ONLINE FINANCIËLE FRAUDE EN SCAMS IN EEN ARTIFICIËLE INTELLIGENTIE WERELD

BLIJF ALERT EN BESCHERM UZELF

Online financiële fraude en oplichting zijn niet nieuw, maar kunstmatige intelligentie (AI) heeft ze slimmer en moeilijker te herkennen gemaakt. Criminelen gebruiken nu valse berichten en websites, valse celebrity-profielen en zelfs AI-gegenereerde stemmen of video's die eruit zien als uw bankier, uw vrienden of uw familie om u voor de gek te houden.

Ze bereiken u vaak via sociale media, e-mails, onverwachte oproepen en berichten-apps die echt klinken.

U kunt worden geconfronteerd met risico's zoals financieel verlies, identiteitsdiefstal en emotionele schade. Wees voorzichtig en volg deze belangrijke tips om veilig te blijven:

Blijf alert voor bestaande online financiële fraude en oplichting die wordt aangedreven door AI, bijvoorbeeld imitatie, phishing, beleggings- en verzekeringszwendel en zelfs romantische fraude en oplichting. Voor meer informatie over verschillende soorten fraude en oplichting blz. 5 en 6.

En hier voor fraude en oplichting die specifiek zijn voor crypto ( ).

Waarschuwingssignalen: Leer verdachte gedragingen, berichten of aanbiedingen herkennen (blz. 2)

Bescherm uzelf: Beveilig uw persoonlijke gegevens (blz. 3) en

Weet wat u moet doen als u het slachtoffer wordt van fraude of oplichting (blz. 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, inclusief van iemand die zich voordoet als een familielid, een vriend of zelfs een publieke figuur.

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

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

Een verzoek om betaling via niet-traceerbare methodes (bv. crypto's, 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, in het bijzonder .exe, .scr, .zip, of macro-enabled Office-bestand (.docm, .xlsm).

Slechte grammatica of opmaak in een officieel ogend document, ook al stelt AI fraudeurs in staat deze fouten effectiever te maskeren.

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 "spraakklonen", ook al kan door AI gegenereerde spraak ook heel natuurlijk klinken.

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

Stappen om uzelf te beschermen

1 **Deel nooit persoonlijke of bankgegevens:**

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

2 **Pauzeer en denk na voordat u handelt:**

Verstuur geen geld, deel geen informatie of klik niet op links- oplichters creëren bewust een gevoel van urgentie (bv. IT-problemen met uw bank, noodoproepen waarbij uw vrienden en familieleden betrokken zijn, dreigende taal enz.). In geval van twijfel, zelfs kleine, 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 uw familie, of zelfs een publieke figuur. Bel of sms bijvoorbeeld uw familie en vrienden via een bekend nummer via een vertrouwd kanaal; ga op zoek naar spelfouten, vreemde URL's of ontbrekende beveiligingsindicatoren (bv. controleren of de link op de website een "s" in "HTTPS" bevat om ervoor te zorgen dat de website veilig is, en controleren 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.

- Kom met uw familie een 'veilig woord' overeen- een geheime uitdrukking die u kunt gebruiken om uw identiteit te bevestigen als iemand met een bekende stem u belt met een dringend verzoek om 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 bedrijfsgidsen gebruiken, eerder bevestigde contactmethoden). Oplichters kunnen beweren dat ze geautoriseerd zijn of de website van een geautoriseerd bedrijf nabootsen. Controleer of er waarschuwingen zijn gepubliceerd door uw nationale financiële 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 **Besteed aandacht aan mogelijke AI-trucs:**

Naarmate de AI-technologie vordert, wordt oplichting overtuigender dan ooit- zelfs met de beste beveiligingstips. Als iets ongewoon aanvoelt of als u een van de hierboven beschreven waarschuwingssignalen detecteert, stop dan en beoordeel opnieuw.

5 **Installeer nooit software voor externe toegang of deel uw scherm niet:**

Banken en financiële instellingen zullen dat nooit van u 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 uw software en antivirusbeveiliging up-to-date en geactiveerd.

7 **Wees voorzichtig met onverwachte en tijdelijke investeringsmogelijkheden:**

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

8 **Denk na voordat u informatie deelt op social media:**

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

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

Stop onmiddellijk transacties

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

Neem contact op met uw bank of financiële onderneming:

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

Wijzig uw wachtwoorden op al uw apparaten en apps/websites.

Fraudeurs kopen gelekte wachtwoorden online en proberen ze op meerdere accounts. Het wijzigen van slechts één wachtwoord is niet voldoende; Zorg ervoor dat u ze allemaal wijzigt, zodat fraudeurs ze niet opnieuw kunnen gebruiken.

Melding en waarschuwing:

Meld het incident aan de politie of uw nationale financiële autoriteit
Vragen over beleggingsfraude? | FSMA) en informeer uw netwerk (bv. vrienden en familie) om het bewustzijn te vergroten. Deze acties kunnen u helpen zichzelf en anderen te beschermen.

