



## Pošast online prijevara: Kako izgubiti novac na internetu? (Četvrti dio): Može li se online prijevarama stati na kraj i koja je uloga policije?

Autor **Petar Radanović** - Wednesday, October 22, 2025, 13:22

Otkrijte više

⚡ produktivnost

⚡ Proizvodnost

Kad je 81-godišnjak iz Labina prijavio da je prevaren za više od 100.000 eura od strane "brokera" koji mu je obećavao zaradu na zlatu i nafti, ili kada je žena iz Umaga ostala bez 85.000 eura nakon intenzivne "investicijske komunikacije" s lažnim brokerom, hrvatska policija je bila pozivana da postupi. No, što se zapravo može učiniti kada se kazneno djelo počinji preko interneta, sa kriminalcem koji se nalazi u drugoj državi, s računima koji se mogu otvoriti u trećoj, a novac prebaciti u četvrtoj državi? Stvarnost je da hrvatska policija gotovo redovito obavještuje javnost o novim slučajevima prijevara, ali je broj razriješenih slučajeva zastrašujuće mali. Prema dostupnim podacima iz istarske policijske uprave, od ukupno 238 internetskih i računalnih prijevara u 2024. godini, razriješeno je samo 11% internetskih prijevara i 32% računalnih prijevara. To znači da 89% internetskih prijevara ostaje nerazriješeno. Iako se ovi brojevi mogu čini obeshrabrujućima, oni pokazuju fundamentalni problem u borbi protiv digitalnog kriminala: internetske prijevare su, po svojoj prirodi, teže za istražiti od tradicionalnih kaznenih djela.

Kako funkcionira istražni proces kada se bavi internetskom prijevarom? Prvo, žrtva mora prijaviti kazneno djelo lokalnoj policiji. Tada policija počinje prikupljati dokaze – e-mail poruke, SMS-eve, snimke razgovora, bankovne transakcije. U sljedećem koraku, policija pokušava identificirati počinitelja, što uključuje praćenje IP adrese, podatke o računu ili aplikaciji preko koje se dogodila komunikacija. Međutim, kada je počinitelj u drugoj zemlji ili koristi anonimne servere i kriptovalute, problem postaje gotovo nerješiv bez međunarodne suradnje.

Ovdje se pojavljuje prvi ključni izazov: Hrvatska policija jednostavno ne može sve izvršiti sama, i to ne zato što ne želi ili ne zna, nego jednostavno ne može. Naime, istraživanje izvan granica

Hrvatske logično zahtijeva suradnju s policijama drugih zemalja – bilo da se radi o SAD-u, Nigeriji, Indiji ili bilo kojoj drugoj zemlji u kojoj se nalaze akteri prijevare. Međunarodna policijska suradnja postoji kroz Interpol i Europol, ali je proces spor, kompliciran i dugotrajan. Zahtjev za pravnom pomoći od druge države može potrajati mjesecima ili čak godinama, a prevaranti se često tijekom tog vremena prebacuju u druge države ili se gube tragovi gdje su pokradeni novci prebačeni.

Otkrijte više

🔗 **Proizvodnost**

🔗 **produktivnost**

Financijska istraga je kompleksna jer se novac često prebacuje kroz povezane lance. Prevaranti prvo prikupe novac od jedne žrtve, a zatim ga prebace drugoj osobi – često korisniku računa koji bez znanja postaje "financijska mula". Ta osoba može biti i sama žrtva prijevare ili osoba koja nije svjesna da se njezin račun koristi za pranje novca. Kad se novac jednom prebaci preko granice, posebno u kriptovalute, ili kad se transferira na nekoliko različitih računa u nekoliko različitih država, gotovo ga je nemoguće ga pratiti, a još teže vratiti.

Što to znači za policijsku istragu? To znači da policija može identificirati kojoj osobi pripada račun na kojeg se prebacivalo novac ali ne može vratiti novac jer je dugi lanac između tog računa i originalnog počinitelja. Osim toga, ako je novac prebačen u kriptovalute kao Bitcoin ili Ethereum, čak i kad bi policija pronašla koji račun drži te kriptovalute, nije jasan pravni okvir kako ih konfiscirati i vratiti žrtvi.

