

VODIČ O FINANCIJSKIM PRIJEVARAMA



SADRŽAJ



4
ŠTO SU FINANCIJSKE
PRIJEVARE I KADA
SU NASTALE?



10
VRSTE
FINANCIJSKIH
PRIJEVARA



19
PRIJEVARE
POVEZANE
S USLUGAMA NA
REGULIRANOM
FINANCIJSKOM
TRŽIŠTU



7
POVIJEST
FINANCIJSKIH
PRIJEVARA



40
PRIJEVARE NA
KRIPTOTRŽIŠTU

31
ŠTO TREBATE ZNATI
O RIZICIMA ULAGANJA
NA KRIPTOTRŽIŠTU?



ŠTO SU FINANCIJSKE PRIJEVARE I KADA SU NASTALE?

Financijska prijevarena događa se kada osoba, odnosno ulagatelj pretrpi financijski gubitak zbog ulaganja na temelju obmanjujućih, nepoštenih ili lažnih poslovnih praksi. Neke od tehnika koje se koriste pri financijskim prijevarama su fantomsko bogatstvo, oskudnost, kredibilitet izvora, društveni konsenzus i reciprocitet. One nisu isključivo tehnike prijevare, već i marketinške tehnike s kojima se svakodnevno susrećemo pa ne izazivaju automatsku sumnjičavost.

FANTOMSKO BOGATSTVO

Tehnika je kojom se osobu mami s obećanjem nečega što nema, a želi. To nešto je često bogatstvo koje ju **čeka u budućnosti, visoki povraci na uloženi novac, laka zarada i slično. Obećanje nagrade u budućnosti** ili čak samo mogućnost da će dobiti nagradu u budućnosti, osobu motivira na preuzimanje rizika.



TAKTIKA OSKUDNOSTI

Odnosi se na lažni osjećaj hitnosti zbog ograničenih zaliha, ograničenog vremena za reagiranje ili ekskluzivnosti ponude. Na taj se način povećava percipirana vrijednost proizvoda ili usluge. Motivirani smo reagirati na izjave poput „ova je ponuda dostupna ograničenom broju ljudi” ili „ovu ponudu možete iskoristiti još samo danas” jer nam je tako prezentiran potencijalni gubitak ako ne reagiramo.

KREDIBILITET IZVORA

Tehnika je koja iskorištava sklonost pojedinca da vjeruje osobama od autoriteta i organizacijama koje smatra legitimnima. Načini kojima se prijevarnim porukama daje kredibilitet su lažno predstavljanje, korištenje profesionalnog jezika i stručnih termina, zatim vizualni dizajn koji oponaša izgled legitimnih organizacija te pružanje informacija koje skreću pažnju i „prodaju priču”, poput informacija o povijesti i poslovanju neke fiktivne kompanije.

SOCIJALNI KONSENZUS

Jedan od načina na koji prevaranti utječu na žrtve financijskih prijevara. Što nam se više čini da veći broj ljudi ima neki stav ili se ponaša na neki način, veća je vjerojatnost da **ćemo im se pridružiti. Zbog socijalnog pritiska** i prirodne sklonosti konformiranju ponekad nam je teško usprotiviti se mišljenju većine. **Prevaranti zato često navode velik broj osoba koji su profitirali od njihove ponude ili pružaju lažne izjave „sretnih dobitnika”.**

RECIPROCITET

Fenomen kod kojeg se očekuje da ćemo na pozitivnu gestu odgovoriti drugom pozitivnom gestom. **Prevaranti** koriste ovu tehniku tako da nam najprije poklone ne-

što zbog čega ćemo biti skloniji uzvratiti im uslugu i, na primjer, uložiti u njihov posao. Taj poklon može biti besplatan obrok na nekom seminaru, popust na neki proizvod koji će nam dobrodušno oduzeti od svoje provizije (a koji nismo tražili) i slično. Nakon pozitivne geste dolazi nam zahtjev prevaranta koji je teže odbiti zbog „duga” koji nam je stvorio. Prijevarena je, dakle, namjeran čin obmane radi osobne koristi ili nanošenja štete drugome, a ona postoji još od razdoblja prije Krista.

“

„Ako pastir kojemu je vlasnik povjerio ovce na čuvanje pogrešno prikaže prirodni prirast ovaca ili ih proda za novac, bit će proglašen krivim i bit će obavezan platiti vlasniku deset puta više od utvrđenog gubitka“.

Zakon je to u kojem je opisana prijevara i kazna za prekršitelje, a nalazi se u Hamurabijevom Babilonskom zakoniku koji datira u davnu 1800. godinu p.n.e. Već se ovdje uočava da je kazna deset puta veća od protupravne koristi kako bi se preventivno djelovalo na moguće prekršitelje.



POVIJEST FINANCIJSKIH PRIJEVARA



Evolucijom ljudskog roda od početaka do danas ono što se nikako nije moglo iskorijeniti jest glad za novcem i moći gdje ljudi ne biraju sredstva kako ih steći. Stoga postoje brojne zabilješke u povijesti o pokušaju prijevara ili o pokušaju donošenja zakona gdje se te prijevare pokušavaju spriječiti. Još u grčkoj mitologiji spominje se prijevara i to u kontekstu boga Hermesa, simbola prijevare, lukavstva, laži i krađe, a od nastanka grčke mitologije i Babilonskog zakonika do danas zabilježeni su pokušaji prijevara koji svojom smjelošću i vrijednošću zaista zapanjuju:



Grčki trgovac Hegestratos

(300. godina p.n.e.) uzeo je zajam uz hipoteku na svoj brod i dobra na njemu. Njegov je plan bio da potopi prazan brod, a zadrži novce i robu. To mu nije uspjelo te se utopio bježeći pred ljutim putnicima i posadom.

1920. Charles Ponzi

došao je na ideju da posudi novce i vrati ih uz primamljivu dobit. Naravno da su ulagači hvaleći se dobrom zaradom širili vijest tako da je sve više i više ljudi kupovalo njegove kupone. Kada se saznalo da je sve prijevara, investitori su izgubili približno 10 milijuna dolara.



193. godine Pretorijska garda

ubila je cara Pertinaksa i ponudila na prodaju cijelo Rimsko carstvo najvećem ponuditelju. Pobjednik je bio Julianus koji je platio 250 zlatnika svakom pripadniku garde što je ukupna protivrijednost od 1 mlrd. dolara u današnjem novcu.



Barry Minkow

bivši američki poduzetnik, pastor i osuđeni zločinac koji je još u srednjoj školi osnovao ZZZZ Best, tvrtku za čišćenje koja se činila izuzetno uspješnom. Međutim, to je zapravo bio paravan za privlačenje investicija za masovnu Ponzijevu shemu. Propao je 1987. godine, koštajući investitore i zajmodavce 100 milijuna dolara. Riječ je o jednoj od najvećih prijevara s investicijama koje je ikad počnila jedna osoba, kao i jednoj od najvećih računovodstvenih prijevara u povijesti.



1925. godine Victor Lustig

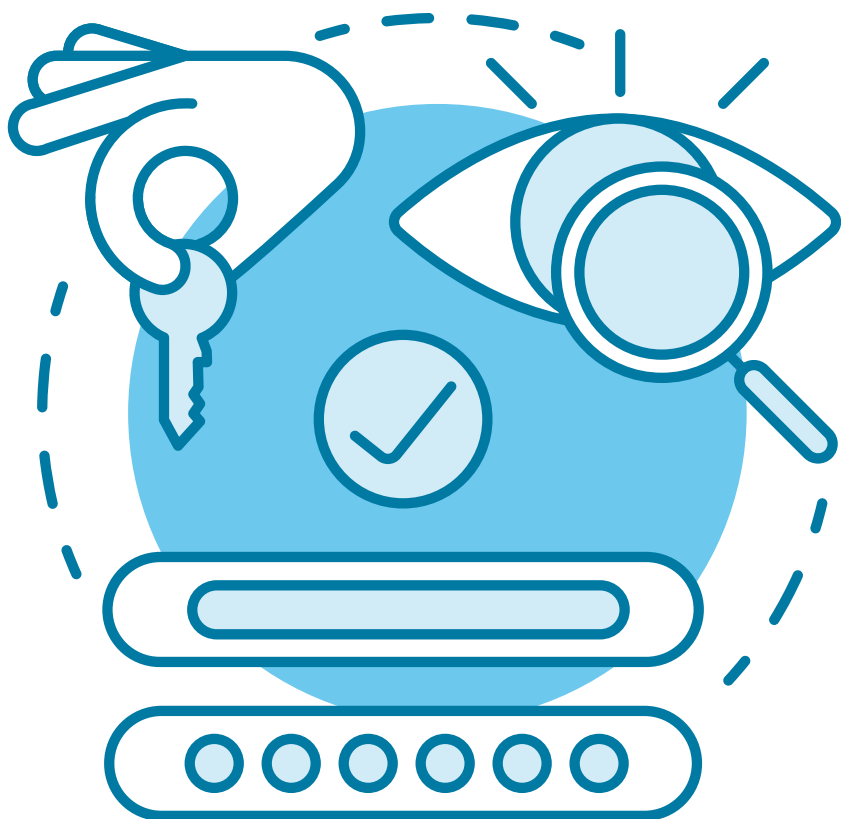
je krivotvorivši dokumente pokušao prodati Eiffelov toranj u staro željezo. Prodao ga je i to dvojici trgovaca starim željezom za 200.000 dolara. On je, naravno, uzeo novac, a Eiffelov toranj i danas stoji u Parizu.



