



ONLINE FINANČNÍ PODVODY VE SVĚTĚ S UMĚLOU INTELIGENCÍ

ZŮSTAŇTE VE STŘEHU A CHRAŇTE SE

Online finanční podvody nejsou nic nového, ale díky umělé inteligenci (AI) jsou důmyslnější a obtížněji rozpoznatelné. Podvodníci používají falešné zprávy a webové stránky, falešné profily celebrit, a dokonce i hlasy nebo videa vytvořené umělou inteligencí, které vypadají jako Váš bankéř, Vaši přátelé nebo Vaše rodina, aby Vás oklamali.

Často Vás oslovují prostřednictvím sociálních sítí, aplikací pro zaslání zpráv, e-mailů a neočekávaných telefonátů, které zní skutečně.

Můžete čelit rizikům, jako je finanční ztráta, krádež identity a citová úzkost. Buďte opatrní a postupujte podle těchto klíčových doporučení, abyste zůstali v bezpečí:



Zůstaňte ve střehu před online finančními podvody, které využívají umělou inteligenci.

Těmi jsou např. podvody spočívající ve vydávání se za jinou osobu, phishing, investiční a pojišťovací podvody a dokonce i romantické podvody. Více o různých typech podvodů se dozvíte na [str. 5](#), [6](#), [7](#) a [8](#).

A na samostatném informativním přehledu o kryptoměnových podvodech ([📄](#)).



Varovné signály:

Naučte se rozpoznat podezřelé chování, zprávy nebo nabídky (viz [str. 2](#))



Chraňte se:

Zabezpečte své osobní údaje (viz [str. 3](#)) a



Vězte, co dělat, pokud se stanete obětí podvodu

(viz [str. 4](#)).



Varovné signály



Slib, který se zdá být příliš dobrý na to, aby byl pravdivý.



Nečekaný hovor z neznámého čísla.



Naléhavá žádost o peníze nebo osobní údaje, a to i od někoho, kdo předstírá, že je rodinným příslušníkem, přítelem nebo dokonce veřejně známou osobou.



Žádost o převzetí kontroly nad Vaším zařízením, stažení aplikace, naskenování QR kódu nebo kliknutí na odkaz.



Žádost o osobní údaje nebo bankovní údaje (např. hesla, čísla kreditních karet, přihlašovací údaje do internetového bankovníctví nebo bezpečnostní kódy).



Žádost o platbu prostřednictvím nevysledovatelných metod (např. kryptoměnami, dárkovými kartami, bezhotovostními převody nebo předplacenou debetní kartou).



Podezřelá nebo nesprávná e-mailová adresa nebo odkaz (např. pravopisné chyby v URL adrese nebo neobvyklé webové adresy).



Příloha z neznámého zdroje, zejména soubory .exe, .scr, .zip nebo soubor Office s podporou maker (.docm, .xlsm).



Pravopisné chyby nebo chybné formátování ve zdánlivě oficiálním dokumentu (umělá inteligence však může podvodníkům umožnit tyto nedostatky účinněji maskovat).



Webová stránka, která vypadá profesionálně, ale postrádá ověřené kontaktní údaje nebo informace o registraci společnosti.



Intonace, která zní nepřírodně, postrádá odmlky a zdá se být příliš plynulá nebo robotická. Dejte si pozor na „napodobování hlasu“, (řeč generovaná umělou inteligencí však také může znít velmi přirozeně).



Videa, která jsou namluvena hlasem, který zní roboticky nebo příliš hladce, pohyby rtů a výrazy v obličeji mohou být v nesouladu s řečí nebo pozadím, osvětlení a stíny mohou být nekonzistentní. Toto jsou časté znaky videí, vytvořených umělou inteligencí (tzv. deepfakes).

Jak se chránit

1

Nikdy nesdílejte osobní nebo bankovní informace:

Licencované společnosti nikdy nepožádají o Vaše PINy, hesla, přihlašovací údaje do internetového bankovníctví nebo bezpečnostní kódy e-mailem, textovou zprávou, přes sociální sítě nebo přes telefon.

2

Zastavte se a zamyslete se, než začnete jednat:

Nespěchejte se zasíláním peněz, sdílením informací nebo kliknutím na odkaz – podvodníci záměrně vytvářejí pocit naléhavosti (např. problémy s IT ve Vaší bance, tísňová volání týkající se Vašich přátel a členů rodiny, výhrušný jazyk atd.). V případě jakýchkoli, i malých, pochybností nejednejte. Ukončete hovor a pečlivě ověřte jeho zdroj nebo identitu volajícího.

