ONLINE FINANCIËLE FRAUDE EN OPLICHTING IN EEN WERELD MET ARTIFICIËLE INTELLIGENTIE

BLIJF ALERT EN BESCHERM JEZELF

Online financiële fraude en oplichting zijn niet nieuw, maar artificiële intelligentie (AI) heeft deze vormen van fraude en oplichting slimmer gemaakt en moeilijker te herkennen. Criminelen gebruiken nu valse berichten en websites, valse-profielen van bekendheden en zelfs AI-gegenereerde stemmen of video's die eruitzien als je bankier, je vrienden of je familie om je voor de gek te houden.

Ze bereiken je vaak via sociale media, e-mails, onverwachte oproepen en app-berichten die echt lijken.

Je 'loopt risico op financiële schade, identiteitsdiefstal en emotionele schade. Wees voorzichtig en volg deze tips om veilig te blijven:

Wees alert op bestaande online financiële fraude en AI-aangedreven oplichting, bijvoorbeeld imitatie, phishing, beleggings- en verzekeringsfraude en zelfs datingfraude. Voor meer informatie over verschillende soorten fraude en oplichting zie pagina 5, 6 en 7.

En zie deze factsheet over fraude en oplichting die specifiek zijn voor crypto ( ).

Let op waarschuwingssignalen: Leer verdachte gedragingen, berichten of aanbiedingen herkennen (zie pagina 2).

Bescherm jezelf: Beveilig persoonsgegevens (zie pagina 3) en

Weet wat je moet doen als je het slachtoffer wordt van fraude of oplichting (zie pagina 4).

Waarschuwingssignalen

Een belofte die te mooi lijkt om waar te zijn.

Een onverwacht telefoontje van een onbekend nummer.

Een dringend verzoek om geld of persoonlijke informatie, ook van iemand die zich voordoet als een familielid, een vriend of zelfs een publieke persoonlijkheid.

Een verzoek om de controle over een apparaat over te nemen, een app te downloaden, een QR-code te scannen of op een link te klikken.

Een verzoek voor persoonlijke informatie of bankgegevens (bijvoorbeeld wachtwoorden, creditcardnummers, inloggegevens voor internetbankieren of beveiligingscodes).

Een verzoek voor betaling via niet-traceerbare methoden (bv. cryptos, cadeaukaarten, overschrijvingen of prepaid debetkaarten).

Een verdacht of onjuist e-mailadres of link (bijvoorbeeld spelfouten in de URL of ongebruikelijke webadressen).

Een bijlage van een onbekende bron, met name een.exe, .scr, .zip of Office-bestand (.docm, .xlsm) met macro's.

Slechte grammatica of opmaak in een officieel ogend document, hoewel AI de fraudeurs in staat kan stellen deze fouten te voorkomen.

Een website die er professioneel uitziet, maar geen geverifieerde contactgegevens of bedrijfsregistratie-informatie heeft.

Intonatie die onnatuurlijk klinkt, pauzes mist en overdreven vloeiend of robotachtig lijkt. Besteed aandacht aan "voice cloning", hoewel door AI gegenereerde spraak ook heel natuurlijk kan klinken.

Video's waarbij de stem robotachtig of overdreven glad klinkt, lipbewegingen en gezichtsuitdrukkingen die verkeerd zijn uitgelijnd met de spraak, of achtergrond, verlichting en schaduwen die inconsistent zijn. Dit zijn vaak AI-gegenereerde video's (deepfakes).

Stappen om jezelf te beschermen

1 **Deel nooit persoonlijke of bankgegevens:**

Betrouwbare bedrijven zullen nooit om pincodes, wachtwoorden, inloggegevens voor internetbankieren of beveiligingscodes vragen via e-mail, sms, sociale media of telefoon.

2 **Neem tijd en denk na voordat je handelt:**

Verstuur geen geld, deel geen informatie en klik niet op links. Oplichters creëren bewust een gevoel van urgentie (bijvoorbeeld IT-problemen met je bank, noodoproepen waarbij vrienden en familieleden betrokken zijn of dreigende taal). Bij twijfel: niet handelen, beëindig de oproep en verifieer de bron of identiteit zorgvuldig.

