



Finansirano sredstvima
Evropske unije

ZaštoNe?

Online prevare **u Bosni i Hercegovini:** Analiza i preporuke za unapređenje odgovora

Autori/ce:

Maida Ćulahović, Lamija Haračić, Marija Ćosić,
Amar Karađuz, Emir Zulejhić i Darko Brkan

Udruženje građana i građanki "Zašto ne"

Online prevare kao rastući društveni i sigurnosni problem

Online prevare danas predstavljaju jedan od najraširenijih oblika digitalnih manipulacija i dezinformacija kojem su izloženi građani i građanke Bosne i Hercegovine. Razvoj digitalnih tehnologija, rast internet-trgovine i gotovo univerzalno rasprostranjena upotreba društvenih mreža otvorili su brojne mogućnosti za komunikaciju, poslovanje i pristup informacijama. Istovremeno, isti digitalni prostor postao je pogodno okruženje za organizovane mreže prevara koje koriste povjerenje korisnika/ca, brzinu širenja sadržaja, nisku razinu medijske i digitalne pismenosti građana/ki i poslovne modele velikih *online* platformi kako bi ostvarile finansijsku korist.

Online prevare više nisu izolovani incidenti ni pojedinačni pokušaji obmane. Riječ je o organizovanim, često internacionalnim kampanjama koje koriste sofisticirane metode digitalnog marketinga, psihološke tehnike uvjeravanja, zloupotrebu identiteta kompanija, institucija i javnih ličnosti, kao i mogućnosti koje pružaju algoritmi društvenih mreža. Njihov cilj nije uvijek samo ostvarivanje jednokratne finansijske koristi već često i prikupljanje ličnih i finansijskih podataka koji se mogu dalje zloupotrebjavati.

Posljednjih godina ovakve prevare postaju sve uvjerljivije zahvaljujući razvoju tehnologija poput generativne vještačke inteligencije (Artificial Intelligence – AI), koje omogućavaju kreiranje lažnih slika, video i audio snimaka, dodatno otežavajući građanima/kama razlikovanje autentičnih od manipulativnih sadržaja.

Od širenja ovakvih prevara korist nemaju samo oni koji ih pokreću, već i velike *online* platforme. Njihovi algoritmi imaju benefita od interakcija koje ovakva objave potiču, ali one imaju i direktnu finansijsku korist. Prema istraživanju Reutersa, kompanija Meta je krajem 2024. godine "interno projicirala da će zaraditi oko 10% svog ukupnog godišnjeg prihoda - ili 16 milijardi dolara - od oglašavanja prevara i zabranjene robe".

"U prosjeku, navodi se u jednom dokumentu iz decembra 2024, kompanija je procijenila da korisnicima/ama svojih platformi svaki dan prikazuje 15 milijardi prevarnih oglasa 'višeg rizika' - onih koji pokazuju jasne znakove prevare. Meta zaradi oko sedam milijardi dolara godišnjeg prihoda od ove kategorije prevarnih oglasa svake godine, navodi se u drugom dokumentu s kraja 2024", ističe Reuters.

Čak iako veliki dio ovakvih prevara nikada ne bude prijavljen, dostupni podaci pokazuju da su njihove razmjere ogromne. Rezultati globalnog istraživanja Global State of Scams za 2025. godinu, koji je objavila neprofitna organizacija Global Anti-Scam Alliance, pokazuju da su *online* prevare postale svakodnevna pojava u digitalnom okruženju. Čak 57% odraslih osoba izjavilo je da je bilo meta neke vrste prevare tokom prethodne godine, dok je 23% ispitanika/ca izgubilo novac, a ukupni globalni finansijski gubici procjenjuju se na oko 442 milijarde američkih dolara godišnje.

