



SPLETNE FINANČNE PREVARE V SVETU UMETNE INTELIGENCE

BODITE POZORNI IN SE ZAŠČITITE

Spletne finančne goljufije in prevare niso nove, vendar jih je s pomočjo orodij umetne inteligence vse težje prepoznati. Storilci kaznivih dejanj lahko uporabljajo lažna sporočila in spletna mesta, lažne profile slavnih in celo glasove ali videoposnetke, ustvarjene z umetno inteligenco, ki so videti kot vaš bančnik, prijatelji ali družina, vse z namenom, da bi vas prevarali.

Pogosto do vas pristopijo prek družbenih omrežij, aplikacij za sporočanje, e-pošte in nepričakovanih telefonskih klicev, ki delujejo resnično.

Zaradi tega se lahko soočite s tveganji, s finančno izgubo, krajo identitete in čustveno stisko. Bodite previdni in upoštevajte te ključne nasvete, da se zaščitite:



Bodite pozorni na obstoječe spletne finančne goljufije in prevare, ki jih poganja umetna inteligenca:

npr. lažno predstavljanje, phishing, naložbene in zavarovalne prevare ter celo romantične prevare. Izvedite več o različnih vrstah goljufij in prevar na [straneh 5, 6 in 7](#).

In tukaj za kripto goljufije in prevare ([ikon](#)).



Posamezni opozorilni znaki:

Naučite se prepoznati sumljivo vedenje, sporočila ali ponudbe ([stran 2](#)).



Zaščitite se:

Zavarujte svoje osebne podatke ([stran 3](#)).



Naučite se, kako ravnati, če postanete žrtev goljufije ali prevare

([stran 4](#)).



Opozorilni znaki



Obljuba, ki je videti preveč dobra, da bi bila resnična



Nepričakovan klic z neznane telefonske številke.



Nujen poziv k posredovanju denarja ali osebnih podatkov, tudi če se oseba pretvarja, da je družinski član, prijatelj ali celo javna osebnost.



Zahteva za prevzem nadzora nad vašo napravo, prenos aplikacije, skeniranje kode QR ali klik na povezavo.



Zahteva k posredovanju osebnih ali bančnih podatkov (npr. gesla, številke kreditnih kartic, poverilnice za spletno bančništvo ali varnostne kode).



Zahtevek za plačilo prek neizsledljivih metod (npr. kriptosredstva, darilne kartice, mednarodni denarni prenosi ali predplačniške kartice).



Sumljiv ali napačen e-poštni naslov ali povezava (npr. pravopisne napake v URL-ju ali nenavadni spletni naslovi).



Priponke iz neznanih virov, zlasti datoteke .exe, .scr, .zip ali Officeova datoteka z omogočeno funkcijo »makros« (.docm, .xlsm).



Slaba slovnica ali nepravilna oblika uradnega dokumenta, čeprav lahko umetna inteligenca te pomanjkljivosti ustrezno prikrije.



Spletno mesto, ki je videti profesionalno, vendar nima preverjenih kontaktnih podatkov ali podatkov o registraciji podjetja.



Intonacija, ki ne zveni naravno, nima premorov in zveni pretirano tekoče ali robotsko. Bodite pozorni na kloniran glas, saj lahko tudi govor, ki ga ustvari umetna inteligenca, zveni zelo naravno.



Videoposnetki, v katerih govor zveni robotsko, gibi ustnic in obrazna mimika so lahko neusklajeni z govorom, ozadje, osvetlitev in sence pa so lahko nedosledni. To so pogosto videoposnetki, ki jih ustvari umetna inteligenca (deepfake).

Koraki za zaščito

1

Nikoli ne delite osebnih ali bančnih podatkov:

Zakonita podjetja ne bodo nikoli zahtevala vaših PIN-ov, gesel, poverilnic za spletno bančništvo ali varnostnih kod po e-pošti, SMS sporočilih, družbenih omrežjih ali telefonu.

2

Razmislite, preden ukrepate:

Ne hitite s pošiljanjem denarja, izmenjavo informacij ali klikom na povezave – prevaranti namenoma ustvarijo občutek nujnosti (npr. težave z informacijsko tehnologijo pri vaši banki, klici v sili, pri katerih sodelujejo vaši prijatelji in družinski člani, zastrahovanje itd.). V primeru kakršnih koli dvomov, tudi manjših, prekinite klic in preverite izvor ali identiteto prek uradnih in preverjenih kanalov.

