



ONLINE FINANČNÉ PODVODY VO SVETE UMELEJ INTELIGENCIE

BUĎTE OSTRÁŽITÍ A CHRÁŇTE SA

Online finančné podvody a podvody nie sú nové, ale umelá inteligencia (AI) ich urobila inteligentnejšími a ťažšie odhaliteľnými. Zločinci dnes používajú falošné správy a webové stránky, falošné profily celebrit a dokonca aj hlasy alebo videá generované umelou inteligenciou, ktoré vyzerajú ako váš bankár, vaši priatelia alebo vaša rodina, len aby vás oklamali.

Často vás oslovujú prostredníctvom sociálnych médií, aplikácií na odosielanie správ, e-mailov a neočakávaných hovorov, ktoré pôsobia veľmi dôveryhodne.

Môžete čeliť rizikám, ako je finančná strata, krádež identity a emocionálna ujma. Buďte opatrní a riadte sa týmito kľúčovými tipmi pre vašu bezpečnosť:



Buďte v pozore pred existujúcimi online podvodmi posilnenými o AI, napr.

krádeže identity, phishing, investičné a poisťné podvody a či dokonca romantické podvody. Ak sa chcete dozvedieť viac o rôznych druhoch podvodov viď [str. 5-7](#).

Pokiaľ ide o podvody špecifické pre kryptoaktíva viď osobitný dokument Podvody s kryptoaktívami ([📄](#)).



Všímajte si varovné signály:

Naučte sa rozpoznať podozrivé správanie, správy alebo ponuky viď [str. 2](#).



Chráňte sa:

Zabezpečte svoje osobné údaje viď [str. 3](#) a.



Majte plán: Zistite, čo robiť, ak sa stanete obeťou podvodu viď [str. 4](#).



Varovné signály



Sľub, ktorý znie príliš dobre na to, aby bol pravdivý.



Neočakávaný hovor z neznámeho čísla.



Naliehavá žiadosť o peniaze alebo osobné informácie, a to aj od niekoho, kto predstiera, že je rodinným príslušníkom, priateľom alebo dokonca verejnou osobnosťou.



Žiadosť o prevzatie kontroly nad zariadením, stiahnutie aplikácie, skenovanie QR kódu alebo kliknutie na odkaz.



Žiadosť o osobné informácie alebo bankové údaje (napr. heslá, čísla kreditných kariet, poverenia internetového bankovníctva alebo bezpečnostné kódy).



Žiadosť o platbu nevystopovateľnými metódami (napr. kryptoaktíva, darčkové karty, bankové prevody alebo predplatené debetné karty).



Podozrivá alebo nesprávna e-mailová adresa alebo odkaz (napr. pravopisné chyby v adrese URL alebo neobvyklé webové adresy).



Príloha z neznámeho zdroja, konkrétne .exe, .scr, .zip alebo súbor balíka Office s podporou makra (.docm, .xlsm).



Zlá gramatika alebo formátovanie v oficiálnom dokumente, hoci umelá inteligencia môže podvodníkom umožniť účinnejšie maskovať tieto nedostatky.



Webová stránka, ktorá vyzerá profesionálne, ale chýba jej overené kontaktné údaje alebo registračné údaje spoločnosti.



Intonácia, ktorá znie neprirodzene, chýbajú pauzy a zdá sa príliš plynulá alebo robotická. Dávajte si pozor na „klonovaní hlasu“, hoci reč generovaná umelou inteligenciou môže znieť aj veľmi prirodzene.



Videá, kde hlas znie roboticky alebo príliš hladko, pohyby pier a výrazy tváre sú nesprávne zosúladené s rečou alebo pozadím, osvetlenie a tieň môžu byť nekonzistentné. Často ide o videá vytvorené umelou inteligenciou (deepfakes).

Ako sa účinne chrániť

1

Nikdy nezdieľajte citlivé údaje:

Legitímne spoločnosti nikdy nebudú žiadať o vaše PIN kódy, heslá, prihlasovacie údaje k internetovému bankovníctvu alebo bezpečnostné kódy prostredníctvom e-mailu, SMS, sociálnych médií alebo telefónu.

