken. Deze denkwijze, die vaak wordt toegepast op romantische oplichting, impliceert dat slachtoffers handelden uit hebzucht of goedgelovigheid en de misdaad hadden kunnen vermijden door online interacties of het gebruik van sociale media te vermijden (Cross, 2015, in Open University, 2024).

Dit soort slachtofferbeschuldiging kan de psychologische impact op slachtoffers van romantische oplichting verergeren, die al worstelen met gevoelens van verraad en schaamte. Veel slachtoffers geven aan dat het pijnlijkste aspect van hun ervaring het oordeel en het gebrek aan empathie is dat ze ervaren van familie en vrienden, die hen mogelijk als medeplichtig aan hun eigen oplichting zien. Wanneer slachtofferbeschuldiging plaatsvindt, kan dit ook zelfverwijt bij het slachtoffer versterken, waardoor het moeilijk voor hen wordt om steun te zoeken of openlijk over hun ervaringen te praten. Dit gebrek aan steun belemmert niet alleen emotioneel herstel, maar kan er ook toe leiden dat slachtoffers zich verder geïsoleerd en onbegrepen voelen, wat na verloop van tijd tot diepere psychologische gevolgen kan leiden (Wang, 2022). Romantische oplichting leidt vaak tot diepgaand emotioneel leed dat verder gaat dan financieel verlies, waardoor slachtoffers gevoelens van schaamte, schuld en sociaal isolement ervaren. Veel slachtoffers geven zichzelf de schuld of schamen zich te veel om de oplichting te melden, terwijl sommigen te maken krijgen met ernstige financiële gevolgen, zoals het verliezen van hun spaargeld of het oplopen van schulden. Slachtoffers die een emotionele band met de oplichter ontwikkelen, kunnen het Stockholm-syndroom ervaren, waarbij ze sympathie of genegenheid voelen voor de dader, zelfs nadat de misleiding aan het licht is gekomen. Deze binding bemoeilijkt hun mogelijkheden om aan de oplichting te ontsnappen of deze te melden (The Debt Advisor, 2023).

1.4.2 Slachtofferprofiel

Onderzoek naar de victimologie van online romantische oplichting onthult specifieke demografische en psychologische kenmerken die de kwetsbaarheid voor dergelijke praktijken vergroten. Studies van Wang (2022) tonen aan dat personen met een hoger risico om slachtoffer te worden van romantische oplichting doorgaans vrouwen, mensen van middelbare leeftijd en hoogopgeleiden zijn. Demografische gegevens suggereren dat 60% van de slachtoffers van romantische oplichting vrouwen zijn, terwijl 40% mannen zijn. Onder de slachtoffers is 63% van middelbare leeftijd, gevolgd door 21% jongvolwassenen en 16% ouderen. Mensen van middelbare leeftijd worden vaak als doelwit gekozen vanwege hun financiële stabiliteit en de grotere kans dat ze online datingplatforms gebruiken, met name na ingrijpende levensgebeurtenissen zoals een scheiding of het verlies van een partner. Dit kan hun vatbaarheid voor de beloftes van gezelschap die oplichters doen, vergroten.

Persoonlijkheidskenmerken spelen ook een rol; mensen met een hoger niveau van vertrouwen, impulsiviteit en minder zelfbeheersing zijn bijzonder kwetsbaar. Oplichters buiten deze eigenschappen uit en lokken slachtoffers in verzonnen romantische relaties door middel van goed doordachte verhalen die empathie, medeleven en vaak een diepe emotionele band opwekken (Wang, 2022). De psychologische impact van romantische oplichting is enorm, vaak gekenmerkt door wat Button et al. (2014) een "dubbele klap" noemen: financieel verlies in combinatie met de emotionele verwoesting van een vermeend verraad in de relatie.

Slachtoffers lijden doorgaans aan ernstig emotioneel leed, waaronder schaamte, schuldgevoel en een verminderd zelfbeeld. Studies van Whitty en Buchanan (2012, 2016) laten zien hoe deze emotionele gevolgen vaak de pijn van financieel verlies overtreffen, omdat slachtoffers het verraad van een relatie die ze als oprecht beschouwden, moeten verwerken. Veel slachtoffers aarzelen om hulp te zoeken of aangifte te doen, uit angst voor kritiek of verwijten van familie en vrienden die hen als 'naïef' of 'goedgelovig' zouden kunnen zien (Buchanan & Whitty, 2014 in Open University, 2024). Cross et al. (2016) onderzochten de dynamiek van romantische oplichting vanuit het perspectief van de theorie over huiselijk geweld en hoe oplichters psychologische manipulatie gebruiken om controle over hun slachtoffers te krijgen. Volgens hun bevindingen tonen slachtoffers van romantische oplichting vaak een hoog niveau van vertrouwen en kwetsbaarheid in online interacties, waardoor ze vatbaarder zijn voor emotionele manipulatie. Oplichters bouwen voort op dit vertrouwen door een schijn van genegenheid op te houden, waardoor het slachtoffer gaat geloven in de legitimiteit van de relatie. Deze aanpak weerspiegelt de tactieken van emotionele manipulatie die worden gezien bij huiselijk geweld, waarbij daders afhankelijkheid creëren en slachtoffers isoleren van hun sociale netwerk. Isolatie is een veelvoorkomend kenmerk van romantische oplichting, omdat oplichters slachtoffers ontmoedigen om details over hun relatie met vrienden of familie te delen. Deze tactiek vergroot de emotionele betrokkenheid en afhankelijkheid van het slachtoffer van de oplichter, waardoor het steeds moeilijker wordt om de misleiding te herkennen of eraan te ontsnappen (Cross et al., 2016).

De financiële gevolgen voor slachtoffers van romantische oplichting zijn vaak ernstig. Veel slachtoffers moeten aanzienlijke spaargelden opgeven of persoonlijke bezittingen verkopen om aan de financiële eisen van de oplichters te voldoen. Deze financiële impact, verergerd door emotionele spanning, kan leiden tot een gevoel van hopeloosheid en machteloosheid. Voor sommigen kunnen de verliezen hun financiële stabiliteit jarenlang beïnvloeden, wat bijdraagt aan de psychische problemen waarmee ze kampen. Cross et al. (2016) merken op dat financiële uitbuiting

Slachtoffers van dergelijke oplichtingspraktijken kunnen diepe gevoelens van schaamte en schuld oproepen, omdat ze worstelen met het besef dat ze gemanipuleerd zijn. Naast de financiële en emotionele schade melden slachtoffers van romantische oplichting diverse fysieke en psychologische symptomen die verband houden met trauma. Studies tonen aan dat slachtoffers vaak symptomen ervaren van posttraumatische stressstoornis (PTSS), depressie, sociaal isolement, dwangmatig gedrag en een overweldigend gevoel van wantrouwen jegens anderen. Fysieke symptomen, zoals hoofdpijn, spijsverteringsproblemen en slaapstoornissen, komen ook vaak voor en verergeren de emotionele impact van de oplichting. Aanvankelijk kunnen slachtoffers hun toevlucht nemen tot onaangepaste copingstrategieën, zoals middelengebruik of vermijdingsgedrag, voordat ze uiteindelijk constructievere ondersteuning zoeken via counseling of belangenbehartiging. Herstel wordt echter vaak belemmerd door maatschappelijke opvattingen die slachtoffers de schuld geven, wat veel voorkomt bij cybercriminaliteit.

Slachtofferbeschuldiging, een belangrijke belemmering voor herstel, vindt zijn oorsprong in maatschappelijke opvattingen en percepties over cybercriminaliteit. Vroege victimologietheorieën, zoals Mendelsohns typologieën uit de jaren 30, gingen ervan uit dat slachtoffers zelf een rol konden spelen in hun slachtofferschap. Hoewel moderne modellen daders over het algemeen verantwoordelijk houden, worden slachtoffers van cybercriminaliteit nog steeds geconfronteerd met maatschappelijke veroordeling, vooral in gevallen van romantische oplichting. Deze veroordeling is vaak gekoppeld aan het idee van een 'rechtvaardige wereld', dat stelt dat de wereld functioneert volgens principes van rechtvaardigheid; daarom moeten slachtoffers wel iets gedaan hebben om het slachtoffer te worden (Lerner, 1980 in Open University, 2024). Toegepast op romantische oplichting impliceert deze denkwijze dat slachtoffers de oplichting hadden kunnen vermijden door offline te blijven of voorzichtiger te zijn, waardoor er een stigma rond hun ervaringen ontstaat (Cross, 2015 in Open University, 2024).

1.4.3 Psychologische revalidatie van het slachtoffer van een liefdesoplichting

Romantische oplichting laat diepe psychologische en emotionele schade achter. Slachtoffers lijden vaak aan een 'dubbel trauma': financieel verlies en het uiteenvallen van wat zij dachten dat een echte relatie was (Cross, 2014; Cross et al., 2018). Studies tonen aan dat bijna twee derde van de slachtoffers van fraude melding maakt van gezondheids- of psychische schade die lang na de oplichting aanhoudt (Button et al., 2014).

Psychologische gevolgen zijn onder meer acute stress en traumareacties, waarbij sommigen symptomen van PTSS ontwikkelen, zoals intrusieve herinneringen, flashbacks, nachtmerries en hyperwaakzaamheid (Coluccia et al., 2020). Depressie, schaamte en zelfverwijt komen vaak voor.

Slachtoffers vragen zich vaak af hoe ze "zo naïef hadden kunnen zijn" (Whitty, 2018). Velen ontwikkelen ook blijvende vertrouwensproblemen, twijfelen aan hun eigen oordeel en hebben moeite met het aangaan van nieuwe relaties (Rege, 2019 in Pietilä & Korhonen, 2024). Slachtoffers trekken zich vaak sociaal terug en omarmen gevoelens van isolatie en vernedering (Whitty & Buchanan, 2012). De lange weg naar herstel vereist een meerlagige ondersteuning:

- Traumagerichte counseling, met name cognitief-gedragsmatige en rouwgerichte benaderingen, is effectief gebleken in het helpen van slachtoffers om hun ervaringen te herinterpreteren en zelfverwijt te verminderen (Against Scams, 2024).
- Lotgenotengroepen bieden een veilige omgeving waar overlevenden ervaringen kunnen delen, emoties kunnen erkennen en hun veerkracht kunnen herstellen (AARP, 2021). Online gemeenschappen gaan ook isolatie tegen door verbinding en normalisering te bieden (AARP, n.d.).
- Inzicht in de relationele en manipulatieve tactieken die oplichters gebruiken, helpt slachtoffers om de schuld van zich af te schuiven en hun zelfvertrouwen terug te winnen (Coluccia et al., 2020).
- Sociale, financiële en maatschappelijke diensten, variërend van juridisch advies tot training in digitale beveiliging, helpen bij het herstel door controle en zeggenschap terug te geven (Pietilä & Korhonen, 2024).

Hoewel herstel geleidelijk verloopt, melden slachtoffers vaak posttraumatische groei zodra schaamte wordt aangepakt en er ondersteunende netwerken zijn (Cross et al., 2018; Whitty, 2018).

Ondersteuning met zorg: goede praktijken voor docenten

Co-funded by
the European Union

Salma Alaaelden

Salma is projectassistent en onderzoeker bij EUth Wonders e.V. en heeft een sterke achtergrond in economie en meer dan zes jaar ervaring in jongerenwerk en projectmanagement. Ze heeft samengewerkt met organisaties wereldwijd en bijgedragen aan initiatieven die jongeren sterker maken en interculturele dialoog bevorderen. Salma heeft bijgedragen aan veel onderzoek naar mentale gezondheid en heeft als trainer workshops over mentaal welzijn gegeven in het kader van haar projecten. Bij EUth Wonders e.V. speelt ze een sleutelrol in het ontwerpen, coördineren en uitvoeren van Erasmus+ en andere internationale projecten. Ze werkt gedurende de volledige projectcyclus en zorgt ervoor dat activiteiten betekenisvol, inclusief en in lijn met onze missie zijn: jongeren over de grenzen heen met elkaar verbinden en hun vaardigheden en kansen verbeteren.

2 GOEDE PRAKTIJKEN VOOR ONDERWIJZERS

2.1 Omvang van dit hoofdstuk

Omdat romantische en liefdesfraude gericht op ouderen een snelgroeiende vorm van cybercriminaliteit in Europa is, met enorme sociale en financiële verliezen en psychische gevolgen zoals sociaal isolement, uitbuiting van emotionele kwetsbaarheden en financiële schade tot gevolg, is de rol van onderwijzers en jongerenwerkers cruciaal om senioren te beschermen tegen liefdesfraude door sociale ondersteuning te bieden, psychische kwetsbaarheid te beheersen en duidelijke paden voor deze senioren te creëren.

Gezien het belang van de rol van jongerenwerkers en opvoeders, biedt dit uitgebreide hoofdstuk de nodige informatie om de psychologische kwetsbaarheden te begrijpen die slachtoffers vatbaar maken voor oplichting, de emotionele en psychologische gevolgen van liefdesoplichting, en zal het opvoeders tevens voorzien van de kennis en instrumenten om sociale en psychologische ondersteuning te bieden aan ouderen die kwetsbaar zijn voor liefdesoplichting door middel van preventieve en reactieve maatregelen, en om hen nuttige informatie te verschaffen in geval van oplichting, en om ondersteuningsnetwerken op te zetten om een veilige en vertrouwde omgeving voor ouderen te creëren.

2.1.1 Belangrijkste doelstellingen en benaderingen van dit hoofdstuk:

Dit hoofdstuk richt zich op een aantal belangrijke doelstellingen die erop gericht zijn senioren en hun ondersteuningsnetwerken in staat te stellen oplichting te herkennen, erop te reageren en te voorkomen. De doelstellingen zijn:

1. Het identificeren van psychologische, sociale en situationele kwetsbaarheden: Inzicht in de factoren die ouderen bijzonder kwetsbaar maken voor oplichting, waaronder psychologische, sociale en situationele elementen, zal helpen bij het herkennen van risicofactoren en het nemen van preventieve maatregelen.

1.2. Het bestuderen van de psychologische en emotionele impact van liefdesfraude op slachtoffers: Het analyseren van de psychologische gevolgen en psychische problemen bij slachtoffers van liefdesfraude zal ons als opvoeders helpen om slachtoffers na de oplichting effectiever te ondersteunen.

3. Praktische voorbeelden van liefdesfraude: Om een uitgebreider inzicht te geven in preventieve maatregelen en reacties op liefdesfraude, worden enkele praktijkvoorbeelden besproken.

Casestudies zullen worden toegelicht en geanalyseerd.

4. Inzicht in de belangrijke rol van jongerenwerkers en opvoeders: In dit onderdeel worden de verschillende factoren uitgelegd die de noodzaak van opvoeders benadrukken bij het ondersteunen van ouderen die gevoelig zijn voor oplichting in de liefde.

5. Richtlijnen voor docenten over preventieve maatregelen om senioren te beschermen tegen liefdesfraude: Het identificeren van de verschillende preventieve maatregelen die docenten kunnen nemen om ervoor te zorgen dat senioren zich bewust zijn van de risico's van liefdesfraude en om te voorkomen dat ze er slachtoffer van worden.

5. Richtlijnen voor docenten over het herkennen van oplichting: In dit onderdeel wordt uitgelegd hoe oplichting kan worden herkend aan de hand van gedragsindicatoren en signalen van slachtoffers, en hoe oudere slachtoffers in dergelijke gevallen kunnen worden ondersteund.

6. Stapsgewijze begeleiding bij het reageren op oplichtingsincidenten: Een duidelijk en concreet stappenplan aanbieden voor senioren en mantelzorgers om te volgen wanneer ze met oplichting te maken krijgen, zodat ze weten hoe ze de situatie effectief kunnen melden en afhandelen.

7. Het opzetten van langetermijnondersteuningsnetwerken: Het creëren en versterken van doorlopende ondersteuningssystemen die senioren kunnen helpen voorkomen dat ze in de toekomst slachtoffer worden van oplichting, door middel van voorlichting, waakzaamheid en contacten binnen de gemeenschap.

8. Onderwijzers en senioren in contact brengen met essentiële hulpmiddelen: Onderwijzers, senioren en hun verzorgers voorzien van de nodige middelen en instrumenten voor herstel en bescherming, zodat zij toegang hebben tot informatie en ondersteuning om zich te beschermen tegen oplichting.

9. Praktische casestudies: Dit onderdeel is een praktische oefening met verschillende hypothetische casestudies die docenten moeten analyseren en uitleggen hoe ze in elke situatie moeten handelen om oudere slachtoffers te ondersteunen.

Deze doelstellingen helpen senioren om geïnformeerd, beschermd en weerbaar te blijven tegen oplichting, waardoor zowel hun onmiddellijke als hun langetermijnveiligheid gewaarborgd is.

2.1.2 Benaderingen

De educatieve focus van dit hoofdstuk benadrukt een tweeledige aanpak om senioren te beschermen tegen romantische oplichting. Ten eerste zullen preventieve maatregelen zich richten op het voorlichten van ouderen en hun mantelzorgers over veelvoorkomende oplichtingstactieken, en hen voorzien van de digitale vaardigheden en sociale ondersteuning die ze nodig hebben om frauduleuze praktijken te herkennen en te vermijden.

Ten tweede biedt Responsive Actions duidelijke protocollen voor interventie en ondersteuning wanneer er zich een oplichting voordoet. Het begeleidt docenten bij elke stap, van de eerste documentatie en melding tot hulpmiddelen voor emotioneel en financieel herstel.

2.2 Psychologische en sociale kwetsbaarheid herkennen

Er is weinig hulp en ondersteuning voor oudere slachtoffers vóór, tijdens en na een oplichting. Dit maakt het niet alleen moeilijk voor oudere slachtoffers om tijdig professionele hulp te krijgen na online oplichting, maar verhoogt ook het risico dat ze daarna opnieuw het slachtoffer worden van een liefdesfraude, waardoor de sociale, psychologische en financiële schade nog groter wordt.

Voordat we ingaan op de verschillende maatregelen om ouderen die slachtoffer zijn geworden van oplichting te voorkomen of hen te ondersteunen, en de noodzaak hiervan, is het belangrijk om eerst de risicofactoren te begrijpen die ouderen vatbaarder maken voor oplichting. Dit is cruciaal voor opvoeders, verzorgers en gemeenschapsleiders, omdat het herkennen van deze factoren vroegtijdige en effectieve interventie mogelijk maakt en de kans biedt om preventieve maatregelen te nemen voordat ouderen slachtoffer worden van fraude.

Een verscheidenheid aan psychologische, sociale en situationele factoren draagt bij aan de kwetsbaarheid van ouderen, die vaak door oplichters wordt uitgebuit. Deze factoren omvatten onder andere sociaal isolement, cognitieve achteruitgang en emotionele behoeften.

Sociale onthouding:

Een van de belangrijkste factoren die ouderen vatbaarder maken voor oplichting, is sociaal isolement. Veel ouderen hebben weinig sociaal contact, wat kan leiden tot gevoelens van eenzaamheid en verveling. In sommige gevallen zoekt deze isolatie gezelschap of emotionele verbondenheid via online platforms. Oplichters, die zich bewust zijn van deze behoefte, gebruiken vaak de schijn van online relaties om deze mensen te misleiden. Ze bouwen vertrouwen en emotionele banden op om hen te manipuleren. Na verloop van tijd kan het slachtoffer ertoe worden overgehaald om geld over te maken of persoonlijke informatie te verstrekken. Het bestrijden van isolement door regelmatige sociale interactie te stimuleren en ondersteunende netwerken op te bouwen, is essentieel om dergelijke uitbuiting te voorkomen.

Cognitieve achteruitgang en vatbaarheid voor oplichting:

Naarmate mensen ouder worden, kunnen ze cognitieve achteruitgang ervaren, waaronder geheugenverlies, moeite met het verwerken van nieuwe informatie en een verminderd vermogen om weloverwogen beslissingen te nemen. Deze cognitieve beperkingen kunnen het voor senioren moeilijk maken om waarschuwingssignalen van oplichting te herkennen, zoals ongevraagde telefoontjes, phishing-e-mails of frauduleuze beleggingsconstructies. Cognitieve achteruitgang kan ook het vermogen van een senior om de gevolgen te begrijpen van het delen van persoonlijke of financiële informatie met vreemden verminderen. Daarom is het essentieel dat opvoeders en verzorgers aandacht besteden aan de cognitieve gezondheid van een senior en strategieën aanbieden om waarschuwingssignalen te herkennen en risicovolle situaties te vermijden. Regelmatige mentale oefeningen, routinematige controles en het gebruik van betrouwbare technologie kunnen allemaal helpen bij het behouden van cognitieve functies en het voorkomen van oplichting.