3

Skrbno preverite vir/identiteto:

- Vedno preverite izvor sporočil, klicev, e-pošte in povezave – tudi če so videti uradno in se zdi, da prihajajo od prijatelja ali vaše družine ali celo javne osebnosti. Na primer, pokličite ali pošljite sporočilo družini in prijateljem z uporabo znane številke prek zaupanja vrednega kanala; preverite pravopisne napake, nenavadne URL-je ali manjkajoče varnostne kazalnike (npr. preverite, ali povezava spletnega mesta vključuje „s“ v „HTTPS“, da se zagotovi varnost spletnega mesta, in preverite morebitne dodane ali manjkajoče črke v imenu podjetja).
- Ne odpirajte povezav iz neželenih sporočil, namestite samo uradne aplikacije prek zaupanja vrednih trgovin z aplikacijami in ne skenirajte neznanih QR kod.
- V družini se dogovorite za »varno besedo« – skrivno geslo, ki ga lahko uporabite za potrditev identitete, če vas nekdo z znanim glasom pokliče z nujno zahtevo za denar in trdi, da je družinski član (npr. starši, sestra / brat, otrok).
- Uporabite preverjene kontaktne podatke za neposreden stik s podjetjem ali posameznikom in se nikoli ne zanašajte na kontaktne podatke, ki jih zagotovi neznani pošiljatelj (npr. neodvisno iskanje imena podjetja, uporaba preverjenih poslovnih imenikov, predhodno potrjene kontaktne metode). Prevaranti lahko trdijo, da so pooblaščen ali posnemajo spletno stran pooblaščenega podjetja. Preverite, ali je vaš nacionalni finančni organ izdal opozorila ali jih vključil na seznam IOSCO I-SCAN (iosco.org/i-scan/). Pri ponudnikih kriptosredstev preverite, ali imajo dovoljenje za ponudnika storitev v zvezi s kriptosredstvi v EU (npr. preverite register ESMA (<https://www.esma.europa.eu/>)).

4

Bodite pozorni na morebitne trike z umetno inteligenco:

Z napredkom tehnologije umetne inteligence postajajo prevare bolj prepričljive kot kadarkoli prej, tudi če se držite najboljših varnostnih nasvetov. Če opazite karkoli nenavadnega ali zaznate katerega od zgoraj navedenih opozorilnih znakov, se ustavite, preverite okoliščine in ponovno ocenite situacijo.

5

Nikoli ne nameščajte programske opreme za oddaljeni dostop ali delite zaslona:

Banke in finančne institucije tega od vas ne bodo nikoli zahtevale.

6

Zaščitite naprave in račune:

Uporabite močna in edinstvena gesla, jih ohranite tajne in se izogibajte ponovni uporabi istih poverilnic na različnih platformah. Omogočite več faktorsko avtentikacijo, kjer je to mogoče. Oglejte si nekaj nasvetov za gesla tukaj ([🔗](#)). Redno posodablajte vašo programsko opremo in vzdržujte aktivno in posodobljeno protivirusno zaščito.

7

Bodite previdni pri nepričakovanih in časovno omejenih naložbenih priložnostih:

Če se sliši preveč dobro, da bi bilo res, verjetno je in gre za poskus prevare.

8

Razmislite, preden delite informacije na družbenih omrežjih:

Skupine za klepet, forumi, objave na družbenih omrežjih in fotografije so lahko dragocene informacije za prevarante. Pretirano razkrivanje informacij vas lahko naredi bolj ranljive za ciljno usmerjene prevare.

Kaj storiti, če postanete žrtev goljufije ali prevare



Takoj ustavite transakcije,

Da preprečite nadaljnje prenose na sumljive račune in se izognete dodatnim izgubam. Prekinite vse stike s prevaranti – prezrite njihove klice in elektronsko pošto ter blokirajte pošiljatelja.



Obvestite svojo banko ali finančno podjetje:

Takoj obvestite svojo banko ali finančno podjetje, da raziščete možnosti za zamrznitev ali razveljavitev transakcij.



Spremenite gesla v vseh svojih napravah in aplikacijah/spletnih računih.

Prevaranti kupujejo ukradena gesla na spletu in jih preizkušajo na različnih platformah. Sprememba zgolj enega gesla ni dovolj – zamenjajte vsa gesla, da preprečite njihovo ponovno zlorabo.