Prema istraživanjima kompanije posvećene digitalnim slobodama Gen, procjenjuje se da se širom svijeta svakog trenutka događa gotovo 174 pokušaja prevare u sekundi, dok je svaka treća odrasla osoba bila meta neke vrste prevare tokom 2025. godine. Podaci pokazuju da je jedna od četiri osobe koje su bile izložene pokušaju prevare na kraju postala žrtva, a 74% prevarenih pretrpjelo je i finansijsku štetu, uz prosječan gubitak od 3.858 američkih dolara po žrtvi.

Finansijske posljedice ovih prevara su ogromne. Samo su u Sjedinjenim Američkim Državama potrošači tokom 2024. godine prijavili više od 12,5 milijardi dolara gubitaka zbog prevara, dok je FBI procijenio da su ukupni gubici od internet-kriminala u 2025. godini dostigli gotovo 21 milijardu dolara, pri čemu značajan dio čine upravo različiti oblici *online* prevara. Razmjere problema potvrđuju i podaci iz Ujedinjenog Kraljevstva, gdje je tokom 2025. godine zabilježeno više od četiri miliona slučajeva prevara u kojima su građani/ke izgubili/e novac, uz ukupne gubitke od gotovo 1,3 milijarde funti.

Višegodišnji rad platforme za provjeru činjenica Raskrinkavanje.ba, kao i drugih platformi iz država Zapadnog Balkana, pokazuje da se građani i građanke ovog regiona svakodnevno susreću s različitim oblicima *online* prevara. Tokom proteklih godina analizirane su stotine slučajeva manipulativnih oglasa, lažnih internet-trgovina, nagradnih igara i humanitarnih akcija, zloupotreba identiteta poznatih kompanija, medija i javnih ličnosti, kao i finansijskih prevara povezanih s navodnim ulaganjima ili brзом zaradom.

Među najčešćim prevarama izdvajaju se lažne nagradne igre, rasprodaje i poklanjanja koja koriste identitete poznatih trgovačkih lanaca i brendova. Korisnicima/ama se obećavaju vrijedne nagrade ili proizvodi po simboličnim cijenama, a zatim ih se navodi da ostave broj telefona, podatke s bankovne kartice ili druge lične podatke na *web* stranicama koje uvjerljivo imitiraju izgled stvarnih kompanija. Nakon toga, umjesto nagrade, dobijaju uvećan telefonski račun, nepredviđen finansijski trošak ili druge probleme povezane s krađom identiteta.

Posebno su zastupljene i prevare koje promovišu neprovjerene proizvode predstavljene kao lijekove ili medicinske preparate. Takvi oglasi koriste lažne medijske članke, izmišljene intervjuje te zloupotrijebljene identitete doktora i doktorica, naučnika/ca i javnih ličnosti, poput poznatih pjevača/ica i glumaca/ica, kako bi stvorili privid kredibilne preporuke. U posljednje vrijeme sve se češće koriste i *deepfake* videozapisi generisani pomoću vještačke inteligencije.

Značajan dio prevara odnosi se i na lažne investicione platforme, trgovinu kriptovalutama i različite piramidalne šeme koje građanima/kama obećavaju sigurnu i brzu zaradu. Ovakvi modeli često funkcionišu putem organizovanih mreža, pri čemu se korisnici/e podstiču na sve veće uplate dok se čitav sistem ne uruši, a građani/ke ne ostanu bez svog novca.

Posljedice za građane/ke, kompanije i društvo

Iako je finansijska šteta najvidljivija posljedica *online* prevara, postoje i one mnogo šire.

Građani i građanke ostaju bez novca, kompromituju svoje bankovne i lične podatke, postaju žrtve krađe identiteta ili neželjenih pretplata, a nerijetko se suočavaju i s dugotrajnim administrativnim i pravnim problemima. Mnogi slučajevi ostaju neprijavljeni zbog osjećaja srama ili uvjerenja da institucije neće moći pomoći.

Istovremeno, značajnu štetu trpe i kompanije, mediji, zdravstvene ustanove i javne ličnosti čiji se identitet zloupotrebljava radi povećanja privida vjerodostojnosti prevara. Takve zloupotrebe narušavaju reputaciju, smanjuju povjerenje građana/ki i zahtijevaju dodatna ulaganja u komunikaciju, sigurnost i zaštitu ličnog i kompanijskog brenda.