Pas op voor “recovery room”-fraude:

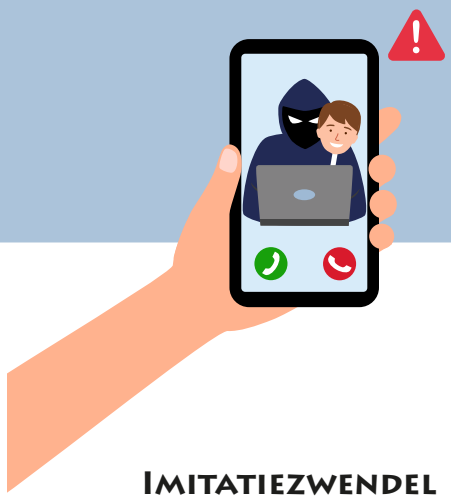
De fraudeur kan contact met u opnemen in de wetenschap dat u het slachtoffer bent van een eerdere zwendel, waarbij hij beweert een overheidsinstantie te zijn (bijv. politie, belasting- of financiële autoriteit enz.) en aanbiedt om uw verloren geld tegen een vergoeding terug te vorderen. Dit is vaak een andere poging om je op te lichten. Vergeet niet: als u eenmaal wordt opgelicht, voorkomt dit niet dat u 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

DOOR AI aangedreven ONLINE FINANCIËLE FRAUDE EN SCAMS



Imitatiezwendel en gebruik van deep fake

U krijgt een onverwacht telefoontje van iemand die beweert uw bank te zijn, een overheidsinstantie (bv. politie, belasting- of financiële autoriteit enz.), een verzekeringsdistributeur, een IT-bedrijf of zelfs een familielid. De beller kan er bij u op aandringen om geld over te maken om het veilig te houden, door te verwijzen naar verdachte activiteiten op uw account of uw verzekeringspolis. Ze kunnen u ook vragen om uw bankgegevens over te maken (bijvoorbeeld betaalkaartnummer, inloggegevens voor internetbankieren of wachtwoorden), op een link te klikken of een software te installeren, alsof het het probleem snel kan oplossen. De beller kan een vervalst nummer gebruiken, dat vaak overeenkomt met het telefoonnummer van uw bank om legitiem te lijken (spoofing).

Oplichters kunnen AI gebruiken om valse video's, afbeeldingen of audio te maken die iemands stem (bv. uw 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 u tot acties die u niet van plan was te ondernemen, zoals het verzenden van geld naar hun account, het klikken op een kwaadaardige link of het installeren van malware op uw apparaat. Dit kan de oplichter directe toegang geven tot uw bankgegevens. Met deze informatie kunnen ze uw wachtwoord wijzigen, toegang krijgen tot uw bankrekening en uw geld stelen. Vergeet niet: het feit dat een beller persoonlijke gegevens over u kent, betekent niet dat hij/zij betrouwbaar is.

Phishing en social engineering

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

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

Wat kan er gebeuren:

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

Beleggings- of verzekeringszwendel

U ziet een advertentie op sociale media of een website die een “beperkte investeringsmogelijkheid met lage risico’s” of een “beperkte tijdskorting” op een verzekering van een bekende onderneming promoot. De advertentie bevat een foto van een beroemdheid en aanbevelingen die vaak nep zijn. Nadat u interesse hebt getoond door op een link te klikken of een formulier in te vullen, wordt u gecontacteerd en doorgestuurd naar een platform of berichtenkanaal waar u professioneel uitziend advies en documenten ontvangt. U 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 valse voorstellen of e-mails zeer overtuigend en moeilijk op te sporen te maken. Ze gebruiken ook AI-aangedreven socialemediabots om nepaccounts te maken die met u communiceren, desinformatie verspreiden en echt gedrag simuleren om vertrouwen te winnen en uw beslissingen te beïnvloeden.

Wat kan er gebeuren:

Na het proberen om uw geld op te nemen of een claim in te dienen, stopt het contact met reageren. U ontdekt dat het bedrijf niet bestaat of dat het niet gedekt is door uw verzekering. U realiseert zich dan dat u geld rechtstreeks naar een oplichter hebt gestuurd als onderdeel van een frauduleus schema. Helaas kunt u uw geld niet terugkrijgen en kunnen uw persoonlijke en financiële gegevens worden gebruikt om verdere fraude te plegen (bijvoorbeeld het ondertekenen van contracten namens u waardoor u mogelijk nog meer geld verliest).

Romantische fraude en oplichting

U bent gecontacteerd op sociale media, dating-apps of via telefoon / sms door iemand die u 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 u om geld over te maken naar een account of begeleidt u bij het opzetten van een account en het maken van een kleine eerste storting om het schema er legitiem uit te laten zien voordat u wordt aangemoedigd om meer te investeren.

Fraudeurs gebruiken AI om nepprofielen te genereren, hun slachtoffers te identificeren op sociale media/dating-apps met behulp van gegevens die u beschikbaar hebt gesteld, of chatbots te gebruiken 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 u geen toegang hebt tot de veronderstelde beleggingen. Naast financieel verlies kunnen de persoonlijke gegevens die u hebt gedeeld, worden gebruikt om uw vrienden en familie te targeten of voor identiteitsdiefstal die financiële of juridische gevolgen voor u kan hebben (de fraudeur kan bijvoorbeeld aankopen doen, leningen op uw naam nemen of u kunt verantwoordelijk worden gehouden voor schulden of misdaden die onder uw naam zijn gepleegd totdat het tegendeel is bewezen).

Aankoopzwendel

U 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 u een link om de aankoop te voltooien. De link leidt u door naar een frauduleuze bankauthenticatiepagina die de officiële website van de bank imiteert en het logo en ontwerp ervan gebruikt, zodat u uw online bankgegevens 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 uw inloggegevens op uw bankrekening en steelt uw geld.