Emotionele behoefte:

Emotionele kwetsbaarheid is een andere belangrijke factor die oplichters uitbuiten. Senioren kunnen te maken krijgen met diverse emotionele uitdagingen, zoals verdriet, het verlies van een partner of gevoelens van eenzaamheid. Deze emoties kunnen ertoe leiden dat ze actief op zoek gaan naar nieuwe relaties of bevestiging, wat een ideale gelegenheid is voor oplichters die misbruik maken van emotionele behoefte. Oplichters kunnen zich voordoen als potentiële partners en genegenheid, gezelschap of een gevoel van verbondenheid beloven. Helaas kunnen deze vormen van oplichting leiden tot financiële verliezen, omdat senioren gemanipuleerd kunnen worden om geld over te maken of andere vormen van steun te bieden. Inzicht in de emotionele toestand van senioren en het bieden van zowel emotionele als sociale steun is essentieel om dit soort oplichting te voorkomen. Toegang bieden tot rouwbegeleiding, steungroepen en andere sociale voorzieningen kan de emotionele kwetsbaarheid die oplichters uitbuiten, helpen verminderen.

Vertrouwen in de natuur (goedgelovigheid):

Uit diverse onderzoeken blijkt dat mensen met een hoge mate van vertrouwen vaker slachtoffer worden van liefdesfraude. Veel senioren, vooral degenen die periodes van vertrouwen en stabiliteit hebben meegemaakt, zijn van nature meer vertrouwend, wat door oplichters kan worden uitgebuit. Oplichters spelen vaak in op de wens van senioren om aardig en behulpzaam te zijn, bijvoorbeeld via een zogenaamd goed doel of een vermeende dringende financiële behoefte. Senioren stellen de intenties van de persoon met wie ze communiceren vaak niet in vraag, waardoor ze een gemakkelijk doelwit zijn voor financiële fraude. Het is daarom belangrijk om een gezonde dosis scepsis te stimuleren en senioren te adviseren om altijd verzoeken om geld of persoonlijke informatie te controleren, zelfs als deze afkomstig zijn van een betrouwbare bron.

Het raadplegen van ogenschijnlijk bekende bronnen is een belangrijke preventieve maatregel.

Samenvattend zijn bovenstaande factoren enkele van de redenen waarom ouderen vatbaarder zijn voor oplichting. Het is belangrijk om te weten dat er voor oplichting meestal niet slechts één kwetsbaarheid bestaat, maar eerder een samenspel van psychologische, cognitieve en sociale kwetsbaarheden die de omstandigheden creëren voor uitbuiting. Deze omstandigheden zijn ernstig en vormen belangrijke risicofactoren die de kans vergroten om doelwit te worden en te worden gemanipuleerd.

2.3 De psychologische impact van liefdesfraude op slachtoffers

Liefdesfraude veroorzaakt schade die verder gaat dan financieel verlies. Het leidt vaak tot diepgaand emotioneel leed, langdurige psychische problemen en sociaal isolement. Onderzoek wijst consequent uit dat dit type fraude tot de meest schadelijke en ingrijpende vormen van oplichting behoort, met name voor ouderen, omdat slachtoffers tot wel tien jaar na de gebeurtenis nog steeds psychologische gevolgen kunnen ondervinden, zoals schaamte, onzekerheid en trauma.

Hieronder staan de verschillende psychologische en andere gevolgen waaraan ouderen kunnen worden blootgesteld in geval van een liefdesoplichting.

✦ Dubbel trauma: emotioneel en financieel verlies

Romantische fraude bestaat doorgaans uit wat omschreven kan worden als een "dubbele klap": het emotioneel verraad van een vermeende intieme relatie, gecombineerd met financiële uitbuiting. Deze oplichtingspraktijken spelen zich vaak over maanden af, waarin de oplichter een overtuigend emotioneel verhaal opbouwt en het vertrouwen van het slachtoffer wint. De impact van fraude is dan ook niet alleen financieel verraad, maar ook diepgaande psychologische schade. Slachtoffers ervaren een diep gevoel van verlatenheid, manipulatie en identiteitsverwarring, wat leidt tot emotioneel trauma dat vaak nog verwoestender is dan het financiële verlies.

Empirische bevindingen tonen aan dat financiële slachtoffers aanzienlijk meer emotionele stress ervaren dan niet-financiële slachtoffers, en dat liefdesfraude de vorm van oplichting is met de grootste emotionele impact. Veel slachtoffers ervaren bovendien emotioneel misbruik, met name wanneer de manipulatie langdurig was en gebaseerd op intiem vertrouwen. In deze gevallen leidt het plotselinge verlies van de 'relatie' vaak tot symptomen van een aanpassingsstoornis of trauma-gerelateerde aandoeningen.

Schaamte en schuld

Na een oplichting geven oudere slachtoffers zichzelf vaak de schuld dat ze zijn bedrogen en beschouwen ze de oplichting vaak als een persoonlijk falen. Schaamte vormt een sterke barrière om hulp te vragen, zelfs aan hun naasten. Volgens een onderzoek vermijden veel slachtoffers het om familie, vrienden of professionals te vertellen wat er is gebeurd uit angst voor afwijzing of spot. Deze reactie kan gevoelens van waardeloosheid versterken en het emotioneel herstel vertragen. Daarom is de rol van de begeleider zo belangrijk: slachtoffers geruststellen, hun vertrouwen winnen, hen het gevoel geven dat ze gezien worden en hen ondersteunen bij het nemen van actie tegen de oplichting.

Depressie en angst

Veel slachtoffers melden symptomen van klinische depressie, waaronder hopeloosheid, slaapstoornissen en een laag energieniveau. Angst komt vaak voor, vooral met betrekking tot financiën, privacy of publieke aandacht. Deze effecten worden versterkt wanneer het slachtoffer al bestaande emotionele kwetsbaarheden heeft, zoals verdriet of eenzaamheid. Deze symptomen zijn niet van tijdelijke aard, aangezien studies wijzen op langdurige psychische schade en een verhoogde behoefte aan psychosociale ondersteuning.

Sociale terugtrekking

Na de onthulling kunnen oudere slachtoffers zich uit schaamte afzonderen van leeftijdsgenoten en de gemeenschap. Sommigen verbreken de banden met mensen die de relatie in twijfel trokken of waarschuwden toen ze wisten van de nep-'relatie'. Deze isolatie en het verlies van vertrouwen strekken zich uit tot zowel persoonlijke als institutionele relaties, wat bijdraagt aan een diepere eenzaamheid en het risico op herhaald slachtofferschap.

Emotionele gehechtheid en rouw

Slachtoffers ontwikkelen vaak een sterke psychologische band met de verzonnen persoonlijkheid van de oplichter, gebaseerd op de relatie die ze online met hem of haar hebben opgebouwd vóór de oplichting. Wanneer de misleiding aan het licht komt, ervaren velen verdriet dat vergelijkbaar is met het verlies van een romantische partner. Slachtoffers beschrijven de oplichter als hun 'ideale partner' of 'emotionele steun' – zelfs als de relatie volledig online was. Sommige slachtoffers melden een gevoel van rouw dat intenser is dan het daadwerkelijke financiële verlies. Dit komt door de lovebombing, valse huwelijksbeloftes en constante emotionele bekrachtiging die tijdens de manipulatiefase werden gebruikt.

Verlies van eigenwaarde en zelfvertrouwen

Veel slachtoffers melden een verminderd gevoel van eigenwaarde en competentie na de oplichting. Het verraad ondermijnt vaak hun zelfvertrouwen bij het nemen van beslissingen en vergroot hun afhankelijkheid van anderen. Deze machteloosheid kan leiden tot emotionele kwetsbaarheid op de lange termijn en terughoudendheid om nieuwe relaties aan te gaan of leermogelijkheden te benutten, evenals twijfels over hun identiteit en sociale rol.

Angst voor oordeel en het vermijden van openbaarmaking

Door het maatschappelijke stigma zijn slachtoffers vaak terughoudend om de oplichting te melden of emotionele steun te zoeken. Degenen die het wel melden, ervaren vaak weinig begrip, wat schuldgevoel en schaamte alleen maar versterkt. Deze negatieve reacties leiden tot verder isolement, wat bijdraagt aan het niet melden van oplichting en de toegang tot hulpverlening beperkt. Daarom is de rol van de opvoeders essentieel om een oordeelvrije omgeving te creëren die openheid en vroegtijdige interventie bevordert.

Risico op herhaalde victimisatie

Slachtoffers die de oplichting niet herkennen of accepteren, vooral degenen die waarschuwingen negeren vanwege hun goedgelovigheid, lopen een groter risico om opnieuw het doelwit te worden. Deze herhaalde slachtofferschap hangt samen met emotionele ontkenning en het aanhoudende geloof dat de oplichter oprechte bedoelingen had.

Dit wordt nog verergerd wanneer slachtoffers waarschuwingen van derden negeren. Daarom moeten docenten in staat zijn om deze overtuigingen op een voorzichtige manier aan te pakken, terwijl ze tegelijkertijd vertrouwen en steun blijven bieden.

Fysieke en mentale gezondheid achteruit

In ernstige gevallen uit psychische stress zich fysiek, waarbij slachtoffers melding maken van hoofdpijn, slaapstoornissen, paniekaanvallen of verergering van chronische ziekten. Sommigen krijgen suïcidale gedachten, vooral degenen die zich niet in een ondersteunende omgeving bevinden, geconfronteerd worden met schaamte en schuldgevoelens vanuit hun naasten en ervoor kiezen zich te isoleren.

Financiële schade en afhankelijkheid

Slachtoffers van de liefdesoplichting meldden financiële verliezen variërend van €50 tot meer dan €800.000.

met een gemiddeld verlies tussen €1.000 en €10.000 per geval. Hierdoor lijden veel slachtoffers onder langdurige economische instabiliteit, beperkte toegang tot basisbehoeften en worden ze in sommige gevallen afhankelijk van familie of een uitkering. Sommigen verliezen zelfs hun huis, pensioen of erfenis, wat hun levenskwaliteit permanent kan veranderen.

✦ Psychologische effecten op lange termijn

Lang na de liefdesoplichting bleek dat slachtoffers tot wel tien jaar na het incident nog steeds te maken kunnen hebben met verdriet en trauma door verraad, het vermijden van online communicatie, wantrouwen jegens anderen, verstoorde interpersoonlijke relaties en aanhoudende financiële en emotionele onzekerheid, een laag zelfbeeld en angstgevoelens.

2.4 Praktische voorbeelden van oplichting via de liefdesmarkt:

Na inzicht te hebben gekregen in de impact van de liefdesoplichting en de gedragsmatige en sociale kwetsbaarheden van oudere slachtoffers die potentieel slachtoffer kunnen worden van liefdesoplichting, worden in dit gedeelte enkele praktijkvoorbeelden besproken. Deze voorbeelden illustreren niet alleen de tactieken die oplichters gebruiken, maar ook de emotionele, financiële en psychologische gevolgen voor de slachtoffers. Deze verhalen dienen als waardevolle leermiddelen voor docenten, omdat ze laten zien hoe oplichtingspraktijken zich ontvouwen, hoe je waarschuwingssignalen in de praktijk kunt herkennen en hoe de complexe wisselwerking tussen kwetsbaarheid, vertrouwen en bedrog zich afspeelt. De volgende casestudies zijn gebaseerd op gedocumenteerde incidenten uit Europa en Australië, met de nadruk op hun relevantie voor de gedragsmatige, emotionele en systemische thema's die in de voorgaande secties zijn besproken.

2.4.1 Casestudie 1: Het Franse slachtoffer van een oplichting met een imitator die zich voordeed als een beroemdheid.

Een van de meest in het nieuws gekomen gevallen van romantische oplichting van de afgelopen jaren betrof de 53-jarige Franse vrouw Anne, die voor ongeveer € 830.000 werd opgelicht door een oplichter die zich voordeed als acteur Brad Pitt. Volgens nieuwsberichten en interviews van Euronews en Le Monde begon de oplichting toen Anne via sociale media werd benaderd door iemand die beweerde de moeder van Pitt te zijn. Deze kennismaking escaleerde tot directe online communicatie met een nep-Brad Pitt, ondersteund door door AI gegenereerde foto's, nep-benefietevenementen en ziekenhuisbeelden.

In de loop van meer dan een jaar verdiepte de relatie zich, raakte Anne sociaal geïsoleerd en werd ze steeds wantrouwiger jegens vrienden en familie die de legitimiteit van haar in twijfel trokken.

De romance speelde een rol, en ze maakte geld over om te voorzien in wat zij beschouwde als dringende financiële behoeften in verband met medische rekeningen en geblokkeerde bankrekeningen tijdens Pitts scheiding. De oplichting maakte gebruik van zowel emotionele manipulatie als technologische misleiding, waaronder het gebruik van AI-beelden en gesimuleerde videochats.

Nadat Anna besefte dat ze was opgelicht, kreeg ze te maken met ernstige psychische gevoelens van vernedering, emotionele schending en depressie. Nadat de oplichting publiekelijk aan het licht was gekomen, werd ze online gepest en bespot, wat haar psychische gezondheid verder verergerde.

2.4.2 Casestudie 1: Het Franse slachtoffer van een oplichting met een imitator die zich voordeed als een beroemdheid.

In 2024 ontdekten de Spaanse autoriteiten een internationale oplichter die zich ook voordeed als Brad Pitt en die via sociale media meerdere oudere vrouwen had opgelicht op basis van psychologische profielen.

In dit geval creëerde de oplichter valse identiteiten, compleet met overtuigende verhalen over romantische relaties en zakelijke ondernemingen. Slachtoffers werden overgehaald om te investeren in fictieve filmprojecten of humanitaire initiatieven die zogenaamd door Pitt werden geleid. De vrouwen werden gezamenlijk voor meer dan € 325.000 opgelicht. Onderzoekers traceerden het geld via een complex witwasnetwerk met meerdere zogenaamde 'muilezelrekeningen'. De autoriteiten namen diverse digitale apparatuur, documenten en mobiele apparaten in beslag die werden gebruikt om de oplichting op te zetten en in stand te houden.

Deze casus illustreert twee belangrijke educatieve inzichten. Ten eerste zijn liefdesfraudegevallen steeds vaker het gevolg van georganiseerde criminele netwerken met een transnationaal bereik en digitale mogelijkheden. Ten tweede hebben slachtoffers vaak een diepe emotionele binding met de gefabriceerde relatie, wat hun beoordelingsvermogen kan belemmeren, zelfs wanneer er steeds meer argwaan ontstaat. Dit benadrukt de noodzaak voor docenten om zowel de cognitieve als de emotionele dimensies aan te pakken in programma's ter preventie van fraude.

2.4.3 Casestudie 3: Veronica Watson en de gevolgen van vertrouwen

Veronica Watson, een 59-jarige Australische grootmoeder, werd een internationale zaak nadat ze in 2013 in Brazilië werd gearresteerd voor het onbewust smokkelen van cocaïne. De misleiding begon met een man die ze online had ontmoet en die beweerde hulp nodig te hebben bij het bezorgen van documenten voor een investering. Na maandenlang haar vertrouwen te hebben gewonnen, overtuigde hij haar om...

Ze nam een koffer mee naar Brazilië met daarin 5 kg cocaïne. Veronica werd vervolgens gearresteerd op de internationale luchthaven van São Paulo en bracht meer dan twee jaar in de gevangenis door voordat ze werd vrijgesproken. De rechtbank erkende dat ze slachtoffer was geworden van fraude. De psychische schade was echter onherstelbaar, waaronder aanhoudende angst, sociaal stigma en een verlies van vertrouwen in haar eigen kunnen.

Deze zaak onderstreept de samenhang tussen romantische oplichting en andere vormen van criminele uitbuiting, waaronder drugshandel en witwassen. Het illustreert ook hoe manipulatie slachtoffers niet alleen financieel verlies kan berokkenen, maar ook levensveranderende juridische gevolgen kan opleveren. Vanuit educatief oogpunt laat het zien hoe belangrijk het is om ouderen niet alleen voor te lichten over financiële oplichting, maar ook over "romantiek en liefdesbedrieging" bij criminele activiteiten.

2.4.4 Casestudie 4: De liefdesfraudezaak van Annette Ford

Annette Ford, een 57-jarige vrouw uit Perth, Australië, werd twee keer slachtoffer van liefdesoplichting via verschillende datingplatforms. In totaal verloor ze ongeveer $780.000 – haar volledige spaargeld. De oplichtingspraktijken vonden plaats na haar scheiding, tijdens een periode van emotionele kwetsbaarheid. In beide gevallen toonden de mannen die ze online ontmoette snel genegenheid en deden ze aan 'love bombing', waarna ze beweerden professionals te zijn die tijdelijk in financiële problemen verkeerden vanwege complicaties in het buitenland.

Annette verkocht haar huis, plunderde haar pensioenrekening en leende geld om naar haar oplichters te sturen. Ze raakte vervreemd van haar familie, die het niet eens was met haar beslissingen. Na de oplichting werd Annette dakloos en afhankelijk van een uitkering. De psychische gevolgen waren onder andere depressie, slapeloosheid en paniekaanvallen.

Haar geval laat langdurige gevolgen zien, waaronder economische achterstand, sociaal isolement en ernstig psychisch leed. Het illustreert ook hoe een eerder opgelopen trauma, zoals een scheiding, in combinatie met blootstelling aan oplichting de emotionele kwetsbaarheid kan vergroten. Voor docenten benadrukt dit de noodzaak van traumagerichte preventiestrategieën die rekening houden met de complexe context waarin oplichting plaatsvindt.

2.4.5 Man uit Noord-Ierland opgelicht voor meer dan £200.000

Een ander geval betreft een man uit Noord-Ierland die ook meer dan £200.000 verloor na een vermeende romantische relatie die begon op een datingapp en duurde van 2020 tot 2025.

Hij dacht dat hij een relatie had met een vrouw die hij online had ontmoet, en maakte in twee jaar tijd grote geldbedragen over naar aanleiding van dringend klinkende verzoeken: juridische kosten in verband met het testament van een familielid; medische rekeningen na een auto-ongeluk; en een gemanipuleerde nep-banklink.

Deze oplichting maakte misbruik van zowel emotionele afhankelijkheid als technologische manipulatie. Het slachtoffer verklaarde dat de oplichting zo omvangrijk was dat het zijn leven bijna verwoestte en hem emotioneel en financieel geruïneerd achterliet. Uiteindelijk nam hij contact op met de politie van Noord-Ierland (PSNI), die hielp bij het terugvinden van het geld.

2.4.6 Man uit Wrexham opgelicht voor £25.000

Bovendien werd begin 2024 een 65-jarige man uit Wrexham, Verenigd Koninkrijk, voor ongeveer £25.000 opgelicht nadat hij zich in maart 2023 had aangemeld bij een online datingsite. Hij deed dit uit een gevoel van eenzaamheid en vervreemding van zijn familie. Hij kwam in contact met iemand via de datingsite, die het gesprek vervolgens via WhatsApp voortzette en hem dagelijks benaderde.

Kort daarna vroeg de oplichter om geld voor een aanbetaling om samen een huis te kopen en stuurde het slachtoffer via verschillende adressen geld, Apple-cadeaubonnen, sieraden en een iPhone.

Dit ging zo door tot januari 2021, toen de man aangifte deed bij de politie. Hij was diep geraakt, omdat de emotionele belofte van een "gedeelde toekomst" een centrale rol speelde in zijn betrokkenheid en het verlies. Hem werden telefonische slachtofferhulp aangeboden om de situatie te verwerken.

2.4.7 Conclusies van bovenstaande casestudies en educatieve implicaties

Deze casestudies onthullen zowel de diversiteit aan oplichtingstactieken als de gemeenschappelijke emotionele drijfveren.

en cognitieve patronen die oplichters uitbuiten. Hieruit kan worden geconcludeerd dat, hoewel slachtoffers afkomstig zijn uit diverse sociaaleconomische milieus en landen, ze verenigd zijn door psychologische thema's zoals verdriet, isolatie en geïdealiseerde romantische verhalen. Dit is waar de rol van opvoeders en jeugdwerkers in beeld komt: zij moeten de diepte van de emotionele band die slachtoffers ontwikkelen, de geraffineerdheid van de tactieken van oplichters en de complexiteit van het herstel na slachtofferschap erkennen. Dit herstel omvat niet alleen financiële schade, maar ook een verslechtering van de geestelijke gezondheid en sociaal stigma.

2.5 Praktische voorbeelden van oplichting via de liefdesmarkt:

Op basis van de eerder beschreven informatie over de psychologische kwetsbaarheden van de slachtoffers, de gevolgen en de inzichten uit de bovengenoemde praktijkvoorbeelden, wordt het steeds duidelijker dat deze opkomende en snelgroeiende dreiging van liefdesfraude onder ouderen een gecoördineerde en proactieve aanpak vereist. Als eerstelijnsmedewerkers binnen de gemeenschap, het onderwijs en de sociale infrastructuur spelen onderwijzers en jongerenwerkers een centrale rol. Zij zijn immers bij uitstek geschikt om vroegtijdige waarschuwingssignalen te herkennen, preventieve maatregelen te implementeren en herstel te faciliteren wanneer slachtoffer wordt. Gezien deze belangrijke rol is het daarom van belang om beter te begrijpen waarom onderwijzers en jongerenwerkers betrokken moeten worden, en niet alleen de juridische autoriteiten of de gemeenschap.