Online prevare tako predstavljaju problem koji prevazilazi pojedinačne žrtve i postaje pitanje sigurnosti digitalnog tržišta, zaštite potrošača i povjerenja u digitalno okruženje.

Pravni okvir u Bosni i Hercegovini

Bosna i Hercegovina trenutno nema jedinstven zakon koji sistemski reguliše *online* prevare niti posebne propise koji uređuju odgovornost velikih *online* platformi za sadržaj i oglase koje distribuiraju.

Zaštita građana/ki zasniva se na kombinaciji propisa iz oblasti zaštite potrošača, krivičnog prava, elektronske trgovine i zaštite ličnih podataka. Zakon o zaštiti potrošača zabranjuje obmanjujuće poslovne prakse i manipulativno oglašavanje, dok krivični zakoni omogućavaju procesuiranje različitih oblika prevara i računarskog kriminala. Zakon o zaštiti ličnih podataka u BiH dodatno unapređuje zaštitu građana/ki u slučajevima nezakonite obrade i zloupotrebe njihovih podataka.

Međutim, u realnosti postoje brojni izazovi. Nadležnosti su podijeljene između različitih nivoa vlasti, identifikacija organizatora prevara često je otežana zbog njihovog međunarodnog karaktera, a institucije se suočavaju s ograničenim tehničkim i kadrovskim kapacitetima za provođenje digitalnih istraga.

Uloga i odgovornost online platformi

Algoritmi *online* platformi omogućavaju brzo širenje sadržaja, dok sistemi digitalnog oglašavanja prevarantima omogućavaju da za relativno male iznose dosegnu stotine hiljada korisnika/ca.

Reakcije platformi na prijave prevarnog sadržaja često nisu dovoljno brze i efikasne. Istovremeno, platforme ostvaruju direktne prihode od dijela oglasa kojima se promovišu prevare, što dodatno otvara pitanje njihove odgovornosti.

Evropska unija posljednjih godina razvija regulatorni okvir koji nastoji odgovoriti upravo na ove izazove. Akt o digitalnim uslugama (Digital Services Act – DSA) uvodi obavezu uspostavljanja efikasnih mehanizama za prijavljivanje nezakonitog sadržaja, veću transparentnost digitalnog oglašavanja, procjenu sistemskih rizika i dodatne obaveze za veoma velike *online* platforme. Iako Bosna i Hercegovina još uvijek nije dio EU te nije obuhvaćena primjenom ovog propisa, evropski pristup predstavlja važan primjer mogućeg razvoja domaćeg regulatornog okvira.

Potreba za koordinisanim odgovorom

Online prevare nije moguće efikasno suzbijati djelovanjem samo jednog aktera. Njihova složenost zahtijeva koordinisan odgovor institucija, poslovnog sektora, online platformi, organizacija civilnog društva, akademske zajednice i samih građana/ki.

Institucije trebaju razvijati efikasnije mehanizme zaštite građana/ki i procesuiranja organizatora prevara. Biznisi trebaju aktivnije štititi svoje brendove i sarađivati s institucijama i *fact-checking* platformama. *Online* platforme moraju preuzeti veću odgovornost za sadržaj čiju distribuciju omogućavaju i od kog zarađuju. Organizacije civilnog društva imaju važnu ulogu u podizanju svijesti građana/ki i njihovom osnaživanju, razotkrivanju novih obrazaca prevara i zagovaranju unapređenja javnih politika.

Preporuke predstavljene u ovoj publikaciji proizlaze iz višegodišnjeg istraživačkog rada Udruženja građana i građanki "Zašto ne" i platforme za provjeru činjenica Raskrinkavanje.ba, analize postojećeg pravnog okvira u Bosni i Hercegovini, iskustava građana/ki koji/e su bili/e žrtve *online* prevara te evropskih regulatornih rješenja. Njihov je cilj ponuditi konkretne i primjenjive mjere koje mogu doprinijeti efikasnijem sprečavanju *online* prevara, jačanju zaštite građana i građanki i povećanju odgovornosti svih aktera koji učestvuju u oblikovanju digitalnog okruženja.