Ovo su samo neki povijesni primjeri gdje su snalažljivi i domišljati pojedinci iskoristavali ljudsku naivnost i želju za brzom zaradom. Kako se približavamo modernom dobu prijevare su postale dio svakodnevice, a pojedinci su tehniku doveli do savršenstva. **Prijevara u današnje vrijeme nisu prestale biti izvor zarade pojedinaca već su postale složenije, a time i unosnije.** Usto, virtualno je doba donijelo posebne izazove. **Zahvaljujući digitalizaciji, prevaranti imaju**

pristup velikom broju potencijalnih žrtava. Nekad bi u jednom danu stigli pokucati na desetak vrata, a danas jednim e-mailom u nekoliko sekundi mogu kontaktirati stotine tisuća meta. Pored toga, s pojavom različitih opcija investiranja i financijskih tehnologija, prosječnoj je osobi sve teže razumjeti moderne financije. Ta činjenica pomaže prevarantima da stručnim i kompliciranim izrazima prikažu mutan posao kao legitimnu financijsku uslugu.

VRSTE FINANCIJSKIH PRIJEVARA



PONZIJEVA SHEMA

Vrsta financijske prijevare koja mami ulagače obećavajući im abnormalno visoke povrate u kratkom vremenu pa joj mnogi već desetljećima ne mogu odoljeti. Shema započinje tako da neki prevarant osnuje ustanovu za prikupljanje **depozita** (ili **ban-ku**). Prevarant poziva javnost da deponira novac kod institucije, nudeći velikodušne **kamate**. Kamate se potom isplaćuju iz novca novih deponenata, dok prevarant udobno živi od starih depozita. Čitava se shema raspada kad više nema dovoljno novih depozita kojima bi se pokrivala isplate kamata dospjele na stare depozite. Prevarant se nada da će tada već živjeti pod novim imenom negdje u tropima, u zemlji koja nema zakon o ekstradiciji. Shema je dobila ime po Charlesu Ponziju, Talijanu koji se proslavio dvadesetih godina prošlog stoljeća tvrdeći da bi mogao udvostručiti novac svojih klijenata u roku od 90 dana, a nakon njega pojavili su se mnogi s istim obećanjima.

Najpoznatiji primjer Ponzijeve sheme svakako je Bernard Madoff, autor najveće financijske prijevare u povijesti, koji je prevario nobelovce, senatore, holivudske glumce, redatelje i bogate Njujorčane, a na njima je zaradio 17,5 milijardi dolara. Bernard Madoff je, naime, desetljećima slovio

za mudrog investitora i inovatora, pionira u elektroničkom trgovanju. Bio je direktor Nasdaq-a i savjetnik Komisije za vrijednosnice i burze, a svoje portfelje povjeravala su mu sveučilišta, banke, fondovi i zaklade. Privukla ih je činjenica da je nudio nevjerojatno stabilne prinose, unatoč fluktuacijama tržišta. U stvarnosti tih prinosa nije bilo. Madoff je sav novac držao na tekućem računu u banci, a „prinos” koji je isplaćivao starim klijentima bio je zapravo keš koji su mu novi klijenti donijeli da ga „investira”. Ta je prevarantska shema funkcionirala barem 16 godina, ako ne i duže. Nužna pretpostavka bila je da svi klijenti ne dođu istog dana podići svoje uloge, što se nije događalo, bar ne do 2008. kada se prevarantski biznis raspao zbog kraha Wall Streeta. Financijska kriza stvorila je paniku na tržištu, a pritisak na Bernarda Madoffa brzo je otkrio da on više nema novac svojih investitora.

PIRAMIDALNA SHEMA

Vrsta prijevare u kojoj prevarant zavarava ljude da izvrše plaćanje uz obećanje da će dobiti neizmjerne pogodnosti. Vrlo je uobičajen način davanja provizije, povrh te isplate, za one koji dovedu novog partnera u shemu i povećanja vrijednosti za one na vrhu, koji se naziva eksponencijalni

rast. Sheme piramida imaju različite oblike; počele su kao lanac poštom, postojao je popis imena i adresa, tko je primio prvo pismo, tražen je mali novac. I tako nastavljaju dalje, svaki put kad je poslano pismo, prvi je dobio veći dio tog novca. Uspjeh ovog oblika trgovine jest grupiranje novih ljudi za lanac. Otuda i naziv „piramida”, što ukazuje na to da će se s više ljudi koji pregovaraju ispod pojedinca postići veći uspjeh, a osoba na vrhu, uzima „proviziju” od svih ispod sebe.

Piramidalna shema bila je veoma popularna u Hrvatskoj tijekom 90-ih i ranih 2000-utih. Posljednja piramidalna obmana otkrivena je 2010. godine kad je desetak „poduzetnika”, lažno se predstavljajući da trguju devizama preko Forexa, oštetilo nekoliko stotina građana RH za nekoliko stotina milijuna kuna. Oni su nasjeli njihovim lažima da će im novac oploditi na međunarodnom tržištu deviza Forex ili u novoosnovanoj austrijsko-britanskoj banci. Također su im neistinito prezentirali da će im se, na temelju ulaganja u Forex, uz minimalni rizik isplatiti visoka dividenda dok

će glavnica ostati neizmijenjena i apsolutno osigurana od gubitka, kao i da novac neće biti iznesen iz Hrvatske, odnosno da će postati dioničari navedene banke s podružnicom u Hrvatskoj na koji način će steći mogućnost dobivanja kredita s manjom kamatnom stopom. Ulagачima su za uplaćene iznose predavali i lažne uplatnice na njemačkom jeziku, kao i isplatnice s naznačenim navodnim profitom te fiktivne dionice na kojima je bio naveden „siguran” iznos glavnice od 5000 eura. Kada su ulagači počeli sumnjati u istinitost njihovih tvrdnji, agenti su im predavali certifikate na kojima su bili naznačeni fiktivni iznosi zarade. Većini ulagača su davali i šifru za ulazak na internetsku stranicu putem koje su trebali biti obaviješteni o stanju uloga, modalitetima i vremenu isplate, uvjeravajući ih da će konačna isplata uslijediti u prvoj polovici 2011. No rokove su nakon toga prolongirali do 2017.

LAŽNI BROKERI I INVESTICIJSKI SAVJETNICI

Prevaranti se predstavljaju kao trgovci i nude niz ulagačkih mogućnosti, uključujući ulaganja u dionice, zemljište, zlato i drago kamenje, ugljični kredit, vino, gospodarske grane u nastajanju ili farmaceutiku. Pozivatelji koriste agresivne prodajne metode i često tvrde da ćete propustiti izvanrednu priliku ne budete li djelovali istoga časa. Unatoč obećanjima o visokim prinosisima, ulaganja obično budu bezvrijedna ili precijenjena. Prevaranti vam pritom često otkrivaju detalje za koje vam se čini da ih mogu imati samo vjerodostojne ulagačke kompanije. Tako će, primjerice, znati detalje o vašim prethodnim ulaganjima i dionicama koje posjedujete ili informacije o vašoj osobnoj situaciji. Prevaranti se uvijek dobro pripreme i saznaju koliko god mogu o svojim žrtvama. Često se potrudite i da sve naizgled bude vjerodostojno pa mogu imati adresu u prestižnom dijelu grada, bespla-



tan telefonski broj, dojmljivu internetsku stranicu ili sjajnu brošuru. Kontaktiraju vas uglavnom telefonski, ali vam ulaganja mogu nuditi i slanjem e-poruka, distribucijom brošura ili putem internetskih stranica. Često će isti broj telefona nazvati više puta kako bi s primateljem poziva razvili prijateljski odnos. Ako na bilo koji način reagirate na njihova nagovaranja, bit će ustrajni, graditi povjerenje i na kraju vas nagovoriti na ulaganje. Nakon što dobiju vaš novac, vjerojatno će vas pokušati nagovoriti i na novo ulaganje.

Trenutačno najaktualniji oblik investicijskih prijevarama na štetu građana jesu prijevare povezane s navodnim ulaganjem s visokim prinosisom (engl. HYIP – High Yield Investment Programs), gdje se građane poziva i nagovara na ulaganje u zlato, naftu ili, što je u posljednje vrijeme najučestaliji slučaj, kriptovalute poput bitcoina, gdje se obećava visok prinosis na ulaganje u kratkom vremenu. Takve su prijevare naročito postale aktualne tijekom pandemije bolesti COVID-19 jer građani više vremena provode na internetu, gdje se prevaranti

aktivno oglašavaju putem internetskih portala i društvenih mreža. Tako je, primjerice, početkom godine 64-godišnjak iz Varaždina pronašao oglas kojim se poziva na investiranje u kriptovalute uz zajamčenu dobit, a na koji se on javio. Prilikom prijave putem elektroničke pošte i aplikacije Viber u više je navrata kontaktirao s nepoznatim osobama, koje su ga navele da na svom računalu instalira aplikaciju za upravljanje



s udaljenog računala Teamviewer. Nakon što je instalirao aplikaciju, na zahtjev nepoznatih počinitelja na računalo je otvorio aplikaciju internetskog bankarstva i prijavio se na svoj račun te omogućio nepoznatom počinitelju da upravlja tom aplikacijom, pri čemu je izvršio nekoliko transakcija kojima su kupljene kriptovalute bitcoin. Kupljene kriptovalute uplaćene su na novčanik nad kojim 64-godišnjak nema kontrolu. Osim toga, prevaranti su 64-godišnjaku otvorili profil na lažnoj stranici Prgntrade.cc kako bi ga držali u zabludi da se radi o stvarnom investicijskom poslu. Visina materijalne štete procjenjuje se na tridesetak tisuća kuna.

