



Pošast online prijevara: Kako izgubiti novac na internetu? (Drugi dio): Lažni brokeri, obećanja ogromnih zarada i bogatstvo kriptovaluta

Autor **Petar Radanović** - Friday, October 3, 2025, 16:17

Otkrijte više

[Proizvodnost](#)

[produktivnost](#)

Kad je 67-godišnjakinja iz Daruvara 2021. godine kliknula na internetski oglas koji je obećavao "brzu i sigurnu zaradu od investicija u kriptovalute", nije znala da je upravo kliknula na jednu od najčešćih i najopasnijih mrežnih prijevara. Tek nekoliko godina kasnije, kad je ukupno prebacila više od 45.000 eura na različite račune, žena je shvatila što joj se dogodilo: kao i mnogi drugi hrvatski građani, postala je žrtva jednog od najčešćih oblika online prijevara – prijevare od strane lažnih brokera koji obećavaju laganu zaradu na burzama, kriptovalutama i "novim financijskim instrumentima".

Za razumijevanje ove vrste prijevare važno je pojasniti što je, zapravo, broker? Broker je posrednik između investitora i financijskih tržišta. Njegova primarna uloga je da pomogne investitorima s kupovanjem i prodavanjem financijskih instrumenata – dionica, obveznica, kriptovaluta – ili drugih vrijednosnih papira. Legitimni brokeri su registrirani kod financijskih regulatora, posjeduju licence za rad i potpadaju pod strogi nadzor što čini njihovo poslovanje transparentnim i sigurnim za klijente. U Hrvatskoj, legitimni brokeri trebaju biti registrirani kod HANFA-e (Hrvatske agencije za nadzor financijskih usluga). Međutim, lažni brokeri nisu registrirani nigdje. Oni su sofisticirani prevaranti koji koriste sve moderne tehnike psihološke obmane i računalnog hakiranja kako bi te privukli, zaveli i otuđili nečiji novac. Često dolaze sa impresivnim web stranicama koje izgledaju kao legitimne – sa profesionalnim dizajnom, preciznim informacijama, često čak i s lažnim dozvolama regulatora za koje koriste ukradene ili krivotvorene logotipe HANFA-e ili Zagrebačke burze.

Kako počinje tipična prijevara od lažnog brokera?

Najčešće sve počinje na društvenim mrežama ili kroz internetske oglase. Žrtva naiđe na oglas koji nudi "bazu za brze dobitke" ili "siguran način da zaradite 30-50% godišnje" od ulaganja. Oglas izgleda profesionalno i često prikazuje fotografije poznatih osoba – političara, glumaca ili pjevača – koji "preporučuju" ulaganje, premda su ta lica bez znanja korištena kao dio prijevare. Žrtva potom klikne na oglas i vrlo brzo je kontaktira "broker", koji se predstavlja kao stručnjak za investicije. Komunikacija je obično profesionalna i pažljiva – prevaranti će odgovoriti na sva pitanja, vrlo su ljubazni, a često i pokazuju veliko znanje o financijama. Na sve se načine trude izgledati kao legitimni brokeri – koriste sve komplicirane financijske izraze, spominju međunarodne burzovne indekse (S&P 500, DAX, Nikkei) te opisuju "strategije" koje jako brzo mogu dovesti do velikog dobitka. Ključni moment dolazi kada prevaranti mole žrtvu da započnu ulagati s nekim "malim ulogom" – obično negdje između 250 i 500 eura. Kažu joj da se radi o "testnom ulaganju" ili "verifikaciji računa", da je potrebna "aktivacijska naknada" ili "provizija menadžera". Žrtva, koja je već intrigirana obećanjem brzog dobitka, obično bude spremna uložiti taj iznos.

I tu dolazi dio gdje se prijevara počinje razvijati. Nakon što žrtva uplati novac, prevarant joj pokazuje lažnu platformu za trgovanje. Na toj platformi, inicijalna uplata od 250 eura se, prema "izračunima" na računalu (koji su naravno potpuno lažni), pretvara u 5.000, 10.000 ili čak 50.000 eura u samo nekoliko dana. Žrtva tako vidi da se njezino "ulaganje" jako brzo povećava iako ne razumije kako to zaista funkcionira, no psihološka manipulacija je savršena – žrtva "vidi" novac koji "raste". Nakon početnog oduševljenja što njezin "profit" raste, prevaranti dolaze s novim zahtjevima: kažu da ako želi iskoristiti tu dobit i zaraditi još više treba uložiti dodatnu sumu, obično veću nego što je uložila prvo, ili joj prikazuju neke "propuste" ili "rizike" koji se trebaju pokrivati kroz dodatne uplate. I tako kreće spirala sve većih troškova odnosno uplata potaknutih prividom sve veće zarade.

Otkrijte više

[Proizvodnost](#)

[produktivnost](#)

39-godišnjakinja iz Umaga, o kojoj su domaći mediji izvijestili potkraj kolovoza ove godine, bila je klasičan primjer tog mehanizma: od početnih malih uplaćenih iznosa, tijekom nekoliko mjeseci prevaranti su je nagovorili na višestruke uplate koje su u konačnici iznosile više od 80.000 eura. Kako bi je zadržali zainteresiranom, čak su joj isplatili nekoliko tisuća eura kao "dobit" – taj novac je zapravo bio njezin vlastiti novac koji je prevaranti vratili kako bi joj pokazali da je sve "legalno" i da je veliki, "pravi profit" čeka na "sljedećoj razini ulaganja". U drugom slučaju, 73-godišnjak iz Rijeke je počeo s 3.000 eura, a završio s gotovo 200.000 eura prebačenih na račune prevaranata, jer je sustavno bio uvjeren da će ostvariti "povrat izgubljenog novca plus dodatno zaraditi".

