



FINANCIJSKE *ONLINE* PRIJEVARE I OBMANE U SVIJETU UMJETNE INTELIGENCIJE

BUDITE OPREZNI I ZAŠTITITE SE

Financijske *online* prijevare i obmane nisu novost, ali ih je umjetna inteligencija učinila uvjerljivijima i težima za raspoznavanje. Prevaranti sada koriste lažne poruke i internetske stranice, lažne profile slavnih osoba, pa čak i glasovne ili videozapise generirane umjetnom inteligencijom koji imitiraju vašeg bankara, vašeg prijatelja ili člana vaše obitelji.

Često vam se obraćaju putem društvenih mreža, aplikacija za razmjenu poruka, e-pošte i neočekivanih poziva koji se čine vjerodostojnima.

Postanete li žrtva prijevare ili obmane, mogli biste se suočiti s rizicima kao što su financijski gubitak, krađa identiteta i uznemirenost. Kako biste se zaštitili, budite oprezni i slijedite ove ključne savjete:



Budite na oprezu u pogledu financijskih *online* prijevara i obmana koje koriste umjetnu inteligenciju,

npr. lažnog predstavljanja, *phishinga*, prijevara povezanih s ulaganjima i osiguranjem, pa čak i prijevara u romantičnom odnosu. Kako biste saznali više o različitim vrstama prijevara i obmana, pogledajte [str. 5.](#), [6.](#) i [7.](#)

Za više informacija o prijevarama i obmanama specifičnima za kriptovalute pogledajte informativni članak o kriptoprijevarama i obmanama ([link](#)).



Uočite znakove upozorenja:

Saznajte kako prepoznati sumnjivo ponašanje, poruke ili ponude (pogledajte [str. 2.](#)).



Zaštitite se:

Zaštitite svoje osobne podatke (pogledajte [str. 3.](#)).



Naučite što poduzeti ako postanete žrtva prijevare ili obmane

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



Znakovi upozorenja



Obećanje koje se čini predobro da bi bilo istinito



Neočekivani poziv s nepoznatog broja



Hitan zahtjev za dostavu novca ili osobnih podataka, uključujući zahtjev od nekoga tko se pretvara da je član obitelji, prijatelj ili čak javna osoba



Zahtjev za preuzimanje kontrole nad vašim uređajem, preuzimanje aplikacije, skeniranje QR koda ili klik na poveznicu



Zahtjev za dostavu osobnih ili bankovnih podataka (npr. lozinki, brojeva kreditnih kartica, vjerodajnica za internetsko bankarstvo ili sigurnosnih kodova)



Zahtjev za plaćanje kanalima kojima je transakciju teško ili nemoguće pratiti (npr. kriptovalutama, darovnim karticama, elektroničkim prijenosom sredstava ili karticama s unaprijed uplaćenim sredstvima)



Sumnjiva ili netočna adresa e-pošte ili poveznica (npr. pravopisne pogreške u URL-u ili neuobičajene internetske adrese)



Privitak iz nepoznatog izvora, posebno onaj s ekstenzijom poput .exe, .scr, .zip ili datoteka sustava Office s omogućenim makronaredbama (.docm, .xlsm)



Loša gramatika ili formatiranje u naizgled službenom dokumentu, iako umjetna inteligencija može omogućiti prevarantima da učinkovitije prikriju te nedostatke



Internetska stranica koja izgleda profesionalno, ali nema provjerene podatke za kontakt ili podatke o registraciji poduzeća



Intonacija koja zvuči neprirodno, audio ili videozapis koji nema stanke i čini se pretjerano tečnim ili robotskim. Obratite pozornost na „kloniranje glasa” iako govor generiran umjetnom inteligencijom također može zvučati vrlo prirodno.



Videozapisi u kojima glas zvuči robotski ili pretjerano glatko, pokreti usana i izrazi lica nisu usklađeni s govorom, a pozadina, osvjetljenje i sjene nisu dosljedni. To su često videozapisi generirani umjetnom inteligencijom (*deepfakes*).

Kako se zaštititi:

1

Nikada ne dijelite osobne ili bankovne informacije:

Legitimna poduzeća nikada neće tražiti vaše PIN-ove, lozinke, vjerodajnice za internetsko bankarstvo ili sigurnosne kodove putem e-pošte, poruke, društvenih mreža ili telefona.

2

Zastanite i razmislite prije nego što nešto poduzmete:

Nemojte žuriti sa slanjem novca, dijeljenjem informacija ili klikom na poveznice – prevaranti namjerno stvaraju osjećaj hitnosti (npr. informatički problemi s bankom, hitni pozivi u koje su uključeni vaši prijatelji i članovi obitelji, prijeteći izričaj itd.). U slučaju bilo kakvih sumnji, čak i manjih, ne poduzimajte ništa; završite poziv ili drugi oblik komunikacije i pažljivo ispitajte izvor ili identitet osobe koja vas kontaktira.

