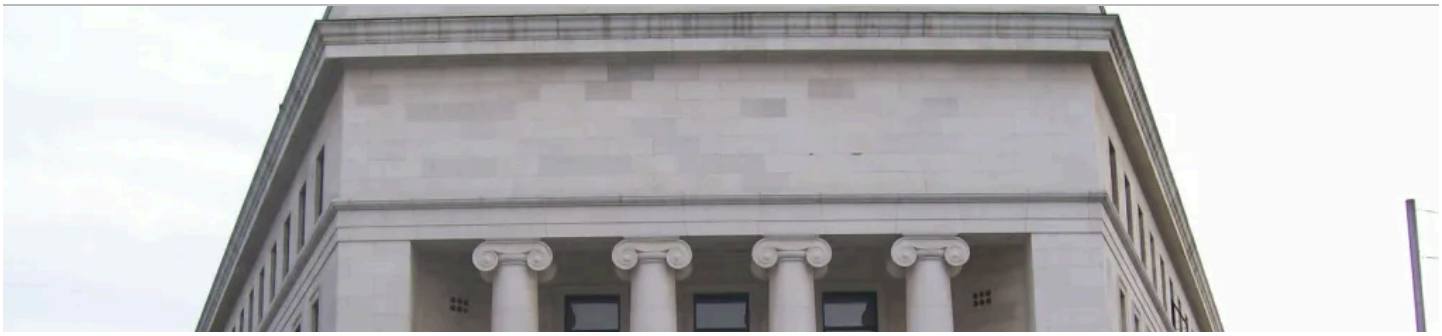

Pošast online prijevara: Kako izgubiti novac na internetu? (Peti dio): Kako se zaštititi i tko je dužan provoditi zaštitu?

Autor **Petar Radanović** - Thursday, October 30, 2025, 16:24

Otkrijte više produktivnost Proizvodnost

Kad je jedan 68-godišnjak iz Dalmacije prijavio da mu je s bankovnog računa skinuto oko 200.000 eura, nakon što je dao pristup svom mobitelu lažnom "brokeru" za kriptovalute, postao je žrtva ne samo prijevare, već i neispunjenih institucionalnih obveza zaštite. Pitanje koje se postavlja nije samo kako je moguće da se to dogodilo, već tko je uopće dužan štititi građane od takvih prijevara? Odgovor je – trebali bi biti svi. No, stvarnost je dakako složenija.

Prema nekim stavovima, najveću odgovornost trebale bi nositi financijske institucije – banke i ostale organizacije koje čuvaju novac i podatke. Banke, naime, imaju alate za detektiranje neuobičajenih transakcija: kad se s računa od nekog umirovljenika naglo prebace deseci tisuća eura na inozemne račune ili u kriptovalute, to je upozorenje koje bi banka prva trebala detektirati. Interna bankovna pravila o poznavanju svog klijenta trebala bi biti takva da se takve transakcije zaustave ili da zatraže dodatnu autorizaciju. Međutim, prema izvorima iz nekoliko banaka smo komunicirali, mnogo tog "zaustavljanja" nikada se ne dogodi. Banke se opravdavaju da su ograničene time što mogu učiniti ako je osoba autorizirala transakciju na svojem vlastitom računu. Međutim, to je vrlo licemjeran stav bankara – ako je starija osoba bila izmanipulirana, što je upravo slučaj u većini tih prijevara, tada nije bila u mogućnosti dati "autorizirani pristanak", već je upravo bila pod utjecajem prijevare.

Što zapravo mogu učiniti banke? U prvom redu, trebale bi imati bolji monitoring za korisnike koji su potencijalno ugroženi odnosno ozbiljno rizični – primjerice starije osobe koje su prethodno bile tražile financijsku pomoć ili čiji su računi naglo prijavili neuobičajene aktivnosti. Drugo, trebale bi imati stroži sustav provjere prije nego što dozvole velike transfere u kriptovalute ili na inozemne

račune koji prethodno nisu bili na listi korisnikovih uobičajenih transfera. Treće, banke bi trebale educirati svoje zaposlenike da mogu prepoznati znakove prijevare kada starija osoba dođe u banku i traži informacije o sumnjivim transferima.

Operatori mobilnih usluga, kao što su Hrvatski Telekom, Telemach i A1 također bi trebali biti dio sprječavanja online kriminala. Te kompanije znaju tko se nalazi u Hrvatskoj, a tko je u inozemstvu i mogu vrlo jednostavno zaustaviti SMS-eve koji dolaze iz inozemstva s pozivnim brojevima koji izgledaju kao domaći. To je relativno jednostavna tehnička mjera, ali dosad nije bila u širokoj primjeni. Ako bi se ta mjera implementirala, velik broj "direktorskih prijevara" ili SMS-eva koji se pretvaraju da dolaze od članova obitelji ne bi nikad stigao do hrvatskih građana.