2.5.1 Onderwijzers als poortwachters van bewustwording en preventie van oplichting.

Docenten die met ouderen werken, met name in buurthuizen en volwasseneneducatieprogramma's, hebben een groot vermogen om vroege signalen van oplichting te herkennen. Zij zijn vaak het eerste vaste aanspreekpunt voor ouderen buiten de familie, omdat zij in staat zijn om gedragsveranderingen objectief te observeren, niet-bedreigende gesprekken aan te knopen en gestructureerde leeromgevingen te bieden die vroege detectie bevorderen.

Uit onderzoek is gebleken dat ouderen eerder geneigd zijn om oplichtingservaringen te delen met docenten dan met autoriteiten of familieleden, vooral wanneer er een open en ondersteunende relatie bestaat waarin docenten niet oordelen. Dit vertrouwen plaatst docenten in een uitstekende positie om preventieve gesprekken aan te gaan, door te verwijzen naar de juiste instanties en het bespreken van oplichtingservaringen te normaliseren.

Bovendien is uit experimenteel onderzoek gebleken dat educatieve activiteiten zoals anti-oplichtingsspellen en -workshops het bewustzijn van ouderen over oplichting aanzienlijk vergroten, hun vatbaarheid ervoor verminderen en hun zelfvertrouwen in het herkennen van oplichtingstactieken vergroten. Ook hun digitale geletterdheid verbetert, waardoor ze minder afhankelijk worden van nep-interacties online. Deze educatieve strategie wordt bovendien beschouwd als de meest effectieve vroegtijdige interventiestrategie tegen financiële uitbuiting. Daarnaast kunnen docenten fungeren als cognitieve steunpilaren, met name voor mensen die in een vroeg stadium cognitieve achteruitgang ervaren, door het geheugen, het oordeelsvermogen en het kritisch denken te versterken via regelmatige interactie. Dit benadrukt het vermogen van educatieve formats en docenten om zowel het gedrag als de denkwijze van oudere leerlingen te beïnvloeden.

2.5.2 Jeugdwerkers als brug naar digitale veiligheid en empathie

Jeugdwerkers spelen een cruciale rol bij het bevorderen van leren tussen generaties. Ouderen missen vaak digitale geletterdheid, een belangrijke risicofactor bij oplichting via datingapps. Door middel van mentorschap kunnen begeleiders ouderen leren hoe ze nepaccounts kunnen herkennen, verdachte berichten kunnen melden en hun online privacyinstellingen kunnen beheren. Belangrijk is dat deze uitwisseling ook de emotionele veerkracht versterkt door sociale inclusie en een gedeeld doel – beide factoren verminderen de kwetsbaarheid voor oplichting.

Onderzoek benadrukte ook dat preventieve maatregelen educatieve programma's moeten omvatten die zijn afgestemd op de kwetsbaarheden van oudere bevolkingsgroepen. Dit houdt onder meer in dat docenten moeten worden opgeleid om niet alleen informatiegebrek, maar ook emotioneel trauma en cognitieve dissonantie als gevolg van blootstelling aan oplichting aan te pakken.

2.5.3 Professioneel vertrouwen en toegang tot het systeem

Docenten bekleden vaak een vertrouwenspositie waardoor ze slachtoffers kunnen aanmoedigen om gevoelige informatie te delen die ze anders misschien niet aan familie of autoriteiten zouden vertellen, zonder zich daarvoor te hoeven schamen of schuldig te voelen. Dit plaatst docenten in een machtige positie, nadat ze een veilig netwerk hebben opgezet, om slachtoffers te begeleiden bij het doen van aangifte, samen te werken met de politie en juridische bijstand, en hulp in te schakelen voor geestelijke gezondheidszorg en financieel herstel.

De opvoeders hebben ook een institutioneel bereik via partnerschappen met bibliotheken, gezondheidscentra, kerken en seniorenverenigingen. Deze contacten kunnen worden ingezet om ouderen te bereiken en hen te ondersteunen bij dergelijke oplichtingspraktijken door middel van preventieve en reactieve maatregelen.

2.5.4 Jeugdwerkers als instrumenten voor intergenerationele empowerment

Jeugdwerkers worden vaak over het hoofd gezien in discussies over de bescherming van ouderen, terwijl hun rol juist essentieel is voor het bevorderen van digitale veiligheid en sociale verbondenheid. Jeugdwerkers fungeren primair als opvoeders die zich richten op het stimuleren van groei en verandering. Dit sluit nauw aan bij de behoeften van ouderen die zich een weg banen in de onbekende wereld van online relaties. Onderzoek heeft bovendien aangetoond dat intergenerationele programma's, waarbij ouderen worden gekoppeld aan jongere digitale mentoren, veelbelovende resultaten laten zien in het verhogen van de detectie van oplichting, het vergroten van het vertrouwen in online tools en het verminderen van sociaal isolement – een van de belangrijkste risicofactoren voor romantische oplichting. Jeugdwerkers faciliteren deze interacties en geven tegelijkertijd het goede voorbeeld door gezonde digitale grenzen te stellen en kritisch te kijken naar online identiteiten.

2.5.5 Het belang van training en structurele ondersteuning

Onderwijzers en jeugdwerkers beschikken over instrumenten en training die nuttig zijn bij het adequaat ondersteunen van ouderen. Dit omvat:
Kennis over oplichtingstypen, manipulatietactieken en gedragssignalen.
Toegang tot checklists, digitale hygiënegidsen en verwijssjablonen.
Samenwerking met de politie, aanbieders van geestelijke gezondheidszorg en instanties voor financiële bescherming van ouderen.
Instrumenten voor anonieme meldingen en een verwijzingsprocedure.
Op basis van bovenstaande elementen is het duidelijk dat in onze snel veranderende wereld de rol van docenten bij het ondersteunen van slachtoffers of potentiële slachtoffers van liefdes- en romantische oplichting niet alleen belangrijk, maar ook noodzakelijk is. Zij hebben immers een grote invloed op de toepassing van verschillende preventieve en reactieve maatregelen, zoals verderop in dit hoofdstuk zal worden toegelicht.

2.6 Preventieve maatregelen om senioren te beschermen tegen oplichters

Om senioren effectief te beschermen tegen mogelijke liefdesfraude, is het essentieel om preventieve maatregelen te nemen die de kans verkleinen dat ze slachtoffer worden van dergelijke praktijken. Door senioren de tools en kennis te bieden die ze nodig hebben om oplichting te herkennen en te vermijden, een ondersteunende sociale omgeving te creëren en de vaardigheden van de slachtoffers te verbeteren, kunnen we hun risico om slachtoffer te worden aanzienlijk verlagen. Deze maatregelen omvatten het bevorderen van digitale geletterdheid en het stimuleren van sociale contacten, die beide een cruciale rol spelen bij het helpen van senioren om hun weg te vinden in een wereld die steeds meer afhankelijk is van technologie en persoonlijke netwerken.

2.6.1 Bewustwording van digitale geletterdheid

Een van de belangrijkste preventieve maatregelen voor senioren is het verbeteren van hun digitale geletterdheid. Naarmate de technologie zich ontwikkelt, passen oplichters hun methoden voortdurend aan door rollenspellen te creëren met verschillende scenario's die lijken op de werkelijkheid. Opvoeders kunnen observeren hoe senioren nepaccounts herkennen, privacyinstellingen begrijpen, waarschuwingssignalen in online situaties opmerken en omgekeerd zoeken naar afbeeldingen. Vervolgens kunnen ze met hen reflecteren door middel van boeiende gesprekken. Door senioren in realistische situaties te plaatsen, kunnen ze hun opgedane kennis in de praktijk toepassen.

Workshops over veelvoorkomende oplichtingstactieken:

Gerichte workshops zijn een effectieve manier om senioren voor te lichten over de meest voorkomende online oplichtingspraktijken waarmee ze te maken kunnen krijgen. Deze workshops moeten de basisprincipes behandelen van het herkennen van phishing-e-mails, nepaccounts op sociale media of datingsites, AI en andere vormen van oplichting, zoals neptelefoontjes naar technische ondersteuning. Docenten moeten zich richten op het geven van praktische voorbeelden van deze tactieken en laten zien hoe oplichters vaak dringende taal, beloftes van beloningen of emotionele argumenten gebruiken om hun slachtoffers te manipuleren. Docenten moeten ook aandacht besteden aan het gebruik van AI en hoe afbeeldingen of teksten die door AI-tools zijn gegenereerd, te vergelijken en te interpreteren. Het doel van deze workshops is om senioren de vaardigheid bij te brengen om waarschuwingssignalen te herkennen en hen het vertrouwen te geven om potentiële oplichting te herkennen.

Praktische training:

Digitale geletterdheid gaat verder dan alleen begrijpen wat oplichting is; het gaat erom senioren de vaardigheden te geven om technologie veilig te gebruiken. Praktische trainingen kunnen senioren leren hoe ze sociale media veilig kunnen gebruiken, inclusief het aanpassen van privacyinstellingen, het verifiëren van de identiteit van mensen die ze online ontmoeten, het herkennen van verdachte links of verzoeken om persoonlijke informatie, en het herkennen van veelvoorkomende gesprekspatronen die oplichters vaak gebruiken. Ze kunnen bijvoorbeeld leren hoe ze een phishing-e-mail kunnen herkennen door het e-mailadres van de afzender te controleren, te zoeken naar spelfouten of verdachte bijlagen te identificeren. Docenten kunnen hen ook leren hoe ze beveiligde websites (met "https://" in de URL) moeten gebruiken en hoe ze kunnen voorkomen dat ze bestanden downloaden van onbetrouwbare bronnen. Daarnaast moeten senioren worden geïnformeerd over hoe ze verdachte activiteiten kunnen melden, of het nu gaat om een frauduleuze e-mail, een oplichtingspoging via de telefoon of een verdacht online profiel. Om deze trainingen effectiever te maken, is het raadzaam dat docenten oefeningen en toepassingsactiviteiten in de training opnemen, zoals het creëren van rollenspellen met verschillende scenario's die lijken op de werkelijkheid, waarbij docenten kunnen observeren wat er misgaat.

De senioren leren nepaccounts te herkennen, privacyinstellingen te begrijpen, verdachte signalen in online situaties op te merken en omgekeerd zoeken naar afbeeldingen uit te voeren. Vervolgens wordt er met hen gereflecteerd door middel van boeiende gesprekken. Door de senioren in vergelijkbare situaties uit het dagelijks leven te plaatsen, kunnen ze hun opgedane kennis in de praktijk toepassen.

Sessies voor gemeenschapsbetrokkenheid:

- Er zouden ook voorlichtingssessies moeten worden aangeboden om voorlichting te geven over de rollen van wetshandhavers, banken en financiële beveiligingsprocedures, cyberbeveiliging en hoe te handelen in geval van een zogenaamde 'love scam', inclusief de bijbehorende procedures. Experts zouden ook moeten worden uitgenodigd voor deze regelmatige voorlichtingssessies. Bovendien zouden sjablonen voor het melden van de verschillende soorten oplichting moeten worden gedeeld. Dit alles kan ook worden opgenomen in gedrukte folders en visuele hulpmiddelen, als geheugensteun en om ouderen gerust te stellen over de volgende stappen in geval van oplichting.

2.6.2 Het bevorderen van sociale verbinding

- Een andere cruciale preventieve maatregel is het bevorderen van sociale contacten. Veel oplichters richten zich op kwetsbare ouderen die zich geïsoleerd of eenzaam voelen. Het creëren van een gemeenschapsgevoel en het stimuleren van sociale interactie helpt ouderen niet alleen om verbonden te blijven, maar biedt hen ook de steun en middelen die ze nodig hebben om te herkennen wanneer er iets niet klopt. Dit kan worden gedaan door middel van groepsgesprekken, bijeenkomsten voor lotgenoten en buddy-systemen.

A. Groepsactiviteiten en een buddy-systeem

Groepsactiviteiten:

Het stimuleren van deelname aan groepsactiviteiten voor senioren kan gevoelens van isolement aanzienlijk verminderen, wat vaak tot kwetsbaarheid leidt. Peer-to-peer clubs, hobbygroepen en online bijeenkomsten zijn uitstekende manieren om senioren samen te brengen, gemeenschappelijke interesses te delen en betekenisvolle relaties op te bouwen. Door regelmatig met anderen in contact te komen, zijn senioren minder vatbaar voor oplichters die misbruik willen maken van hun emotionele of sociale behoeften. Groepsactiviteiten bieden ook een veilige omgeving waar mensen verdachte ervaringen kunnen bespreken, advies van lotgenoten kunnen krijgen en op de hoogte kunnen blijven van mogelijke oplichtingspraktijken in de gemeenschap. Een boekenclub of knutselgroep kan bijvoorbeeld een waardevolle manier zijn om senioren in een sociale omgeving te betrekken, wat zowel mentale stimulatie als sociaal welzijn bevordert.

Buddy-systemen:

Een andere effectieve manier om sociale contacten te bevorderen en isolatie te verminderen, is door middel van buddy-systemen. Door senioren aan elkaar te koppelen voor regelmatige contactmomenten, het delen van ervaringen en het bieden van wederzijdse steun, ontstaat een gevoel van saamhorigheid. Wanneer senioren zich meer verbonden voelen met anderen, is de kans kleiner dat ze slachtoffer worden van oplichting, omdat ze een vertrouwd persoon hebben om te raadplegen wanneer ze verdachte situaties tegenkomen. Een buddy-systeem biedt senioren ook de mogelijkheid om op de hoogte te blijven van mogelijke oplichtingspraktijken, doordat ze informatie kunnen uitwisselen over recente oplichtingspraktijken of waarschuwingssignalen die ze zijn tegengekomen. Bovendien kan de emotionele steun van een buddy senioren een gevoel van veiligheid geven, waardoor de kans kleiner wordt dat ze gezelschap zoeken bij mogelijk frauduleuze bronnen.

B. Uitbreiding van sociale en emotionele ondersteuning

- Naast groepsactiviteiten en buddy-systemen is het essentieel om een breder ondersteunend netwerk op te bouwen. Lokale buurthuizen, seniorenorganisaties en online groepen gericht op specifieke interesses kunnen senioren helpen een actief sociaal leven te behouden, waardoor de kans op isolatie of emotionele kwetsbaarheid kleiner wordt. Wanneer senioren een sterk sociaal netwerk hebben, zijn ze beter in staat om te gaan met situaties waarin ze zich gemanipuleerd of onder druk gezet voelen, omdat ze kunnen rekenen op de begeleiding van vertrouwde vrienden of familieleden.

- Daarnaast kan het bieden van emotionele steun aan ouderen die rouwen, eenzaamheid ervaren of worstelen met andere emotionele problemen, voorkomen dat oplichters misbruik maken van deze kwetsbaarheden. Rouwbegeleiding, therapiegroepen en mentorprogramma's kunnen allemaal essentieel zijn om ouderen te helpen hun emotioneel welzijn te behouden, waardoor ze minder snel het doelwit worden van oplichters die op zoek zijn naar een makkelijke prooi.

Door inspanningen om digitale geletterdheid te bevorderen te combineren met strategieën om sociale contacten te stimuleren, kunnen senioren beter bestand zijn tegen oplichting en fraude. Onderwijzers, verzorgers en gemeenschapsleiders spelen een cruciale rol bij de implementatie van deze preventieve maatregelen. Of het nu gaat om workshops over digitale veiligheid of om sociale programma's die isolatie tegengaan, deze initiatieven helpen senioren hun onafhankelijkheid en veiligheid te behouden in een wereld die steeds meer afhankelijk is van technologie en sociale interactie. Samen vormen deze preventieve maatregelen een solide basis voor de bescherming van senioren tegen de steeds groter wordende dreiging van oplichting.

2.7 Liefdesoplichting in een vroeg stadium stoppen op basis van gedragsindicatoren die wijzen op mogelijke oplichting:

- Nadat we hebben geleerd welke maatregelen docenten kunnen nemen om te voorkomen dat ouderen in de toekomst slachtoffer worden van oplichting, is het ook de moeite waard om na te denken over de maatregelen die docenten moeten nemen als ze een lopende vorm van liefdesoplichting bij ouderen signaleren. Om dit aan te pakken, zullen we gedragsindicatoren bespreken, waarvan sommige in de bovengenoemde praktijkvoorbeelden aan bod kwamen, om docenten, jongerenwerkers en verzorgers te ondersteunen bij het vroegtijdig herkennen van liefdesoplichting. Vervolgens zullen we enkele beoordelingsinstrumenten en maatregelen bespreken, zodat docenten weten hoe ze moeten handelen als ze een lopende vorm van liefdesoplichting signaleren.

2.7.1 Gedragssignalen die waarschuwen bij oudere slachtoffers

- Het voorkomen van de schade van romantische oplichting vereist niet alleen een breed bewustzijn, maar ook de vroege herkenning van gedrags- en emotionele waarschuwingssignalen die erop wijzen dat iemand mogelijk het slachtoffer wordt van romantische oplichting. Talrijke studies bevestigen dat romantische oplichting doorgaans een gestructureerd proces volgt, van eerste contact, via emotionele manipulatie en financiële werving, tot uiteindelijk sociale isolatie. Elk van deze fasen wordt gekenmerkt door specifieke gedragsveranderingen die, mits correct geïnterpreteerd, kunnen duiden op de noodzaak van tijdige en gerichte interventie. Deze signalen omvatten onder andere de volgende:

Geheimhouding rondom nieuwe online relaties:

- Slachtoffers houden hun communicatie met de oplichter vaak geheim uit angst voor veroordeling of het gevoel dat hun online 'partner' hen verraadt. Dit komt overeen met bevindingen uit onderzoek waaruit blijkt dat slachtoffers bewust vermijden om informatie te delen, vooral wanneer ze emotioneel betrokken zijn.

Plotseling overmatig telefoon- of internetgebruik:

- Slachtoffers neigen ertoe dwangmatig gebruik te maken van digitale communicatie en lijken vaak emotioneel afhankelijk te zijn van berichtenapps of videochats.

Sociale terugtrekking:

- Naarmate het misbruik intensiever wordt, kunnen slachtoffers gemeenschapsevenementen en bijeenkomsten met leeftijdsgenoten gaan vermijden.

- en zelfs familierelaties. Ze kunnen ook defensief reageren op online activiteiten. Uit onderzoek is gebleken dat oplichters er baat bij hebben hun slachtoffers te isoleren van concurrerende invloedsbronnen.

✦ **Verhoogde emotionele toestanden:**

- Slachtoffers kunnen gevoelens ervaren die variëren van euforie (wanneer ze berichten van de oplichter ontvangen) tot angst of verdriet (wanneer de oplichter afwezig is of om geld vraagt). Ook kunnen ze te maken krijgen met plotselinge stemmingswisselingen of gedragsveranderingen. Deze stemmingsschommelingen moeten niet worden afgedaan als algemene stemmingswisselingen, maar moeten worden beoordeeld in de context van nieuwe sociale contacten.

✦ **Onverklaarbare financiële activiteiten:**

- Docenten en familieleden merken mogelijk geldopnames bij geldautomaten, plotselinge overboekingen of verzoeken om hulp bij internationale bankzaken op. Een van de onderzoeken verklaart dat verminderde cognitieve controle en een gebrek aan financiële rekenvaardigheid vaak aan dergelijke transacties voorafgaan.

2.7.2. De rol van de docent bij het opsporen van een lopende oplichting en het ondersteunen van ouderen.

- Opvoeders en jeugdwerkers bevinden zich in een unieke positie om deze vroege signalen te herkennen. In tegenstelling tot familieleden, die mogelijk geen objectief inzicht hebben in de emotionele toestand van de persoon, zijn opvoeders vaak ingebed in gestructureerde groepsomgevingen waar ze veranderingen in de loop van de tijd objectief kunnen observeren. Denk bijvoorbeeld aan ouderen die ongewoon enthousiast worden over een nieuwe online kennis, vaak praten over een geïdealiseerde relatie of zich terugtrekken uit gemeenschapsactiviteiten zoals hierboven beschreven.

Opvoeders moeten een combinatie van observatievermogen en inzicht in gedrag kunnen gebruiken, om onderscheid te maken tussen algemene ouderdomsverschijnselen of stemmingswisselingen. Ze kunnen korte, niet-invasieve screeningsinstrumenten inzetten in groepsverband of tijdens individuele gesprekken. Bij twijfel kunnen opvoeders een individueel gesprek starten door neutrale, open vragen te stellen die confrontatie en schaamte vermijden, zoals: "Heb je je veilig en gerespecteerd gevoeld in je online interacties?" of "Heb je ongebruikelijke verzoeken of gesprekken online opgemerkt?", "Heb je onlangs iemand nieuw online ontmoet?" of "Heeft iemand je om financiële gegevens gevraagd?"