2

Zastavte sa a zamyslite sa:

Neponáhľajte sa s posielaním peňazí ani klikaním na odkazy – podvodníci zámerné vytvárajú stres a pocit naliehavosti (napr. údajné IT problémy v banke, núdzové volania o nehode blízkych, vyhrážky). V prípade akýchkoľvek pochybností nekonajte. Ukončite hovor a dôkladne si overte zdroj alebo totožnosť volajúceho.

3

Dôkladne overujte zdroje:

- Vždy si overte pôvod správ, hovorov a e-mailov- aj keď vyzerajú oficiálne, zdá sa, že pochádzajú od priateľa alebo vašej rodiny, alebo dokonca od známej osobnosti. Zavolajte alebo napíšte svojej rodine a priateľom pomocou známeho čísla prostredníctvom dôveryhodného kanála; všímajte si pravopisné chyby, podivné URL adresy alebo chýbajúce bezpečnostné indikátory (napr. overte, či odkaz na webové sídlo obsahuje „s“ v „HTTPS“, aby ste sa uistili, že webové sídlo je bezpečné, a skontrolujte všetky pridané alebo chýbajúce písmená v názve spoločnosti).
- Neotvárajte odkazy z nevyžiadaných správ, inštalujte iba oficiálne aplikácie prostredníctvom dôveryhodných obchodov s aplikáciami a neskenujte neznáme QR kódy.
- Dohodnite sa so svojou rodinou na “bezpečnom slove”- tajnej fráze, ktorú môžete použiť na potvrdenie totožnosti, ak vám niekto so známym hlasom zavolá s naliehavou žiadosťou o peniaze a tvrdí, že je rodinným príslušníkom (napr. rodičia, sestra / brat, dieťa).
- Používajte len overené kontaktné údaje. Nikdy sa nespoliehajte na kontakty, ktoré vám pošle podozrivá osoba (firmu si vyhľadajte nezávisle cez oficiálne registre).. Podvodníci môžu tvrdiť, že sú autorizovaní alebo napodobňujú webové sídlo autorizovanej spoločnosti. Overte, či váš vnútroštátny orgán dohľadu nad finančným trhom vydal nejaké varovania alebo či boli zahrnuté do zoznamu IOSCO I-SCAN (iosco.org/i-scan/). V prípade poskytovateľov kryptoaktív skontrolujte, či majú povolenie v EÚ [napr. skontrolujte register orgánu ESMA ([↗](#))].

4

Pozor na triky umelej inteligencie:

S pokrokom AI sú podvody presvedčivejšie než kedykoľvek predtým. Ak sa vám niečo nepozdáva, okamžite zastavte komunikáciu a situáciu prehodnoťte.

5

Nikdy neinštalujte softvér na vzdialený prístup ani nezdieľajte obrazovku:

Banky a finančné inštitúcie vás o to nikdy nepožiadajú.

6

Zabezpečte zariadenia a účty:

Používajte silné a jedinečné heslá, udržiavajte ich v tajnosti a vyhýbajte sa opätovnému používaniu rovnakých poverení na rôznych platformách. Ak je to možné, povoľte viacfaktorovú autentifikáciu. Pozrite si niekoľko tipov na heslá. Aktualizujte a aktivujte svoj softvér a antivírusovú ochranu.

7

Buďte opatrní pri neočakávaných a časovo obmedzených investičných príležitostiach:

Ak to znie príliš dobre na to, aby to bola pravda, pravdepodobne to tak je.

8

Rozmýšľajte, čo zdieľate na sociálnych sieťach:

Chatové skupiny, fóra, príspevky na sociálnych médiách a fotografie môžu byť cenným zdrojom vedomostí pre podvodníkov. Odhalenie príliš veľa o sebe alebo vašich investíciách vás môže urobiť ľahkým cieľom.

Čo robiť, keď ste sa stali obeťou podvodu



Okamžite zastavte transakcie

S cieľom zablokovat' akékoľvek ďalšie prevody na podozrivé účty a zabrániť ďalším stratám. Zastavte akýkoľvek kontakt s podvodníkmi – ignorujte ich hovory a e-maily a zablokujte odosielateľa.



Obráťte sa na svoju banku alebo finančnú spoločnosť:

Okamžite informujte svoju banku alebo finančnú spoločnosť prostredníctvom oficiálnych kontaktných kanálov a požiadajte o zmrazenie účtu alebo storno transakcií.