Društvene mreže – Facebook, Instagram, Viber i drugi – trebale bi biti daleko aktivnije u detektiranju i uklanjanju profila koji se koriste za prijevaru. Trenutačno te platforme imaju neka pravila protiv prijevara, ali oni su, kako se to kaže, često mrtvo slovo na papiru. Kad se na Facebooku pojavi profil čija je profilna slika ukradena fotografija nekog drugog korisnika, i još se taj novi profil koristi za slanje privatnih poruka novim korisnicima s ponudama investicija, to bi trebalo biti detektirano automatski kroz AI, blokirano i uklonjeno. Međutim, za društvene mreže to ne predstavlja prioritet jer ne narušava njihovu primarnu misiju – prikazivanje oglasa. Zapravo, njihovi algoritmi često pojačavaju oglase s investicijskim ponudama jer znaju da se oni često klikaju, što društvenim mrežama donosi zaradu.

I regulatori kao HANFA trebali bi biti puno aktivniji. Trenutačno HANFA objavljuje upozorenja na svojoj web stranici, što je korisno, ali nije dovoljno. HANFA bi trebala imati ovlaštenja da se obrati financijskim institucijama i naloži im da dodatno nadziru račune koji pokazuju znakove prijevare. Također, trebala bi biti u suradnji s policijom – kada HANFA detektira nove vrste lažnih brokera koji operiraju, trebala bi odmah obavijestiti policiju. Prema našim saznanjima, ona to i čini, ali samo povremeno.

Ministarstvo unutarnjih poslova je razvilo projekt "Web Heroj" koji ima za cilj edukaciju građana o online sigurnosti i prijevarama. To je dobar početak, ali je projekt zasad premalo promoviran, gotovo da se za nj ni ne zna. Većina hrvatskih građana nije čak čula za Web Heroj, pogotovo vrlo ranjiva skupina – stariji građani. Projekt je vrijedan i trebao bi biti proširen, dostupan u lokalnim zajednicama i morao bi sadržavati vizualne materijale, letke, brošure i jednostavne vodiče za starije osobe.

Što sami građani mogu i trebali bi učiniti? To je dio odgovornosti koji često bude zanemarivan, jer, budimo iskreni, često je jednostavnije za sve okriviti institucije. Međutim, sami građani trebali bi preuzeti neophodni dio obrane. Prvo, trebali bi biti sumnjičavi i postavljati pitanja – ako netko nudi laganu zaradu, to je gotovo sigurno prijevara. Drugo, trebali bi razgovarati sa svojom bankom o tome kako se zaštititi – što je sve što trebam znati ako netko pokusa pristupiti mom računu. Treće, trebali bi biti svjesni da nikada i nikome ne trebaju dati pristup svojem mobitelu.

Obitelj je često prva crta obrane. Ako imate starije članove u obitelji, trebali bi biti svjesni da su oni u riziku. Trebali biste redovito razgovarati s njima, objasniti im što su online prijevare i kako se one manifestiraju. Ako primijetite da oni naglo počnu primati nove pozive ili poruke od "brokera", to je upozorenje. Ako se iznenada zainteresiraju za vijesti iz financija ili počnu govoriti o "brzoj zaradi" ili investiranju, to su jasni znakovi da trebate intervenirati. To može biti neugodan razgovor, ali je potreban.

Tehnološka rješenja postoje, ali trebate ih aktivirati. Većina banaka sada nudi "two-factor authentication" – sustav gdje trebate unijeti kod koji vam se pošalje na mobitel kada se prijavljujete u svoj račun ili želite izvršiti transakciju. To čini gotovo nemoguće da prevaranti pristupe računu čak i ako znaju vašu lozinku. Takvu zaštitu trebali biste aktivirati to na svim svojim računima – online bankingu, e-mailovima ili društvenim mrežama. Nadalje, trebali biste koristiti kompliciranije lozinke koje sadrže brojeve, veliko i malo slova i posebne znakove ili biste trebali početi koristiti "password manager" aplikacije, koje kreiraju sigurne lozinke te ih ujedno i bilježi tako da ne trebate memorirati stotine različitih. Sve to može zvučati kao previše, ali to je realnost digitalnog svijeta.

Edukacija, zaštita i odgovornost trebale bi biti podijeljene između svih aktera – institucija, regulatora, policije, obitelji i samih građana. Ako jedan od tih aktera posustane, cijela struktura pada u vodu. Trenutačno u Hrvatskoj struktura obrade pada na većim crtama obrane jer institucije nedostatno rade – no to ne smije biti razlog da pojedinci ostanu pasivni i ne štite se kako mogu. Znanje je zaista moć, a u slučaju prijevara, znanje je najbolja obrana.

Otkrijte više produktivnost Proizvodnost

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