- "Een gunst verlenen of iets geheimhouden?". Deze vragen stellen ouderen in staat om te reflecteren zonder in de verdediging te schieten. Op deze manier creëren begeleiders een sfeer van vertrouwen in plaats van opdringerigheid. Als blijkt dat de oudere niet goed reageert op de vragen, kunnen gesimuleerde scenario's met behulp van geanonimiseerde verhalen of hypothetische personages worden gebruikt. Op deze manier kunnen begeleiders de risico's bespreken en toelichten zonder de persoon direct te confronteren. Deze methode blijkt schaamte te verminderen en reflectief denken te bevorderen.

- Zodra gedragssignalen worden opgemerkt en informatie is bevestigd waaruit blijkt dat ouderen het slachtoffer zijn van oplichting, moeten hulpverleners een zachte triage-aanpak hanteren: betrekken, voorlichten en evalueren. De fase van betrekken richt zich op luisteren en betrokkenheid tonen, terwijl tegelijkertijd wordt benadrukt dat er geen oordeel wordt geveld. De voorlichtingsfase omvat het verstrekken van algemene informatie over online liefdesfraude, bij voorkeur via neutrale formats zoals folders, video's of geanonimiseerde casusbesprekingen. Deze indirecte methode stelt mensen in staat zich te herkennen in de beschreven patronen zonder zich beschuldigd te voelen. De evaluatiefase, die vaak informeel plaatsvindt, omvat het beoordelen of de persoon openstaat voor verder gesprek of ondersteuning, of dat een externe verwijzing nodig is.

Bovendien verbeteren indirecte, groepsgerichte benaderingen de vroegtijdige detectie. Wanneer voorlichting over oplichting wordt geïntegreerd in reguliere programma's, herkennen ouderen eerder manipulatie in hun eigen ervaringen of die van anderen. Ze voelen zich ook gezien en niet alleen, waardoor ze zich minder schamen en meer openstaan voor hulp. Daarnaast zorgt het organiseren van groepsbijeenkomsten en het betrekken van ouderen bij verschillende activiteiten ervoor dat ze zich weer meer verbonden voelen met de gemeenschap en minder met de oplichter, wat er uiteindelijk toe kan leiden dat ze de oplichter verlaten.

Samenvattend moeten docenten vroege gedragsindicatoren niet als geïsoleerde curiositeiten beschouwen, maar als potentiële hulpmiddelen. Door observatievermogen te ontwikkelen, geïnformeerde communicatie te gebruiken en het herkennen van oplichting te integreren, kunnen ze romantische oplichting in een vroeg stadium opsporen en stoppen, voordat er financiële of psychische schade ontstaat.

2.8 Responsieve maatregelen in geval een slachtoffer slachtoffer wordt van een liefdesoplichting

- Na te hebben onderzocht welke maatregelen genomen moeten worden om een liefdesfraude te voorkomen, of wat opvoeders moeten doen om te herkennen of een senior op het punt staat slachtoffer te worden van een dergelijke fraude, en om hen in een vroeg stadium te behoeden voor oplichting, analyseert dit gedeelte de te nemen maatregelen wanneer een senior daadwerkelijk slachtoffer wordt van een liefdesfraude. In dat geval is het essentieel om de situatie met zorg, empathie en een gestructureerde aanpak te benaderen. Deze vormen van oplichting zijn bijzonder schadelijk omdat ze inspelen op de emotionele kwetsbaarheid van senioren, wat vaak leidt tot aanzienlijk emotioneel leed en financieel verlies. Het is belangrijk om snel te reageren en ervoor te zorgen dat de senior zich gesteund en in staat voelt om de nodige stappen te ondernemen om te herstellen van de fraude. Hieronder volgen de maatregelen die genomen moeten worden wanneer een oplichting zich in een laat stadium voordoet:

A. Luister en stel gerust

- De eerste stap bij het aanpakken van een liefdesfraude is om zonder oordeel naar de ervaring van de senior te luisteren. Veel senioren die slachtoffer worden van romantische oplichting voelen zich vaak beschaamd, vernederd of zelfs gekleineerd. Ze hebben mogelijk niet alleen geld, maar ook hun emotionele energie geïnvesteerd in een relatie waarvan ze dachten dat die oprecht was. Het is cruciaal om hun gevoelens te erkennen en hen gerust te stellen dat ze geen schuld hebben. Daarom moeten hulpverleners reageren met een gestructureerde en traumagerichte aanpak die rekening houdt met de waardigheid van het slachtoffer en de psychologische stabilisatie. Een verkeerde aanpak van het moment van onthulling kan namelijk leiden tot hernieuwde traumatisering of verder zwijgen, met name bij senioren die mogelijk al worstelen met digitale uitsluiting en een generatiegebonden wantrouwen jegens autoriteiten.

- Oplichters zijn bedreven in het manipuleren van emoties en het creëren van een vals gevoel van intimiteit, waardoor ouderen gemakkelijk het slachtoffer kunnen worden. Het is daarom belangrijk dat opvoeders de ervaring van het slachtoffer erkennen en op een vriendelijke manier uitleggen dat ze niet alleen zijn en dat veel anderen slachtoffer zijn geworden van soortgelijke oplichting. Verzeker hen ervan dat deze daders criminelen zijn en dat hun emotionele en financiële verliezen een direct gevolg zijn van frauduleuze handelingen, en niet van hun eigen slechte inschatting.

Het tonen van empathie en begrip kan gevoelens van schuld of schaamte verlichten, die een belemmering kunnen vormen om het incident te melden en hulp te zoeken. Laat de oudere weten dat

- Ze hebben uw volledige steun en herstel is mogelijk. Geef ze geen verwijten, ondervraag ze niet en bagatelliseer hun ervaring niet, want dit zal leiden tot diepe emotionele schade en ervoor zorgen dat ze in de toekomst steeds opnieuw in oplichtingstrucs trappen.

B. Documenteer het incident

- Zodra de oudere zich gesteund voelt, is de volgende stap om hem of haar te helpen de details van de oplichting vast te leggen. Het vastleggen van belangrijke informatie zal de politie en consumentenbeschermingsorganisaties helpen bij hun onderzoek. Moedig de oudere aan om de volgende details op te schrijven:

- **Data: Noteer wanneer de oplichting begon, wanneer betalingen werden gedaan en alle andere belangrijke interacties.**
- **Namen gebruikt door de oplichter: De naam/namen die de oplichter heeft gebruikt, ook als deze verzonnen of vals zijn. Dit kan de autoriteiten helpen de oplichter op te sporen.**
- **Verzonden bedragen: Noteer het bedrag dat naar de oplichter is overgemaakt, evenals alle andere financiële transacties en de rekeninggegevens van de oplichter.**
- **Communicatiekanalen: Documenteer hoe de oplichter met de senior communiceerde (bijv. e-mail, telefoongesprekken, sociale media of datingwebsites).**

- Deze documentatie is van essentieel belang, omdat het een duidelijk beeld geeft van de oplichting en als bewijsmateriaal kan dienen bij onderzoeken. Het helpt ook bij het indienen van meldingen bij de bevoegde instanties.

C. Meld het onmiddellijk.

- De volgende cruciale stap is het melden van de oplichting. Snel handelen is essentieel om verder financieel verlies te beperken en het onderzoek te ondersteunen. Begeleid de senior bij het melden van de oplichting aan de relevante instanties, zoals de lokale politie, consumentenbeschermingsorganisaties of de landelijke hotline voor het melden van fraude. Enkele belangrijke instanties waar je een liefdesoplichting kunt melden zijn:

- **Lokale politie: Doe zo snel mogelijk aangifte bij de politie. Bij aanzienlijk financieel verlies kan de lokale politie een onderzoek starten of het slachtoffer doorverwijzen naar de juiste instantie.**

- **Federal Trade Commission (FTC): De FTC is de Amerikaanse overheidsinstantie die verantwoordelijk is voor de bescherming van consumenten. Senioren kunnen oplichting melden via hun website ReportFraud.ftc.gov. De FTC biedt ook waardevolle informatie over hoe men zich in de toekomst tegen oplichting kan beschermen.**
- **Internet Crime Complaint Center (IC3): Senioren die het slachtoffer zijn geworden van oplichters via online platforms (zoals datingwebsites of sociale media) kunnen de oplichting melden bij het IC3, een samenwerkingsverband tussen de FBI en het National White Collar Crime Center. Ga naar IC3.gov voor meer informatie.**
- **Nationale fraudemeldlijn: Landen beschikken over diensten voor het melden van fraude, waarmee autoriteiten de fraudeur kunnen onderzoeken en opsporen. In het Verenigd Koninkrijk kunnen senioren bijvoorbeeld contact opnemen met Action Fraud via ActionFraud.police.uk voor hulp.**
- **Consumentenbeschermingsinstanties: Veel deelstaten of gemeenten hebben consumentenbeschermingsinstanties die zich bezighouden met fraudegevallen. De trainer moet de instantie in zijn of haar land opzoeken en het slachtoffer ernaar doorverwijzen. In Duitsland kunnen senioren bijvoorbeeld contact opnemen met de Verbraucherzentrale Bundesverband (VZBV), de centrale consumentenbeschermingsinstantie die uitgebreide ondersteuning biedt aan slachtoffers van fraude, waaronder juridische sjablonen, adviesgesprekken en richtlijnen voor digitale veiligheid. Op Europees niveau kunnen slachtoffers grensoverschrijdende digitale fraude melden via het European Consumer Centres Network (ECC-Net) of transnationale klachten indienen via de EUROPOL-interface voor internetcriminaliteitsmeldingen.**
- **Financiële instellingen en banken: Meld de oplichting bij de lokale bank waarvandaan het slachtoffer het geld naar de oplichter heeft overgemaakt. Dit helpt bij het traceren van de overdracht en mogelijk bij het melden ervan, zodat het slachtoffer zijn geld terugkrijgt.**
- **Psychologische ondersteuningscentra: slachtoffers moeten ook worden doorverwezen naar organisaties die psychologische begeleiding, slachtofferhulp en begeleiding bij rechtszaken bieden. In Duitsland kunnen ze bijvoorbeeld terecht bij Weißer Ring, de grootste organisatie voor slachtoffers van misdrijven in Duitsland, die gratis psychologische ondersteuning biedt. Bovendien kunnen grensoverschrijdende zaken met internationale oplichters worden gemeld bij het OLAF (Europees Bureau voor Fraudebestrijding) of via de Europese Financiële en**

1. Economisch misdaadcentrum (EFECC) voor mogelijke internationale opsporing.

- Door de oplichting direct te melden, beschermen senioren zichzelf niet alleen tegen verdere verliezen, maar helpen ze de politie ook bij het opsporen van oplichters en voorkomen ze dat anderen slachtoffer worden van soortgelijke vormen van oplichting.

2.9 Het opzetten van langetermijnsteunnetwerken:

- Nadat de oudere slachtoffers geholpen zijn bij het melden van de oplichters, is het cruciaal om de slachtoffers in de weken en maanden na de melding te blijven volgen. Studies tonen aan dat veel ouderen te maken krijgen met secundaire victimisatie, zoals afwijzing, ongeloof of spot van familie of de gemeenschap. Dit kan het trauma verergeren en leiden tot langdurig isolement, herhaalde victimisatie of posttraumatische stressstoornis. Daarom is emotionele revalidatie, sociale re-integratie en empowerment op de lange termijn van essentieel belang. Onderwijzers en jongerenwerkers spelen in deze fase een cruciale rol door contact te onderhouden en re-integratie in de gemeenschap en emotionele re-integratie te bevorderen.

Om dit te bereiken, moeten jongerenwerkers en opvoeders slachtoffers allereerst aanmoedigen om deel te nemen aan steungroepen of door lotgenoten geleide herstelcirkels, waar overlevenden hun ervaringen vertrouwelijk en zonder oordeel kunnen delen. Deze groepen kunnen worden georganiseerd door centra voor volwassenenonderwijs, waar ze werkzaam zijn, of in leeftijdsinclusieve clubs. Dit zal hun isolement verminderen en sociale integratie bevorderen, aangezien onderzoek heeft aangetoond dat ouderen die na een oplichting deelnemen aan gestructureerde lotgenotengroepen een aanzienlijk verbeterde psychologische veerkracht en een verminderde kwetsbaarheid voor herhaling van het delict ervaren.

Een ander cruciaal onderdeel is dat docenten follow-up bieden door middel van het inplannen van contactmomenten en voortdurende educatieve ondersteuning. Dit helpt docenten de behoeften van de slachtoffers te begrijpen en geeft hen een gevoel van steun, wat hen zal helpen emotioneel te herstellen en weer sociaal actief te worden. Het is ook belangrijk om te benadrukken dat in alle fasen van de hulpverlening het leidende principe respect voor de autonomie en waardigheid van het slachtoffer moet zijn. Docenten zijn geen onderzoekers of hulpverleners, maar vertrouwde bondgenoten in een herstelproces waarbij mogelijk meerdere professionals betrokken zijn. Hun rol is om de ervaring van het slachtoffer te erkennen, hen weer in contact te brengen met hun eigen kracht en ervoor te zorgen dat ze de nasleep niet in isolement hoeven te verwerken.

- Bovendien kunnen opvoeders slachtoffers aanmoedigen om deel te nemen aan groepstherapie, traumagerichte begeleiding en oefeningen in het reconstrueren van hun levensverhaal, aangezien is aangetoond dat deze bijdragen aan het herstel van identiteit en zelfredzaamheid. In Duitsland kunnen overlevenden bijvoorbeeld via lokale zorgverzekeraars (zoals AOK en TK) of organisaties zoals Weißer Ring, die gespecialiseerde begeleiding bieden bij trauma's als gevolg van criminaliteit, toegang krijgen tot dergelijke diensten. Gemeentelijke seniorencentra en gezondheidsnetwerken kunnen ook dienen als toegangspunten voor niet-stigmatiserende geestelijke gezondheidszorg.

- **Digitale re-integratie is een ander belangrijk element van herstel op de lange termijn. Veel slachtoffers worden bang om opnieuw digitale tools te gebruiken, waardoor hun isolement toeneemt. Docenten en jongerenwerkers kunnen helpen het zelfvertrouwen te herstellen door workshops aan te bieden over digitale herintegratie. Deze workshops zijn ontworpen om online veiligheid, privacyinstellingen, het herkennen van oplichting en communicatiegrenzen aan te leren. Dit is met name effectief om ouderen te helpen op een veilige en ondersteunende manier weer deel te nemen aan de digitale wereld.**

Een ander cruciaal punt is het aanbieden van begeleidings- en informatiepakketten en workshops voor de families en vrienden van deze slachtoffers, waarin open dialoog wordt aangemoedigd en informatie wordt gegeven over hoe te reageren en de ouderen te ondersteunen om hun herstelproces te bevorderen, evenals hoe moeilijke gesprekken te voeren. Dit zorgt voor een omgeving waarin de slachtoffers niet worden beschuldigd of beschaamd, maar juist worden ondersteund.

Ten slotte moet re-integratie ook mogelijkheden bieden voor zelfredzaamheid, waarbij slachtoffers worden aangemoedigd om over hun ervaringen te praten, omdat ze meer vertrouwen genieten van hun medebewoners. Slachtoffers die doorgroeien naar functies als docent, belangenbehartiger of ervaringsdeskundige geven vaak aan een sterker gevoel van controle en herstel te ervaren. Platforms voor de gemeenschap zouden overlevenden ook de mogelijkheid moeten bieden om hun verhalen anoniem te delen via nieuwsbrieven, openbare fora of bewustwordingscampagnes, waardoor persoonlijk leed wordt omgezet in collectieve bescherming. Een dergelijke participatieve herstelaanpak is niet alleen gunstig voor het individu, maar versterkt ook de collectieve waakzaamheid tegen fraude.

Kortom, zelfredzaam herstel is geen lineair proces, maar een circulair proces dat voortdurende emotionele ondersteuning, gestructureerde digitale revalidatie, robuuste institutionele coördinatie en zinvolle sociale participatie vereist. De rol van de docent in dit traject is...

- Het is zowel faciliterend als herstellend, waardoor slachtoffers niet alleen de oplichting achter zich kunnen laten, maar ook een sterker en veerkrachtiger persoon kunnen worden.

2.10 Praktische casestudies

- Op basis van de voorgaande paragrafen over het herkennen van fraude, de psychologische gevolgen, de rol van de opvoeder en interventiestrategieën, worden de volgende praktische scenario's gepresenteerd om opvoeders en jeugdwerkers te helpen de belangrijkste leerdoelen in de praktijk toe te passen. Elk scenario vertegenwoordigt een veelvoorkomende situatie uit de praktijk en wordt vergezeld van reflectievragen om het beoordelingsvermogen, de communicatiestrategieën en de ethische gevoeligheid te toetsen.

2.10.1 Casestudie 1:

- Anna, 71, is de afgelopen maanden behoorlijk actief geworden op Facebook. Tijdens een koffiepauze in de workshop van het buurthuis vertelt ze enthousiast dat ze een "geweldige weduwnaar" heeft ontmoet. "Hij begrijpt me echt," zegt ze, "het is alsof hij precies weet wat ik voel." Ze voegt eraan toe dat hij misschien binnenkort op bezoek komt en dat ze de laatste tijd vragen stelt over internationaal bankieren.

<u>Reflectievragen:</u>
Welke signalen wijzen erop dat Anna gevaar loopt?
Welke specifieke signalen wijzen erop dat Anna kwetsbaar kan zijn voor een romantische oplichting?
Hoe zou je een niet-confronterend, vertrouwenwekkend gesprek aangaan om meer te weten te komen over de oplichter, zonder schaamte op te wekken?
Welke educatieve hulpmiddelen of gespreksstrategieën met leeftijdsgenoten zou je kunnen gebruiken om Anna te helpen kritisch over haar situatie na te denken?
Als Anna voet bij stuk houdt, hoe kun je dan een vangnet creëren zonder haar autonomie te beperken?

2.10.2 Casestudie 2:

- Walter, 78, is de laatste tijd steeds vaker afwezig bij de bijeenkomsten van jullie gespreksgroep voor senioren. Als hij er wel bij is, zit hij stil en vermijdt hij oogcontact. Je merkt dat hij veel aan het sms'en is en zichtbaar angstig. Op een dag hoor je hem zeggen dat hij geld overmaakt om een "vriend" die hij online heeft ontmoet te helpen aan een paspoort, zodat die vriend zich bij hem in Duitsland kan voegen.

- Reflectievragen:
- Welke gedragskenmerken van Walter komen overeen met bekende indicatoren van betrokkenheid bij oplichting?
- Hoe begin je een dialoog die respectvol is, rekening houdt met trauma's en geen defensieve reacties oproept?
- Welke ondersteuningsbronnen of samenwerkingsverbanden zou u kunnen inschakelen (bijv. rechtsbijstand, hulplijnen voor fraude)?
- Hoe kun je Walters waardigheid en autonomie behouden en tegelijkertijd beschermende maatregelen aanmoedigen?

2.10.3 Casestudie 3:

- Je ontvangt een telefoontje van Lara, de dochter van Maria, een van je vaste deelnemers. Lara is overstuur en bezorgd: "Mijn moeder heeft net €5.000 overgemaakt naar een man die ze nog nooit heeft ontmoet! Hij zegt dat hij in het leger zit en in het buitenland gestrand is. Ze denkt dat ze verliefd zijn – het is waanzin!" Lara is woedend en vindt dat haar moeder zich onverstandig gedraagt. Ze wil dat je Maria confronteert en haar ervan overtuigt ermee te stoppen.

Reflectievragen:

Hoe zou je Maria benaderen om haar vertrouwen te behouden en tegelijkertijd voorzichtig haar zorgen ter sprake te brengen?

Welke strategieën uit de traumagerichte zorg zou je kunnen gebruiken om schaamte te verminderen en een veilige ruimte te creëren voor openheid?

Hoe zou je Lara op een ondersteunende, niet-dwingende manier benaderen en haar helpen de emotionele aspecten van dergelijke oplichtingspraktijken te begrijpen?

Welke rol kunt u spelen om beide partijen te helpen een gemeenschappelijke basis te vinden voor herstel en toekomstige bescherming?

Digitale verdediging: basisprincipes van cyberbeveiliging voor beginners

Co-funded by
the European Union

Jim Boelhouwer

Ik ben een ervaren projectmanager en IT-expert met een passie voor continue bijscholing en het behalen van uitstekende resultaten. Met een sterke achtergrond in het managen van complexe projecten en een diepgaand begrip van IT-systemen, brengt Jim een schat aan expertise mee naar elk project dat hij aanpakt.