3

Pečlivě zkontrolujte zdroj/identitu protistrany:

- Vždy ověřte, odkud pocházejí zprávy, hovory, e-maily a odkazy - i když vypadají oficiálně nebo vypadají, že pocházejí od přátel nebo Vaší rodiny, nebo dokonce od veřejně známé osoby. Můžete například zavolat nebo napsat své rodině a přátelům pomocí známého čísla a prostřednictvím důvěryhodného kanálu; všimněte si pravopisných chyb, zvláštních URL adres nebo chybějícího bezpečnostního ukazatele (např. ověřte, zda odkaz na internetové stránky obsahuje „s“ v předponě na začátku adresy „HTTPS“, abyste se ujistili, že internetové stránky jsou bezpečné, a zkontrolovat, zda v názvu společnosti nejsou přidána nebo chybí písmena).
- Neotevírejte odkazy z nevyžádaných zpráv, instalujte si pouze oficiální aplikace prostřednictvím důvěryhodných obchodů s aplikacemi a neskenujte neznámé QR kódy.
- Dohodněte se s rodinou na “bezpečném slově” - tajné frázi, kterou můžete použít k potvrzení identity, pokud Vám někdo známým hlasem zavolá s naléhavou žádostí o peníze a tvrdí, že je členem rodiny (např. rodiče, sourozenec nebo Vaše dítě).
- Použijte ověřené kontaktní údaje k přímému oslovení společnosti nebo jednotlivce a nikdy se nespolehejte na kontaktní informace poskytnuté osobou, u které podezíráte, že by mohla být podvodník (např. nezávisle vyhledejte název společnosti, použijte ověřené obchodní adresáře nebo dříve potvrzené kontaktní metody). Podvodníci mohou tvrdit, že jsou licencovanou společností nebo napodobují webové stránky licencované společnosti. Ověřte, zda Váš vnitrostátní orgán dohledu nad finančním trhem vydal nějaké varování nebo zda je společnost uvedena na seznamu I-SCAN organizace IOSCO (iosco.org/i-scan/). U poskytovatelů služeb souvisejících s kryptoakivou zkontrolujte, zda mají povolení v EU (např. zkontrolujte registr ESMA (esma.europa.eu/)).

4

Věnujte pozornost potenciálním podvodům využívajících umělou inteligenci:

S vývojem umělé inteligence se podvody stávají přesvědčivější než kdy jindy - a to i navzdory těm nejlepším bezpečnostním doporučením. Pokud se Vám něco zdá neobvyklé nebo si všimnete některého z výše uvedených varovných signálů, zastavte, co děláte, a znovu to vyhodnoťte.

5

Nikdy neinstalujte software pro vzdálený přístup ani nesdílejte obrazovku:

Banky a finanční společnosti Vás o to nikdy nepožádají.

6

Udržujte zařízení a účty v bezpečí:

Používejte silná a jedinečná hesla, udržujte je v tajnosti a vyvarujte se opakovanému používání stejných přihlašovacích údajů na různých platformách. Pokud je to možné, povolte vícefaktorové ověřování. Zde naleznete několik tipů ohledně hesel ([🔗](#)). Udržujte svůj software a antivirovou ochranu aktuální a aktivovanou.

7

Buďte opatrní u neočekávaných a časově omezených investičních příležitostí:

Pokud to zní příliš dobře na to, aby to byla pravda, pravděpodobně to pravda není.

8

Zamyslet se, než nasdílíte informace na sociálních sítích:

Chatové skupiny, fóra, příspěvky na sociálních sítích a fotografie mohou být cenným zdrojem znalostí pro podvodníky. Pokud o sobě nebo svých investicích sdělíte na sociálních sítích příliš mnoho, můžete se stát snadným cílem pro podvodníky.

Co dělat, když jste se stali obětí podvodu



Okamžitě zastavte transakce,

abyste zablokovali další převody na podezřelé účty a vyhnuli se dalším ztrátám. Zastavte veškerý kontakt s podvodníky – ignorujte jejich hovory a e-maily a zablokujte odesílatele.



Obraťte se na svou banku nebo finanční společnost.

Okamžitě informujte svou banku nebo finanční společnost prostřednictvím oficiálních kontaktních kanálů, abyste prozkoumali možnosti zmrazení nebo zrušení transakcí.