Prijavite in opozorite:

Prijavite incident policiji ali svojemu nacionalnemu finančnemu organu (👮) in obvestite svojo mrežo (npr. prijatelje in družino), da jih opozorite. Ti ukrepi vam lahko pomagajo zaščititi sebe in druge.



Pazite se prevar s povračilom sredstev (»recovery rooms«):

Prevarant lahko stopi v stik z vami kot žrtvijo prejšnje prevare in trdi, da je pooblaščen organ (npr. policija, davčni ali finančni organ itd.) in ponuja povračilo izgubljenega denarja, če mu zato plačate. To je pogosto ponoven poskus prevare. Zapomnite si: Če ste bili enkrat prevarani, še ne pomeni, da vas ne bodo poskusili ponovno prevarati.

VRSTE SPLETNIH FINANČNIH PREVAR Z UPORABO UMETNE INTEIGENCE



PREVARE Z LAŽNIM PREDSTAVLJANJEM IN UPORABO DEEFAKE VSEBIN

Prejmete nepričakovan klic nekoga, ki trdi, da je vaša banka, javni organ (npr. policija, davčni ali finančni organ itd.), zavarovalni posrednik, IT podjetje ali celo družinski član. Klicatelj vas lahko pozove, da zaradi domnevno sumljive aktivnosti na vašem računu ali zavarovalni polici prenesete sredstva na "varni račun". Morda vas bodo tudi prosili, da razkrijete svoje bančne podatke (npr. številko plačilne kartice, prijavne podatke za spletno bančništvo ali gesla), kliknete na povezavo ali namestite programsko opremo, ki naj bi hitro rešila težavo. Pogosto uporabijo ponarejeno telefonsko številko, ki je enaka ali zelo podobna uradni številki vaše banke (t. i. spoofing), zaradi česar klic deluje povsem verodostojen.

Prevaranti lahko s pomočjo umetne inteligence ustvarijo izjemno prepričljive videoposnetke, slike ali zvočne posnetke, ki posnemajo glas vašega bančnika, družinskega člana ali znane osebe. Takšne vsebine se imenujejo »deepfake«.

Kaj se lahko zgodi:

S sklicevanjem na osebne podatke in ustvarjanjem občutka nujnosti vas prevarant zvabi v dejanja, ki jih sicer ne bi storili, kot so pošiljanje denarja na njihov račun, klik na zlonamerno povezavo ali namestitev zlonamerne programske opreme na vašo napravo. To lahko prevarantu omogoči neposreden dostop do vaših bančnih poverilnic. S temi podatki lahko spremenijo vaše geslo, dostopajo do vašega bančnega računa in vam ukradejo denar. Zapomnite si: samo zato, ker klicatelj pozna vaše osebne podatke, še ne pomeni, da mu lahko zaupate.



LAŽNO PREDSTAVLJANJE (»PHISHING«) IN SOCIALNI INŽENIRING

Prejmete lahko e-pošto ali sporočilo, za katerega se zdi, da prihaja od vaše banke ali finančnega podjetja, ki vas opozarja na „sumljivo dejavnost“ na vašem računu. Logotip, postavitev in jezik so videti profesionalni, sporočilo pa se lahko prikaže v enaki vsebini kot drugi pogovori iz vaše banke. Sporočilo vas poziva, da kliknete na povezavo, da preverite svoj račun ali ponastavite geslo. Povezava vodi do lažne spletne strani, ki je videti identična vaši spletni banki. Ne da bi se tega zavedali, vnesete svoje podatke, ki jih prevaranti nato uporabijo za krajo vaših osebnih in finančnih informacij.

Prevaranti z uporabo umetne inteligence ustvarjajo zelo prepričljiva sporočila, ki temeljijo na analizi javno dostopnih podatkov z družbenih omrežij. Na ta način sporočila prilagodijo posameznemu prejemniku in povečajo verjetnost uspeha prevare.

Kaj se lahko zgodi:

Prevarant dobi dostop do vašega bančnega računa in vam ukrade denar ali ustvari ponarejen profil z vašimi osebnimi podatki, preko katerega izvede goljufijo.



INVESTICIJSKA ALI ZAVAROVALNA PREVARA

Prevaranti uporabljajo napredna orodja umetne inteligence, s katerimi ustvarijo izjemno prepričljive lažne ponudbe in komunikacijo. Pogosto uporabljajo tudi avtomatizirane račune (bote), ki temeljijo na umetni inteligenci, da ustvarijo vtis pristnosti, širijo napačne informacije in posnemajo resnično vedenje, kar krepi zaupanje žrtve ter spodbuja k sprejetju napačnih odločitev.