3

Pažljivo provjerite izvor/identitet osobe koja vas kontaktira:

- Uvijek provjerite odakle dolaze poruke, pozivi, e-pošta i poveznice – čak i ako izgledaju službeno ili se čini da dolaze od prijatelja, člana vaše obitelji ili čak javne osobe. Na primjer, nazovite ili pošaljite poruku svojoj obitelji i prijateljima koristeći poznati broj putem pouzdanog kanala; obratite pažnju na pravopisne pogreške, čudne URL-ove ili izostanak sigurnosnih pokazatelja (npr. provjerite sadržava li poveznica na internetsku stranicu „s” u „HTTPS-u” kako biste se uvjerali u sigurnost te internetske stranice i provjerite jesu li u nazivu poduzeća neka slova dodana ili možda neka nedostaju).
- Ne otvarajte poveznice iz neželjenih poruka, instalirajte samo službene aplikacije putem pouzdanih trgovina aplikacija i ne skenirajte nepoznate QR kodove.
- Dogovorite sa svojom obitelji „sigurnu riječ” – tajnu frazu koju možete koristiti za potvrdu identiteta ako vas netko s poznatim glasom poziva s hitnim zahtjevom za novac i tvrdi da je član obitelji (npr. roditelji, sestra/brat, dijete).
- Koristite provjerene podatke za kontakt kako biste izravno stupili u kontakt s poduzećem ili pojedincem i nikada se ne oslanjajte na podatke za kontakt koje je dostavio potencijalni prevarant (npr. samostalno pretražite naziv poduzeća, upotrebljavajte provjerene poslovne imenike ili prethodno potvrđene metode kontakta). Prevaranti mogu tvrditi da su ovlašteni pružatelji usluga ili oponašati internetske stranice ovlaštenog poduzeća. Provjerite je li vaš nacionalni financijski regulator izdao upozorenja ili postoje li upozorenja na IOSCO-ovu I-SCAN popisu (iosco.org/i-scan/). Za pružatelje usluga povezanih s kriptoinovinom provjerite imaju li odobrenje za rad u EU-u (npr. provjerite registar ESMA-e [\(🔗\)](#)).

4

Obratite pozornost na moguće trikove povezane s umjetnom inteligencijom:

Kako tehnologija umjetne inteligencije napreduje, prijave postaju sve uvjerljivije – čak i uz najbolje sigurnosne savjete. Ako vam se nešto čini neobičnim ili ako otkrijete bilo koji od gore navedenih znakova upozorenja, zastanite i ponovno procijenite.

5

Nikada ne instalirajte softver za daljinski pristup i ne dijelite svoj zaslon:

Banke i financijske institucije to od vas nikada neće tražiti.

6

Pobrinite se za sigurnost svojih uređaja i računara:

Upotrebljavajte snažne i jedinstvene lozinke, čuvajte ih u tajnosti i izbjegavajte ponovno korištenje istih vjerodajnica na različitim platformama. Omogućite višefaktorsku autentifikaciju ako je to moguće. Pročitajte nekoliko savjeta u vezi s lozinkama ovdje [\(🔗\)](#). Održavajte svoj softver i antivirusnu zaštitu ažuriranima i aktiviranima.

7

Budite oprezni u pogledu neočekivanih mogućnosti ulaganja s ograničenim vremenom:

Ako nešto zvuči predobro da bi bilo istinito, vjerojatno nije istinito.

8

Razmislite prije nego što podijelite informacije na društvenim mrežama:

Chat grupe, forumi, objave i fotografije na društvenim mrežama mogu biti vrijedni izvori znanja za prevarante. Otkrivanje previše toga o sebi ili svojim ulaganjima može vas učiniti lakom metom.

Što učiniti kada postanete žrtva prijevare ili obmane:



Odmah zaustavite transakcije:

Kako biste blokirali sve daljnje prijenose na sumnjive račune i izbjegli dodatne gubitke. Prekinite svaki kontakt s prevarantima – ignorirajte njihove pozive i e-poštu i blokirajte pošiljatelja.



Obratite se svojoj banci ili drugoj financijskoj instituciji:

Odmah obavijestite svoju banku ili drugu financijsku instituciju putem službenih kanala za kontakt kako biste istražili mogućnosti zamrzavanja ili poništavanja transakcija.



Promijenite lozinke na svim uređajima i aplikacijama / internetskim stranicama:

Prevaranti kupuju kompromitirane lozinke na internetu i isprobavaju ih na više računa. Promjena samo jedne lozinke nije dovoljna; svakako ih promijenite sve kako ih prevaranti ne bi mogli ponovno upotrijebiti.



