



FRAUDE ȘI ESCROCHERII FINANCIARE ONLINE ÎN LUMEA INTELIGENȚEI ARTIFICIALE

FIȚI VIGILENȚI ȘI PROTEJAȚI-VĂ

Fraudele și escrocheriile financiare online nu sunt noi, dar inteligența artificială (IA) le-a făcut mai inteligente și mai greu de depistat. Infractorii folosesc acum mesaje și site-uri false, profiluri false de celebrități și chiar voci sau videoclipuri generate de IA care arată ca bancherul, prietenii sau familia dvs. pentru a vă păcăli.

Ei ajung adesea la dvs. prin intermediul social media, aplicații de mesagerie, e-mailuri și apeluri neașteptate care sună real.

S-ar putea să vă confrunțați cu riscuri cum ar fi pierderea financiară, furtul de identitate și suferința emoțională. Fiți precauți și urmați aceste sfaturi cheie pentru a rămâne în siguranță:



Fiți atenți la fraudele și înșelătoriile financiare online existente bazate pe IA,

de exemplu, imitarea, phishingul, înșelătoriile în materie de investiții și asigurări și chiar fraudele și înșelătoriile romantice. Pentru a afla mai multe despre diferitele tipuri de fraudă și înșelătorii vedeți [paginile 5, 6 și 7](#), iar despre fraude și înșelătorii specifice criptomonedelor vedeți fișa informativă dedicată privind fraudele și escrocheriile cu crypto ([📄](#)).



Identificați semnalele de alarmă:

Învățați să recunoașteți comportamentele, mesajele sau ofertele suspecte (vedeți [pagina 2](#)).



Protejați-vă:

Securizați-vă informațiile cu caracter personal (vedeți [pagina 3](#)).



Aflați ce trebuie să faceți dacă sunteți victima unei fraude sau a unor escrocherii (vedeți [pagina 4](#)).



Semne de avertizare



O promisiune care pare prea bună pentru a fi adevărată.



Un apel neașteptat de la un număr necunoscut.



O cerere urgentă de bani sau informații personale, inclusiv de la cineva care pretinde a fi un membru al familiei, un prieten sau chiar o persoană publică.



O solicitare de a prelua controlul asupra dispozitivului, de a descărca o aplicație, de a scana un cod QR sau de a face clic pe un link.



O solicitare de informații personale sau detalii bancare (de exemplu, parole, numere de carduri de credit, datele de autentificare pentru servicii bancare prin internet sau coduri de securitate).



O cerere de plată prin intermediul unor metode ce nu pot fi urmărite (de exemplu, cripto, carduri cadou, transferuri bancare sau carduri de debit preplătite).



O adresă de e-mail suspectă sau incorectă sau un link (de exemplu, erori de ortografie în URL sau adrese web neobișnuite).



Un atașament provenit dintr-o sursă necunoscută, în special fișiere .exe, .scr, .zip sau fișiere Office cu macro-uri activate (.docm, .xlsm).



Gramatica slabă sau formatarea într-un document cu aspect oficial, deși IA poate permite autorilor fraudelor să mascheze mai eficient aceste deficiențe.



Un site web care arată profesional, dar nu are date de contact verificabile sau informații de înregistrare a companiei.



Intonație care sună nefiresc, nu are pauze și pare prea fluentă sau robotică. Acordați atenție „clonării vocale”, deși discursul generat de IA poate suna, de asemenea, foarte natural.



Videoclipurile în care vocea poate suna robotic sau prea uniformă, mișcările buzelor și expresiile faciale pot fi nealiniate cu vorbirea sau fundalul, iluminarea și umbrele pot fi inconsecvente. Acestea sunt adesea videoclipuri generate de IA (deepfake-uri).

Pași pentru a vă proteja

1

Nu partajați niciodată informații personale sau bancare:

Companiile legitime nu vă vor solicita niciodată PIN-urile, parolele, datele de autentificare pentru servicii bancare prin internet sau codurile de securitate prin e-mail, text, social media sau telefon.

2

Opriti-vă și gândiți-vă înainte de a acționa:

Nu vă grăbiți să trimiteți bani, să faceți schimb de informații sau să faceți clic pe linkuri – escrocii creează în mod deliberat un sentiment de urgență (de exemplu, probleme informatice cu banca dvs., apeluri de urgență care implică prietenii și membrii familiei dvs., limbaj amenințător etc.). În caz de îndoieli, chiar minore, nu acționați; terminați apelul și verificați cu atenție sursa sau identitatea.