MASOVNA MARKETINŠKA PRIJEVARA

Riječ je o prijevari koja započinje masovnim slanjem pošte, telefonskim pozivima ili neželjenom e-poštom. To također uključuje lažne financijske proizvode, dobrotvorne organizacije, lutrije, pozivnice i još mnogo toga, a žrtvama se obećavaju velike nagrade, nasljedstva ili slični dobitci. Međutim, za primitak takve dobiti najprije je potrebno platiti predujam koji je predstavljen kao aktivacijska naknada, porez, trošak dostave i slično. Pritom se često koristi tehnika kojom se osobi najprije postavlja manji zahtjev (npr. odgovor na e-mail), a zatim sve veći i veći zahtjevi u obliku novčanih uplata. Pristankom na manji zahtjev osoba ima osjećaj da je nešto već uložila i da će, ako sada odustane, taj napor biti nizašto. Iako dolaze sve veći i veći zahtjevi, osoba ih ispunjava zbog potrebe da ostane konzistentna u vlastitom ponašanju. Primjerice, prijevara može početi tako da žrtva dobije poruku da je osvojila nagradu na nagradnoj igri, dobitnik je lutrije ili je tisućiti posjetitelj na nekoj stranici. No, da bi primila svoju nagradu, najprije mora uplatiti porez, trošak dostave ako se radi o materijalnoj nagradi ili aktivacijsku naknadu. Također, od žrtve se traže osobni podaci

i podaci o bankovnom računu za uplatu dobitka. Naravno, novčana nagrada nikada se ne dobije.

Jedan od poznatijih primjera takvog tipa prijevara jest **Nigerijska prijevara** – žrtva dobije e-mail fiktivne osobe iz neke egzotične zemlje s molbom za pomoć i obećanjem velikodušne nagrade. Pomoć koja se traži najčešće uključuje veliko bogatstvo kojem pošiljatelj iz nekog nategnutog pravnog razloga nema pristup i do njega može doći jedino uz pomoć žrtve. Pritom se od žrtve traže uplate sve većih i većih iznosa financijske pomoći. Transakcija nagrade



Poruke najčešće izgledaju kao da dolaze od banaka, popularnih društvenih mreža ili internetskih stranica za prodaju i kupnju. *Phishing* se uglavnom izvodi putem e-poruka ili tekstualnih poruka u kojima se od korisnika često traži da na lažnim internetskim stranicama (koje su gotovo identične stvarnim stranicama) ostave svoje podatke. Čak i dok koristite legitimne stranice banke, ponekad se na njima mogu pojaviti lažni skočni prozori (*pop-ups*). Čim kliknete na takav prozor ili unesete svoje osobne podatke ili podatke za identifikaciju, vaši podaci odlaze nekom drugom pružatelju usluga ili trećoj strani koja nije vaša banka. To znači da od toga trenutka nadalje netko drugi može pristupiti vašim računima. Postoje e-poruke koje sadrže linkove i žele vas navesti da posjetite internetske stranice na kojima ćete preuzeti štetne ili maliciozne programe (*malware*), uz čiju pomoć prevaranti mogu doći do vaših podataka i vašeg novca. Iz privitka se, osim *malwarea*, može instalirati i tzv. *ransomware*. Takvi programi šifriraju vaše datoteke, uključujući glazbu i fotografije, a prevaranti od vas traže „otkupninu“ kako biste ih dobili natrag.

VISHING

Sličan *phishingu*, ali se odnosi na lažne telefonske pozive u kojima se prevaranti predstavljaju kao zaposlenici banke ili druge poznate organizacije te od vas traže da novac s vlastitoga računa prebacite na neki nepoznati račun. Kako bi vas nagovorili da otkrijete svoje podatke, prevaranti će vam pokušati „prodati“ uvjerljivu priču. Primjerice, prevarant će se predstaviti kao djelatnik pružatelja usluga telekoma ili komunalnoga poduzeća i ponuditi vam povrat novca. U tu će svrhu od vas tražiti da svoju debitnu karticu umetnete u token i date im kôd za autorizaciju transakcija (MAC). Kôd će zatim iskoristiti kako bi izvršili transakcije s vašeg računa.

prema žrtvi iz nekog se razloga stalno odgađa, a prijevara se nastavlja sve dok žrtva ne shvati da je preveslana.

KRAĐA IDENTITETA PUTEM INTERNETA: PHISHING

Proces putem kojega prevaranti dobivaju pristup osjetljivim podacima poput korisničkih imena, lozinki ili podataka s kreditnih kartica slanjem lažnih elektroničkih ili tekstualnih poruka koje izgledaju kao da su ih poslale legitimne organizacije.



KRIVOTVORENE MREŽNE STRANICE BANAKA

Koristi se lažna e-pošta banke s poveznicom na krivotvorenu mrežnu stranicu. Jednom kada kliknete na poveznicu, koriste se razne metode prikupljanja vaših financijskih i osobnih informacija. Stranica izgleda kao prava mrežna stranica uz nekoliko malih razlika. Takve stranice često prikazuju poruke hitnosti, skočne prozore (koji se koriste za prikupljanje vaših osobnih informacija) te lošiji dizajn i pogreške u pravopisu i gramatici.

PRIJEVARA S KURIRIMA (COURIER FRAUD)

Prevaranti se često predstavljaju kao djelatnici banke ili policijski službenici te vas obavještavaju da postoje određeni problemi s vašom debitnom ili kreditnom karticom. Primjerice, kažu da je zloupotrijebljena i da je podignut određeni iznos s računa. Obično kažu da će doći po karticu i PIN radi istrage, sprječavanja daljnje zloupotrebe ili povrata novca. Može se dogoditi i da vas traže da unesete svoj PIN putem telefona te kažu da će poslati dostavljača po vašu karticu. Osim toga, mogu vas zamoliti da podignete određeni iznos novca

s računa ili kupite neki skupi proizvod te ga predate dostavljaču i na taj način pomognete u tekućoj istrazi. Isto vas tako mogu pokušati nagovoriti da prebacite sredstva na novi, „sigurniji“ račun.

MALWARE

Zajednički naziv za štetne ili maliciozne programe koje prevaranti koriste kako bi pristupili vašim računalima. Takvi su programi obično skriveni u privicima ili besplatnom sadržaju. Koriste se za niz nezakonitih radnji kao što su krađa osobnih podataka, brisanje ili oštećivanje podataka, stvaranje *botnet* mreža (mreža zaraženih računala) i zaobilazanje sigurnosnih programa. Postoji cijeli niz različitih štetnih programa, uključujući viruse, trojance, špijunske programe (*spyware*), reklamne programe (*adware*) i programe za zastrašivanje (*scareware*).

PRIJEVARE PRILIKOM INTERNETSKE KUPOVINE

Prevaranti će oglašavati proizvode/usluge koje ili ne postoje ili nisu njihove, a kako bi ih prodavali. Uvjjerit će vas u izravno plaćanje na njihov račun, ali vam roba nikada neće stići. Prije nego što se odlučite na kupovinu putem interneta, istražite prodavatelje kako biste bili sigurni da su pouzdani i izbjegavajte one s lošim ocjenama. Inzistirajte na tome da vidite visokovrijednu robu prije plaćanja. Koristite poznate (renomirane) servise za plaćanje poput PayPal a i provjerite je li internetska stranica putem koje kupujete sigurna i pouzdana prije nego što ostavite podatke sa svoje kartice odnosno prije nego što provedete plaćanje.

POSREDNIK ZA PRIJENOS NOVCA (TZV. FINANCIJSKA MULA)

Money mule ili posrednik za prijenos novca naziv je za osobu koju prevaranti nagovore

na pranje nezakonito stečenoga novca. Posrednik na svoj račun primi određeni iznos novca, a zatim ga prenosi dalje, uglavnom u inozemstvo, uz određenu proviziju. Riječ je o novcu koji su prevaranti ukrali od drugih ljudi. Kriminalci tako putem e-pošta, stranica za traženje posla ili oglasa regrutiraju nevine osobe za prijenos novca uz određenu naknadu. Prevaranti se drže dosta povučeno pa će gotovo uvijek od vas tražiti da banci ili policiji ne otkrivete razlog uplata i isplata. Kriminalci će pokušati nasamariti nevine žrtve nagovorom da sudjeluju u pranju novca predstavljajući im poslovnu ponudu što legitimnijom. Najčešće ciljaju na novopridošlice u državu, nezaposlene,

studente i osobe lošijeg imovinskog stanja, kao i muškarce između 18 i 34 godine željne lake zarade.

Prijevarama počinje vrebanjem osoba koje traže posao, kojima se plasira priča o, primjerice, otvaranju nove firme, za koje je potrebna pomoć pri prijenosu novca. Sve se odvija telefonski i *online*, bez susreta, šalje se ugovor, a jedini je zadatak „zaposlenika“ da u „nekoliko klikova“ u određeno vrijeme novac koji mu sjedne na račun prosljedi te uzme dogovoreni postotak. Ono što željni brze zarade vrlo vjerojatno ne znaju, jest da tako čine kazneno djelo pomaganja u pranju novca, za što su propisane zatvorske kazne od šest mjeseci do pet godina.



Financijske investicijske prijevare u današnjem virtualnom svijetu rastu, a dijelimo ih na:

1. Prijevare povezane s uslugama na reguliranom financijskom tržištu
2. Prijevare na kriptotržištu koje nije regulirano (i gdje ne postoji sustav zaštite malih ulagača)

PRIJEVARE POVEZANE S USLUGAMA NA REGULIRANOM FINANCIJSKOM TRŽIŠTU

Na što obratiti pozornost

Građanima Republike Hrvatske učestalo se putem oglasa na internetu ili izravnim telefonskim kontaktom nudi mogućnost trgovanja financijskim instrumentima online odnosno putem raznih internetskih stranica. Takvim internetskim stranicama (koje još nazivamo trgovinske platforme) upravljaju razna investicijska društva (poznatija kao brokerska društva) koja omogućavaju svojim klijentima da, nakon što na platformi naprave svoj račun (account), na jednostavan način zadaju kupovne i prodajne naloge i kontinuirano prate kako se kreće vrijednost njihove investicije.

Međutim, velikim brojem takvih online trgovinskih platformi upravljaju društva koja za to nemaju ovlaštenje ili društva koja ne smiju hrvatskim građanima nuditi svoje brokerske usluge. Često se radi o običnim prevarama. Trgovanje putem takvih online platformi izlaže vas visokom riziku da u konačnici ostanete bez novca koji ste uplatili za trgovanje, a da potom imate jako malo opcija kome se obratiti za pomoć.