Změňte si hesla na všech svých zařízeních a aplikacích/internetových stránkách.

Podvodníci nakupují uniklá hesla online a zkouší je na více účtech. Změnit pouze jedno heslo nestačí. Ujistěte se, že je všechny změníte, aby je podvodníci nemohli znovu použít.



Nahláste podvod a varujte okolí.

Nahlaste incident policii a České národní bance (🇵🇸) a informujte své okolí (např. přátele a rodinu), abyste zvýšili i jejich povědomí o podvodu. Tyto kroky Vám mohou pomoci chránit sebe i ostatní.



Pozor na tzv. „recovery room“ podvody.

Podvodník Vás může kontaktovat s vědomím, že jste obětí předchozího podvodu, a prohlašovat, že je orgánem veřejné moci (např. policie, daňový nebo finanční orgán atd.) a nabízet Vám vrácení ztracených peněz za poplatek. To je často další pokus o to Vás podvést. Nezapomeňte: To, že jste byli podvedeni jednou, nebrání tomu, abyste byli podvedeni znovu.

TYPY FINANČNÍCH PODVODŮ ONLINE VYUŽÍVAJÍCÍCH AI



PODVOVNÍCI VYDÁVAJÍCÍ SE ZA NĚKoho JINÉHO A VYUŽÍVÁNÍ TZV. DEEPPFAKE

Obdržíte neočekávaný hovor od někoho, kdo tvrdí, že je Vaší bankou, orgánem veřejné moci (např. policie, daňový nebo finanční orgán atd.), distributorem pojištění, IT společností nebo dokonce Vaším rodinným příslušníkem. Volající Vás může vyzvat, abyste převedli finanční prostředky do bezpečí, a to kvůli podezřelé aktivitě na Vašem účtu nebo související s Vaším pojištěním. Mohou po Vás také požádat, abyste jim sdělili své bankovní údaje (např. číslo platební karty, přihlašovací údaje k internetovému bankovníctví nebo hesla), klikli na odkaz nebo si nainstalovali software a předstírají, že toto může rychle vyřešit Váš problém. Volající může použít falešné číslo, které často vypadá jako telefonní číslo Vaší banky, aby se zdálo důvěryhodné (tzv. spoofing).

Podvodníci mohou využít umělou inteligenci k vytvoření falešných videí, obrázků nebo zvuku, který napodobuje něčí hlas (např. Vášeho bankéře nebo člena rodiny), obličej (např. celebrity) nebo pohyby. **Toto se nazývá „deepfake“.**

Co se může stát:

Zmíněním osobních údajů a vytvořením pocitu naléhavosti Vás podvodník přiměje k úkonům, které jste neměli v úmyslu učinit – např. odeslání peněz na jejich účet, kliknutí na škodlivý odkaz nebo instalaci malwaru do Vašeho zařízení. To může poskytnout podvodníkovi přístupové údaje k Vašemu bankovnímu účtu, S těmito údaji může podvodník změnit Vaše heslo, ovládnout Váš bankovní účet a ukrást Vaše peníze. Nezapomeňte: jen proto, že volající zná Vaše osobní údaje, neznamená, že je důvěryhodný.



PHISHING A SOCIÁLNÍ INŽENÝRSTVÍ

Obdržíte e-mail nebo zprávu od Vaší banky nebo finanční společnosti, která Vás upozorní na „podezřelou činnost“ na Vašem účtu. Logo, vzhled a jazyk vypadají profesionálně a zpráva se může zobrazit ve stejném vlákně jako ostatní konverzace s Vaší bankou. Zpráva Vás vyzývá, abyste klikli na odkaz pro ověření Vašeho účtu nebo resetování hesla. Odkaz vede na falešné webové stránky, které vypadají stejně jako Vaše internetové bankovníctví. Aniž byste si to uvědomili, zadáváte své údaje na webové stránky určené ke krádeži Vašich osobních údajů.

Podvodníci používají umělou inteligenci k vytváření přesvědčivých phishingových zpráv tím, že analyzují data na sociálních sítích, aby identifikovali své oběti a upravili obsah zpráv podle toho, na koho jejich podvod cílí.

Co se může stát:

Podvodník získá přístup k Vašemu bankovnímu účtu a ukradne Vaše peníze nebo vytvoří falešný profil s Vašimi osobními údaji, aby spáchal podvod.