3

Verificați cu atenție sursa/identitatea:

- Verificați întotdeauna de unde provin mesajele, apelurile, e-mailurile și linkurile - chiar dacă par oficiale, par să provină de la un prieten sau de la familia dvs. sau chiar de la o persoană publică. De exemplu, apăsați sau trimiteți un mesaj familiei și prietenilor utilizând un număr cunoscut printr-un canal de încredere; căutați erori de ortografie, URL-uri ciudate sau indicatori de securitate care lipsesc (de exemplu, verificați dacă linkul site-ului web include un „s” în „HTTPS” pentru a vă asigura că site-ul web este securizat și verificați dacă există litere adăugate sau lipsă în numele societății).
- Nu deschideți linkuri din mesaje nesolicitate, instalați numai aplicații oficiale prin intermediul magazinelor de aplicații de încredere și nu scanați coduri QR necunoscute.
- Stabiliți împreună cu familia dvs. un „cuvânt de siguranță” - o frază secretă pe care o puteți folosi pentru a confirma identitatea dacă cineva cu o voce familiară vă sună cu o cerere urgentă de bani și pretinde a fi un membru al familiei (de exemplu, părinți, soră / frate, copil).
- Utilizați datele de contact verificate pentru a ajunge direct la societate sau la persoana fizică și nu vă bazați niciodată pe informațiile de contact furnizate de persoana suspectată de fraudă (de exemplu, căutați numele societății în mod independent, utilizați anuare profesionale verificate, metode de contact confirmate anterior). Este posibil ca escrocii să pretindă că sunt autorizați sau să imite site-ul web al unei companii autorizate. Verificați dacă autoritatea financiară națională din țara dumneavoastră a emis avertismente sau dacă acestea au fost incluse în lista I-SCAN a IOSCO (iosco.org/i-scan/). Pentru furnizorii de criptomonede, verificați dacă aceștia sunt autorizați în UE [de exemplu, verificați registrul ESMA (www.esma.europa.eu)].

4

Acordați atenție potențialelor trucuri IA:

Pe măsură ce tehnologia IA avansează, înșelătoriile devin mai convingătoare ca niciodată - chiar și cu cele mai bune sfaturi de securitate. Dacă ceva pare neobișnuit sau detectați oricare dintre semnele de avertizare prezentate mai sus, opriți-vă și reevaluați.

5

Nu instalați niciodată software de acces de la distanță și nu partajați ecranul:

Băncile și instituțiile financiare nu vă vor solicita niciodată acest lucru.

6

Păstrați dispozitivele și conturile securizate:

Utilizați parole puternice și unice, păstrați-le secrete și evitați reutilizarea aceluiași date de autentificare pe platforme diferite. Activați autentificarea multi-factor acolo unde este posibil. A se vedea câteva sfaturi privind parolele aici ([🔗](#)). Păstrați software-ul și protecția antivirus actualizate și activate.

7

Fiți precauți cu privire la oportunități de investiții neașteptate și limitate în timp:

Dacă sună prea bine ca să fie adevărat, probabil că este.

8

Gândiți-vă înainte de a partaja informații pe platformele de comunicare socială:

Grupurile de chat, forumurile, postările de pe platformele de comunicare socială și fotografiile pot fi surse valoroase de cunoștințe pentru autorii fraudelor. Dezvăluirea prea multor lucruri despre dvs. sau despre investițiile dvs. vă pot face o țintă ușoară.

Ce trebuie să faceți atunci când ați devenit victima unei fraude sau a unei înșelătorii



Opriți imediat tranzacțiile

Pentru a bloca orice transferuri ulterioare către conturi suspecte și pentru a evita pierderi suplimentare. Opriți orice contact cu escrocii – ignorați apelurile și e-mailurile acestora și blocați expeditorul.



Contactați banca sau societatea financiară:

Informați imediat banca sau instituția financiară prin intermediul canalelor oficiale de contact, pentru a explora opțiunile de blocare sau inversare a tranzacțiilor.



Modificați-vă parolele pe toate dispozitivele și aplicațiile/site-urile web:

Escrocii cumpără parole compromise online și le încearcă pe mai multe conturi. Schimbarea unei singure parole nu este suficientă; asigurați-vă că le schimbați pe toate, astfel încât autorii fraudelor să nu le poată reutiliza.