Preporuke

Biznisi

- **Uspostaviti sistem aktivnog praćenja zloupotreba brenda**

Efikasna zaštita brendova zahtijeva proaktivan pristup, a ne isključivo reakciju na učinjenu štetu. Biznisi trebaju uspostaviti sistem redovnog praćenja društvenih mreža i *online* sadržaja radi otkrivanja stranica, objava i oglasa u kojima se neovlašteno koristi njihov identitet. Pravovremenim detektovanjem lažnih profila, stranica i objava, kompanije mogu spriječiti širu distribuciju prevara prije nego što one nanesu ozbiljnu reputacijsku štetu.

- **Uvesti jasnu politiku komunikacije s kupcima ili korisnicima/ama**

Kompanije moraju uvesti i strogo primjenjivati jasnu politiku komunikacije s kupcima i/ili korisnicima. Neophodno je transparentno i jasno komunicirati gdje objavljuju svoje stvarne nagradne igre i promocije te nedvosmisleno naglasiti publici da nikada neće tražiti bankovne kartice, slike ličnih dokumenata i slično. Ovakva praksa direktno edukuje građane/ke i ostavlja znatno manje prostora za manipulaciju.

- **Brzo reagovati na zloupotrebe identiteta**

Vrijeme reakcije predstavlja jedan od najvažnijih faktora u suzbijanju širenja *online* prevara i drugog lažnog sadržaja. Kada otkriju zloupotrebu, biznisi moraju brzo prijaviti slučaj relevantnim institucijama i drugim akterima, poput platformi za provjeru činjenica. Istovremeno, od izuzetne je važnosti odmah upozoriti i građane/ke na postojanje lažnih objava, koje ugrožavaju i njihovu i sigurnost brenda.

- **Sarađivati s *fact-checking* platformama**

Sinergija između privatnog sektora i platformi za provjeru činjenica od suštinske je važnosti u borbi protiv prevara i zloupotreba identiteta. Biznisi bi trebali uspostaviti direktnu saradnju s organizacijama koje rade na razotkrivanju *online* prevara i manipulacija. Ovakav sistemski pristup omogućava da se lažni sadržaj znatno brže označi te da se na njega upozori mnogo veći broj ljudi u digitalnom prostoru.

- **Aktivno prijavljivati zloupotrebe nadležnim institucijama i platformama**

Oslanjanje isključivo na interno obavješćavanje javnosti nije dovoljno; kompanije moraju

uspostaviti interne procedure za brzo prijavljivanje lažnih oglasa, profila i stranica, najprije *online* platformama na kojima su takvi sadržaji objavljeni. Nadalje, izuzetno je važno ove slučajeve prijavljivati i nadležnim policijskim organima, odjelima za visokotehnološki kriminal i drugim nadležnim institucijama kako bi se pokrenuli odgovarajući postupci.

- **Evidentirati i dokumentovati slučajeve zloupotrebe brenda**

Ozbiljan pristup borbi protiv digitalnih manipulacija zahtijeva vođenje detaljne arhive. Kompanije moraju evidentirati i dokumentovati slučajeve zloupotrebe brendova. U svrhu olakšanja administrativnih i pravnih postupaka, kao i kasnijeg zagovaranja za unapređenje regulativa, preporučuje se vođenje interne evidencije prijavljenih prevara, koja uključuje linkove, digitalne arhive, slike ekrana, kao i svu komunikaciju s platformama i institucijama.

- **Uspostaviti saradnju i razmjenu informacija s drugim kompanijama**

Razvijati mehanizme saradnje putem privrednih komora, sektorskih udruženja ili neformalnih mreža radi razmjene informacija o novim obrascima prevara, zloupotrebama brendova i efikasnim načinima reagovanja.