Kriminalistički timovi koji se bave internetskim prijevarama u Hrvatskoj postoje, ali teško je očekivati da mogu riješiti sve ili veći dio tako kompleksnih slučajeva kao što su online prijevare. Ministarstvo unutarnjih poslova ima odjel za cyber kriminal, ali njezini resursi su ograničeni. Hrvatska policija, na žalost, nema ni dovoljnog broja kadrova, ni dovoljno specijaliziranog znanja, ni adekvatnih financijskih sredstava da bi efikasno pratila sve oblike internetskog kriminala. To je problem koji nije samo hrvatski – gotovo sve svjetske policije se suočavaju s tim, ali je u manjim zemljama kao Hrvatska resursna problematika mnogo veća.

Koju ulogu ima HANFA – Hrvatska agencija za nadzor financijskih usluga? HANFA je regulatorno tijelo zaduženo za nadzor financijskih usluga u Hrvatskoj. Kada se brokeri pojave na internetu i nude usluge koje nisu regulirane, HANFA može pokrenuti istrage, ali samo ako su osobe ili tvrtke registrirane u Hrvatskoj. Kad se brokeri nalaze u inozemstvu, HANFA nema jurisdikciju nad njima. Zapravo, jedino što može učiniti jest objaviti upozorenja na svojoj web stranici, što redovito čini, ali to nisu obvezne mjere – žrtva još uvijek može biti prevarena iako je institucija objavila upozorenje.

Otkrijte više

🔗 **Proizvodnost**

🔗 **produktivnost**

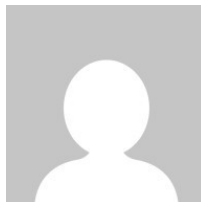
Suradnja između hrvatskih policijskih uprava bolja je nego prije, ali je i dalje fragmentirana. Različite policijske uprave imaju različite pristupe, različite nivoe edukacije i različite nivoe uspjeha u razrješavanju slučajeva. Također, nema jedinstvene baze podataka o internetskim prijevarama što bi mogla pomoći da se otkriju modus operandi ili ako se jedan počinitelj pretvara kao više osoba u istoj vrsti prijevare.

Međunarodna suradnja je ključna, ali je neefikasna. Europol, međunarodna policijska organizacija, ima jedinice posvećene cyber kriminalu, ali njihovi kapaciteti su ograničeni s obzirom na ogromnu količinu digitalnog kriminala koji se svakodnevno počinjava u cijeloj Europskoj uniji. Kada Hrvatska policija inicira suradnju s Europolom na nekom slučaju, često je potrebno čekati mjesecima za odgovor. Isto tako, ako poželi suradnju s policijom u državi gdje se počinitelj nalazi, potrebni su službeni diplomatski kanali, što dodatno usporava proces.

Očigledna rješenja su veće financiranje odjela za cyber kriminal, bolja edukacija kadrova, jača međunarodna suradnja i moderniji tehnološki alati. Međutim, sve to kaska i potrebne su godine da se donesu političke odluke i potom provedu u konkretna poboljšanja, a za to vrijeme kriminalci su iz dana u dan sve brži i sve kreativniji. Umjesto toga, što se može učiniti? Kao prvo, preventiva je mnogo jeftinija od istraga. Umjesto da se policija bavi s tisućama prevarenih žrtava, edukacija građana trebala bi biti prioritet, ne samo policije nego i drugih nadležnih tijela i institucija. Drugo, financijske institucije trebale bi biti angažiranije u sprječavanju internetskih prijevvara. Banke imaju alate za detektiranje neuobičajenih transfera i mogu zaustaviti novac prije nego što napusti zemlju, a o educiranju građana odnosno svojih klijenata da i ne govorimo. Treće, društvene mreže trebale bi biti dužne provjeravati oglase koji nude investicije i biti manje tolerantne prema sumnjivim profilima koji šalju privatne poruke novim korisnicima s ponudama investicija.

Zaključno, nije da policija "ništa ne radi" – policija radi što može s resursima koje ima. Problem je što resursi nisu adekvatni za opseg problema. Dok broj internetskih prijevvara eksponencijalno raste, broj razriješenih slučajeva ostaje relativno malen. To je realnost digitalnog svijeta i suština problema s kojim se hrvatsko pravosuđe, kao i pravosuđe brojnih država svijeta, suočava: tehnologija koja omogućava zločin ide puno brže od tehnologije i kapaciteta koje imamo da je sprječimo.

***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**

---