Raport și alertă:

Raportați incidentul la poliție sau la autoritatea financiară națională din țara dumneavoastră și informați rețeaua dumneavoastră (de exemplu, prietenii și familia) pentru a crește gradul de conștientizare. Aceste acțiuni vă pot ajuta să vă protejați pe dvs. și pe ceilalți.



Atenție la fraudele legate de „camera de recuperare”:

Fraudatorul vă poate contacta știind că sunteți victima unei escrocherii anterioare, pretinzând că este o autoritate publică (de exemplu, poliție, autoritate fiscală sau financiară etc.) și oferindu-se să vă ajute să recuperați banii pierduți în schimbul unei taxe. Aceasta este adesea o altă încercare de a vă înșela. Nu uitați: Faptul că ați fost înșelat o dată nu vă împiedică să fiți înșelați din nou.

TIPURI DE FRAUDE ȘI ESCROCHERII FINANCIARE ONLINE BAZATE PE IA



ÎNȘELĂTORIE PRIN UZURPAREA IDENTITĂȚII ȘI UTILIZAREA DE FALSURI PROFUNDE (DEEP FAKE)

Primiți un apel neașteptat de la cineva care pretinde că este banca dvs., o autoritate publică (de exemplu, poliție, autoritate fiscală sau financiară etc.), un distribuitor de asigurări, o companie IT sau chiar un membru al familiei. Apelantul vă poate îndemna să transferați fonduri pentru a le menține în siguranță, invocând activitatea suspectă din contul dvs. sau din polița de asigurare. De asemenea, vă pot solicita să dezvăluiți detaliile dvs. bancare (de exemplu, numărul cardului de plată, datele de autentificare pentru servicii bancare prin internet sau parolele), să faceți clic pe un link sau să instalați un software, pretinzând că poate rezolva rapid problema. Apelantul ar putea utiliza un număr falsificat, care corespunde adesea numărului de telefon al băncii dvs. pentru a părea legitim (spoofing).

Escrocii pot utiliza IA pentru a crea videoclipuri, imagini sau materiale audio false care imită vocea unei persoane (de exemplu, bancherul sau un membru al familiei), fața (de exemplu, o celebritate) sau mișcările acesteia. **Acest lucru este cunoscut sub denumirea de „fals profund” („deepfake”).**

Ce s-ar putea întâmpla:

Menționând detaliile personale și creând un sentiment de urgență, escrocul vă păcălește să întreprindeți acțiuni pe care nu intenționați să le întreprindeți – cum ar fi trimiterea de bani în contul lor, accesarea unui link rău intenționat sau instalarea unui program malware pe dispozitivul dumneavoastră. Acest lucru poate oferi escrocului acces direct la datele dvs. de autentificare pentru servicii bancare. Cu aceste informații, vă pot schimba parola, vă pot accesa contul bancar și vă pot fura banii. Nu uitați: doar pentru că un apelant cunoaște detalii personale despre dumneavoastră, nu înseamnă că este demn de încredere.



PHISHING ȘI INGINERIE SOCIALĂ

Primiți un e-mail sau un mesaj care pare să provină de la banca dumneavoastră sau de la o societate financiară, avertizându-vă cu privire la o „activitate suspectă” în contul dumneavoastră. Logo-ul, aspectul și limba arată profesional, iar mesajul poate apărea în același fir ca și alte conversații cu banca. Mesajul vă îndeamnă să faceți clic pe un link pentru a vă verifica contul sau pentru a vă reseta parola. Link-ul duce la un site fals care arată identic cu internet banking-ul dvs. Fără să vă dați seama, introduceți detaliile dvs. într-un site web conceput pentru a vă fura informațiile personale.

Escrocii utilizează IA pentru a crea mesaje de phishing convingătoare, analizând datele de pe platformele de comunicare socială pentru a-și identifica victimele și adaptând conținutul pentru fiecare țintă.

Ce s-ar putea întâmpla:

Escrocul accesează contul dvs. bancar și vă fură banii sau creează un profil fals cu detaliile dvs. personale pentru a comite fraudă.