1. „Telefonski su me nazvale osobe i nudile mi trgovanje dionicama na jednostavan način uz sigurnu zaradu.“

Ovo se našim građanima često događa, a vjerojatno ste i sami jedna od osoba koju su nazvali. Telefonsko zvanje osoba i nuđenje usluga bez da su te osobe prethodno iskazale interes za takve usluge (u ovome slučaju za trgovanje dionicama) zove se cold calling. Takva praksa u RH nije zabranjena, ali u svakome slučaju otvara nekoliko pitanja o kojima trebate voditi računa.

Za početak, slobodno **pitajte osobu koja vas zove na koji način je došla do vašeg telefonskog broja**. Živimo u vrijeme kada je zaštita osobnih podataka važna.

Ako niste zadovoljni s odgovorom ili odgovor ne dobijete, prekinite razgovor.

Na što je nadalje potrebno obratiti pozornost:



Saznajte točan naziv brokerskog društva čije vam se usluge nude

Ako se radi o legalnom, licenciranom brokerskom društvu, ono će na svojoj stranici jasno istaknuti svoj puni naziv, adresu i licencu regulatora koji mu je izdao odobrenje za rad. Svako brokersko društvo iz RH ili EU-a mora imati odobrenje svojeg nacionalnog regulatora ako želi pružati usluge trgovanja financijskim instrumentima.

Ako vam osoba koja vas je nazvala ne želi nedvosmisleno reći naziv brokerskog društva, ako se na online trgovinskoj platformi ne navodi naziv i adresa društva (najčešće na dnu stranice) ili ako se u dokumentima koji su objavljeni na stranici ne navodi naziv i adresa društva (primjerice, u Općim uvjetima), ne ulazite u poslovni odnos s takvim društvom. Najvjerojatnije se radi o prevari.



Napominjemo kako u većini slučajeva naziv online trgovinske platforme odnosno njezina internetska adresa nije identična kao i sam naziv društva koje njom upravlja (primjerice, adresa platforme je www.ime111.com, dok je naziv društva XYZ abcd Trading Ltd London).

Provjerite u registrima Hanfe smije li brokersko društvo pružati usluge na području RH

Samo određena brokerska društva smiju pružati svoje brokerske usluge na području RH. To su:

- **brokerska društva** kojima je sama Hanfa dala odobrenje za rad
- **brokerska društva iz drugih zemalja EU-a** koja su dobila odobrenje za rad od svojeg nacionalnog regulatora, a koja su izrazila namjeru pružati usluge na području RH
- **brokerska društva iz trećih zemalja** (bilo koja zemlja koja nije dio EU-a), a koja na području RH osnuju podružnicu. Ovakvih društava u pravilu ili uopće nema ili ima iznimno malo.

O SVIM TIM DRUŠTVIMA HANFA VODI EVIDENCIJE NA WWW.HANFA.HR:

- Evidencija društava kojima je Hanfa dala odobrenje za rad
- Evidencija društava iz drugih zemalja EU-a koja su izrazila namjeru pružati svoje usluge na području RH

Dakle, provjerite nalazi li se društvo čije vas je osoblje kontaktiralo u navedenim Hanfinim registrima ili kontaktirajte Hanfu izravno na sljedeće kontakte:



investment.firms@hanfa.hr
potrosaci@hanfa.hr info@hanfa.hr
01/6173-200



Ako se društvo ne nalazi u registrima, ne ulazite u poslovni odnos s takvim društvom. Najvjerojatnije se radi o prevari.

Vodite računa o brokerskim društvima iz trećih zemalja (bilo koja zemlja koja nije dio EU-a), a posebno ako društva imaju **registrirano sjedište na egzotičnim otocima** kao što su: Sveti Vincent i Grenadini, Vanuatu, Maršalovi Otoci i slično. Takva su područja poznata po slabijoj regulaciji te se brokerska društva tamo znaju povezivati s nekim oblicima prevare. **Hanfa preporučuje da se ne upuštate u poslovni odnos s takvim društvima.**

Vodite računa o sljedećim znakovima koji ukazuju na to da se vjerojatno radi o prevari:

Osim prethodno navedenih aktivnosti koje morate poduzeti prije bilo kakvog stupanja u poslovni odnos s nekim brokerskim društvom, obavezno vodite računa o sljedećim znakovima koji su jasan pokazatelj da tu nešto „ne štima“:

1. Uvjeravaju vas da ćete **sigurno zaraditi** i da je „sada prilika koja se događa jednom u životu“ da trgujete i zaradite.
2. Govore vam da trenutno **imaju „akciju“** koju „trebate iskoristiti odmah“ jer traje „samo još par sati/dana“.
3. Nagovaraju vas da uplatite manji iznos sredstava i da se na svoju ruku uvjerite kako je „**jednostavno zaraditi**“.
4. **Nagovaraju vas na trgovanje** neovisno o tome što vi nemate nikakvog iskustva u trgovanju jer ćete „dobiti svojeg mentora“ koji će vam pomagati prilikom trgovanja.
5. **Vrlo su uporni**, zovu vas po nekoliko puta dnevno i ne prihvaćaju „ne“ za odgovor.
6. Osobe se predstavljaju **imenima i prezimenima koja su popularna** i teško se mogu provjeriti, primjerice „Ivan Bošnjak“.
7. Govore vam da je „**vrlo jednostavno trgovati**“ i da ćete trgovati „dionicama“, a zapravo prešućuju da ćete trgovati kompleksnim izvedenicama odnosno financijskim instrumentima koje vjerojatno ne razumijete.
8. Govore vam da ćete **trgovati na „burzi“** i da imaju sve potrebne licence Hanfe ili nekog drugog regulatora.
9. Na trgovinskoj platformi **nema jasno navedenih kontakata** kojima se odmah i izravno možete obratiti, itd.

U tim slučajevima, ne ulazite u poslovni odnos s takvim društvom. Najvjerojatnije se radi o prevari.

Većina online trgovinskih platformi brokerskih društava nisu nikakve „burze“ odnosno tu se ne radi o trgovanju dionicama kao na npr. Zagrebačkoj, Ljubljanskoj ili Frankfurtskoj burzi koje predstavljaju uređena mjesta trgovanja. Tu se zapravo radi o tzv. OTC (over-the-counter), trgovanju izvan uređenih mjesta trgovanja. **Takva vrsta trgovanja sama po sebi nije zabranjena, ali je kompleksna za shvatiti, karakterizira je niži stupanj transparentnosti i zaštite malih ulagatelja, kao što ste vi.**

Tu nećete trgovati „dionicama“ već tzv. CFD-ovima (ugovori za razlike, contracts for difference), koji su kompleksni financijski instrumenti koji vam omogućavaju trgovati određenom vrstom imovine (najčešće su to dionice, strane valute, indeksi, zlato i nafta), bez da postajete vlasnik te imovine.

Kupnjom CFD-a razmjenjujete razliku u novcu između kupovne i prodajne cijene te imovine. Ako je razlika pozitivna, ostvarujete dobit koju vam dodjeljuje provider. Ako je negativna, vi ste dužni provideru.

Sve te osobine čine ove instrumente kompleksnima za shvatiti i često osobe koje vas kontaktiraju „propuštaju“ reći čime biste zaista trgovali putem njihove platforme (CFD-ovi) i koje su karakteristike tih instrumenata. I zato jednostavno kažu – dionice, što nije istina.

Ako ste ipak stupili u poslovni odnos s takvim brokerskim društvom, sljedeći su znakovi siguran pokazatelj da tu nešto ne štima:



Zovu vas učestalo na njihovu inicijativu te vam govore koje naloge otvoriti i po kojoj cijeni.



Stalno vas nagovaraju na uplatu dodatnog, sve većeg novca.



Vaš vas „mentor“ zove s nekog telefonskog broja koji nije iz RH i to je jedini način na koji komunicira s vama (odnosno nema pisanog traga komunikacije).



Ne možete ih dobiti na telefonske brojeve s kojih su vas zvali.



Učestalo se mijenja osoba s kojom razgovarate, a koja vam je dodijeljena kao „mentor“.



Prestaju se javljati kada date zahtjev da vam isplate natrag vaša sredstva ili kada vaši otvoreni nalozi počnu gubiti novac – baš tada su „uzeli godišnji“ ili „završili u bolnici“ pa vam se danima ne javljaju.



Traže da uplatite dodatan novac za potrebe „plaćanja poreza“, prije nego što oni vama isplate vaša sredstva natrag.



Postaju agresivni i nepristojni kada tražite odgovore i na najjednostavnija pitanja (posebno kada se radi o isplati novca natrag), itd.

Kada vam se to dogodi, nikako ne uplaćujte dodatni novac već ustrajte u isplati svojeg novca.

Prijavite slučaj policiji. U tim slučajevima, ako se radi o društvu koje nema odobrenje za rad kao broker i koje nije iz RH, ako je s egzotičnog otočja ili posebno ako uopće ne znate koji je naziv ili sjedište društva, najvjerojatnije se radi o prevari i teško ćete dobiti svoj novac natrag. Zato je posebno važno prije ikakvog stupanja u poslovni odnos s nekim društvom online ili prije uplate novčanih sredstava provjeriti s kime zapravo poslujete.



Prednost trgovanja putem licenciranih brokera je da se uvijek možete javiti regulatoru koji može u okvirima svojih ovlasti zaštititi male ulagače

Ako želite trgovati financijskim instrumentima, uvijek poslušajte s brokerskim društvima koja imaju odgovarajuću dozvolu za poslovanje i koja smiju svoje brokerske usluge pružati na području RH.