Ik heb een indrukwekkende staat van dienst in het succesvol leiden en opleveren van prestigieuze projecten in de IT-sector. Mijn uitgebreide ervaring strekt zich uit over diverse domeinen, waaronder softwareontwikkeling, infrastructuurimplementatie en systeemintegratie. Mijn vermogen om effectief multidisciplinaire teams aan te sturen en projectdoelstellingen af te stemmen op de organisatiedoelen heeft er steevast toe geleid dat projecten op tijd en binnen budget worden afgerond.

Co-funded by
the European Union

3 Basisprincipes van cyberbeveiliging voor beginners

3.1 Belangrijke onderdelen van veiligheidsbewustzijn

- In het vorige hoofdstuk werd uitgelegd welke tactieken en methoden criminelen gebruiken om kwetsbare ouderen te benaderen en hen financieel te beroven.

- Een van de manieren waarop deze tactieken en methoden worden misbruikt, is via digitale communicatie. We zijn steeds meer met elkaar verbonden door een gedigitaliseerde wereld. Dit betekent dat kwetsbare ouderen zich bewust moeten zijn van de risico's die dit met zich meebrengt. Het ontvangen van e-mails of het starten van chatgesprekken kan het begin zijn van een proces van financiële oplichting.

Beveiligingsbewustzijn is het begrijpen en herkennen van potentiële cyberdreigingen en de beste werkwijzen voor de bescherming van gevoelige informatie en systemen. Het omvat het voorlichten van mensen over verschillende aspecten van cyberbeveiliging om het risico op beveiligingsinbreuken en gegevensverlies te verminderen. De belangrijkste onderdelen van beveiligingsbewustzijn zijn:

Phishingaanvallen en hoe je ze kunt herkennen
Wachtwoordbeveiliging en sterke authenticatie
Veilig gebruik van verwijderbare media
Social engineering-tactieken
Correct gebruik van sociale media en e-mail
Best practices voor cloudbeveiliging

3.2 Phishingaanvallen en hoe je ze kunt herkennen

- Phishingaanvallen zijn frauduleuze pogingen om gevoelige informatie zoals gebruikersnamen, wachtwoorden, creditcardgegevens of andere persoonlijke gegevens te bemachtigen door zich voor te doen als een betrouwbare partij. Aanvallers gebruiken doorgaans misleidende e-mails, sms-berichten of websites die er legitiem uitzien om ontvangers ertoe te verleiden hun gegevens prijs te geven of op schadelijke links te klikken die leiden tot de installatie van malware. Hieronder vindt u een overzicht van veelvoorkomende soorten phishingaanvallen en hoe u ze kunt herkennen.

A. Phishing-aanvallen

Soorten phishingaanvallen:

E-mailphishing: Dit is een van de meest voorkomende vormen van phishing. Aanvallers gebruiken e-mails om zich voor te doen als vertrouwde organisaties of personen, met als doel ontvangers ertoe te verleiden gevoelige gegevens te delen of op schadelijke links te klikken.

- **Spearphishing: Een meer gerichte variant van phishing waarbij e-mails specifiek op individuen of organisaties zijn afgestemd.**
- **Smishing (sms-phishing): Aanvallers gebruiken sms-berichten met schadelijke links of telefoonnummers om persoonlijke gegevens te verzamelen of apparaten te infecteren met malware.**
- **Vishing (Voice Phishing): Hierbij worden telefoontjes gepleegd waarbij vertrouwde personen worden nagebootst. Dankzij AI-gestuurde stemreplicatie kunnen deze telefoontjes zeer realistisch klinken.**
- **Clone Phishing: Aanvallers maken kopieën van legitieme e-mails en vervangen de originele links door kwaadaardige links.**
- **Pop-up phishing: kwaadaardige pop-ups op websites die het downloaden van malware kunnen activeren of gebruikers naar nepwebsites kunnen doorverwijzen.**
- **Evil Twin Phishing: Aanvallers creëren nep-wifi-hotspots om gegevens te onderscheppen van gebruikers die er verbinding mee maken.**

B. Hoe herken je phishingaanvallen?

- Om ze te herkennen, let dan op ongebruikelijke afzenderinformatie, dringende of dreigende taal, verzoeken om persoonlijke gegevens, verdachte links en bijlagen, en standaard begroetingen. Wees extra voorzichtig met e-mails die te mooi lijken om waar te zijn, zoals aanbiedingen voor gratis producten of diensten.

Verdachte e-mailkenmerken:

Verzoeken om gevoelige informatie (bijv. wachtwoorden, creditcardgegevens)
Dringende of alarmerende berichten die paniek veroorzaken.
Onbekende of licht gewijzigde e-mailadressen van de afzender

- Spelfouten en grammaticale fouten
- Algemene begroetingen in plaats van persoonlijke.

Waarschuwingssignalen met betrekking tot links en bijlagen:
Verkorte of gemaskeerde URL's die de werkelijke bestemming verbergen.
Linktekst en daadwerkelijke URL komen niet overeen (beweeg de muis eroverheen om te controleren).

- **Ongevraagde bijlagen, vooral van onbekende afzenders.**

Waarschuwingssignalen voor de inhoud:
Aanbiedingen die te mooi lijken om waar te zijn (bijv. gratis cadeaubonnen)
Onverwachte accountgerelateerde meldingen of problemen
Verzoeken om accountgegevens te verifiëren of bij te werken via e-mail.

Technische voorzorgsmaatregelen:
Controleer of de URL van een website HTTPS gebruikt, vooral bij gevoelige transacties.
Wees alert op dubbele wifi-hotspots op openbare plaatsen.
Gebruik pop-upblokkers en wees voorzichtig met meldingen van je browser.

Door alert te blijven en deze richtlijnen te volgen, kunt u het risico om slachtoffer te worden van phishingaanvallen aanzienlijk verkleinen. Onthoud dat legitieme organisaties nooit om gevoelige informatie zullen vragen via ongevraagde e-mails of berichten.

3.3 Wachtwoordbeveiliging en sterke authenticatie

- Wachtwoordbeveiliging en sterke authenticatie zijn cruciale onderdelen van cybersecurity in het huidige digitale landschap. Om de bescherming van online accounts en gevoelige informatie te garanderen, is het essentieel om robuuste beveiligingsmaatregelen te implementeren.

3.3.1 Sterke wachtwoorden

- Het aanmaken van sterke wachtwoorden is de eerste verdedigingslinie tegen ongeautoriseerde toegang. Een sterk wachtwoord moet aan de volgende eisen voldoen:
- De tekst moet minimaal 10 tekens lang zijn.
- Gebruik een mix van hoofdletters en kleine letters, cijfers en symbolen.

- Vermijd veelvoorkomende woorden of gemakkelijk te raden woordcombinaties.

- Om een sterk wachtwoord te maken van een zin, kun je verschillende technieken gebruiken. Een populaire methode is om de eerste letter van elk woord in de zin te gebruiken, eventueel aangevuld met cijfers of symbolen, en ervoor te zorgen dat het wachtwoord lang genoeg is.

Hieronder een overzicht van de methoden:

1. Afkortingen:
Neem de eerste letter van elk woord in de door jou gekozen zin.
De zin "Mijn favoriete kleur is blauw" zou bijvoorbeeld "Mfcib" kunnen worden.
Overweeg om cijfers of symbolen toe te voegen om het krachtiger te maken, zoals "Mfcib12!".

2. Vervanging:
Vervang letters door gelijksoortig uitziende cijfers of symbolen (bijv. "a" door "@", "e" door "3").
De zin "Ik hou van katten" zou bijvoorbeeld "1 l0v3 c@ts" kunnen worden.

3. Spelfouten en hoofdlettergebruik:
Spel woorden in je zin opzettelijk verkeerd, of gebruik hoofdletters om een unieke combinatie te creëren.
Bijvoorbeeld, "The quick brown fox" zou "Th3 q!ck bruin f0x" of "ThE qUiCk bRoWn FoX" kunnen worden.

- 4. Technieken combineren:
- Je kunt afkortingen, vervangingen, spelfouten en hoofdletters combineren voor een nog sterker wachtwoord.
- Het gebruik van de zin "Dit is een test" zou bijvoorbeeld kunnen worden veranderd in "T!s!s@t3s7t".

3.3.2 Beste werkwijzen voor wachtwoordbeheer

- Goede praktijken voor een sterk wachtwoordbeleid omvatten het instellen van een minimale wachtwoordlengte, het vereisen van een mix van tekens (hoofdletters, kleine letters, cijfers, symbolen) en het aanmoedigen van het gebruik van wachtzinnen of wachtwoordmanagers. Om de wachtwoordbeveiliging te verbeteren:

Gebruik unieke wachtwoorden voor elk account.
Wijzig je wachtwoorden regelmatig, idealiter elke 3 maanden.
Overweeg het gebruik van een wachtwoordmanager om complexe wachtwoorden veilig op te slaan en te genereren.
Vermijd het delen van wachtwoorden of het gebruik van gemakkelijk te raden gegevens.

3.3.3 Multifactorauthenticatie (MFA)

Sterke authenticatie gaat verder dan wachtwoorden door middel van multifactorauthenticatie (MFA). MFA vereist minstens twee identiteitscomponenten om de identiteit van een gebruiker te verifiëren. Deze componenten omvatten doorgaans:

Iets wat de gebruiker weet (bijv. wachtwoord of pincode)
Iets wat de gebruiker bezit (bijvoorbeeld een smartphone of hardwaretoken).
Iets wat de gebruiker is (bijvoorbeeld biometrische gegevens zoals vingerafdrukken of gezichtsherkenning)

Het inschakelen van MFA (multi-factor authenticatie) voor alle accounts waar mogelijk verhoogt de beveiliging aanzienlijk door een extra beschermingslaag toe te voegen.

3.3.4 Sterke authenticatietechnieken

Sterke authenticatie is erop gericht de identiteit van gebruikers op een robuuste manier te verifiëren en ongeautoriseerde toegang te voorkomen. Enkele belangrijke aspecten van sterke authenticatie zijn:

Niet uitsluitend vertrouwen op gedeelde geheimen of symmetrische sleutels
Het afweren van pogingen tot phishing en identiteitsfraude.
Het gebruik van hardwarematige cryptografische tokens, zoals FIDO-sleutels of smartcards, voor het hoogste beveiligingsniveau.

3.3.5 Voordelen van sterke authenticatie

Het implementeren van sterke authenticatieprocedures biedt verschillende voordelen:

Verbeterde bescherming tegen diefstal van inloggegevens en ongeautoriseerde toegang.

Verminderd risico op succesvolle phishingaanvallen
Verbeterde naleving van wettelijke voorschriften
Verhoogd vertrouwen in gebruikersidentiteiten en de algehele systeembeveiliging.

Door sterke wachtwoorden te combineren met multifactorauthenticatie en de beste werkwijzen te volgen, kunt u uw cyberbeveiliging aanzienlijk verbeteren en gevoelige informatie beschermen tegen potentiële bedreigingen.

3.4 Veilig gebruik van verwijderbare media

Het gebruik van verwijderbare opslagmedia zoals USB-sticks, externe harde schijven, SD-kaarten, enzovoort, is wijdverbreid geraakt vanwege hun compacte formaat en grote opslagcapaciteit. Deze gebruiksvriendelijke eigenschappen maken ze echter ook aantrekkelijke doelwitten voor cybercriminelen die gevoelige informatie willen stelen.

Volgens een onderzoek van IBM Security was menselijke fouten verantwoordelijk voor meer dan 90% van de beveiligingsincidenten met verwijderbare opslagmedia. Veelvoorkomende fouten, zoals het kwijtraken of verkeerd plaatsen van deze apparaten, kunnen leiden tot ongeautoriseerde toegang tot of diefstal van vertrouwelijke gegevens.

Bovendien komen kwaadaardige aanvallen, zoals malware-infecties via besmette USB-sticks, steeds vaker voor.

Volgens Astra Security en DeepStrike worden er dagelijks ongeveer 560.000 nieuwe malwareprogramma's gedetecteerd. Dit cijfer vertegenwoordigt een aanzienlijk aantal, bovenop het toch al enorme aantal malwareprogramma's dat al meer dan 1 miljard bedraagt.

Om ervoor te zorgen dat verwijderbare media veilig gebruikt kunnen worden, dient u deze richtlijnen te volgen:

Gebruik alleen vertrouwde apparaten:

- Sluit nooit gevonden of onbekende verwisselbare media aan op uw computer.

1. Implementeer veiligheidsmaatregelen:

- Installeer en onderhoud actuele antivirussoftware die verwijderbare media actief scant wanneer deze worden aangesloten.

Schakel de functies voor automatisch uitvoeren en afspelen op uw computer uit om te voorkomen dat schadelijke code automatisch wordt uitgevoerd.
Versleutel alle verwijderbare opslagmedia om gegevens te beschermen in geval van verlies of diefstal.
Beveilig verwijderbare opslagmedia met een sterk wachtwoord.

- 3. Ga op de juiste manier met gegevens om:

Houd persoonlijke en werkgerelateerde gegevens gescheiden.
Verwijder gevoelige gegevens na gebruik veilig van verwisselbare media.
Beperk het gebruik van verwijderbare media tot alleen wanneer dit noodzakelijk en toegestaan is.

- 4. Zorg voor fysieke beveiliging:

Laat verwijderbare media nooit onbeheerd achter en berg ze veilig op wanneer ze niet in gebruik zijn.
Schakel onnodige draadloze services zoals Bluetooth en Wi-Fi uit op apparaten.

- 5. Regelmatig onderhoud:

Voer regelmatig scans uit op verwijderbare media om malware op te sporen.
Voer regelmatig controles uit en monitor het gebruik van verwijderbare media om verdachte activiteiten op te sporen.

Door deze richtlijnen te volgen, kunt u de risico's die gepaard gaan met het gebruik van verwijderbare media aanzienlijk verminderen, terwijl u toch profiteert van het gemak en de draagbaarheid ervan.

3.5 Social engineering-tactieken

Social engineering is de psychologische manipulatie van mensen om toegang te krijgen tot vertrouwelijke informatie of om hen ertoe aan te zetten handelingen te verrichten die mogelijk niet in hun eigen belang zijn. Naast de reeds genoemde phishing-tactieken zijn er ook de volgende:

Lokken: iets aantrekkelijks aanbieden (zoals gratis software) dat malware bevat of de beveiliging in gevaar brengt wanneer het wordt gebruikt.
Quid pro quo: het beloven van een voordeel in ruil voor informatie of actie, zoals het aanbieden van gratis IT-ondersteuning die vervolgens malware installeert.
Scareware: het gebruik van angsttactieken om slachtoffers te manipuleren en tot actie aan te zetten, zoals valse viruswaarschuwingen.
Watering hole-aanvallen: het compromitteren van websites die veelvuldig door het doelwit worden bezocht om malware te verspreiden.

In de volgende twee paragrafen gaan we dieper in op twee bekende vormen van social engineering: de romance scam en de pig butchery scam.

3.5.1 Romantische oplichting

Een romantische oplichting is een vorm van bedrog waarbij romantische intenties worden geveinsd, de genegenheid van het slachtoffer wordt gewonnen en vervolgens die goodwill wordt gebruikt om het slachtoffer geld te laten overmaken onder valse voorwendsels of om fraude tegen het slachtoffer te plegen. Frauduleuze handelingen kunnen bestaan uit toegang tot het geld, de bankrekeningen, creditcards, paspoorten, e-mailaccounts of burgerservicenummers van het slachtoffer, of het slachtoffer dwingen om namens hem financiële fraude te plegen. Deze oplichtingspraktijken worden vaak uitgevoerd door fraudenetwerken van georganiseerde criminele bendes die samenwerken om meerdere slachtoffers tegelijk geld af te troeven. De varkensslachtfraude (PBS of PB Scam) is een steeds vaker voorkomende vorm van romantische oplichting, die meestal ook gepaard gaat met de zogenaamde 'high yield investment program' (HYIP)-fraude. We zullen dit soort oplichting in een aparte paragraaf bespreken.

Gestolen afbeeldingen

Oplichters die zich voordoen als iemand die zich voordoet als iemand anders, maken persoonlijke profielen aan met gestolen foto's van aantrekkelijke mensen om anderen te vragen contact met hen op te nemen. Dit wordt vaak catfishing genoemd. Vaak worden foto's van onbekende actrices of modellen gebruikt om het slachtoffer te laten geloven dat ze met die persoon praten. Ook worden er vaak Amerikaanse militairen geïmiteerd, omdat het doen alsof je in het leger dient verklaart waarom de oplichter niet beschikbaar is voor een persoonlijke ontmoeting.

Omdat de oplichters er vaak totaal anders uitzien dan op de foto's die ze naar de slachtoffers sturen, ontmoeten ze de slachtoffers zelden in het echt of zelfs maar via een videogesprek. Ze misleiden hun potentiële slachtoffers met aannemelijk klinkende excuses voor hun onwil om hun gezicht te laten zien, bijvoorbeeld door te zeggen dat ze nog niet kunnen afspreken omdat ze tijdelijk op reis zijn of een kapotte webcam hebben.

Het slachtoffer misleiden

Oplichters zijn er zeer bedreven in om hun slachtoffers te manipuleren – ze sturen liefdesgedichten, spelen seksspelletjes via e-mail en bouwen een zogenaamde 'liefdesrelatie' op met talloze beloftes als 'ooit zullen we trouwen'. Oplichters stellen hun slachtoffers veel vragen, maar delen weinig over zichzelf.

Ze overladen de slachtoffers vaak met complimenten.

Er vindt een communicatieproces plaats tussen de oplichter en het slachtoffer, dat soms maanden of zelfs een heel jaar duurt, totdat de oplichter het gevoel heeft dat hij of zij voldoende band met het slachtoffer heeft opgebouwd om geld te vragen. Oplichters maken misbruik van het valse gevoel van verbondenheid bij het slachtoffer om hem of haar ertoe te verleiden geld over te maken.

Deze verzoeken kunnen gaan over benzinegeld, bus- of vliegtickets om het slachtoffer te bezoeken, medische kosten of studiekosten. Meestal wordt daarbij de belofte gedaan dat de oplichter op een dag bij het slachtoffer in huis zal komen wonen.

Slachtoffers worden soms uitgenodigd om naar het land van de oplichter te reizen; in sommige gevallen komen de slachtoffers aan met gevraagd cadeaugeld voor familieleden of steekpenningen van corrupte ambtenaren, om vervolgens te worden mishandeld, beroofd of vermoord.

De oplichting eindigt meestal wanneer het slachtoffer beseft dat hij of zij wordt opgelicht of stopt met het overmaken van geld. Mensen hebben echter vaak moeite om de realiteit te accepteren, en het stigma dat gepaard gaat met het bezwijken voor dergelijke misleiding kan hen ervan weerhouden om fraude bij de politie te melden. Veel slachtoffers, zelfs wanneer ze met sterk bewijs worden geconfronteerd, kunnen niet geloven dat de persoon die zo liefdevol overkomt in sms-berichten in werkelijkheid een criminele oplichter is. Ze kunnen boos of zelfs gewelddadig reageren op iedereen die bezwaar maakt. Banken kunnen het geld van het slachtoffer blokkeren, vooral wanneer er een vermoeden bestaat van financieel misbruik van een oudere.

Criminele groepen

Criminele netwerken lichten eenzame mensen over de hele wereld op met valse beloftes van liefde en romantiek. Oplichters plaatsen profielen op datingsites, sociale media-accounts die niet specifiek voor dating bedoeld zijn, advertentiesites en zelfs online forums om nieuwe slachtoffers te vinden. De oplichter probeert meestal een meer persoonlijke communicatiemethode te bemachtigen, zoals een e-mailadres of telefoonnummer, om vertrouwen te winnen bij het slachtoffer.

Omdat de oplichters in groepen werken, kan iemand uit de groep op elk moment online zijn en e-mails of sms-berichten naar het slachtoffer sturen. De wisseling tussen verschillende oplichters, die allemaal beweren dezelfde persoon te zijn, is moeilijk te detecteren bij tekstgebaseerde communicatie.

berichten, terwijl het overduidelijk zou zijn als er een ander persoon zou verschijnen bij een persoonlijke ontmoeting of tijdens een video- of telefoongesprek.

3.5.2 Oplichting met varkensslachtingen:

Oplichtingstrucs met zogenaamde 'varkensslachtingen' zijn in 2016 of eerder ontstaan als een regionale vorm van oplichting in China. Aanvankelijk werden slachtoffers gevonden op datingsites voor mensen van hetzelfde geslacht, maar later breidde de oplichting zich uit naar datingsites voor mensen van verschillend geslacht. De term 'varkensslachting' is afgeleid van een analogie tussen de eerste fase, waarin het vertrouwen van de slachtoffers wordt gewonnen, en het vetmesten van varkens vóór de slacht.