Prijavite i upozorite:

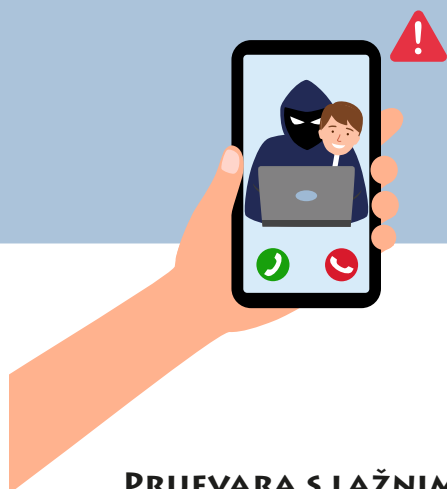
Prijavite incident policiji ili svojem nacionalnom financijskom regulatoru ([Hrvatska agencija za nadzor financijskih usluga \(Hanfa\)](#) i [Hrvatska narodna banka \(HNB\)](#)) i obavijestite svoju okolinu (npr. prijatelje i obitelj) radi podizanja svijesti. To je najbolji način da zaštitite sebe i druge.



Čuvajte se ponovne prijevare kojom se nudi oporavak:

Prevarant vas može kontaktirati znajući da ste žrtva prethodne prijevare, tvrdeći da je predstavnik javnog tijela (npr. policije, porezne uprave, financijskog regulatora itd.) i nudeći povrat izgubljenog novca uz naknadu. To je često još jedan pokušaj prijevare. Zapamtite: ako ste prevareni jednom, to ne znači da ne možete biti prevareni ponovno.

VRSTE FINANCIJSKIH *ONLINE* PRIJEVARA SMIŠLJENIH UZ POMOĆ UMJETNE INTELIGENCIJE



PRIJEVARA S LAŽNIM PREDSTAVLJANJEM I UPOTREBA UVJERLJIVOG KRIVOTVORENOG SADRŽAJA

Primate neočekivani poziv od osobe koja tvrdi da je vaša banka, javno tijelo (npr. policija, porezna uprava, financijski regulator itd.), distributer osiguranja, informatička tvrtka ili čak član obitelji. Pozivatelj vas može poticati da prenesete sredstva kako biste ih zaštitili, navodeći sumnjive aktivnosti na vašem računu ili polici osiguranja. Također od vas može zatražiti da otkrijete svoje bankovne podatke (npr. broj platne kartice, vjerodajnice za internetsko bankarstvo ili lozinke), kliknete na poveznicu ili instalirate softver, pretvarajući se da može brzo riješiti problem. Može upotrijebiti i krivotvoreni broj koji se često podudara s telefonskim brojem vaše banke kako bi se činio legitimnim (*spoofing*).

Prevaranti se mogu služiti umjetnom inteligencijom za stvaranje lažnih videozapisa, slika ili zvuka koji oponašaju nečiji glas (npr. vašeg bankara ili člana obitelji), lice (npr. slavne osobe) ili pokrete. **To je poznato kao *deepfake*.**

Što bi se moglo dogoditi:

Spominjanjem osobnih podataka i stvaranjem osjećaja hitnosti prevaranti vas navode na radnje koje niste namjeravali poduzeti, kao što su slanje novca na njihov račun, klik na zlonamjernu poveznicu ili instaliranje zlonamjernog softvera na vaš uređaj. To prevarantu može dati izravan pristup vašim bankovnim vjerodajnicama. Pomoću tih informacija on može promijeniti vašu lozinku, pristupiti vašem bankovnom računu i ukrasti vaš novac. Zapamtite: to što pozivatelj zna vaše osobne podatke, ne znači da je pouzdan.



PHISHING I SOCIJALNI INŽENJERING

Primate poruku e-pošte ili poruku za koju se čini da dolazi iz vaše banke ili druge financijske institucije i kojom vas se upozorava na „sumnjivu aktivnost” na vašem računu. Logotip, dizajn i jezik izgledaju profesionalno, a poruka se može pojaviti u istoj prepisci u kojoj su i druge poruke vaše banke. Poruka vas poziva da kliknete na poveznicu kako biste potvrdili svoj račun ili resetirali lozinku. Poveznica vodi do lažne internetske stranice koja izgleda identično vašem internetskom bankarstvu. Nesvjesni toga, unosite svoje podatke na internetsku stranicu dizajniranu za krađu vaših osobnih podataka.

Prevaranti se koriste umjetnom inteligencijom za izradu uvjerljivih *phishing* poruka analizom podataka na društvenim mrežama kako bi identificirali svoje žrtve i prilagodili sadržaj za svaki cilj.

Što bi se moglo dogoditi:

Prevarant pristupa vašem bankovnom računu i krade vaš novac ili stvara lažni profil s vašim osobnim podacima kako bi počinio prijevaru.