Iako je mehanizam isti, prijave se razlikuju u detaljima ovisno o ciljanoj skupini: prve su kriptovalutne prijave. Žrtvi se nude ulaganja u Bitcoin, Ethereum, ili "nove kriptovalute koje će biti sljedeći Bitcoin". Prevaranti koriste činjenicu da većina ljudi ne razumije kako kriptovalute funkcioniraju i koriste to neznanje kao alat manipulacije. Obično će reći da je "sada pravi trenutak" da se uloži jer bi određena kriptovaluta trebala snažno povećati svoju vrijednost ili da je "nova kriptovaluta" dostupna samo "u ograničenom vremenu". Druga vrsta su burzovne prijave. Žrtvi se nude ulaganja u "sigurne" dionice, nekad i hrvatskih kompanija (česte su bile lažne ponude za dionice PPD i INA-e gdje su se nudile "ekskluzivne šanse" za kupnju dionica po "povoljnim cijenama"). Treće su tzv. valutne prijave, poznatije kao forex, koje su bile aktualne još prije petnaestak godina: Žrtvi se nudilo ulaganje na deviznom tržištu, često s obećanjima o zaradama od 30-50% mjesečno – što je gotovo sigurna indicija da se radi o prijevari, jer legitimni forex brokeri rijetko dostižu toliku zaradu za klijente. I konačno, nude se i razne "nove investicijske prilike": prevaranti često izmišljaju novu vrstu ulaganja ili "novu platformu" koja je "samo za odabrane ljude" i koja može donijeti "nevjerojatne povrate". Popis je neograničen – all share trading, forex, altcoins, blockchain investicije i tko zna što još sve ne.

Tehnike koje koriste prevaranti

Internetske stranice i aplikacije: prevaranti postavljaju izuzetno napredne lažne web stranice i mobilne aplikacije koje izgledaju kao pravi brokeri. Nerijetko se događa da kloniraju izgled stranica ili aplikacija stvarnih brokera – koriste isti logo, istu boju, isti stil – ali s malo drugačijom domenom. Na primjer, umjesto "brokerA.com" mogu biti "brokerAa.com" ili "broker-a.com". Većini žrtava ne primijeti razliku sve dok nije prekasno. .

Lažni regulatorni dokumenti: prevaranti često prilažu "dokaze" da su regulirani – lažne certifikate, krivotvorene logotipe HANFA-e ili međunarodnih regulatora kao što su FCA (Financial Conduct Authority) ili SEC (Securities and Exchange Commission). Često koriste i imena legitimnih tvrtki ili regulatora kao što je DNCA Finance Luxembourg, kako bi dodali kredibilitet svojim lažnim zahtjevima.

Otkrijte više

[Proizvodnost](#)

[produktivnost](#)

Menadžeri računa: Nakon što žrtva uloži neki iznos, često joj biva "dodijeljena" specifična osoba koja se predstavlja kao njezin "osobni menadžer računa". Ta osoba žrtvi redovito šalje "izvještaje" o rastu ulaganja, nudi "savjete" i aktivno nagovara na dodatne uplate. Komunikacija je često veoma profesionalna i pažljiva, što prijevari daje dodatnu, dakako lažnu, kredibilitet.

Lažne platforme za trading: Ključna taktika je da žrtva dobije pristup "privatnoj platformi" gdje može "pratiti" svoj investicijski račun. Ta platforma je u potpunosti lažna – brojevi koji se prikazuju su potpuno fiktivni. Grafikon je programiran da ide gornjom linijom, pokazujući "dobit" iako u stvarnosti ništa od toga nije točno ni stvarno.

No, što se događa kada žrtva u nekom trenutku pokuša povući svoj novac? Onda stvari postanu komplicirane, jer se suočava s različitim izgovorima zašto to nije moguće: "Račun je zamrznut iz sigurnosnih razloga jer je detektirana neuobičajena aktivnost" odnosno hakerski napad, "Trebate uložiti dodatnih 10% kao 'depozit za povlačenje'", "Sredstva trebaju biti u računu još 30 dana prije nego što mogu biti povučena", "Trebate platiti poreze" – često od nekoliko tisuća eura – prije nego što sredstva budu dostupna ili ih se uvjerava da trebaju pričekati "bolje tržišne uvjete da bi povlačenje bilo optimalno". Ubrzo dolazi trenutak u kojem žrtva shvaća da je prevarena i pokradena, a lažni brokeri misteriozno joj se prestaju javljati.

Tada preostaje tek prijava policiji i suočavanje s bolnom činjenicom da je novac nepovratno nestao i da počinitelji vjerojatno nikad neće biti identificirani niti kažnjeni.

Ovaj novinarski projekt ostvaren je u okviru financijske potpore novinarskim radovima Agencije za elektroničke medije u okviru projekta poticanja novinarske izvrsnosti i slobodan je za korištenje i prenošenje.



Petar Radanović

Otkrijte više

[Proizvodnost](#)

[produktivnost](#)