- **Uključiti se u međunarodne inicijative za borbu protiv *online* prevara**

Uključivanje u međunarodne mreže i inicijative koje se bave sprečavanjem *online* prevara, razmjenom obavještajnih podataka i razvojem dobrih praksi, poput Global Anti-Scam Alliance (GASA) ili sličnih organizacija

Donosioci odluka i relevantne nadležne institucije

- **Unaprijediti koordinaciju između nadležnih institucija**

Efikasno suzbijanje *online* prevara zahtijeva jasnu podjelu nadležnosti i kontinuiranu saradnju svih institucija koje imaju ulogu u njihovom otkrivanju, sprečavanju i procesuiranju. Građani/ke često ne znaju kojoj instituciji trebaju prijaviti prevaru, dok se informacije o istim slučajevima ne razmjenjuju sistematski između policijskih agencija, tužilaštava, regulatornih tijela, institucija za zaštitu potrošača, Agencije za zaštitu ličnih podataka i drugih nadležnih organa.

Potrebno je uspostaviti formalne protokole saradnje kojima bi se definisale nadležnosti pojedinačnih institucija, procedure razmjene informacija i koordinisano postupanje u slučajevima *online* prevara. Takav sistem omogućio bi bržu identifikaciju organizovanih obrazaca prevara, efikasnije procesuiranje odgovornih osoba i pravovremeno informisanje građana/ki o novim prijetnjama.

- **Kontinuirano provoditi kampanje medijske i digitalne pismenosti i podsticati prijavljivanje prevara**

Prevenција predstavlja jedan od najvažnijih mehanizama zaštite građana/ki od *online* prevara. Zbog brzog razvoja digitalnih tehnologija i stalnog pojavljivanja novih oblika prevara, potrebno je kontinuirano provoditi javne kampanje kojima će se građani/ke upoznavati s najčešćim metodama obmane i načinima zaštite.

Takve kampanje trebale bi biti koordinisane između nadležnih institucija, obrazovnih ustanova, organizacija civilnog društva i medija te uključivati praktične informacije o tome kako prepoznati sumnjive oglase, lažne nagradne igre, *phishing* poruke i druge oblike prevara, kako provjeriti vjerodostojnost internet-stranica i *online* prodavača te kome i na koji način prijaviti sumnjive aktivnosti. Poseban fokus potrebno je usmjeriti na grupe koje su češće izložene riziku, poput starijih osoba i korisnika/ca s nižim nivoom digitalnih kompetencija.

- **Jačati međunarodnu saradnju s evropskim institucijama i mrežama za borbu protiv prekograničnih *online* prevara**

Online prevare sve češće imaju prekogranični karakter, pri čemu se počinioci, digitalna infrastruktura i finansijski tokovi često nalaze u različitim državama. Zbog toga je potrebno unaprijediti saradnju domaćih institucija s relevantnim evropskim tijelima i mrežama, posebno Europolom, ali i drugim nadležnim institucijama Evropske unije u oblastima koje se odnose na suzbijanje finansijskog kriminala i zaštitu finansijskih interesa EU.

Takva saradnja trebala bi uključivati razmjenu operativnih informacija, učešće u zajedničkim istragama i operacijama, razmjenu dobrih praksi, obuke za nadležne institucije te korištenje evropskih mehanizama za rano upozoravanje na nove obrasce *online* prevara. Istovremeno, potrebno je nastaviti usklađivanje domaćih kapaciteta i procedura s evropskim standardima kako bi Bosna i Hercegovina mogla efikasnije odgovoriti na sve sofisticiranije oblike prekograničnog digitalnog kriminala.