INVESTIČNÍ NEBO POJIŠŤOVACÍ PODVOV

Na sociálních sítích nebo na webových stránkách vidíte reklamu propagující časově omezenou investiční příležitost s nízkým rizikem nebo časově omezenou slevu na pojištění od známé společnosti. Reklama obsahuje fotografii celebrity a doporučení, které jsou často falešné. Po vyjádření zájmu kliknutím na odkaz nebo vyplněním formuláře jste kontaktováni a přesměrováni na platformu nebo komunikační kanál, kde obdržíte profesionálně vypadající rady a dokumenty. Jste povzbuzováni, abyste investovali malou částku, následovanou většími částkami, nebo zaplatili pojištění na zdánlivě bezpečný účet.

Podvodníci používají umělou inteligenci k tomu, aby tyto falešné nabídky nebo e-maily byly vysoce přesvědčivé a obtížně odhalitelné. Také používají roboty na sociálních sítích, kteří využívají umělou inteligenci k vytváření falešných účtů, které s Vámi komunikují, šíří dezinformace a simulují skutečné chování, aby získali Vaši důvěru a ovlivnili Vaše rozhodnutí.

Co se může stát:

Po pokusu o výběr peněz nebo uplatnění pojištění s Vámi kontaktní osoba přestane komunikovat. Zjistíte, že společnost neexistuje nebo že pojištěné riziko není ve skutečnosti kryto. Uvědomíte si, že jste peníze posílali přímo podvodníkovi v rámci jeho podvodného schématu. Bohužel nemůžete získat své peníze zpět a Vaše osobní a finanční údaje mohou být použity k páčání dalších podvodů (např. podepsání smluv Vaším jménem, což by mohlo vést ke ztrátě ještě více peněz).



ROMANTICKÉ PODVOVY

Byli jste kontaktováni na sociálních sítích, seznamovacích aplikacích nebo telefonicky/textovou zprávou někým, koho jste fyzicky nikdy nepotkali. Tato osoba se s Vámi dá do častých osobních i romantických rozhovorů a buduje důvěru pomocí falešných profilů. Postupem času se konverzace přesouvá směrem k penězům nebo finančním příležitostem, jako jsou krypto-investice se slibem vysokých výnosů a nízkého rizika. Daná osoba Vás požádá o převod peněz na účet nebo Vás provede zřízením účtu a provedením malého počátečního vkladu, aby vše vypadalo legitimně, než Vás povzbudí, abyste investovali více.

Podvodníci používají umělou inteligenci k vytváření falešných profilů, identifikaci obětí na sociálních sítích s využitím dat, která jste zpřístupnili, nebo k zaslání zpráv psaných chatboty.

Co se může stát:

Podvodník z Vás vyláká co nejvíce peněz, pak přeruší veškerou komunikaci a zmizí. Podvodné investiční webové stránky nebo aplikace jsou offline, takže nemáte přístup k Vaším domnělým investicím. Kromě finanční ztráty mohou být osobní údaje, které jste sdíleli, použity k oslovení Vašich přátel a rodiny nebo ke krádeži Vaší identity, která pro Vás může mít finanční nebo právní důsledky (např. podvodník může provádět nákupy, brát si půjčky Vaším jménem nebo můžete být činěni odpovědnými za dluhy nebo trestné činy spáchané pod Vaším jménem, dokud se neprokáže opak).



NÁKUPNÍ PODVODY

Narazíte na atraktivní nabídku pro nákup na online tržišti. Společnost, která nabídku činí, požádá o platbu mimo oficiální platformu a tvrdí, že používá „bezpečný platební systém“, a zašle Vám odkaz na dokončení nákupu. Odkaz Vás přesměruje na podvodnou stránku, která se vydává za ověřovací stránku banky – napodobuje oficiální webové stránky banky a používá její logo a design – kam zadáte údaje k Vašemu online bankovníctví, abyste mohli provést platbu.

Podvodníci využívají umělou inteligenci k vytvoření vysoce přesvědčivých falešných bankovních webových stránek, potvrzení objednávek a faktur. AI jim pomáhá napodobit tón, branding a styl skutečných společností. V některých případech používají AI chatboty k zodpovězení Vašich otázek, aby se nabídka zdála důvěryhodnější.

Co se může stát:

Platba prostřednictvím odkazu na platební systém třetí strany obchází ochranu poskytovanou online tržištěm. Podvodník získá přihlašovací údaje k Vašemu bankovnímu účtu a ukradne Vaše peníze.