3 **Controleer de bron/identiteit zorgvuldig:**

- Controleer altijd waar berichten, oproepen, e-mails en links vandaan komen- zelfs als ze er officieel uitzien, lijken te komen van een vriend of familie, of zelfs een publieke persoonlijkheid. Bel of sms bijvoorbeeld familie en vrienden via een bekend nummer via een vertrouwd kanaal en let op spelfouten, vreemde URL's of ontbrekende beveiligingsindicatoren (bv. controleer of de link op de website een "s" in "HTTPS" bevat om ervoor te zorgen dat de website veilig is, en controleer op toegevoegde of ontbrekende letters in de bedrijfsnaam).

- Open geen links vanuit ongevraagde berichten, installeer alleen officiële applicaties via vertrouwde appstores en scan geen onbekende QR-codes.

- Spreek met je familie een 'safe word' af- een geheim woord dat je kunt gebruiken om je identiteit te bevestigen als iemand met een bekende stem je belt met een dringend verzoek voor geld en beweert een familielid te zijn (bijvoorbeeld ouders, zus/broer, kind).

- Gebruik geverifieerde contactgegevens om het bedrijf of de persoon rechtstreeks te bereiken en vertrouw nooit op de contactgegevens die door de vermoedelijke fraudeur zijn verstrekt (bijvoorbeeld onafhankelijk naar de bedrijfsnaam zoeken, geverifieerde bedrijfsinformatie gebruiken, eerder bevestigde contactmethoden). Oplichters kunnen beweren dat ze geautoriseerd zijn of de website van een geautoriseerd bedrijf nabootsen. Controleer of er waarschuwingen zijn afgegeven door uw nationale financiële toezichthoudende autoriteit of zijn opgenomen in de IOSCO I-SCAN-lijst (iosco.org/i-scan/). Controleer voor cryptoaanbieders of zij een vergunning hebben in de EU (zie bijvoorbeeld het ESMA-register ( ).

4 **Let op mogelijke AI-trucs:**

Naarmate de AI-technologie vordert, worden scams overtuigender dan ooit- zelfs met de beste beveiligingstips. Als iets ongewoon aanvoelt of als je een van de hierboven beschreven waarschuwingssignalen herkent, stop dan en beoordeel opnieuw.

5 **Installeer nooit software voor externe toegang en deel je scherm niet:**

Banken en financiële instellingen zullen dat nooit van je vragen.

6 **Houd apparaten en accounts veilig:**

Gebruik sterke en unieke wachtwoorden, houd ze geheim en vermijd het hergebruik van dezelfde inloggegevens op verschillende platforms. Schakel waar mogelijk multifactorauthenticatie in. Zie hier enkele tips voor wachtwoorden ( ). Houd software en antivirusbeveiliging up-to-date en geactiveerd.

7 **Wees voorzichtig met onverwachte en in tijd beperkte investeringsmogelijkheden:**

Als het te mooi klinkt om waar te zijn, dan is het dat waarschijnlijk ook.

8 **Denk na voordat je informatie deelt op sociale media:**

Chatgroepen, forums, posts en foto's op sociale media kunnen waardevolle bronnen zijn voor fraudeurs. Te veel onthullen over jezelf of je investeringen kan je een gemakkelijk doelwit maken.

Wat te doen als je slachtoffer bent geworden van fraude of oplichting

Stop transacties onmiddellijk

Om verdere overboekingen naar verdachte accounts te blokkeren en extra verliezen te voorkomen. Stop alle communicatie met de oplichters – negeer hun oproepen en e-mails en blokkeer de afzender.

Neem contact op met de bank of financiële onderneming:

Informeer de bank of financiële onderneming onmiddellijk via officiële contactkanalen, om opties te verkennen voor het bevriezen of terugdraaien van transacties.

Wijzig wachtwoorden op al je apparaten en apps/websites.

Fraudeurs kopen gelekte wachtwoorden online en proberen ze op meerdere accounts. Het wijzigen van slechts één wachtwoord is niet voldoende: wijzig alle wachtwoorden, zodat fraudeurs ze niet opnieuw kunnen gebruiken.