PRIJEVARA POVEZANA S ULAGANJIMA ILI OSIGURANJEM

Uočavate oglas na društvenim mrežama ili internetskim stranicama na kojem se reklamira „mogućnost ulaganja s ograničenim vremenom i niskim rizicima” ili „popust s ograničenim vremenom” na osiguranje koje nudi poznato društvo za osiguranje. Na oglasu se nalazi fotografija slavne osobe i preporuke koje su često lažne. Nakon što ste iskazali interes klikom na poveznicu ili ispunjavanjem obrasca, kontaktirat će vas se i preusmjeriti na platformu ili kanal za razmjenu poruka, gdje ćete dobiti savjete i dokumente koji izgledaju profesionalno. Potiče vas se da uložite mali iznos, a nakon toga i veći, ili da uplatite premiju na račun koji se čini sigurnim.

Prevaranti upotrebljavaju alate umjetne inteligencije kako bi takve lažne prijedloge ili poruke e-pošte učinili vrlo uvjerljivima i kako bi ih bilo teško otkriti. Na društvenim mrežama također koriste *botove* koje pokreće umjetna inteligencija za stvaranje lažnih računa koji s vama komuniciraju, šire dezinformacije i simuliraju stvarno ponašanje kako bi zadobili povjerenje i utjecali na vaše odluke.

Što bi se moglo dogoditi:

Nakon što pokušate povući svoj novac ili podnijeti zahtjev za isplatu, druga strana prestaje komunicirati. Otkrivete da poduzeće ne postoji ili da rizik od kojeg ste se osigurali nije pokriven. Tada shvaćate da ste novac poslali izravno prevarantu kao dio lažne sheme. Nažalost, ne možete vratiti svoj novac, a vaši osobni i financijski podaci mogu se upotrijebiti za počinjenje daljnjih prijevara (npr. potpisivanje ugovora u vaše ime zbog kojih biste mogli izgubiti još više novca).



PRIJEVARE I OBMANE U ROMANTIČNOM ODNOSU

Na društvenim mrežama, aplikacijama za upoznavanje ili telefonom/porukom kontaktirao vas je netko koga niste upoznali u stvarnom životu. Ta se osoba upušta u česte, osobne i romantične razgovore gradeći povjerenje korištenjem lažnih profila. Tijekom vremena razgovor se pomiče prema novcu ili financijskim mogućnostima kao što su kriptoulaganja s obećanjima visokog prinosa i niskog rizika. Osoba od vas traži da prenesete novac na račun ili vas vodi kroz proces otvaranja računa i uplate malog početnog iznosa kako bi se shema činila legitimnom prije nego što vas potakne da uložite više.

Prevaranti se služe umjetnom inteligencijom za generiranje lažnih profila i identificiranje svojih žrtava na društvenim mrežama ili aplikacijama za upoznavanje koristeći podatke koje ste učinili dostupnima ili se služe *chatbotovima* za generiranje poruka.

Što bi se moglo dogoditi:

Prevarant izvlači što je moguće više novca, a zatim prekida svu komunikaciju i nestaje. Prijevarna internetska stranica ili aplikacija za ulaganja uklonjena je s interneta, zbog čega ne možete pristupiti navodnim ulaganjima. Osim financijskog gubitka, osobni podaci koje ste podijelili mogu se upotrijebiti za ciljanje vaših prijatelja i obitelji ili za krađu identiteta koja može imati financijske ili pravne posljedice za vas (npr. prevarant bi mogao kupovati, uzimati zajmove u vaše ime ili biste mogli biti odgovorni za dugove ili kaznena djela počinjena pod vašim imenom dok se ne dokaže suprotno).



PRIJEVARA PRI KUPNJI

Nailazite na atraktivnu ponudu za kupnju u internetskoj trgovini. Poduzeće koje nudi kupnju traži plaćanje izvan službene platforme tvrdeći da koristi „siguran sustav plaćanja” i šalje vam poveznicu za dovršetak kupnje. Poveznica vas preusmjerava na lažnu stranicu za provjeru autentičnosti banke, koja oponaša službenu internetsku stranicu banke i koristi njezin logotip i dizajn, i vi unosite svoje podatke o internetskom bankarstvu kako biste izvršili plaćanje.

Prevaranti koriste umjetnu inteligenciju za stvaranje vrlo uvjerljivih lažnih internetskih stranica banaka, potvrda narudžbi i računa. Umjetna inteligencija pomaže im oponašati ton, brendiranje i stil stvarnih poduzeća. U nekim slučajevima koriste *chatbotove* koje pokreće umjetna inteligencija kako bi odgovorili na pitanja i kupnju učinili uvjerljivijom.

Što bi se moglo dogoditi:

Plaćanje putem poveznice treće strane zaobilazi standardne slojeve zaštite. Prevarant dobiva vaše podatke za prijavu na vaš bankovni račun i krade vaš novac.