De modus operandi verspreidde zich later over Zuidoost-Azië tijdens het hoogtepunt van de coronapandemie. In Cambodja, ooit een welvarende gokstad, transformeerden veel lokale gokkersbendes casino's tot centra voor oplichting, waar ze zich bezighielden met het slachten van varkens. Dit was waarschijnlijk een gevolg van de afname van het aantal casinobezoekers door de coronapandemie en het harde optreden van de Cambodjaanse overheid tegen commercieel gokken. Veel van deze operaties worden ook uitgevoerd vanuit gebieden in Myanmar die vanwege de burgeroorlog buiten de controle van de centrale overheid vallen, met als belangrijk knooppunt de stad Myawaddy, nabij de grens met Thailand. Volgens het VN-Bureau voor de Mensenrechten zijn honderdduizenden mensen slachtoffer geworden van mensenhandel en zitten ze vast in oplichtingscentra in Cambodja en Myanmar, terwijl andere operaties worden uitgevoerd vanuit Laos, de Filipijnen en Thailand. Veel van de groepen die zich bezighouden met het slachten van varkens zijn Chinese criminele syndicaten in het buitenland, gevestigd in Zuidoost-Azië, die etnische Chinezen en anderen naar fraudefabrieken smokkelen en hen dwingen de fraude te plegen.

Oplichting met nepvarkensslachtingen kreeg internationale bekendheid door de uitbuiting van online datingapps en sociale mediaplatformen. Oplichters creëerden uitgebreide valse identiteiten om romantische of emotionele banden met slachtoffers aan te knopen, waarmee ze afweken van traditionele financiële oplichting door psychologische manipulatie toe te passen. Deze vroege fase van deze oplichting richtte zich voornamelijk op lokale bevolkingsgroepen, maar breidde zich snel uit naarmate de digitale connectiviteit toenam.

De oplichtingspraktijken zijn aanzienlijk geëvolueerd door de integratie van geavanceerde technieken, waaronder het creëren van nep-online beleggingsplatformen en het gebruik van social engineering.

Door het wijdverbreide gebruik van platforms zoals WhatsApp en Telegram kunnen willekeurige personen het doelwit worden van oplichting, simpelweg door een gesprek te starten. Een belangrijk aspect van deze ontwikkeling was het gebruik van cryptovaluta voor transacties, wat aantrekkelijk was voor oplichters vanwege de moeilijkheid om transacties te traceren en terug te vorderen. De globalisering van deze oplichting kan worden toegeschreven aan de toegenomen alomtegenwoordigheid van digitale interacties en de groeiende populariteit van cryptovaluta, die een nieuwe mogelijkheid boden voor dergelijke frauduleuze activiteiten op wereldwijde schaal.

Criminele groepen

Oplichting met nepvarkensslachtingen omvat een reeks zorgvuldig geplande stappen om slachtoffers te misleiden en uit te buiten, meestal gericht op fraude met cryptovaluta-investeringen.

Vertrouwen winnen: Oplichting begint vaak met informele gesprekken die worden geïnitieerd door de oplichter, die bijvoorbeeld kan doen alsof hij de contactgegevens van het slachtoffer per ongeluk of via een gemeenschappelijke kennis heeft gekregen. Deze eerste interacties zijn bedoeld om vertrouwen op te bouwen en kunnen gepaard gaan met het gebruik van aantrekkelijke profielfoto's om slachtoffers te lokken.
De investering introduceren: Zodra er vertrouwen is gewonnen, introduceert de oplichter het slachtoffer een frauduleuze beleggingsconstructie, waarbij aanzienlijke rendementen op korte termijn worden beloofd. De oplichters gebruiken overtuigende tactieken en vervalste beleggingsportefeuilles om slachtoffers te overtuigen van de legitimiteit van de constructie.
Geld innen: Nadat oplichters het slachtoffer hebben overgehaald om te investeren, innen ze het geld, vaak via digitale betaalplatformen of cryptovaluta, om het traceren van de transacties te bemoeilijken.
Verdwijnen van de oplichter: Zodra een aanzienlijk bedrag is geïncasseerd, of wanneer slachtoffers proberen geld op te nemen, worden oplichters onbereikbaar, verwijderen ze hun online aanwezigheid of creëren ze nieuwe identiteiten, waardoor de slachtoffers geen mogelijkheid meer hebben om hun geld terug te krijgen.

Bovendien ontwikkelen de oplichters nep-brokerwebsites en mobiele apps om hun oplichtingspraktijken geloofwaardiger te maken, waardoor het voor slachtoffers moeilijk is om ze te onderscheiden van legitieme platforms.

3.6 Correct gebruik van sociale media en e-mail

Sociale media zijn natuurlijk lang niet alleen maar slecht. Er zijn vaak concrete voordelen verbonden aan het gebruik ervan. Velen van ons loggen in op sociale media voor een gevoel van verbondenheid, zelfexpressie, nieuwsgierigheid of de behoefte om contact te leggen. Apps zoals Facebook, Instagram, WhatsApp, Telegram en Twitter stellen ons in staat om in contact te blijven met familie en vrienden die ver van elkaar wonen, te communiceren met gelijkgestemden over onze interesses en ons aan te sluiten bij een online gemeenschap om op te komen voor zaken die ons na aan het hart liggen.

We moeten allemaal zelf, op basis van onze eigen ervaringen, beslissingen nemen over het gebruik van sociale media. Door onderzoek te doen, kunnen we de voor- en nadelen afwegen en weloverwogen beslissingen nemen. Hoewel de geest uit de fles is, kunnen we, zoals Shakya en Christakis stellen, ontdekken dat "online sociale interacties geen vervanging zijn voor de echte", en dat gezonde relaties in het echt essentieel zijn voor de maatschappij en ons eigen welzijn. We doen er goed aan die waarheid te onthouden en niet al onze eieren in één mandje te leggen: sociale media.

Algemene richtlijnen:

Bescherm uw privacy door de instellingen regelmatig te controleren.
Denk goed na voordat je iets plaatst - content kan oneindig lang online blijven staan.
Wees respectvol en attent in alle interacties.
Controleer de informatie voordat je deze deelt om de verspreiding van misinformatie te voorkomen.
Onthoud dat uw digitale voetafdruk van invloed is op uw persoonlijke en professionele reputatie.

Beveiligingsbewustzijn:

Wees voorzichtig met links en bijlagen.
Controleer de afzenderadressen voordat u reageert op verdachte e-mails.
Deel nooit gevoelige informatie, tenzij u zeker bent van de veiligheid.
Gebruik encryptie voor gevoelige communicatie.

- Gebruik sterke, unieke wachtwoorden en schakel tweefactorauthenticatie in.

3.7 De introductie van kunstmatige intelligentie (AI)

Kunstmatige intelligentie (AI) verwijst naar de ontwikkeling van computersystemen die in staat zijn taken uit te voeren die normaal gesproken menselijke intelligentie vereisen. Deze taken omvatten onder andere leren,

Probleemoplossing, besluitvorming en het begrijpen van natuurlijke taal. AI omvat een breed scala aan technieken en benaderingen, van eenvoudige op regels gebaseerde systemen tot complexe machine learning-modellen. Hieronder volgt een meer gedetailleerde beschrijving van de kernconcepten:

Het nabootsen van menselijke intelligentie: AI streeft ernaar machines te creëren die taken kunnen uitvoeren die mensen normaal gesproken met hun intelligentie doen.
Leren en probleemoplossing: AI-systemen kunnen leren van data, patronen herkennen en op basis van dat leerproces beslissingen nemen.
Diverse toepassingen: AI wordt gebruikt in uiteenlopende sectoren, waaronder de gezondheidszorg, financiën, onderwijs en transport.
Machine learning: een kernonderdeel van moderne AI, waarbij algoritmen leren van data zonder expliciete programmering.
Natuurlijke taalverwerking: Hiermee kunnen machines menselijke taal begrijpen en ermee interageren.
Computervisie: Hiermee kunnen machines beelden en video's "zien" en interpreteren.

Voorbeelden van AI-toepassingen:
Spraakassistenten: zoals Siri of Alexa, die spraakopdrachten begrijpen en erop reageren.
Aanbevelingssystemen: Deze worden door online platforms gebruikt om producten of content voor te stellen op basis van gebruikersvoorkeuren.

- **Zelfrijdende auto's: AI inzetten voor navigatie en besluitvorming in autonome voertuigen.**
- **Fraudedetectie: AI inzetten om verdachte transacties in financiële systemen te identificeren.**

- **In essentie is AI een snel evoluerend vakgebied met het potentieel om diverse aspecten van ons leven te transformeren. Dezelfde principes gelden voor romantische oplichting, waarbij door AI gegenereerde persona's die zich voordoen als vrienden, familie of collega's van de oplichter, met het slachtoffer communiceren om de relatie te bevestigen en hun twijfels weg te nemen. Deze interacties simuleren sociale bewijsdrang, waardoor het voor slachtoffers moeilijker wordt om inconsistenties in twijfel te trekken.**

3.7.1 Eerste contact

De geloofwaardigheid van een oplichtersprofiel is cruciaal in de beginfase van romantische fraude, omdat het mede bepaalt of een slachtoffer in zee gaat met een nep-identiteit. Hoewel oplichters traditioneel afbeeldingen van echte gebruikers stalen, konden omgekeerde beeldzoekacties en fotoforensisch onderzoek worden gebruikt om deze vormen van bedrog te ontmaskeren. Door de integratie van LLM's (Live-Label Marketing) en deepfake-beeldgeneratie kunnen fraudeurs nu echter gemakkelijk op grote schaal synthetische identiteiten produceren die sterk lijken op echte gebruikers. Deze profielen zijn ontworpen om detectiemechanismen op sociale media, datingplatforms en professionele netwerken te omzeilen en slachtoffers effectief te misleiden.

De schaal van AI-gestuurde profielcreatie is enorm. Zo verwijderde Meta naar verluidt miljarden nepaccounts in 2024 (waaronder alle accounts waarvan het bedrijf vermoedde dat ze met kwade bedoelingen of namens niet-menselijke entiteiten waren aangemaakt). De explosieve groei van door AI gegenereerde frauduleuze profielen dwong datingplatform Tinder ertoe om in 2024 zijn identiteitsverificatieprogramma uit te breiden en strengere maatregelen in de VS en het VK in te voeren. Deze maatregelen vereisen dat gebruikers door de overheid uitgegeven identiteitsbewijzen en zelfgemaakte video's indienen. Deze maatregelen zijn echter mogelijk niet voldoende om de toenemende geavanceerdheid van generatieve AI aan te pakken, aangezien de technologie uitdagingen vormt voor KYC-controles en andere identiteitsverificatieprocessen.

Door AI gegenereerde profielen werken niet op zichzelf. Oplichters kunnen synthetische persona's combineren met geautomatiseerde communicatie, waardoor er grootschalige processen ontstaan waarbij duizenden realistische profielen tegelijkertijd door LLM gegenereerde berichten versturen. Zoals in de vorige sectie besproken, zullen oplichters LLM's waarschijnlijk eerder gebruiken bij de eerste benadering dan bij latere interacties. Dit komt doordat:

Het eerste bericht vereist minimale personalisatie, waardoor ze gemakkelijk op grote schaal te genereren zijn.
Het versturen van introductieberichten is zeer repetitief werk, waardoor automatisering een hoge prioriteit heeft voor fraudeurs die hun efficiëntie willen verhogen.
LLM's presteren het best in gestructureerde scenario's met een lage context, waardoor ze bijzonder geschikt zijn voor deze fase.

- Dit betekent dat AI al goed gepositioneerd is om de schaalbaarheid van romantische oplichting in een vroeg stadium te vergroten. Oplichters kunnen de technologie op meerdere platforms inzetten en daarbij vertrouwen op...

Op LLM-berichten worden gebruikt om efficiënt gesprekken te starten. Zodra een slachtoffer reageert, kunnen oplichters overschakelen naar handmatige interventie of verfijnde, door AI ondersteunde interacties om de misleiding vol te houden.

Naarmate door AI gegenereerde profielen en outreach geavanceerder worden, kunnen traditionele detectiemethoden zoals profielverificatie en tekstgebaseerde anomaliedetectie moeite hebben om gelijke tred te houden, waardoor adaptieve tegenmaatregelen nodig zijn.

3.7.2 Relatieopbouw

Zodra oplichters het eerste contact hebben gelegd, gaan ze over naar de fase van relatieopbouw, waarin ze proberen een diepere emotionele band te creëren en vertrouwen op te bouwen bij hun slachtoffers. AI-gestuurde tools hebben het vermogen van oplichters om misleiding op grotere schaal en op maat te maken vergroot, maar ze hebben slechts beperkte mogelijkheden om deze fase te automatiseren. In tegenstelling tot de eerste contactfase, die baat heeft bij standaardscripts en grootschalige automatisering, vereist relatieopbouw aanpassingsvermogen, emotionele intelligentie en op maat gemaakte reacties op interacties met het slachtoffer.

Een belangrijk verschil tussen door AI aangedreven en door mensen geleide misleiding is aanpassingsvermogen. Menselijke oplichters kunnen hun verhalen dynamisch aanpassen op basis van de reacties van slachtoffers, waardoor gesprekken emotioneel boeiend blijven en zich ontwikkelen richting financiële uitbuiting. Hoewel LLM's procedureel accurate oplichtingsberichten kunnen genereren, hebben ze moeite om continuïteit en diepgaande personalisatie te behouden gedurende langdurige interacties. Zonder menselijk toezicht lopen door AI gegenereerde berichten het risico op inconsistenties in toon, tegenstrijdigheden en herhaalde formuleringen, wat de geloofwaardigheid in de loop van de tijd kan ondermijnen. Het Bureau van de Verenigde Naties voor Drugs en Misdaad[29] meldt dat, hoewel AI al wordt gebruikt bij cybercriminaliteit, de meeste oplichtingspraktijken nog steeds afhankelijk zijn van menselijk toezicht om de geloofwaardigheid te behouden en complexe interpersoonlijke dynamieken te beheren.

Kunstmatige intelligentie kan deze fase echter op verschillende manieren verbeteren:

Optimalisatie van oplichtingsscripts: fraudeurs kunnen LLM's gebruiken om oplichtingsscripts te verfijnen, verschillende formuleringen en emotionele argumenten te testen om de betrokkenheid te maximaliseren.

Meertalige chatondersteuning: vertaling stelt oplichters in staat om slachtoffers in meerdere talen vloeiender te benaderen.
Geautomatiseerd relatiebeheer: AI-tools kunnen fraudeurs helpen om meerdere slachtoffers tegelijk te beheren, door suggesties voor reacties en communicatiestrategieën te geven en inconsistenties in gesprekken te minimaliseren.

Hoewel door LLM gegenereerde tekst schaalbare en gepersonaliseerde interactie mogelijk maakt, biedt deepfake-media een extra laag authenticiteit, waardoor frauduleuze persona's overtuigender en steeds moeilijker te verifiëren zijn. AI-gestuurde tools voor stemklonen stellen oplichters in staat om content te genereren die spraakpatronen, accenten en emotionele intonaties nabootst, waardoor de behoefte aan directe menselijke interactie afneemt. Op dezelfde manier kunnen fraudeurs AI-gegenereerde video gebruiken om visueel bewijs van identiteit te fabriceren, waardoor ze verificatieverzoeken kunnen omzeilen en het vertrouwen van potentiële slachtoffers kunnen vergroten. Hoewel volledig autonome deepfake-interacties technisch gezien nog steeds een uitdaging vormen, maken oplichters al gebruik van vooraf opgenomen synthetische videocontent, waardoor ze een misleiding langer kunnen volhouden.

Recente spraakmakende gevallen benadrukken de groeiende impact van deepfake-fraude. Een Brits ingenieursbureau meldde in januari 2024 dat criminelen een deepfake-video gebruikten om zich succesvol voor te doen als topmanagers, waarmee ze een bedrijfsfraude van 25 miljoen dollar pleegden. In oktober 2024 gebruikten oplichters deepfake-beelden om slachtoffers te laten geloven dat ze een echte relatie hadden, en wisten ze uiteindelijk 46 miljoen dollar van hen af te troggelen. Hoewel recentere gevallen zich richten op de rol van deepfakes bij romantische oplichting, breiden de onderliggende tactieken zich uit naar andere domeinen, waaronder beleggingsfraude.

De vooruitgang in AI-technologie voor het naadloos integreren van gegenereerde content in bestaande afbeeldingen of video's heeft het realisme van dit misleidende materiaal verder vergroot, waardoor detectie steeds moeilijker wordt voor zowel mensen als geautomatiseerde systemen. Naarmate AI nieuwe mogelijkheden ontwikkelt, zal de rol ervan in het opbouwen van frauduleuze relaties waarschijnlijk evolueren, waarbij geautomatiseerde misleiding wordt gecombineerd met strategisch menselijk toezicht om de effectiviteit van oplichting te maximaliseren.

3.7.3 Poetsen

Naarmate een relatie zich verdiept, verschuiven fraudeurs van het opbouwen van algemeen vertrouwen naar zeer gerichte psychologische manipulatie. Deze fase, vaak aangeduid als grooming, omvat het vergroten van de emotionele afhankelijkheid en het isoleren van het slachtoffer van externe invloeden om hun kwetsbaarheid voor financiële of persoonlijke uitbuiting te vergroten. AI verbetert en personaliseert dit proces door het online gedrag van een slachtoffer te analyseren, hun emotionele toestand te monitoren en communicatiepatronen aan te passen, mogelijk in realtime. Door deze manipulatietechnieken te automatiseren, stelt AI fraudeurs in staat om bedrog op grote schaal te optimaliseren, waardoor hun tactieken geavanceerder en efficiënter worden, en bovendien moeilijker te detecteren.

AI-gestuurde systemen kunnen snel gegevens uit meerdere bronnen verzamelen en analyseren, waaronder sociale media en openbare registers, om een uitgebreid psychologisch profiel van potentiële slachtoffers te creëren. Traditioneel vereiste dergelijke profilering veel handmatige inspanning, maar AI kan dit proces binnen enkele seconden automatiseren en verfijnen, waardoor oplichters zeer kwetsbare doelwitten kunnen identificeren en prioriteren. AI-gestuurde profilering is goed gedocumenteerd in de context van social engineering, met name bij spear-phishingaanvallen, waarbij berichten worden afgestemd op de angsten, verlangens of onzekerheden van individuen.

Oplichters kunnen deze AI-gestuurde profilering uitbreiden naar realtime gedragsanalyse, waarbij ze de reacties, interactiepatronen en emotionele signalen van een slachtoffer volgen. Door lopende gesprekken te verwerken, kan AI oplichters helpen hun toon, timing en boodschap dynamisch aan te passen om de illusie van een echte connectie te creëren. Dit maakt een geleidelijke, maar zeer berekende, verdieping van de emotionele afhankelijkheid van het slachtoffer mogelijk, gebaseerd op het gecreëerde imago van de oplichter.

Het vermogen van AI om meeslepende online omgevingen te creëren, versterkt het manipulatieproces verder door de verzonnen identiteit van de oplichter te bevestigen en de scepsis van slachtoffers over het proces te verminderen. Onderzoek naar door AI aangedreven politieke en marketingovertuiging heeft aangetoond dat modellen individuen nauwkeurig kunnen benaderen met gepersonaliseerde berichten, waardoor hun betrokkenheid toeneemt en hun overtuigingen worden gevormd. Dezelfde principes gelden voor romantische oplichting, waarbij door AI gegenereerde persona's die zich voordoen als vrienden, familie of collega's van de oplichter, met het slachtoffer communiceren om de relatie te bevestigen en hun twijfels weg te nemen. Deze interacties simuleren sociale bewijsdrang, waardoor het voor slachtoffers moeilijker wordt om inconsistenties in twijfel te trekken.

Daarnaast is het type AI-gestuurde contentcreatie en bot-gestuurde versterking vaak

Zoals te zien is in politieke beïnvloedingscampagnes, kunnen online ruimtes overspoeld worden met verhalen die elkaar versterken. Dit zorgt ervoor dat wanneer een slachtoffer zoekt naar de naam van zijn of haar partner, hij of zij verzonnen getuigenissen, nepprofielen of door AI gegenereerde artikelen vindt die de geloofwaardigheid van de oplichting versterken. Net zoals publieke figuren AI kunnen gebruiken om het publieke debat te sturen en politieke verhalen te versterken, kunnen fraudeurs het misbruiken om een kunstmatig digitaal netwerk te creëren dat het slachtoffer isoleert.

3.7.4 Uitvoering

Naarmate het vertrouwen groeit, gaan fraudeurs over van emotionele manipulatie naar financiële uitbuiting, waarbij ze de emotionele band van het slachtoffer misbruiken om betalingsverzoeken te rechtvaardigen. Deze fase omvat vaak verzonnen crises, zoals medische noodgevallen, logistieke problemen of juridische problemen, die allemaal bedoeld zijn om urgentie te creëren en het slachtoffer onder druk te zetten om geld over te maken. Cadeaubonnen blijven een veelgebruikte methode om geld af te troeven en komen voor in 24% van de gemelde gevallen van romantische oplichting, maar cryptovaluta en bankoverschrijvingen leiden tot aanzienlijk hogere verliezen per slachtoffer. Rapporten geven aan dat de verliezen door romantische oplichting de afgelopen jaren sterk zijn gestegen en het Britse publiek meer dan £80 miljoen per jaar kosten. In Australië bedroegen de gemelde verliezen in 2024 meer dan AU$23 miljoen, waarbij AI een belangrijke rol speelde in deze toename.