Melden en waarschuwen:

Meld het incident aan de politie of denationale financiële toezichthoudende autoriteit (↖) en informeer je netwerk (bv. vrienden en familie) om het bewustzijn te vergroten. Deze acties kunnen je helpen jezelf en anderen te beschermen.

Pas op voor ”recovery scams”:

De fraudeur kan contact opnemen met een slachtoffer van een eerdere oplichting, waarbij de fraudeur beweert een overheidsinstantie te zijn (bijvoorbeeld politie, belastingdienst of financiële toezichthouder) en aanbiedt om verloren geld tegen een vergoeding terug te vorderen. Dit is vaak een nieuwe poging tot oplichting. Vergeet niet: Als je eenmaal bent opgelicht, voorkomt dit niet dat je opnieuw wordt opgelicht. .

Europese Bankautoriteit, Europese Autoriteit voor verzekeringen en bedrijfspensioenen, Europese Autoriteit voor effecten en markten, 2025

Luxemburg: Bureau voor publicaties van de Europese Unie, 2025

PDF ISBN 978-92-9407-214-6 doi:10.2853/1793679 DZ-01-25-102-NL-N

SOORTEN DOOR AI AANGEDREVEN ONLINE FINANCIËLE FRAUDE EN OPLICHTING

Identiteitsfraude en gebruik van deep fakes

Je krijgt een onverwacht telefoontje van iemand die beweert van een bank te zijn, een overheidsinstantie (bijvoorbeeld politie, belastingdienst of financiële toezichthouder), een verzekeringsdistributeur, een IT-bedrijf of zelfs een familielid. De beller kan er op aandringen om geld over te maken om het geld veilig te houden, onder vermelding van verdachte activiteiten op een bankrekening of verzekeringspolis. Ze kunnen je ook vragen om bankgegevens bekend te maken (bijvoorbeeld betaalkaartnummer, inloggegevens voor internetbankieren of wachtwoorden), op een link te klikken of een software te installeren, ondeer het voorwensdel dat dit het probleem snel kan oplossen. De beller kan een vervalst nummer gebruiken, dat vaak overeenkomt met het telefoonnummer van een echte bank om legitiem te lijken (spoofing).

Oplichters kunnen AI gebruiken om nepvideo's, afbeeldingen of audio te maken die iemands stem (bijvoorbeeld een bankier of een familielid), gezicht (bv. een beroemdheid) of bewegingen nabootsen. **Dit staat bekend als "deepfake".**

Wat kan er gebeuren:

Door persoonlijke gegevens te vermelden en een gevoel van urgentie te creëren, misleidt de oplichter jou tot acties die je niet van plan was te ondernemen, zoals het verzenden van geld naar hun account, het klikken op een schadelijke link of het installeren van malware op een apparaat. Dit kan de oplichter directe toegang geven tot jouw bankgegevens. Met deze informatie kunnen ze je wachtwoord wijzigen, toegang krijgen tot een bankrekening en geld stelen. Vergeet niet: het feit dat een beller persoonlijke informatie over jou heeft, betekent niet dat hij/zij betrouwbaar is.

Phishing en social engineering

Je ontvangt een e-mail of bericht van een bank of een financiële onderneming waarin je wordt gewaarschuwd voor "verdachte activiteiten" op je rekening. Het logo, de lay-out en de taal zien er professioneel uit en het bericht kan in dezelfde thread verschijnen als andere gesprekken met de bank. Het bericht dringt erop aan om op een link te klikken om je account te verifiëren of een wachtwoord opnieuw in te stellen. De link leidt naar een nepwebsite die er identiek is aan de website voor internetbankieren. Zonder het te beseffen, voert je jouw gegevens in op een website die is ontworpen om persoonlijke gegevens te stelen.

Oplichters gebruiken AI om overtuigende phishingberichten te maken door sociale-mediagegevens te analyseren om hun slachtoffers te identificeren en de inhoud voor elk doelwit aan te passen.

Wat kan er gebeuren:

De oplichter opent jouw bankrekening en steelt geld of maakt een nepprofiel aan met jouw persoonlijke gegevens om fraude te plegen.