Međutim, posjedovanje odgovarajuće dozvole i činjenica da Hanfa ili neki drugi regulator iz EU-a kontroliraju zakonitost poslovanja takvih društava ne znači da baš sva brokerska društva uvijek postupaju u vašem najboljem interesu. Regulatori ne kontroliraju postupanja brokera 24 sata na dan. No prednost trgovanja putem licenciranog brokera je ta da se uvijek možete obratiti njegovom regulatoru koji može u konačnici zaštititi vaše interese kao klijenta brokerskog društva, što nije slučaj ako trgujete putem nelicenciranog brokera.

NA ŠTO JE POTREBNO DODATNO OBRATITI POZORNOST?

Boiler roomovi

Praksa je pokazala da inozemna brokerska društva znaju angažirati tzv. boiler roomove za potrebe dolaska do novih klijenata s područja RH. **Boiler roomovi su zasebna društva čiji zaposlenici telefonski prodaju brokerske usluge drugog društva, odnosno u našem slučaju telefonski nagovaraju potencijalne klijente na trgovanje.**

Navedena praksa označava postupanje koje nije u najboljem interesu klijenta jer se zaposlenici *boiler rooma* često predstavljaju kao zaposlenici brokerskog društva i često sami kao „brokeri“ ili „mentori u trgovanju“.

Boiler roomovi nemaju dozvolu za rad kao brokersko društvo što znači da vam brokerske usluge nude neovlaštene osobe za koje je vrlo upitno imaju li ikakvo znanje o financijskim tržištima i financijskim instrumentima. Inozemna brokerska društva angažiraju domaće *boiler roomove* prvenstveno zato jer naši građani lakše komuniciraju na našem jeziku.

Dodatan je razlog što strana brokerska društva ne odgovaraju za postupanja zaposlenika boiler rooma, za razliku od slučaja kada za promociju svojih usluga angažiraju legalno društvo (tzv. vezanog zastupnika).

Kako prepoznati boiler room?

Uz znakove upozorenja opisane u prethodnoj točki, jasan je znak i kada brokersko društvo iz druge zemlje (npr. Velika Britanija, Cipar) komunicira s vama putem osoba koje govore hrvatski jezik ili je jasno da su s govornog područja bivše Jugoslavije. Za više detalja o tome pogledajte jedno od Hanfinih prethodnih upozorenja.

Ako prepoznate bilo koji od znakova upozorenja koji su navedeni u prethodnoj točki, ne ulazite u poslovni odnos s takvim društvom te se javite Hanfi i prijavite takvo ponašanje.



INVESTICIJSKO SAVJETOVANJE




Inozemna brokerska društva (i to najčešće preko zaposlenika boiler roomova) znaju nago-varati naše građane na trgovanje obećavajući im osobu koja će im „pomoći u trgovanju“ ili „osobnog mentora“ koji će biti u učestalom telefonskom kontaktu nakon uspostavljanja poslovnog odnosa. Pri tome se to „mentorstvo“ svodi na to da takve osobe na svoju inicijativu nazivaju klijente iz RH i potom im jasno govore koji instrument kupiti (odnosno koji CFD nalog otvoriti ili zatvoriti), u koje vrijeme i po kojoj cijeni.

U konačnici, ugovorni se odnos svede na to da naš građanin postupka isključivo kako mu kaže osoba s druge strane telefonske žice, odnosno u potpunosti se oslanja na dane savjete.

Ovdje je bitno za znati da se u tom slučaju klijentu pruža usluga investicijskog savjetovanja. **Investicijsko savjetovanje je kada društvo daje osobne preporuke klijentu s kojim instrumentom trgovati, kada i po kojoj cijeni, a koje u tom slučaju nisu namijenjene široj javnosti.**

U većini slučajeva pružanje takve usluge nije ugovoreno s klijentom, odnosno klijentu se službeno ne pruža takva usluga. Zašto onda društva pristupaju takvoj taktici? Kako bi nagovorila klijente koji nemaju nikakvog prethodnog iskustva da počnu trgovati, kako bi stekla povjerenje klijenta, kako bi klijent otvarao sve veće i rizičnije pozicije temeljem kojih društvo uzima veće provizije za sebe i tako dalje. **Pri tome će društvo paziti da takva ko-**



Broker je osoba koja samo izvršava odluke i naloge koje mu je zadao ulagatelj, dok investicijski savjetnik može malim ulagateljima davati i savjete s kojim konkretnim financijskim instrumentom trgovati, a može čak i samostalno upravljati imovinom malog ulagatelja.

munikacija (davanje savjeta) ne bude pisana, odnosno da joj se teško može ući u trag jer se radi o nedopuštenim aktivnostima.

I što je najvažnije, u slučaju da izgubite novac trgovanjem prateći savjete društva, društvo će odbacivati odgovornost jer ste „vi sami u konačnici donijeli odluke s čime trgovati“ odnosno da vam službeno nije davalo savjete jer to nije ugovoreno između klijenta i društva. To definitivno nije postupanje u najboljem interesu klijenta.


I zato, **ako sami nemate znanja i vještina da znate u kojem smjeru bi se mogla kretati cijena CFD-a i ako bi vaše odluke o trgovanju ovisile isključivo o tuđim uputama za koje te osobe u konačnici ne bi odgovarale, onda bi najbolje bilo uopće ne trgovati i ne plaćivati novac.**

2. „Naišla sam na oglas na internetu i izgleda da lako mogu zaraditi veliki novac trgujući dionicama. I drugi njihovi klijenti kažu da su zaradili!“




Na novinskim portalima, profilima na Facebooku, Youtube poveznicama i ostalim popularnim stranicama često se može naići na poveznice u kojima se „odaju tajne“ kako brzo zaraditi novac na internetu ili u kojima fizičke osobe (nerijetko slavne hrvatske osobe kao što su sportaši, poduzetnici ili osobe iz javnog života) objašnjavaju na koji način su „zapravo“ zgrnule veliko bogatstvo ili izašle iz financijskih problema te su upravo sada spremne podijeliti tu strogo čuvanu tajnu.

Te su poveznice zapravo prikriveni oglasi kojima vas se želi nagovoriti da počnete trgovati financijskim instrumentima (CFD-ovima) putem online trgovinskih platformi, odnosno nagovoriti vas da na takve platforme uplatite novac. **Teško je utvrditi tko stoji iza takvih platformi/oglasa, a uglavnom se radi o inozemnim društvima koja nemaju dozvolu za pružanje investicijskih/brokerskih usluga na području Republike Hrvatske.** U mnogim se slučajevima zapravo radi o nekom obliku prevare.



Radi se o lažnim člancima na koje ne smijete nasjedati. Ne uspostavljajte odnos s takvim stranicama i nikako ne uplaćujte novac na njihove račune.

Na koji način prepoznati takve lažne članke?

- 
1. Obećava se sigurna i laka zarada na način da se počne trgovati online.
 2. Navode se primjeri osoba koje su u „teškim životnim situacijama“ skoro preko noći zaradile veliki novac i izašle iz financijskih problema pri čemu ne postoji nikakav način da se provjeri autentičnost tih navoda ili identitet osobe.
 3. Daju se opisi lagodnog života ostvarenog lako zarađenim novcem (putovanja, bezbrižnost) te se daju fotografije velike količine novca, luksuznih automobila, kuća na moru, skupih odijela i satova i slično.
 4. Ispod članka je veliki broj isključivo pozitivnih komentara „osoba“ koje su navodno primjenom trgovinskih metoda puno zaradile i koje „potvrđuju“ uspješnost platforme.
 5. Opisuje se „odavanje velikih tajni“ trgovanja koje navodno nitko ne smije znati i koje su samo za vas i koje će vam se odati samo kada date svoje kontaktpodatke.
 6. Navodi se da su poznate hrvatske/svjetske osobe stekle bogatstvo trgujući upravo tom platformom prateći „nekoliko jednostavnih koraka“ pri čemu se stavljaju slike tih poznatih osoba s kojima se često provode intervjui na temu zarade.
 7. Spominju se „akcije“ na koje je potrebno reagirati odmah i slično.



Ukoliko odlučite trgovati financijskim instrumentima prvo se dobro informirajte i upoznajte sa svim rizicima takvih poduhavata te izaberite samo provjerena i registrirana investicijska društva koja imaju važeće licence regulatora.

ŠTO TREBATE ZNATI O RIZICIMA ULAGANJA NA KRIPTOTRŽIŠTU?



U posljednjih četiri godine intenzivno raste promet trgovanja kriptovalutama. Istovremeno, bombardirani smo jakim marketinškim kampanjama koje putem medija ili na društvenim mrežama potiču mnoge na takva ulaganja.

U odnosu na druga ulaganja na tržištu kapitala, ulaganje u kriptovalute nosi dodatan rizik jer je podložno iznimnim oscilacijama u vrijednosti, a osim toga nije ni regulirano. Tempo rasta i razvoja tržišta kriptovalute značajno je brži od nužnog razvoja pratećeg regulatornog okvira tog tržišta.

Stoga je i stupanj zaštite korisnika i ulagačelja u kriptovalutinu trenutno značajno manji nego što je to slučaj kod klasičnih financijskih usluga (kao što je trgovanje na burzama ili kupovanje udjela u investicijskim fondovima) iako se na razini Europske unije (EU) uspostavljaju mehanizmi regulacije i nadzora kriptotrižšta, no oni neće zaživjeti prije 2024. godine.

TKO NADZIRE TRGOVANJE KRIPTOIMOVINOM?

Na razini EU-a i u Hrvatskoj trgovanje kriptovalutama nije regulirano propisima iz područja financijskih usluga, izuzev u dijelu sprječavanja pranja novca i financiranja terorizma.

Tako je od početka 2020. Hanfa u pogledu trgovanja kriptovalutama nadležna za područje primjene Zakona o sprječavanju pranja novca i financiranja terorizma, i to u odnosu na osobe koje se bave djelatnošću pružanja usluga razmjene virtualnih i fiducijarnih valuta i/ili pružanja skrbničke usluge novčanika. Hanfa kroz svoje nadzor-

ne aktivnosti provjerava provode li takve osobe sve mjere i postupke propisane tim zakonom.