Naast timing en schaal helpt AI fraudeurs bij het uitvoeren van geavanceerde vormen van bedrog, het fabriceren van financiële legitimiteit en het stroomlijnen van witwassen, waardoor financiële afpersing subtieler en effectiever wordt. Een zorgwekkende ontwikkeling betreft het vermogen van AI om financiële geloofwaardigheid te fabriceren. Net als veel andere criminelen gebruiken romantische oplichters nepbedrijven om hun illegale winsten te verbergen. Fraudeurs gebruiken nu generatieve AI om overtuigende financiële overzichten, juridische documenten en synthetische identiteiten te vervalsen om de controles van financiële instellingen te omzeilen. Zoals eerder besproken, gebruiken criminelen steeds vaker door AI gegenereerde synthetische identiteiten om KYC-verificatie te omzeilen, waardoor ze frauduleuze bankrekeningen kunnen openen en witwassen op grote schaal mogelijk maken. Hun door AI gegenereerde identiteiten kunnen legitieme financiële netwerken infiltreren op manieren die traditionele fraudebewakingssystemen steeds moeilijker kunnen detecteren.

AI speelt ook een cruciale rol in de opkomst van oplichtingspraktijken met betrekking tot het slachten van varkens, een van de meest voorkomende vormen van criminaliteit.

Een van de meest lucratieve vormen van financiële afpersing is romantische fraude. Bij deze oplichtingspraktijken bewerken oplichters slachtoffers weken of maandenlang voordat ze hen introduceren bij nep-cryptovaluta- of beleggingsplatformen, waarop ze worden verleid om steeds grotere bedragen te storten. Oplichters vergroten de geloofwaardigheid en het realisme van deze nep-beleggingssites door niet alleen code van echte beleggingsplatformen te kopiëren, maar ook door AI te gebruiken om content te genereren. Ze zetten ook AI-gestuurde chatbots in als nep-beleggingsadviseurs om slachtoffers door het platform te leiden, waardoor zelfs sceptische gebruikers zich gerustgesteld voelen door verzonnen markttrends en gepersonaliseerd advies. Deze chatbots lokken slachtoffers verder in de val door schadelijke links in hun berichten te plaatsen, die hen naar andere frauduleuze praktijken leiden en hun financiële verliezen vergroten.

De inkomsten uit cryptovaluta-fraude bereikten in 2024 naar schatting 12,4 miljard dollar in de VS, waarbij oplichting met neppe varkensslachtingen een aanzienlijk deel van deze verliezen voor zijn rekening nam. Tegelijkertijd hebben AI-ondersteunde codeertools de technische vaardigheden die nodig zijn om nep-investeringsplatformen te lanceren, verminderd, waardoor oplichters met minimale inspanning massaal frauduleuze websites kunnen produceren.

Naarmate AI steeds meer oplichting automatiseert en fraudeoperaties stroomlijnt, raken oplichtingspraktijken met nepvarkensslachtingen steeds meer verweven met romantische oplichting. De mogelijkheid om hypergepersonaliseerde, door AI aangedreven beleggingsfraude te creëren, maakt deze oplichtingspraktijken nog verraderlijker en schaadt slachtoffers zowel financieel als psychisch.

3.7.5 Uitgang of escalatie

Naarmate romantische oplichting de laatste fase bereikt, verdwijnen de oplichters abrupt nadat ze geld van hun slachtoffers hebben afgetroggeld, of voeren ze hun bedrog op om nog meer geld te verkrijgen. AI maakt steeds complexere ontsnappingsstrategieën mogelijk, waardoor de uitbuiting van slachtoffers wordt verlengd door technieken zoals deepfake-chantage en identiteitsfraude.

Zoals de Federal Trade Commission onlangs meldde, is een oplichtingstactiek die steeds vaker wordt toegepast, het gebruik van AI-gestuurde imitatie van wetshandhavers of incassobureaus. Bij dit soort oplichting benaderen fraudeurs slachtoffers met valse beloftes van financiële compensatie. Ze doen zich voor als politieagenten, financiële toezichthouders of onderzoekers en beweren dat ze tegen betaling kunnen helpen bij het terugvinden van verloren geld.

3.8 Casestudy van Sarah Thompson, een oplichtingszaak in de liefdeswereld.

Achtergrond

Sarah Thompson, een 58-jarige weduwe uit Portland, Oregon, verloor in 2022 haar man aan kanker na 30 jaar huwelijk. Na een jaar van rouw moedigden haar volwassen kinderen haar aan om online dating te proberen als een manier om weer sociaal contact te leggen. Met weinig ervaring in het digitale datingtijdperk maakte Sarah in maart 2023 een profiel aan op een populaire datingsite.

Eerste contact

Binnen twee weken na haar aanmelding op het platform ontving Sarah een bericht van "William Pierce", die beweerde een 62-jarige Amerikaanse civiel ingenieur te zijn die aan een project in Maleisië werkte. Zijn profiel bevatte foto's van een aantrekkelijke man met zilvergrijs haar en een warme glimlach. William gaf aan dat hij ook weduwnaar was en op zoek naar gezelschap.

Hun gesprekken verplaatsten zich al snel van het datingplatform naar e-mail en WhatsApp, wat eigenlijk al een waarschuwingssignaal had moeten zijn. William was attent, romantisch en leek oprecht geïnteresseerd in Sarah's leven. Ze communiceerden dagelijks via berichten en af en toe via spraakoproepen, hoewel William altijd wel een excuus had waarom videobellen niet mogelijk was – slechte internetverbinding, een drukke werkplanning of tijdsverschillen.

Relatieontwikkeling

In de daaropvolgende twee maanden bouwde William een emotionele band op met Sarah door:
Dagelijkse goedemorgen- en goedenachtberichten
Hij deelde persoonlijke verhalen over zijn overleden vrouw en kinderen.
We bespreken plannen voor de toekomst om elkaar weer te zien en mogelijk samen een leven op te bouwen.
Af en toe cadeautjes (bloemen, chocolaatjes) naar Sarah's huis sturen.
Relatief snel diepe romantische gevoelens uiten

De financiële aanvragen

Ongeveer drie maanden na het begin van hun relatie begon William financiële eisen te stellen:

Eerste verzoek: William beweerde dat zijn project vertraging had opgelopen door een defect aan de apparatuur. Hij had $3.000 nodig om onderdelen te vervangen, maar kon niet over zijn geld beschikken vanwege "bankproblemen in het buitenland". Sarah, bezorgd om zijn situatie, maakte het geld over via een bankoverschrijving.

- **Escalatie: Nadat William zijn enorme dankbaarheid had geuit, kondigde hij aan dat het project bijna voltooid was en dat hij binnen enkele weken naar de VS zou terugkeren. Vervolgens beweerde hij echter dat hij een medisch noodgeval had (appendicitis) en 7.500 dollar nodig had voor een operatie die niet door zijn verzekering werd gedekt. Sarah, die nu emotioneel betrokken was, leende geld van haar pensioen om het bedrag over te maken.**

Crisissituatie: Vlak voor zijn vermeende terugkeer naar Amerika beweerde William dat hij een ongeluk had gehad op de bouwplaats. Hij had $15.000 nodig voor medische kosten en om een juridisch geschil met het lokale bedrijf op te lossen om zijn paspoort terug te krijgen. Hij beloofde alles terug te betalen bij zijn terugkeer.

Waarschuwingssignalen die Sarah over het hoofd zag

Achteraf gezien herkende Sarah verschillende waarschuwingssignalen die ze over het hoofd had gezien:

Williams terughoudendheid om te videochatten
Inconsistenties in zijn verhalen over familie en werk.
Zijn kennis van techniek leek vaag toen er naar details werd gevraagd.
Er zijn nooit foto's van hem in Maleisië of op werklocaties te zien.
Alle gesprekken draaiden om hun relatie of zijn problemen.
Zijn teksten bevatten grammaticale fouten die niet stroken met wat een moedertaalspreker van het Engels zou verwachten.
De redenen waarom hij geen toegang had tot zijn eigen aanzienlijke vermogen werden steeds ingewikkelder.

Het keerpunt

Sarah werd achterdochtig toen Williams eisen toenamen en zijn verhalen steeds ingewikkelder werden. Toen ze voorstelde hem in Maleisië te bezoeken, raadde hij dat ten zeerste af. Haar dochter, bezorgd over de financiële situatie van haar moeder, stond erop Williams correspondentie te bekijken en herkende de patronen van een romantische oplichting.

Om hun vermoedens te bevestigen, voerde Sarah's dochter een omgekeerde beeldzoekactie uit op Williams foto's. Ze ontdekte dat de foto's toebehoorden aan een gepensioneerde professor in Canada die geen

- verbinding met de oplichter.

Oplossing en nasleep

Sarah verloor uiteindelijk ongeveer $25.500 aan de oplichter voordat ze het contact verbrak. Toen ze "William" ermee confronteerde, ontkende hij aanvankelijk de oplichting, werd vervolgens agressief en verdween daarna spoorloos. Sarah meldde de oplichting aan:

Lokale politie
Het Internet Crime Complaint Center (IC3) van de FBI
Het datingplatform waar ze elkaar ontmoetten.
Haar bank en financiële instellingen

Hoewel ze het verloren geld niet kon terugkrijgen, leidde de ervaring Sarah tot het volgende:
Sluit je aan bij een steungroep voor slachtoffers van romantische oplichting.
Werk samen met een financieel adviseur om haar pensioenspaargeld weer op te bouwen.
Word een voorvechter voor bewustwording over romantische oplichting in seniorengemeenschappen.
Ontwikkel gezondere grenzen in relaties.

Psychologische impact

Sarah heeft door de oplichting aanzienlijk emotioneel trauma opgelopen:
Diepe schaamte en gêne
Vertrouwensproblemen in nieuwe relaties
Depressie en angst
Financiële problemen als gevolg van de verliezen
Verdriet om de relatie die ze dacht te hebben

Belangrijkste lessen

Deze zaak belicht verschillende belangrijke aspecten van romantische oplichting:

Oplichters richten zich op kwetsbare personen, met name mensen die recent verlies hebben geleden.

1. Ze bouwen eerst een emotionele band op voordat ze financiële verzoeken doen.

3. Ze isoleren slachtoffers van steunnetwerken die de oplichterij zouden kunnen ontmaskeren.
4. Ze creëren een gevoel van urgentie en emotionele druk rond financiële verzoeken.
5. Ze hebben plausibele verklaringen waarom ze niet kunnen videobellen of elkaar persoonlijk kunnen ontmoeten.

Preventiestrategieën

Uit Sarah's ervaring komen verschillende preventiestrategieën naar voren:
Stuur nooit geld naar iemand die je nog nooit persoonlijk hebt ontmoet.
Sta erop om al vroeg in online relaties videogesprekken te voeren.
Zoek informatie en foto's van de persoon op.

1. Bespreek nieuwe relaties met vertrouwde vrienden of familieleden.
2. Wees op je hoede voor relaties die zich ongewoon snel ontwikkelen.

Vraag je af waarom iemand met aanspraak op financiële middelen jouw financiële hulp nodig heeft?
Wees sceptisch ten opzichte van herhaalde noodsituaties en crises.

Conclusie

Het geval van Sarah is representatief voor de duizenden romantische oplichtingspraktijken die jaarlijks plaatsvinden. Hoewel ze veel geld verloor, bleek de emotionele impact van het verraad nog veel verwoestender. Dankzij therapie en steungroepen heeft Sarah haar leven weer opgebouwd en helpt ze nu anderen de waarschuwingssignalen van romantische oplichting te herkennen voordat ze hun spaargeld – of hun hart – verliezen aan bekwame manipulators.

Kennen en Groeien: Zelfevaluatie en Beoordeling.

Co-funded by
the European Union

4 Zelfevaluatie en beoordeling

4.1 Zelfevaluatietoetsen over hoofdstuk 1: Liefdesfraude begrijpen

- 1. Wat is het voornaamste doel van een liefdesoplichting?
- A) Om echte romantische partners te vinden B) Om emotionele banden te exploiteren voor financieel gewin C) Om gezonde online relaties te bevorderen D) Om datingadvies te geven
- Correct antwoord: B

2. Op welke historische oplichtingsmethode zou de liefdesoplichting zijn oorsprong vinden?

- A) Ponzi-fraude B) De "Spaanse gevangenenfraude" C) Piramidespel D) Nigeriaanse prinsenfraude
- Correct antwoord: B

- 3. Wat is de beginfase in Whitty's raamwerk voor de stadia van een romantische oplichting?
- A) Voorbereidingsfase B) Profileringsfase C) Exploitatiefase D) Onthullingsfase
- Correct antwoord: B

- 4. Bij romantische oplichting wordt de tactiek om het slachtoffer te overladen met genegenheid en aandacht als volgt omschreven:
- A) Schuldgevoel opwekken B) Crisis creëren C) Lovebombing D) Financiële uitbuiting
- Correct antwoord: C

5. Welke van de volgende is een veelvoorkomend waarschuwingssignaal bij romantische oplichting?

- A) Verzoeken om elkaar direct persoonlijk te ontmoeten B) Beperkte of vage persoonlijke gegevens op het profiel van de oplichter C) Duidelijke en consistente levensverhalen D) Openbare aanwezigheid op sociale media
- Correct antwoord: B

6. Welke groep loopt volgens onderzoek een groter risico om slachtoffer te worden van romantische oplichting?

- A) Jongvolwassenen van 18-25 jaar B) Oudere mannen boven de 70 C) Vrouwen van middelbare leeftijd van 40-60 jaar D) Tieners
- Correct antwoord: C

7. Welke betaalmethode wordt doorgaans gevraagd door oplichters bij liefdesfraude?

- A) Persoonlijke cheques B) Cryptovaluta of cadeaukaarten C) Creditcardbetalingen D) Directe storting op een bankrekening
- Correct antwoord: B

8. Hoe proberen oplichters vaak te voorkomen dat slachtoffers de oplichting herkennen?

- A) Door slachtoffers regelmatig te ontmoeten B) Alleen via videogesprekken C) Door slachtoffers te vragen hun relatiegegevens niet met anderen te delen D) Door slachtoffers aan te moedigen hen aan te geven
- Correct antwoord: C

10. Welke van de volgende maatregelen wordt aanbevolen als preventieve maatregel tegen romantische oplichting?

- A) Snel geld overmaken om de relatie niet te verliezen B) Gegevens geheimhouden en achtergrondchecks uitvoeren op nieuwe contacten C) Vriendschappen en relaties helemaal vermijden D) Elk gevoel van wantrouwen negeren
- Correct antwoord: B

9. Wat is volgens Button et al. (2014) vaak de psychologische impact op slachtoffers van romantische oplichting?

- A) Opluchting en tevredenheid B) Alleen financieel verlies zonder emotionele impact C) Ernstig emotioneel trauma en financieel verlies (Correct) D) Zich veiliger voelen
- Correct antwoord: C

4.2 Zelfevaluatietoetsen over hoofdstuk 2: Goede praktijken voor docenten

1. Wat is een van de belangrijkste redenen waarom oplichters zich richten op sociaal geïsoleerde ouderen?

- A) Ze investeren eerder in risicovolle aandelen. B) Ze zijn leergierig en willen graag nieuwe technologieën leren. C) Ze zijn doorgaans rijk. D) Ze zijn emotioneel kwetsbaar en zoeken verbinding.

Correct antwoord: D

- 2. Welke factoren dragen het vaakst bij aan de kwetsbaarheid van senioren voor liefdesfraude?
- A) Hoog inkomen en gebrek aan ervaring met sociale media B) Vertrouwensvolle aard, cognitieve achteruitgang en emotionele behoeften C) Vrije tijd en goede steun van het gezin D) Ze zijn doorgaans rijk

Correct antwoord: B

- 3. Welke tactiek gebruiken oplichters vaak om hun slachtoffers emotioneel te manipuleren?
- A) Strikte juridische taal B) Beloftes van een vroege erfenis C) Love bombing en emotionele bekrachtiging D) Het bespotten van hun eenzaamheid

Correct antwoord: C

4. Welk dubbel trauma ervaren slachtoffers van liefdesoplichting vaak?

- A) Emotioneel verraad en financieel verlies B) Juridische problemen en achteruitgang van de gezondheid C) Familieconflicten en schaamte D) Misbruik van technologie en baanverlies

Correct antwoord: A

5. Welke gevolgen kunnen jaren na de oplichting aanhouden als ze geen adequate ondersteuning hebben gekregen?

A) Verbeterd beoordelingsvermogen B) Langdurig trauma en vermijding van relaties C) Betere online gewoonten D) Beter zelfbeeld

- Correct antwoord: A

6. Waarom melden ouderen oplichtingspraktijken vaak niet?

- A) Ze begrijpen niet hoe het melden werkt B) Ze worden er emotioneel niet door geraakt C) Ze vrezen schaamte, spot of veroordeling D) Ze willen de oplichter beschermen
- Correct antwoord: C

7. Waarom zijn docenten vaak effectiever dan familieleden in het vroegtijdig opsporen van oplichting?

- A) Ze hebben de wettelijke bevoegdheid om onderzoek te doen. B) Ze beperken het online gebruik. C) Senioren voelen zich minder veroordeeld en meer op hun gemak om hun vertrouwen in hen te stellen. D) Ze wonen samen met de senioren.
- Correct antwoord: C

8. Welke rol kunnen jongerenwerkers spelen bij het verminderen van de kwetsbaarheid van ouderen voor oplichting?

- A) Meld oplichtingspraktijken namens senioren bij banken B) Bied intergenerationele digitale begeleiding en empathie aan C) Verwijder senioren van online platforms D) Vervang docenten in alle workshops
- Correct antwoord: B

9. Wat is de voornaamste reden waarom digitale geletterdheid zo belangrijk is bij het voorkomen van oplichting?

- A) Om de vatbaarheid voor online fraude te verminderen B) Om senioren meer tijd online te laten doorbrengen C) Om hen te leren bloggen D) Om te voorkomen dat de politie moet ingrijpen

Correct antwoord: A

10. Waarom zijn 'buddy-systemen' effectief in het voorkomen van oplichting?

- A) Ze verlagen de reiskosten voor docenten. B) Ze beperken telefoongesprekken. C) Ze controleren internetgebruik. D) Ze bieden ouderen iemand om verdachte activiteiten mee te bespreken.

Correct antwoord: D

11. Waar moeten docenten prioriteit aan geven bij het ontwerpen van workshops ter voorkoming van oplichting? A) Complexe technische taal en lange sessies B) Schaamtevolle waarschuwingsverhalen C) Toegankelijke, interactieve methoden voor emotioneel en digitaal bewustzijn D) Senioren vertellen dat ze moeten stoppen met het gebruik van technologie

Correct antwoord: C

12. Welk gedrag is een vroeg waarschuwingssignaal voor een lopende romantische oplichting?

A) Vaker vrijwilligerswerk doen B) Meer familiebezoeken C) Digitale geletterdheidscursussen volgen D) Plotselinge geheimhouding over een nieuwe online relatie (Correct)

- Correct antwoord: D

13. Welke is GEEN aanbevolen detectiemethode?

- A) Directe confrontatie B) Vertrouwensopbouwende gesprekken C) Emotionele betrokkenheid D) Gedrag observeren
- Correct antwoord: A

14. Wat is "triage" in een strategie voor het bestrijden van oplichting?

- A) Het slachtoffer de schuld geven B) Evalueren, beschuldigen, rapporteren C) Negeer, observeren, analyseren D) Betrek, voorlichten, evalueren

Correct antwoord: D

15. Hoe moeten docenten omgaan met emotioneel betrokken ouderen die actief slachtoffer zijn van oplichting?

- A) Angstaanjagende tactieken gebruiken B) Geanonimiseerde scenario's en gerichte vragen gebruiken C) Erop aandringen dat ze de oplichting onmiddellijk melden D) Hun familie zonder toestemming waarschuwen

Correct antwoord: B

16. Hoe kunnen docenten helpen de isolatie na een oplichting te verminderen?

- A) Geheimhouding aanmoedigen B) Slachtoffers opnieuw in contact brengen met veilige sociale activiteiten en steungroepen C) Hun sociale media monitoren D) Internetgebruik afsluiten

Correct antwoord: B

17. Waarom zouden docenten de families van slachtoffers op een gevoelige manier moeten betrekken?

- A) Hen de schuld geven B) De druk opvoeren C) Verantwoordelijkheid overdragen D) Steun opbouwen en de schaamte van het slachtoffer verminderen
- Correct antwoord: D

18. Waarom zijn partnerschappen met bibliotheken, gezondheidscentra en buurtcentra cruciaal voor het voorkomen van oplichting?