Na družbenih omrežjih ali spletnih straneh lahko naletite na oglas, ki oglašuje „naložbeno priložnost z omejenim časom in nizkimi tveganji“ ali posebno, časovno omejeno zavarovanje pri domnevno priznani družbi. Oglas vključuje fotografijo znane osebe in priporočila, ki so praviloma ponarejena. S klikom na povezavo ali izpolnitvijo spletnega obrazca izrazite zanimanje, prevaranti vas nato kontaktirajo in preusmerijo na platformo ali komunikacijski kanal, kjer prejmete navodila in dokumente, ki delujejo profesionalno in legitimno. Nato vas spodbudijo, da vložite majhen znesek, ki mu sledijo večji zneski, ali pa vas prepričajo, da plačate premijo na račun, ki naj bi bil varen.

Kaj se lahko zgodi:

Ko poskusite dvigniti svoj denar ali vložiti zavarovalni zahtevek, se komunikacija nenadoma prekine. Odkrijete, da podjetje ne obstaja ali da kritje ni veljavno. Nato ugotovite, da ste denar poslali neposredno prevarantu. Denarja ne morete dobiti nazaj, vaše osebne in finančne podatke pa lahko uporabijo za nadaljnje zlorabe (npr. sklepanje pogodb v vašem imenu, zaradi česar lahko doživite dodatne izgube).



ROMANTIČNA PREVARA

Na družbenih omrežjih, aplikacijah za zmenke, ali po telefonu / SMS sporočilu vas lahko kontaktira nekdo, ki ga v resničnem življenju niste nikoli srečali. Z vami vse bolj pogosto komunicira, z osebnimi in romantičnimi pogovori gradi zaupanje z uporabo lažnega profila. Sčasoma se pogovor preusmeri v finančne priložnosti, kot so na primer kripto naložbe z obljubami o visokih donosih in nizkem tveganju. Oseba vas prosi, da prenesete denar na račun ali vas vodi skozi postopek odpiranja računa z majhnim začetnim pologom, z namenom, da proces deluje legitimno, pred vlaganjem večjih zneskov.

Prevaranti za ustvarjanje takšnih lažnih identitet uporabljajo orodja umetne inteligence: generirajo lažne profile, analizirajo podatke, ki jih objavljate na družbenih medijih ali v aplikacijah za zmenke, ter uporabljajo klepetalne bote, ki samodejno ustvarjajo sporočila in vzdržujejo komunikacijo.

Kaj se lahko zgodi:

Prevarant poskuša od vas pridobiti čim večjo količino denarja, nato prekine vso komunikacijo in izgine. Lažna naložbena platforma ali aplikacija izgine z interneta, kar onemogoči dostop do domnevnih naložb. Poleg finančne izgube lahko osebni podatki, ki ste jih delili, služijo za nadaljnje zlorabe – npr. ciljanje na vaše prijatelje in družino ali krajo identitete. Posledice so lahko finančne in pravne: prevarant lahko v vašem imenu kupuje, najema posojila ali celo povzroči, da ste odgovorni za dolgove ali kazniva dejanja, dokler ne dokažete nasprotnega.



NAKUP PREVARA

Na spletu naletite na privlačno ponudbo za nakup izdelka. Podjetje vas nato pozove, da plačilo opravite zunaj uradne platforme in trdi, da uporablja „varen plačilni sistem“, ter vam pošlje povezavo za dokončanje nakupa. Povezava vas preusmeri na goljufivo stran za preverjanje pristnosti banke, ki posnema uradno spletno stran banke in uporablja njen logotip in obliko, tako da vnesete svoje spletne bančne podatke za plačilo.

Prevaranti z uporabo orodij umetne inteligence ustvarjajo izjemno prepričljive lažne bančne spletne strani, potrdila naročil in račune.

Z uporabo orodij umetne inteligence posnemajo ton, blagovno znamko in slog resničnih podjetij. V nekaterih primerih uporabljajo klepetalne bote, ki z odgovorjanjem na vprašanja dodatno ustvarjajo vtis legitimnosti in povečajo verjetnost nakupa.

Kaj se lahko zgodi:

Plačilo prek povezave tretje osebe obide zaščitne mehanizme spletne trgovine. Prevarant pridobi vaše prijavnne podatke za spletno banko in lahko neposredno dostopa do vašega bančnega računa in vam ukrade denar.