Zmeňte svoje heslá na všetkých svojich zariadeniach a aplikáciách/webových stránkach.

Podvodníci kupujú uniknuté heslá online a skúšajú ich na viacerých účtoch. Zmeniť len jedno heslo nestačí. Uistite sa, že ich všetky zmeníte, aby ich podvodníci nemohli opätovne použiť.



Správa a upozornenie:

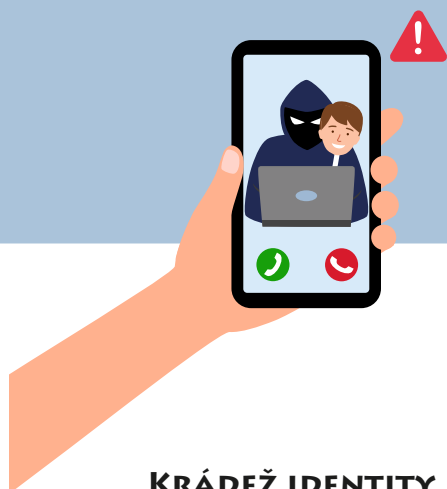
Nahláste incident polícii alebo váš vnútroštátnemu orgánu dohľadu nad finančným trhom (<https://podanie.nbs.sk/>) a informujte svoju sieť (napr. priateľov a rodinu) s cieľom zvýšiť informovanosť. Tieto opatrenia vám môžu pomôcť chrániť seba a ostatných.



Pozor na „vymáhacie“ podvody:

Podvodník vás môže kontaktovať s tým, že vie o vašej strate. Môže sa vydávať za políciu či úrad a ponúkať vrátenie peňazí za poplatok. Často ide o ďalší pokus o podvod. Pamätajte: to, že vás raz oklamali, neznamená, že to neskúsia znova.

TYPY ONLINE FINANČNÝCH PODVODOV S VYUŽITÍM AI



KRÁDEŽ IDENTITY (IMPERSONATION) A DEEPAKE

Dostanete neočakávaný hovor od niekoho, kto tvrdí, že je z vašej banky, polície, poisťovne, IT firmy, alebo dokonca že je váš príbuzný. Volajúci vás tlačí do prevodu peňazí „do bezpečia“ pod zámienkou podozrivej aktivity na účte. Môžu vás tiež požiadať, aby ste zverejnili svoje bankové údaje (napr. číslo platobnej karty, prihlasovacie údaje k internetovému bankovníctvu alebo heslá), klikli na odkaz alebo nainštalovali softvér na „vyriešenie problému“. Volajúci môže použiť falšované číslo, ktoré sa často zhoduje s telefónnym číslom vašej banky, aby sa zdalo legitímne (spoofing).

Podvodníci využívajú AI na tvorbu falošných videí, obrázkov alebo zvuku, ktoré imitujú hlas či tvár skutočnej osoby. Toto sa nazýva „Deepfake“.

Čo sa môže stať:

Spomenutím osobných údajov a vytvorením pocitu naliehavosti vás podvodník zmanipuluje na konanie, ktoré ste nemali v úmysle podniknúť – napríklad poslať peniaze, kliknúť na škodlivý odkaz alebo si nainštalovať vírus. Tým získa prístup k vášmu internetovému bankovníctvu, zmení heslá a ukradne peniaze. Pamätajte: to, že volajúci pozná vaše osobné údaje, ešte neznamená, že je dôveryhodný.



PHISHING A SOCIÁLNE INŽINIERSTVO

Dostanete e-mail alebo správu, ktorá zrejme pochádza od vašej banky alebo finančnej spoločnosti a ktorá vás upozorní na „podozrivú činnosť“ na vašom účte. Logo aj jazyk vyzerajú profesionálne a správa sa dokonca môže zaradiť do skutočného vlákna konverzácie s bankou. Správa vás vyzýva, aby ste klikli na odkaz na overenie vášho účtu alebo obnovenie hesla. Odkaz vedie k falošnej webovej stránke, ktorá vyzerá rovnako ako vaše internetové bankovníctvo. Bez toho, aby ste si to uvedomili, zadáte svoje údaje na webovú stránku určenú na ukradnutie vašich osobných údajov.