- A) Ze verminderen de papierwinkel B) Ze vervangen het werk van de docent C) Ze helpen ouderen te bereiken en bieden een vertrouwde omgeving D) Ze kunnen juridische stappen afdwingen

Correct antwoord: C

4.3 Zelfevaluatietoetsen over hoofdstuk 3: Basisprincipes van cyberbeveiliging voor beginners

1: Wat is het voornaamste kenmerk van een phishingaanval?

a) Het installeren van malware via USB-apparaten b) Het misbruiken van softwarekwetsbaarheden

c) Personen misleiden om gevoelige informatie prijs te geven door middel van frauduleuze communicatie.

d) Fysiek inbreken in computersystemen

Correct antwoord: C

2: Waarin verschilt spear phishing van reguliere phishing?

a) Het maakt gebruik van telefoongesprekken in plaats van e-mails b) Het richt zich met gepersonaliseerde aanvallen op specifieke personen of organisaties c) Het richt zich uitsluitend op overheidsinstanties d) Het maakt gebruik van fysieke post in plaats van elektronische communicatie

Correct antwoord: B

3: Wat is pretexting in sociale manipulatie?

- a) Het versturen van massamails naar willekeurige ontvangers b) Het creëren van een verzonnen scenario om slachtoffers te lokken en informatie te stelen c) Het gebruiken van technische exploits om toegang tot systemen te verkrijgen d) Het installeren van keyloggers op doelcomputers

Correct antwoord: B

4: Welk scenario beschrijft een lokaanval het beste?

- a) Geïnfecteerde USB-sticks achterlaten op parkeerterreinen zodat medewerkers ze kunnen vinden b) Dreigende e-mails versturen met betalingseisen c) Telefonisch optreden alsof je IT-ondersteuning bent d) Nep-sociale mediaprofielen aanmaken
- Juist antwoord: A

5: Wat is tailgating in de context van sociale manipulatie?

a) Iemands online activiteiten volgen b) Netwerkverkeer monitoren c) Iemand zonder de juiste toestemming door een beveiligde deur volgen d) Iemands toetsaanslagen kopiëren

Correct antwoord: C

6: Waar verwijst "vishing" naar?

- a) Visuele phishing via nepwebsites b) Virale phishing via sociale media c) Videophishing via nepvideogesprekken d) Spraakphishing via telefoongesprekken
- Correct antwoord: D

7: Welk psychologisch principe maken sociale ingenieurs doorgaans gebruik van?

- a) Technische complexiteit b) Netwerkprotocollen c) Autoriteit en vertrouwen d) Versleutelingsalgoritmen

Correct antwoord: C

8: Wat is een waterplaatsaanval?

- a) Het vergiftigen van daadwerkelijke watervoorraden b) Het compromitteren van websites die veelvuldig door doelorganisaties worden bezocht c) Het aanvallen van waterbedrijven d) Het versturen van phishing-e-mails met een waterthema
- Correct antwoord: B

9: Wat kenmerkt een quid pro quo social engineering-aanval?

- a) Iets aanbieden in ruil voor informatie of toegang b) Dreigen met juridische stappen c) Uitsluitend technische methoden gebruiken d) Alleen leidinggevenden als doelwit nemen

Juist antwoord: A

10: Wat is omgekeerde sociale manipulatie?

a) Sociale netwerken in omgekeerde chronologische volgorde manipuleren b) Wanneer de aanvaller zich voordoet als behulpzaam en wacht tot het slachtoffer contact opneemt c) De effecten van social engineering omkeren d) Sociale media in omgekeerde chronologische volgorde gebruiken

Correct antwoord: B

11: Welke van de volgende signalen is een waarschuwingssignaal dat kan duiden op een poging tot social engineering?

- a) Verzoeken om software-updates b) Dringende verzoeken om gevoelige informatie met dreigingen van consequenties c) Regelmatige privécommunicatie d) Geplande ontmoetingen met bekende personen

Correct antwoord: B

Bronnen

AARP. (z.d.). Romantische oplichting. https://www.aarp.org/money/scams-fraud/

AARP. (2021). AARP VOA ReST-programma: Herstel na fraude. AARP Fraud Watch Network. https://www.aarp.org/fraudwatchnetwork

AARP. (z.d.). Emotionele steun voor slachtoffers van fraude. https://states.aarp.org/maryland/emotional-support-for-victims-of-fraud#

Against Scams. (2024). Het belang van traumatherapie voor slachtoffers van oplichting. https://againstscams.org/importance-of-trauma-therapy-for-scam-victims-2024

Action Fraud. (z.d.). Romantische fraude. https://www.actionfraud.police.uk/

Action Fraud. (30 januari 2025). Ons onderzoek en onze statistieken over romantische oplichting – advies van Action Fraud over schadeclaims. https://www.actionfraud.org.uk/research-and-statistics-on-romance-scams-fraud/

Ayoobi, N., Shahriar, S., & Mukherjee, A. (2023, 5 september). De dreiging van nep- en door LLM gegenereerde LinkedIn-profielen: uitdagingen en kansen voor detectie en preventie. arXiv. https://doi.org/10.1145/3603163.3609064

BBC News. (2024, 7 mei). Hoe een 'Brad Pitt'-oplichting het hart van mijn moeder brak. https://www.bbc.com/news/articles/ckgnz8rw1xgo

Berry, K. (2024, 24 november). Oplichting: 'Ik ben erin getrapt door een deepfake-advertentie van Martin Lewis'. BBC News. https://www.bbc.co.uk/news/articles/clyvj754d9lo

Boulat, P.-A., & Wake, P. (2024, 15 mei). Kunnen door AI gegenereerde deepfakes de 'know your customer' (KYC)-authenticatie in gevaar brengen? techUK. https://www.techuk.org/resource/can-ai-generated-deepfakes-compromise-know-your-customer-kyc-authentication.html

Bronnen

Brady, S. (2024, 20 februari). Tinder versterkt identiteitsverificatie te midden van toename van AI-fraude. Verdict. https://www.verdict.co.uk/tinder-bolsters-id-verification-amid-surge-in-ai-scams/?cf-view&cf-closed

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online fraude: Leren van slachtoffers waarom ze in deze oplichtingstrucs trappen. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224 (Oorspronkelijk werk gepubliceerd in 2014)

Politiebureau (redactionele noot). Romantische oplichting. Staatspolitie. https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/truffe-romantiche-romance-scam/index.html

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romantische oplichting: relationele dynamiek en psychologische kenmerken van de slachtoffers en oplichters. Een verkennend literatuuronderzoek. Clin Pract Epidemiol Ment Health, 16 https://doi.org/10.2174/1745017902016010024

Cross, C. (2014). Liefde doet pijn: de kostbare realiteit van online romantische fraude. The Conversation.

Cross, C., Dragiewicz, M., & Richards, K. (2016). Inzicht in romantische fraude: inzichten uit de theorie over huiselijk geweld. Cyberpsychology, Behavior, and Social Networking, 19(7), 419-423. https://doi.org/10.1089/cyber.2016.0729

Cross, C., & Layt, R. (2021). “Ik vermoed dat de foto's gestolen zijn”: Romantische fraude, identiteitsfraude en reageren op vermoedens van onechte identiteiten. Social Science Computer Review, 40(4), 1043–1058. https://doi.org/10.1177/0894439321999311

Cross, C. (2022). Het gebruik van kunstmatige intelligentie (AI) en deepfakes om slachtoffers te misleiden: De noodzaak om de huidige berichten ter voorkoming van romantische fraude te herzien. Crime Prevention and Community Safety, 24(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Bronnen

Cunha, H. S. (z.d.). Waarom zijn romantische oplichtingspraktijken zo krachtig? https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf

CybSafe. (2023). Romantische oplichting: de statistieken en wat ze betekenen voor uw organisatie. https://www.cybsafe.com/blog/romance-scams-stats-for-organizations/

Daily Mail. (2024, 1 juni). Britse grootmoeder gearresteerd in Brazilië voor cocaïnesmokkel. https://www.dailymail.co.uk/news/article-14718249/Grandmother-Veronica-Watson-Brazil-drugs.html

Dellinger, A. J. (2019). Anatomie van een oplichting: Nigeriaanse romantische oplichter deelt geheimen. Forbes. https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/

Dogma. Romantische oplichting: de signalen en hoe u uzelf kunt beschermen. https://www.dogma.it/it/news/truffe-sentimentali--i-segnali-e-come-difendersi

Eberhart, C. (2023, 26 mei). Wie houdt je in de gaten? AI kan nietsvermoedende slachtoffers met 'gemak en precisie' bespioneren: Experts. Fox News. https://www.foxnews.com/us/who-is-watching-you-ai-can-stalk-unsuspecting-victims-ease-precision-experts

Europol. 13 arrestaties in Italië voor het bedriegen van ouderen in een liefdesrelatie. https://www.europol.europa.eu/media-press/newsroom/news/13-arrested-in-italy-for-tricking-elderly-love

Europol. Hoe voorkom je dat je in de val trapt van de 'lover boy'-truc? Europol. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-not-to-fall-for-lover-boy-scam

Bronnen

Europol. (2023). Spotlightrapport: Online fraudeschema's. https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Europol. (2017). Online seksuele dwang en afpersing als misdrijf dat kinderen treft. Agentschap van de Europese Unie voor rechtshandhavingssamenwerking. https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Federal Bureau of Investigation. (2024, 3 december). Criminelen gebruiken generatieve kunstmatige intelligentie om financiële fraude te faciliteren. https://www.ic3.gov/PSA/2024/PSA241203

Federal Trade Commission. (2023). De favoriete leugens van romantische oplichters ontmaskerd. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

Federale Handelscommissie. Meld fraude. https://reportfraud.ftc.gov/

Federale Handelscommissie. Online romantische oplichting voorkomen. https://www.consumer.ftc.gov

Finney, G. (2023). Project Zero Trust. Cybersecurity Insights. https://www.cybersecurityinsights.com/project-zero-trust

Fintech Global. (2025, 13 februari). Banken lopen een verhoogd reputatie- en financieel risico door de toename van romantische oplichting. https://fintech.global/2025/02/13/banks-face-heightened-reputational-and-financial-risks-as-romance-scams-surge/

Goodwin, L. (2024, 19 december). 'AI deepfake-romantiekscam heeft me voor £17.000 opgelicht'. BBC News. https://www.bbc.co.uk/news/articles/cdr0g1em52go

Bronnen

Gozzi, L. (2025, 15 januari). Franse vrouw die door AI-gestuurde Brad Pitt werd misleid, wordt online bespot. BBC News. https://www.bbc.co.uk/news/articles/ckgnz8rw1xgo

Howard, R. (2023). Cybersecurity First Principles: A Reboot of Strategy and Tactics. John Wiley & Sons. https://www.wiley.com/en-us/Cybersecurity%2BFirst%2BPrinciples%3A%2BA%2BReboot%2Bof%2BStrategy%2Band%2BTactics-p-9781394173099

Internet Crime Complaint Center (IC3). (z.d.). Romantische oplichting. https://www.ic3.gov/

Interpol. (2022). Interpol-rapport over trends in sextortion. Internationale Criminele Politieorganisatie. Geraadpleegd via https://www.interpol.int

Kollmorgen, A. (2025). Door AI aangedreven romantische oplichting leidt waarschijnlijk tot hogere verliezen. Choice. https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/romance-scams-and-how-to-avoid-them

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online seksuele uitbuiting van kinderen: prevalentie, proces en kenmerken van daders. Trauma, geweld & misbruik, 15(2), 126–139. https://doi.org/10.1177/1524838013511543

Lee, Y., & Gelman, B. (2023, 27 november). De donkere kant van AI: Grootschalige oplichtingscampagnes mogelijk gemaakt door generatieve AI. Sophos News. https://news.sophos.com/en-us/2023/11/27/the-dark-side-of-ai-large-scale-scam-campaigns-made-possible-by-generative-ai/

Magramo, K. (2024, 17 mei). Britse ingenieursgigant Arup blijkt slachtoffer van deepfake-oplichting ter waarde van 25 miljoen dollar. CNN. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

Bronnen

Mattackal, L. P. (2025, 14 februari). Crypto-oplichting bereikt waarschijnlijk een nieuw record in 2024, mede dankzij AI, aldus Chainalysis. Reuters. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/

Narang, S. (2024, 14 februari). Oplichting met het slachten van varkens: Hoe investeringen in Bitcoin, Ethereum, Litecoin en spotgoud (XAUUSD) worden gebruikt bij romantische oplichting om honderden miljoenen te stelen. Tenable. https://www.tenable.com/blog/pig-butchering-scam-bitcoin-ethereum-litecoin-spot-gold-xauusd-romance-scam

Nationaal Centrum voor Cyberbeveiliging. (24 januari 2024). De impact van AI op cyberdreigingen op de korte termijn. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

National Crime Agency [NCA]. (2021). Rapport over sextortion-dreigingen. NCA Cybercrime Unit. https://www.nationalcrimeagency.gov.uk

Newcastle University. (z.d.). Slachtoffers van online datingfraude: Psychologische impactanalyse. https://doi.org/10.54097/ehss.v4i.2740

Newman, L. H., & Burgess, M. (2024, 30 september). De invasie van de varkensslachterij is begonnen. Wired. https://www.wired.com/story/pig-butchering-scam-invasion/

Newman, L. H., & Burgess, M. (2025, 13 februari). De eenzaamheidsepidemie is een veiligheidscrisis. Wired. https://www.wired.com/story/loneliness-epidemic-romance-scams-security-crisis/

Nielson, S. J. (2023). Ontdekking van cyberbeveiliging: een technische inleiding voor de absolute beginner. Apress. https://doi.org/10.1007/978-1-4842-9560-1

Patchin, J. W., & Hinduja, S. (2020). Sextortion onder adolescenten: resultaten van een nationale enquête onder Amerikaanse jongeren. Sexual abuse: a journal of research and treatment, 32(1), 30–54. https://doi.org/10.1177/1079063218800469

Bronnen

Patel, M. (2025). Cyberbeveiliging voor beginners: leer praktische vaardigheden om je te verdedigen tegen cyberdreigingen en bereid je voor op certificeringsexamens. Michael Patel. ISBN-13: 9798227516435.

pen University. (2024). De psychologie van cybercriminaliteit. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

Pietilä, E. & Korhonen, H. (5.06.2024). De harde realiteit van romantische oplichting. https://nordicwelfare.org/popnad/en/artiklar/the-harsh-realities-of-romance-scams/

Policija.si. (z.d.). Romantische oplichting. Sloveense politie. https://www.policija.si/eng/prevention/internet-security/romance-scams

Rege, A. (2009). Vervalsde liefde: Een systematisch literatuuronderzoek naar online romantische oplichting. Interacting with Computers, 21(5-6), 427–437. https://doi.org/10.1016/j.intcom.2009.06.006

Rogiers, A., et al. (2024, 11 november). Overtuiging met grote taalmodellen: een overzicht. arXiv. https://doi.org/10.48550/arxiv.2411.06837

Sanction Scanner. (2024, 16 september). Hoe generatieve kunstmatige intelligentie geld witwast. https://www.sanctionscanner.com/blog/ais-dark-side-how-generative-artificial-intelligence-launders-money-863

ScamWatch. (2024, 15 augustus). Oplichting via online dating en romantische relaties. https://www.scamwatch.gov.au/types-of-scams/online-dating-and-romance-scams

SciSpace. (z.d.). Online romantische oplichting: relationele dynamiek en psychologische inzichten. https://scispace.com/papers/online-romance-scams-relational-dynamics-and-psychological-5cckseevfj

Bronnen

Shea, S., & Krishnan, A. (2024). Hoe AI phishingaanvallen gevaarlijker maakt. TechTarget. https://www.techtarget.com/searchSecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

Shepardson, D. (2024). Consultant beboet met 6 miljoen dollar voor het gebruik van AI om Bidens stem te vervalsen in geautomatiseerde telefoontjes. Reuters. https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/

Statista. (2025). Aantal nepaccounts dat Facebook per kwartaal wereldwijd heeft verwijderd, vanaf het eerste kwartaal van 2025. https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hall, J., & Kieran. (2024, november). Door AI mogelijk gemaakte beïnvloedingsoperaties: Toekomstige verkiezingen veiligstellen. CETaS Research Reports.

Politie van Surrey. Romantische oplichting. Politie van Surrey. https://www.surrey.police.uk/romancefraud

Tech Report. Statistieken over romantische oplichting. https://techreport.com/statistics/cybersecurity/romance-scam-statistics/

The Debt Advisor. (2023). Romantische oplichting: een groeiende bedreiging voor zowel mannen als vrouwen. https://www.thedebtadvisor.co.uk/romance-scams/

The Guardian. (2024). Spaanse politie arresteert vijf mensen in verband met nep-Brad Pitt-oplichting. https://www.theguardian.com/film/2024/sep/23/spanish-police-arrest-five-people-over-fake-brad-pitt-scam

Bronnen

Bureau van de Verenigde Naties voor Drugsbestrijding en Misdaadpreventie (2024). Transnationale georganiseerde misdaad en de convergentie van cyberfraude, illegaal bankieren en technologische innovatie in Zuidoost-Azië: een veranderend dreigingslandschap. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

Amerikaanse Federal Reserve. (2024). Synthetische identiteitsfraude: Generatieve AI-toolkit voor het detecteren van betalingsfraude. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

Amerikaanse immigratie- en douanedienst (ICE). (10-02-2025). Sextortion. https://www.ice.gov/features/sextortion#

Bureau van de Verenigde Naties voor Drugsbestrijding en Misdaadpreventie (2024). Transnationale georganiseerde misdaad en de convergentie van cyberfraude, illegaal bankieren en technologische innovatie in Zuidoost-Azië: een veranderend dreigingslandschap. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

Amerikaanse Federal Reserve. (2024). Synthetische identiteitsfraude: Generatieve AI-toolkit voor het detecteren van betalingsfraude. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

Wang, C. (2022). Psychologische impactanalyse bij slachtoffers van online datingfraude. Journal of Education, Humanities and Social Sciences, 4, 149-154. https://doi.org/10.54097/ehss.v4i.2740

Wang, F. (2024). Het stilzwijgen doorbreken: Onderzoek naar het proces van cybersextortion en de copingstrategieën van slachtoffers. International Review of Victimology, 31(1), 91-116. https://doi.org/10.1177/02697580241234331 (Oorspronkelijk werk gepubliceerd in 2025)

Bronnen

Whitty, M. T., & Buchanan, T. (2016). Hou je van me? Psychologische kenmerken van slachtoffers van romantische oplichting. Psychologische kenmerken van slachtoffers van romantische oplichting - PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5297105/

Whitty, M. T., & Buchanan, T. (2016). De online dating-romantiekoplichting: oorzaken en gevolgen van slachtofferschap [PDF]. Universiteit van Warwick. https://wrap.warwick.ac.uk/id/eprint/81382/1/WRAP_whitty__buchananpsychological_impact_romance_scam_final_version.pdf

Whitty, M. & Buchanan, T. (2012). De online romantische oplichting: een ernstig cybermisdrijf. Cyberpsychologie, gedrag en sociale netwerken. 15. 181-3. 10.1089/cyber.2011.0352.

Wrexham.com. (2024, 13 februari). Man uit Wrexham voor £25.000 opgelicht in romantische oplichting. https://wrexham.com/news/warning-issued-after-wrexham-man-conned-out-of-25k-in-romance-scam-247088.html

Yeung, J. (2024, 15 oktober). Deepfake-romantiekfraude leverde 46 miljoen dollar op van mannen in heel Azië, aldus de politie. CNN. https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk/index.html

Zhang, D., et al. (2024, 9 februari). IP-Adapter inpainting: Bestuurbare inpainting met IP-Adapter. arXiv. https://arxiv.org/html/2502.06593v1

Zvelo. (2023, 8 november). De rol van AI in social engineering. https://zvelo.com/the-role-of-ai-in-social-engineering

Zvelo. (2023, 8 november). De rol van AI in social engineering. U

Neem contact met ons op!

Deze handleiding is gezamenlijk ontwikkeld door de FALS-projectcoördinatoren: EUW (Duitsland), ECREC (Nederland) en IVI (Italië).

Om in contact te blijven en voor vragen, opmerkingen of suggesties, kunt u gerust contact met ons opnemen via onderstaande kanalen.

ECREC (Nederland)

Telefoon
+31 70 200 2595

E-mail
info@ecrec.eu

Website
https://ecrec.eu/

EUW (Duitsland)

Telefoon
+49 176 55030502

E-mail
projects@euthwonders.org

Website
www.euthwonders.org

IVI (Italië)

Telefoon
+39 329 599 7585

E-mail
igorvitaleinternational@gmail.com

Website
https://www.igorvitale.org/

Co-funded by the European Union