ŠTO SU KRIPTOMJENJAČNICE?

Kriptomjenjačnice pružaju usluge konverzije kriptovaluta u novac i obrnuto. Hanfi je trenutno prijavljeno 20-tak društava koja pružaju takve usluge i prati ih u pogledu primjene Zakona o sprečavanju pranja novca i financiranja terorizma, ali ne izdaje odobrenja za njihov rad, ne licencira članove uprava društava, niti je ovlaštena nadzirati ih, kao što to čini u drugim djelatnostima na financijskom tržištu.

ŠTO JE ICO?

ICO je metoda prikupljanja sredstava u javnosti, uz upotrebu takozvanih *coina* odnosno *tokena*. Svaki ICO može se razlikovati u odnosu na njegovu strukturu i prava koja kupac stječe kupnjom tokena, što znači da prava povezana s kupnjom određenih

tokena nisu standardizirana. U većini slučajeva proizvodi u okviru ICO-a kupuju se za određenu kriptovalutu (npr. *bitcoin*, *eter*). Tokeni se stvaraju i distribuiraju pomoću takozvane *Distributed Ledger Technology* (DLT) kao širokopojasne tehnologije primjenjive u raznim područjima, primjerice u vođenju raznih elektroničkih baza podataka u industriji, uslužnim djelatnostima, financijskom sektoru, državnoj upravi itd., gdje nema centralnog administratora ili pohrane podataka, dok se sekundarno trgovanje tokenima u pravilu organizira na posebnim trgovinskim platformama namijenjenima kupovini, prodaji ili razmjeni kriptovaluta.

KOJI SU RIZICI POVEZANI S KRIPTOVALUTAMA I ICO?

- Uglavnom neregulirano područje, uslijed čega je češća mogućnost prijevara i drugih nepravilnosti
- Manjak pouzdanih i relevantnih informacija
- Visok rizik od gubitka dijela ili svih uloženi sredstava
- Izrazita volatilitnost vrijednosti ulaganja i

nemogućnost svakodobnog „izlaska“ iz ulaganja

- Rizici vezani uz informatičku tehnologiju koja se koristi za izradu i distribuciju tokena (primjerice, hakerski napadi, nemogućnost pristupa tokenima, gubitak ključa za pristup tzv. digitalnom novčaniku).

KOJA JE RAZLIKA IZMEĐU TRANSAKCIJE KRIPTOVALUTAMA I KREDITNIM/DEBITNIM KARTICAMA?

Kod transakcije debitnim/kreditnim transakcijama uvijek **postoji treća strana**, koja pruža uslugu posredovanja u provođenju transakcije između dvije strane, kupca i prodavatelja. Drugim riječima, krajnji korisnici svoje povjerenje daju nekoj trećoj strani, posredniku, te provođenje transakcije ovisi o postupanju te treće strane.

Nasuprot toga, kod *kriptoimovine* provođenje transakcije kontrolira određeni distribuirani računalni protokol (ovisno o vrsti blockchaina), a svatko može provjeriti





koliko kriptoinovine ima određeni račun u sustavu te gdje je i kada poslan određeni iznos. **U takvom sustavu korisnici mogu međusobno izvršavati transakcije bez korištenja posrednika.**

POSTOJI LI REGISTAR LICENCIRANIH PRUŽATELJA USLUGA RAZMJENE VIRTUALNIH VALUTA?

Djelatnosti razmjene virtualnih i fiducijarnih valuta i skrbničke usluge novčanika u EU-u

nisu regulirane što se tiče davanja odobrenja za njihov rad od strane regulatornih tijela, tj. njihova licenciranja. Hanfa stoga ne izdaje odobrenja za rad osobama koje se bave djelatnošću pružanja usluga razmjene virtualnih i fiducijarnih valuta i/ili pružanja skrbničke usluge novčanika.

Međutim, sva društva koja su osnovana u Hrvatskoj i pružaju spomenute usluge moraju se javiti Hanfi u skladu s odredbama Zakona o sprječavanju pranja novca i financiranja terorizma te se ona nalaze na Hanfinu popisu osoba osnovanih u Republici Hrvatskoj koje se bave djelatnošću

ŠTO JE KRIPTONOVČANIK (WALLET)?

Za trgovanje kriptovalutama potreban vam je novčanik (tzv. *wallet*) na kojem se pohranjuju vaše kriptovalute. Kriptonovčanik sličan je bankovnom računu. On omogućuje transakciju i pohranu virtualnih valuta, ali za razliku od sredstava na bankovnom računu, **sredstva odnosno kriptoinovina spremljena u walletu nije zaštićena nikakvom jamstvenom shemom poput sustava osiguranja depozita.** Prilikom kreiranja računa, odnosno otvaranja novčanika sustav će generirati jedinstveni privatni ključ (kod), pomoću kojeg se pristupa novčaniku te se odobravaju transakcije, slično bankovnom PIN-u. **U praksi su česti slučajevi gubitka ili krađe privatnog ključa za pristup walletu.**



pružanja usluga razmjene virtualnih i fiducijarnih valuta i/ili pružanja skrbničke usluge novčanika.

KOLIKO JE TRGOVANJE VIRTUALNIM VALUTAMA SIGURNO?

Trgovanje virtualnim valutama, **odnosno ulaganje u kriptoinovinu nije posebno regulirano pa ne postoje određeni zaštitni mehanizmi i kontrole za ulagatelje, kao što je slučaj kod trgovanja dionicama ili drugim klasičnim financijskim instrumentima.**

Riječ je o špekulativnim ulaganjima, **koja su zbog svoje visoke volatilnosti, ali i drugih tržišnih rizika, visokorizična.** Takva ulaganja mogu biti posebno rizična za male

ulagatelje, i to osobito one koji nemaju sve informacije o obilježjima kriptovaluta i/ili nemaju dovoljno predznanja iz područja financija i tehnologije na kojoj se zasnivaju kriptovalute. Posebnu pozornost treba obratiti i na zavaravajuće, lažne oglase o trgovanju kriptovalutama. Najčešće je riječ o fiktivnim kriptovalutama. Takvi oglasi oponašaju objave poznatih financijskih časopisa te koriste lažna svjedočanstva poznatih osoba o financijskim dobitcima kako bi potakli građane da uplate novac.

ŠTO AKO IZGUBIM ILI ZABORAVIM ŠIFRU SVOG KRIPTORAČUNA/ KRIPTONOVČANIKA?

Svi vlasnici kriptoinovine trebaju voditi računa o svojim jedinstvenim privatnim klju-

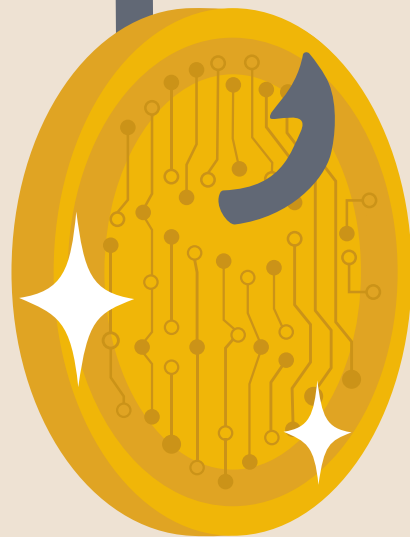
čevima, tj. šiframa za pristup kriptovalutama. Naime, u slučaju gubitka privatnog ključa ne postoji mogućnost povrata imovine koja se nalazila pod tim ključem. Prema nekim istraživanjima oko 20 % ponude bitcoina izgubljeno je jer su vlasnici izgubili ili zaboravili svoje privatne ključeve.

KOJA JE RAZLIKA IZMEĐU TRANSAKCIJA KRYPTOVALUTAMA I TRGOVANJA FINANCIJSKIM INSTRUMENTIMA?

Trgovanje financijskim instrumentima strogo je regulirano. U pravilu je za trgovanje financijskim instrumentima potreban financijski posrednik, najčešće investicijski savjetnik ili broker, tj. investicijsko društvo ili kreditna institucija (ili bolje izraz banka?). Pritom investicijska društva ili banke mogu pružati i savjetodavne usluge, a mogu i odbiti izvršenje određene transakcije ako smatraju da ona nije prikladna za pojedinog ulagatelja.

Kroz **sustav zaštite ulagatelja** formiran je i **Fond za zaštitu ulagatelja**. Svrha je fonda zaštita tražbina klijenata društava ovlaštenih za pružanje investicijskih usluga u slučaju kada ta društva nisu u mogućnosti takvu tražbinu isplatiti i/ili vratiti klijentu.

Treba istaknuti kako Fond za zaštitu ula-



Kod kriptovalut ne postoji sustav zaštite ulagatelja, a transakcije provodi i kontrolira računalni sustav (protokol) u kojem korisnici mogu izvršavati transakcije bez posrednika.

gatelja **ne štiti ulagatelje od tržišnih gubitaka, već samo u slučaju kada je društvo ovlašteno za pružanje investicijskih usluga u stečaju ili je Hanfa utvrdila da je nastupila nemogućnost ispunjavanja obveza prema klijentu.**

Osim toga, na kriptoburzama ulagatelji u pravilu mogu trgovati izravno, bez korištenja usluga posrednika, odnosno brokera. Dovoljna je registracija na neku od kripto-

burzi, nakon čega investitor sam direktno trguje kriptovalutama.

POSTOJI LI NAZNAKA REGULACIJE TRŽIŠTA KRYPTOIMOVINE?