Podvodníci využívajú AI na tvorbu presvedčivých správ – analyzujú dáta zo sociálnych sietí a obsah prispôbujú priamo obeti na mieru.

Čo sa môže stať:

Podvodník prístupuje k vášmu bankovému účtu a ukradne vaše peniaze alebo vytvorí falošný profil s vašimi osobnými údajmi na páchanie ďalších podvodov.



INVESTIČNÝ ALEBO POISTNÝ PODVOD

Na sociálnych médiách alebo na webovom sídle sa zobrazuje reklama propagujúca „investičnú príležitosť na obmedzený čas s nízkym rizikom“ alebo „zľavu na obmedzený čas“ na poistenie od známej spoločnosti. Reklama obsahuje fotografiu celebrity a odporúčania, ktoré sú často falošné. Po kliknutí vás kontaktujú, presmerujú na chatovaciu platformu a pošlú profesionálne vyzerajúce dokumenty. Povzbudzujú vás investovať najprv malú sumu, neskôr väčšie čiastky, na zdanlivo bezpečný účet.

Podvodníci používajú nástroje umelej inteligencie na to, aby boli tieto falošné návrhy alebo e-maily vysoko presvedčivé a ťažko odhaliteľné. Používajú tiež AI botov na sociálnych sieťach, ktorí s vami komunikujú a simulujú reálne správanie, aby si získali vašu dôveru.

Čo sa môže stať:

Keď si chcete vybrať peniaze, kontakt prestane reagovať. Zistíte, že firma neexistuje alebo, že riziko, ktoré ste si poistili, nie je kryté. Uvedomíte si, že ste peniaze poslali priamo podvodníkovi. Peniaze už zväčša nezískate späť a vaše údaje môžu zneužiť na ďalšie podvody (napr. podpisovanie zmlúv vo vašom mene).



ROMANTICKÉ PODVODY

Kontaktuje vás niekto na zoznamke alebo sociálnej sieti, koho ste v reálnom živote nestretli. Táto osoba s vami vedie intenzívne romantické rozhovory a buduje si dôveru cez falošný profil. V priebehu času sa konverzácia presúva smerom k peniazom alebo finančným príležitostiam, ako sú krypto-investície s príslubmi vysokých výnosov a nízkeho rizika. Osoba vás navedie na založenie účtu a vloženie malého vkladu, aby systém vyzeral legitímne, a potom vás tlačí do vyšších investícií.

Podvodníci používajú umelú inteligenciu na generovanie falošných profilov, identifikáciu svojich obetí na sociálnych médiách/datovacích aplikáciách pomocou údajov, ktoré ste sprístupnili, alebo používajú chatboty na generovanie správ.

Čo sa môže stať:

Podvodník z vás vytiahne čo najviac peňazí, potom preruší kontakt a zmizne. Podvodné investičné webové stránky alebo aplikácie sú offline, takže nemáte prístup k predpokladaným investíciám. Okrem finančnej straty môžu byť osobné informácie, ktoré ste poskytli, použité na zacielenie na vašich priateľov a rodinu alebo na krádež totožnosti, ktorá môže mať pre vás finančné alebo právne dôsledky (napr. podvodník by mohol nakupovať, brať si pôžičky vo vašom mene alebo by ste mohli byť zodpovedný za dlhy alebo trestné činy spáchané pod vašim menom, kým sa nepreukáže opak).



NÁKUPNÉ PODVODY

Na online bazári alebo trhovisku narazíte na výhodnú ponuku. Predávajúci žiada platbu mimo oficiálnej platformy cez „bezpečný platobný systém“ a pošle vám odkaz. Odkaz vedie na falošnú bankovú bránu, ktorá imituje dizajn vašej banky, kde zadáte svoje prihlasovacie údaje.

Podvodníci využívajú AI na tvorbu veľmi presvedčivých falošných stránok, potvrdení a faktúr. AI im pomáha napodobniť tón a štýl skutočných firiem. V niektorých prípadoch používajú chatboty AI, aby odpovedali na otázky a aby sa dohoda zdala byť uveriteľnejšia.

Čo sa môže stať:

Platbou cez externý odkaz obídete ochranu trhoviska. Podvodník získa prístup k vášmu účtu a ukradne vaše peniaze.