Beleggings- of verzekeringsfraude

Je ziet een advertentie op sociale media of een website die een “tijdelijke investeringsmogelijkheid met lage risico’s” of een “tijdelijkekorting” op een verzekering van een bekende onderneming promoot. De advertentie bevat een foto van een beroemdheid en aanbevelingen die vaak nep zijn. Nadat je interesse hebt getoond door op een link te klikken of een formulier in te vullen, word je gecontacteerd en doorgestuurd naar een platform of berichtenkanaal waar je professioneel uitziend advies en documenten ontvangt. Je wordt aangemoedigd om een klein bedrag te investeren, gevolgd door grotere bedragen, of om de premie te betalen op wat een veilige account lijkt te zijn.

Fraudeurs gebruiken AI-tools om deze nep voorstellen of e-mails zeer overtuigend en moeilijk op te sporen te maken. Ze gebruiken ook AI-aangedreven sociale mediabots om nepaccounts te maken die met communiceren, desinformatie verspreiden en echt gedrag simuleren om vertrouwen te winnen en beslissingen te beïnvloeden.

Wat kan er gebeuren:

Na een poging om je geld op te nemen of een claim in te dienen, stopt de contactpersoon met reageren. Je ontdekt dat het bedrijf niet bestaat of dat het verzekerde risico niet gedekt is. Je realiseert je dan dat hetgeld rechtstreeks naar een oplichter is gestuurd als onderdeel van een fraude. Helaas kun je je geld niet terugkrijgen en kunnen je persoonlijke en financiële gegevens worden gebruikt om verdere fraude te plegen (bijvoorbeeld het ondertekenen van contracten in jouw naam waardoor je mogelijk nog meer geld verliest).

Datingfraude

Je bent benaderd op sociale media, dating-apps of via telefoon/sms door iemand die je in het echte leven niet hebt ontmoet. Deze persoon voert frequente, persoonlijke en romantische gesprekken en bouwt vertrouwen op met behulp van nepprofielen. Na verloop van tijd verschuift het gesprek naar geld of financiële kansen, zoals crypto-investeringen met beloften van een hoog rendement en een laag risico. De persoon vraagt om geld over te maken naar een account of begeleidt je bij het opzetten van een account en het maken van een kleine eerste storting om de oplichting legitiem te laten lijken,waarna je wordt aangemoedigd om meer te investeren.

Fraudeurs gebruiken AI om nepprofielen te maken, hun slachtoffers te identificeren op sociale media/ dating-apps met behulp van gegevens die je beschikbaar hebt gesteld, of zij gebruiken chatbots om berichten te genereren.

Wat kan er gebeuren:

De oplichter haalt zoveel mogelijk geld binnen, verbreekt vervolgens alle communicatie en verdwijnt. De frauduleuze beleggingswebsite of -app wordt offline gehaald, waardoor je geen toegang hebt tot de veronderstelde beleggingen. Naast financieel verlies kunnen de persoonlijke gegevens die je hebt gedeeld, worden gebruikt om vrienden en familie te targeten of voor identiteitsdiefstal die financiële of juridische gevolgen voor jou kan hebben (de fraudeur kan bijvoorbeeld aankopen doen, leningen op jouw naam nemen of je kunt verantwoordelijk worden gehouden voor schulden of misdaden die onder jouw naam zijn gepleegd totdat het tegendeel is bewezen).

Oplichting bij een aankoop

Je komt een aantrekkelijke deal tegen voor een aankoop op een online marktplaats. Het bedrijf dat de deal aanbiedt, vraagt om een betaling buiten het officiële platform, beweert dat het een “veilig betalingssysteem” gebruikt en stuurt een link om de aankoop te voltooien. De link leidt door naar een frauduleuze bankauthenticatiepagina die de officiële website van de bank imiteert en het logo en ontwerp ervan gebruikt, waardoor je jouw onlinebankgegevens invoert om de betaling te doen.

Oplichters gebruiken AI om zeer overtuigende nepbankwebsites, orderbevestigingen en facturen te maken. AI helpt hen de toon, branding en stijl van echte bedrijven na te bootsen. In sommige gevallen gebruiken ze AI-chatbots om vragen te beantwoorden en de deal geloofwaardiger te maken.

Wat kan er gebeuren:

De betaling via een externe link omzeilt de bescherming van de marktplaats. De oplichter verkrijgt deinloggegevens van jouw bankrekening en steelt je geld.