EU priprema regulatorni okvir za tržište kriptovalut (prijedlog Uredbe o tržištima





kriptoimovine, engl. *Markets in Crypto-assets Regulation*, MiCA), koji bi regulirao subjekte koji pružaju usluge povezane s kriptoimovinom, primjerice usluge skrbništva i upravljanja kriptoimovinom u ime trećih strana te savjetovanja o kriptoimovini. Za razliku od trenutne situacije, usluge u vezi s kriptoimovinom **smjele bi pružati pravne osobe koje imaju registrirano**

sjedište u državi članici EU-a, a koje su dobile odobrenje za pružanje takvih usluga od nadležnog nadzornog tijela. Regulativom bi se obuhvatili i izdavatelji kriptoimovine koji namjeravaju nuditi kriptoimovinu ili tražiti uvrštenja na platforme za trgovanje kriptoimovinom u EU-u. Očekuje se da ova uredba biti donijeta tek u **2024. godini.**

KOJI SU NAJČEŠĆI RIZICI TRGOVANJA KRIPTOVALUTAMA?

Osim visoke volatilnosti tržišta, izražena je i **moгуćnost zloporabe tržišta, kao što su lažne informacije, asimetrične informacije te lažni volumen trgovanja.** Kod reguliranih sustava trgovanja zloporaba tržišta strogo se nadzire, a takva postupanja predstavljaju kaznena i prekršajna djela za koja su predviđene i zatvorske kazne.



Razlike kod ulaganja na (nereguliranom) kriptotržištu i tradicionalnom (reguliranom financijskom tržištu)

Kriptotržište

Nema financijskih posrednika, izravno trgovanje

Visoka volatilnost, visoki rizici, špekulativno tržište

Neregulirano tržište, ne postoje zakoni i propisi koji reguliraju trgovanje

Nema sustava zaštite potrošača ni zaštitnog fonda

Tradicionalna financijska tržišta

Za trgovanje potreban financijski posrednik

Niža volatilnost, ovisno o financijskom instrumentu i povezanim rizicima

Regulirano tržište, postoje zakoni i propisi koji reguliraju rad društava

Postoji sustav zaštite potrošača i zaštitnog fonda, moguće se obratiti regulatoru u slučaju nepravilnosti



PRIJEVARE NA KRIPTOTRŽIŠTU



Takozvane „ugledne platforme“ mogu preko noći prestati s radom (tzv. izlazne prijevare)



Osim tog iznimno naglašenog tržišnog rizika, ulagatelji se trebaju upoznati i s ostalim rizicima povezanim s takvim ulaganjima, imovinom i projektima koji su u podlozi imovine u koju ulažu te osobama koje stoje iza pojedinog projekta. U nastavku navodimo **samo neke** od rizika i prijevara koji se često povezuju s kriptoinovinom:

KRAĐA IDENTITETA (TZV. PHISHING)

Ulagatelji u kriptoinovinu vrlo su često izloženi različitim pokušajima krađe identiteta putem interneta. Osobe koje se lažno predstavljaju kao pružatelji usluga pokušavaju navesti ulagatelje da otkriju osobne informacije, posebice lozinke ili privatne ključeve (*private key*, *seed words*), njihovim upisivanjem na lažiranoj internetskoj stranici, poveznici danoj na društvenoj mreži ili putem poruke.



LAŽNE INTERNETSKE STRANICE

Lažne internetske stranice i poruke osoba koje žele nezakonito doći do osobnih podataka i financijskih sredstava ulagatelja jako su slične internetskim stranicama i porukama autentičnih pružatelja usluga, zbog čega ih je često vrlo teško razlikovati. Postoji iznenađujući broj internetskih stranica koje su postavljene tako da nalikuju originalnim, valjanim stranicama *startup* tvrtki. Ako u blizini URL trake nema male ikone lokota koja ukazuje na sigurnost i u

adresi web-mjesta ne postoji “https”, razmislite dvaput.

Čak i ako stranica izgleda identično onoj koju mislite da posjećujete, možda ćete biti preusmjereni na drugu platformu za plaćanje. Na primjer, kliknete na vezu koja izgleda kao legitimna stranica, ali napadači su prethodno stvorili lažni URL s nulom umjesto slova „o“. Ta vas platforma, naravno, ne vodi do ulaganja u kriptovalute koje ste već istražili. Da biste to izbjegli, pažljivo upišite točan URL u svoj preglednik. Dvaput provjerite i to.

LAŽNE MOBILNE APLIKACIJE

Još jedan uobičajeni način na koji prevaranti varaju ulagače u kriptovalute uključuje lažne aplikacije dostupne za preuzimanje putem “mobilnih dućana”. Dok ih operatori dućana otkriju i uklone, već naprave štetu. Tisuće ljudi već su preuzele lažne aplikacije za kriptovalute, prenosi Bitcoin News. Iako je veći rizik od takvih aplikacija za korisnike Androida, svaki bi investitor trebao biti svjestan tih opasnosti. Postoje li očite pravopisne pogreške u tekstu ili čak nazivu aplikacije? Izgleda li robna marka neautentično s čudnim bojama ili nepoznatim logotipom? Razmislite o preuzimanju takvih aplikacija.



Dobar je primjer platforma Thodex Exchange, koja je naprasno ugašena. Naizgled pouzdana i respektabilna platforma nekoć je obrtala milijarde dolara prometa kriptovalutama, ali su u travnju 2021. obustavljene sve aktivnosti nakon pritužbi investitora koji nisu mogli povući sredstva sa svojih računata.

Riječ je o gotovo 400 tisuća klijenata koji su, navodno, ostali bez kriptovaluta u protivrijednosti od dvije milijarde dolara. Masovna uhićenja koja su nakon toga uslijedila teško mogu utješiti ulagače – Thodex Ex-

change vjerojatno je poslužio kao paravan za *exit scam*, u kojem je cilj stvoriti naizgled respektabilnu platformu, a potom opelješiti klijente i pobjeći. Uz *exit scam*, *rug pull* (u slobodnom prijevodu nešto kao „izmicanje tla pod nogama“) vrlo je slična taktika rezervirana za kriptodomenu. Riječ je o malicioznom manevru u kojem pokretači platforme (najčešće je riječ o sustavima DeFi) u prikladnom trenutku napuštaju razvoj i nakon toga im se gubi svaki trag. Naravno, i prikupljenim sredstvima ulagača.

Kako razlikovati „prave“ od lažnih platformi? Jako teško. U svijetu društvenih medija prekid rada u praksi znači da korisnici privremeno nisu u mogućnosti kreirati ili pretraživati sadržaj. Isti takav zastoj u svijetu kriptovaluta podrazumijeva nimalo bezazlen prekid trgovine ili, u lošijoj varijanti, gubitak ulaganja.



PONUDE PREKO LAŽNIH PROFILA NA DRUŠTVENIM MREŽAMA

Možda ste greškom pratili varalicu ili *bota* koji vam može dati zlonamjerne ponude u vezi s kriptovalutama. Ne biste trebali vjerovati nikakvim investicijskim savjetima koji dolaze s popularnih društvenih mreža poput Facebooka ili Twittera.

Šanse da ne dobijete svoj novac natrag vrlo su velike. Trebali biste biti posebno oprezni i ne nasjedati na takve ponude zbog sudjelovanja više ljudi u odjeljku za komentare.

Decentralizirano financiranje omogućuje korisnicima da ulože svoje kriptovalute i osiguraju maksimalnu dobit kroz kamate. Dok neke renomirane DeFi platforme osiguravaju maksimalan povrat na posuđeni novac, neke su prijevare. Takve lažne platforme mame ulagače da posuđuju novac obećavajući veliku zaradu, ali novac koji investitori posuđuju stavljaju u džep. Takve se prijevare izvode tako lukavo da ulagači često ne uspijevaju povratiti izgubljeni iznos.

PRIJEVARE S NEZAMJENJIVIM TOKENIMA

Nezamjenjivi tokeni ili NFT-ovi trenutno su popularni. Nezamjenjivi tokeni digitalna su imovina koja predstavlja širok raspon jedinstvenih materijalnih i nematerijalnih predmeta, od kolekcionarskih sportskih karata do virtualnih nekretnina, digitalnih tenisača, digitalnih memorabilija, animacija i slika.

LAŽNE PORUKE PUTEM ELEKTRONIČKE POŠTE ILI APLIKACIJA ZA KOMUNIKACIJU

Čak i ako izgleda točno kao e-mail ili poruka na WhatsAppu ili Telegramu koju ste primili od legitimne tvrtke za kriptovalute, pripazite prije nego što uložite svoju digitalnu valutu. Je li e-pošta potpuno ista i jesu li logotip i robna marka identični?

Možete li potvrditi da su adresa e-pošte ili telefonski broj legitimno povezani s tvrtkom? Mogućnost da to provjerite jedan je od razloga zašto je važno odabrati tvrtku koja ima stvarne ljude koji rade za nju.

Ako sumnjate u e-mail adresu ili telefonski broj pitajte nekoga tko tamo radi. I nikada nemojte kliknuti na vezu u poruci da biste došli do stranice.

LAŽNE DeFI PLATFORME

DeFi je kratica za „decentralizirane financije”, pokušaj obnove i transformacije tradicionalnih metoda i modela trgovanja.

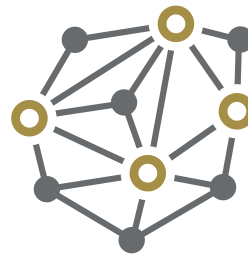
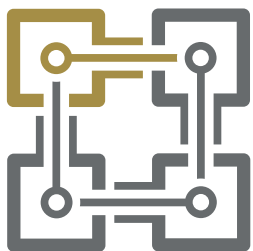


Kao i kod svakog ulaganja u digitalnom obliku, postoji rizik od malicioznog koda koji može dovesti do toga da izgubite svoje ulaganje, a u konkretnom slučaju NFT-a i do toga da digitalna imovina koju ste kupili nije zaista „original“ odnosno „unikat“ koji vam je obećan prilikom kupnje.