ÎNȘELĂTORIE ÎN MATERIE DE INVESTIȚII SAU ASIGURĂRI

Puteți vedea un anunț pe platformele de comunicare socială sau pe un site internet care promovează o „oportunitate de investiții pe durată limitată cu riscuri scăzute” sau o „reducere pe durată limitată” la o asigurare de la o societate bine-cunoscută. Anunțul conține o fotografie a unei celebrități și recomandări care sunt adesea false. După ce vă exprimați interesul făcând clic pe un link sau completând un formular, sunteți contactat și redirecționat către o platformă sau un canal de mesagerie unde primiți sfaturi și documente cu aspect profesional. Sunteți încurajați să investiți o sumă mică, urmată de sume mai mari, sau să plătiți prima în ceea ce pare a fi un cont sigur.

Escrocii utilizează instrumente de IA pentru a face aceste propuneri false sau e-mailuri extrem de convingătoare și dificil de detectat. Ei folosesc, de asemenea, roboți de social media alimentați de IA pentru a crea conturi false care interacționează cu dvs., răspundez dezinformarea și simulează comportamente reale pentru a câștiga încredere și a vă influența deciziile.

Ce s-ar putea întâmpla:

După ce încercați să vă retrageți banii sau să faceți o reclamație, contactul nu mai răspunde. Descoperiți că societatea nu există sau că riscul pe care l-ați asigurat nu este acoperit. Apoi vă dați seama că ați trimis bani direct unui escroc, ca parte a unei scheme frauduloase. Din păcate, nu puteți obține banii înapoi, iar detaliile dvs. personale și financiare pot fi utilizate pentru a comite fraude suplimentare (de exemplu, semnarea contractelor în numele dvs., ceea ce ar putea duce la pierderea și mai multor bani).



FRAUDĂ ROMANTICĂ ȘI ÎNȘELĂTORIE

Ați fost contactat pe social media, aplicații de întâlniri sau prin telefon / text de către cineva pe care nu l-ați întâlnit în viața reală. Această persoană inițiază conversații frecvente, personale și romantice, construind încredere folosind profiluri false. De-a lungul timpului, conversația se îndreaptă spre bani sau oportunități financiare, cum ar fi cripto-investițiile cu promisiuni de randamente ridicate și risc scăzut. Persoana vă cere să transferați bani într-un cont sau vă ghidează prin crearea unui cont și efectuarea unui mic depozit inițial pentru a face schema să pară legitimă înainte de a vă încuraja să investiți mai mult.

Escrocii utilizează IA pentru a genera profiluri false, pentru a-și identifica victimele pe platformele de comunicare socială/în aplicațiile de întâlniri utilizând datele pe care le-ați pus la dispoziție sau pentru a genera mesaje cu ajutorul roboților de conversație.

Ce s-ar putea întâmpla:

Escrocul extrage cât mai mulți bani posibil, apoi întrerupe orice comunicare și dispare. Site-ul sau aplicația de investiții frauduloase este lăsată offline, lăsându-vă în imposibilitatea de a accesa investițiile presupuse. Pe lângă pierderile financiare, informațiile cu caracter personal pe care le-ați partajat ar putea fi utilizate pentru a vă viza prietenii și familia sau pentru furtul de identitate care poate avea consecințe financiare sau juridice pentru dumneavoastră (de exemplu, autorul fraudei ar putea face achiziții, ar putea lua împrumuturi în numele dumneavoastră sau ați putea fi considerat responsabil pentru datorii sau infracțiuni comise sub numele dumneavoastră până la proba contrarie).



ÎNȘELĂTORIE LA CUMPĂRARE

Întâlniți o ofertă atractivă pentru o achiziție pe o piață online. Societatea care oferă tranzacția solicită o plată în afara platformei oficiale, susținând că utilizează un „sistem de plată sigur” și vă trimite un link pentru a finaliza achiziția. Link-ul vă redirecționează către o pagină de autentificare bancară frauduloasă care imită site-ul oficial al băncii și utilizează logo-ul și designul acesteia, astfel încât să introduceți detaliile dvs. bancare online pentru a efectua plata.

Escrocii folosesc IA pentru a crea site-uri bancare false extrem de convingătoare, confirmări de comenzi și facturi. IA îi ajută să imite tonul, imaginea de marcă și stilul companiilor reale. În unele cazuri, ei folosesc roboți de conversație cu IA pentru a răspunde la întrebări și pentru a face afacerea să pară mai credibilă.

Ce s-ar putea întâmpla:

Plata printr-o legătură terță ocolește protecția pieței. Escrocul obține informațiile dvs. de conectare în contul dvs. bancar și vă fură banii.