PRIJEVARA PUTEM JAVNE PONUDE KRIPTOVALUTA

Prva ponuda određene kriptovalute na prodaju, najčešće nazvana *Initial Coin Offering* ili ICO, ali prisutna i u drugim varijantama

kao što su inicijalna ponuda putem burze (*Initial Exchange Offering* ili IEO), te inicijalna ponuda putem decentralizirane burze (*Initial Dex Offering* ili IDO), a u zadnje vrijeme i inicijalna ponuda udjela ili ISO (*Initial stake offering* - najčešće se promovira na *block-chain* platformi *Cardano*), također može biti sredstvo za krađu sredstava. Naime, mnoge takve ponude potpuno su izmišljene, s lažnim biografijama nepostojećih članova tima i tehničkim dokumentima kopiranim iz drugih, legitimnih kriptovaluta. Ove prijevare obično su inačica Ponzi sheme u kojoj se novac prikuplja od novih članova i koristi se kako bi se stvorila iluzija isplativog ulaganja.



PRIJEVARE UZROKOVANE VIRUSIMA I ZLONAMJERNIM SOFTVEROM

Stalno nove strategije i kreativni pokušaji provale u novčanik investitora ponekad mogu biti zamorni. Uz mnoštvo novih načina hakeri i kriminalci pribjegavaju i prastarim zlonamjernim softverima i virusima kako bi dobili pristup tuđim kriptonovčanicima. Samo iz tog razloga dvofaktorska autentifikacija trebala bi biti minimalna razina sigurnosti koju koristite prilikom ulaganja u kriptovalute.

To može potrajati dulje vrijeme, međutim s ovim vrstama prijevara krajnji rezultat uvijek je isti, a kreatori sheme nestaju s ulagačkim sredstvima.

Trgovanje kriptovalutama i ICO često se u medijima spominju kao atraktivne aktivnosti kojima se lako i na jednostavan način može zaraditi ili doći do sredstava za financiranje određenih projekata.

Lažni ICO-evi uglavnom se provode putem interneta i društvenih mreža, često su inicirani izvan Republike Hrvatske ili čak izvan Europske unije, a u njihovoj promociji ponekad su eksponirani i uspješni poduzetnici i osobe iz javnog života poznate pojedinom lokalnom odnosno nacionalnom tržištu, a kako bi se pridobilo povjerenje ulagačke javnosti.

Ipak, osim očito lažnih projekata, projekti koji skupljaju sredstva na ovaj način mogu biti i sofisticirane prijevare koje je teško jednostavno prepoznati. U takvim oblicima javne ponude tokena njezini kreatori duže vrijeme, ako ne i godinama, troše dio prikupljenih sredstva ulagatelja na održavanje privida uz predočenje navodnih dokaza o razvoju projekta i održavanjem marketinga u vezi s projek-

tom, dok zapravo nikad nisu imali pravu namjeru razviti projekt ili nikad nisu imali ideju kako bi to napravili te se samo radi o dobro razrađenoj i sofisticiranoj prijevare, a većina sredstava utrošena je na osobne potrebe kreatora projekata i s njima povezanih osoba.

Međutim, ovdje je često riječ o visokorizičnim i nereguliranim aktivnostima pa potencijalni ulagatelji moraju biti posebno svjesni mogućnosti gubitka svih uloženi sredstava i mogućeg nedostatka pravne zaštite.

Naime, s obzirom na razne pojavne oblike kriptovaluta, njihove strukture, načina na koji se nude te činjenice da ne postoji specifična regulativa kriptovaluta na europskoj i nacionalnoj razini, procjena pravne naravi kriptovaluta ovisit će o tome kako je ICO strukturiran u svakom pojedinom slučaju.

PUMP AND DUMP (PONZIJEVE) SCHEME I GRUPE

Kripto može ponuditi novu varijaciju klasične *pump and dump* sheme, gdje vlasnici dionica pokušavaju podići cijenu prije nego što rasprodaju svoje udjele na umjetnom vrhuncu. U svijetu kriptovaluta to je uobi-

čajeno u fazi ICO-a, ili čak i izvan nje, kad god lažne tvrdnje mogu potaknuti potražnju i dopustiti izvornicima ili dominantnim vlasnicima kriptovalute da zarade ogromne lažne zarade.

Ova pojava nije neuobičajena na drugim mjestima trgovanja, posebno na dioničkim tržištima, ali nedostatak regulacije znači da prijevare koje bi izazvale ovu vrstu manipulacije cijenama nisu ilegalne u kriptosvijetu.

Cilj je da se kroz ulaganja velikog broja ljudi (koji nisu pravi igrači) napumpa vrijednost nekog tokena. Uglavnom se odvijaju unutar grupa na kriptoplatformama (Didsord, Reddit, Telegram), u okviru njih se potiče ulagače da nauče prepoznati kada je trenutak da se uloženo proda (kako imati tzv. dijamantne ruke).

Ako imate „dijamantne ruke”, spremni ste zadržati poziciju do krajnjeg cilja, usprkos potencijalnom riziku i gubicima. Većina maloprodajnih investitora želi dokazati da su sposobni opstati pod pritiskom, što je

za ove sheme od ključnog značaja. Broj takvih polujavnih grupa, kao i njihovih članova, raste, a mnogi koji se upuštaju u odluke na temelju razgovora i nagovora nisu svjesni rizika koliko mogu biti izigrani. Na kraju, posljednji ljudi koji uđu u ove sheme zajamčeno gube novac.

POKLONI ZA KRYPTOVALUTE

Još jedna uobičajena prijevarena s kriptovalutom dolazi u obliku dijeljenja. Koristeći se društvenim mrežama, e-poštom ili drugim sredstvima, prevarant se predstavlja kao poznata osoba i tvrdi da daje poklon za kriptovalute. Dijeljenje se obično oglašava u obliku „Besplatni BTC pokloni! Pošaljite 0,1 ETH na ovu adresu i zauzvat primite 1 BTC!”.

Ali nakon što žrtve pošalju svoj novac, prevaranti nestaju bez davanja obećane nagrade. Ljudi često postaju žrtve ove vrste prijevare jer se ti prevaranti jako trude da bi se činili legitimnim.

Kako se možete zaštititi od prijevare s kriptovalutom?

- 1. Budite oprezni i budite sumnjičavi;** ako se čini predobro da bi bilo istina, vjerojatno jest.
- 2. Imajte plan i držite ga se;** ne reagirajte brzo na emocije poput pohlepe ili straha od propuštanja dobiti. Napravite plan ulaganja i držite ga se.
- 3. Spremite svoja sredstva na siguran način;** što sigurnije pohranite svoja sredstva (na primjer, na hardverski novčanik), to je manja vjerojatnost da postanete žrtvom krađe identiteta ili zlonamjernog softvera.
- 4. Pošaljite testnu transakciju.** Niste sigurni imate li zlonamjerni softver? Prvo pošaljite malu testnu transakciju da biste vidjeli hoće li sredstva stići na adresu primatelja ili ne. Ako ne uspije, možete biti prilično sigurni da se nešto sumnjivo događa.
- 5. Uložite minimalno malo novca.** Ako nikada dosada niste ulagali u kriptovalute, **a pogotovo ne cijelu svoju ušteđevinu**, a ipak se za to odlučite, nikad nemojte ulagati veći iznos novca.
- 6. Izbjegavajte zajamčenu dobit,** to je gotovo uvijek prijevarena. Čak i one prijevare koje nisu očite vjerojatno će vas na neki način koštati novca.



Što učiniti ako ste žrtva prijevare?



1. Prijavite svoj slučaj policiji kako bi istražila slučaj.
2. Koristite li isti privatni ključ ili lozinku za pohranu više kriptovaluta? Ako je to slučaj, premjestite ostale novčiće ili promijenite lozinke.
3. Je li vaše računalo zahvaćeno zlonamjernim softverom? Ako je tako, prestanite ga koristiti!
4. Zapitajte se postoji li šansa za buduće gubitke od ove prijevare. Učinite sve što je potrebno da biste ih izbjegli.

Što treba u svakom slučaju uzeti u obzir prije nego što se odlučite za ulaganje u kriptoinovinu?

- Tržišta kriptoinovine česta su **meta prijevara** pa treba biti posebno oprezan.
- **Ako vam je obećan siguran ili iznimno visok povrat, ako vas požuruju da donesete odluku ili ako prilika koja vam se nudi zvuči predobro da bi istinita, budite posebno oprezni.**
- Budite sigurni da ste dobro provjerili sve okolnosti u vezi s određenom kriptoinovinom, kao što su informacije o izdavatelju proizvoda i osobama koje vam nude ulaganje u taj proizvod. Ako ulažete u nečiji poslovni poduhvat, iznimno značajna za ostvarivanje vaših prava može biti i činjenica gdje se nalazi subjekt u čije poslovanje ulažete. **Veća je vjerojatnost da ćete svoja prava ostvariti ako ulazite u poslovni odnos sa subjektima iz Hrvatske odnosno Europske unije.**
- Vrijednost kriptoinovine iznimno je **volatilna**, a kako brzo može rasti tako brzo može i padati njezina vrijednost.
- Kriptoinovina je špekulativno ulaganje koje sa sobom donosi brojne različite rizike. Ako se odlučite za ulaganje u kriptoinovinu, **trebate biti spremni izgubiti cijeli iznos svojeg ulaganja.**
- **Dobro se raspitajte o poreznom tretmanu takvih ulaganja.**



Svakog
15. u mjesecu

Javna *online* predavanja Hanfe

15. 12. 2021. u 10:00 sati

Tema 3: MIROVINSKA ŠTEDNJA - 2. I 3. STUP

Prijaviti se možete e-mailom na edukacija@hanfa.hr

Više informacija o sektoru finansijskih usluga
i registriranim finansijskim društvima
potražite na:

www.hanfa.hr
www.novaczasutra.hr