Tijela za zaštitu potrošača

Tijela za zaštitu potrošača imaju važnu ulogu u prevenciji *online* prevara putem informisanja građana/ki, pružanja podrške žrtvama i evidentiranja novih obrazaca prevarnih aktivnosti. Iako njihove nadležnosti ne obuhvataju krivično gonjenje počilaca, mogu značajno doprinijeti ranom otkrivanju prevara, pravovremenom upozoravanju javnosti i usmjeravanju građana/ki prema odgovarajućim institucijama.

- **Uspostaviti jedinstvenu tačku za prijavu *online* prevara**

Građani/ke se trenutno suočavaju s velikim brojem različitih institucija kojima bi potencijalno mogli prijaviti *online* prevanu, što često dovodi do odustajanja od prijavljivanja ili podnošenja prijave pogrešnim organima.

Potrebno je uspostaviti jedinstvenu kontakt-tačku putem koje bi građani/ke mogli/e prijaviti sve oblike internet-prevara bez potrebe da sami procjenjuju koja je institucija nadležna za konkretan

slučaj. Takva tačka trebala bi zaprimati prijave, pružati osnovne informacije o daljnjem postupanju te ih, prema jasno definisanim procedurama, prosljeđivati nadležnim institucijama. Time bi se pojednostavio postupak prijavljivanja, povećao broj prijavljenih slučajeva i omogućilo efikasnije prikupljanje podataka o rasprostranjenosti *online* prevara.

- **Redovno objavljivati upozorenja o aktuelnim prevarama**

Jedan od najefikasnijih načina prevencije jeste pravovremeno informisanje građana/ki o novim i aktuelnim oblicima *online* prevara. Nadležne institucije trebale bi redovno objavljivati upozorenja o najčešćim prevarama koje su identifikovane u Bosni i Hercegovini, kao i o novim metodama kojima se prevaranti služe.

Takva upozorenja trebala bi biti dostupna putem službenih internet-stranica, društvenih mreža, medija i drugih komunikacijskih kanala te sadržavati praktične informacije o tome kako prepoznati konkretnu prevaru, koje su njene karakteristične osobine i koje korake građani/ke trebaju poduzeti ukoliko su bili meta ili žrtva prevare.

- **Razviti sistem brzog upozoravanja između institucija, banaka, telekom-operatera, medija i drugih relevantnih aktera**

Online prevare često se šire velikom brzinom, zbog čega je pravovremena razmjena informacija ključna za njihovo suzbijanje. Potrebno je uspostaviti sistem brzog upozoravanja koji bi omogućio da informacije o novootkrivenim prevarama budu odmah dostupne svim relevantnim akterima.

Takav sistem trebao bi uključivati policijske agencije, tijela za zaštitu potrošača, banke, telekom-operatere, medije, organizacije civilnog društva i druge institucije koje mogu doprinijeti brzom informisanju javnosti. Nakon prijave ili identifikovanja nove prevare, učesnici sistema trebali bi, prema unaprijed definisanim procedurama, razmijeniti informacije i koordinisano upozoriti građane/ke putem svojih komunikacijskih kanala. Time bi se značajno smanjio broj potencijalnih žrtava i ograničilo širenje prevara.

- **Uspostaviti dostupnu bazu prijavljenih *online* prevara**

Građani/ke trenutno nemaju mogućnost da na jednom mjestu provjere da li je određena internet-stranica, profil na društvenim mrežama ili *online* trgovina već prijavljena kao potencijalna prevara.

Potrebno je uspostaviti javno dostupnu bazu prijavljenih *online* prevara koja bi sadržavala informacije o identifikovanim lažnim internet-stranicama, profilima, oglasima i drugim oblicima digitalnih prevara. Baza bi građanima/kama omogućila da prije *online* kupovine ili ostavljanja ličnih podataka provjere da li su slični slučajevi već evidentirani, dok bi nadležnim institucijama predstavljala vrijedan izvor podataka za identifikaciju obrazaca djelovanja i povezivanje pojedinačnih slučajeva u organizovane prevare.

Donosioci odluka

Donosioci odluka imaju ključnu ulogu u uspostavljanju zakonodavnog i institucionalnog okvira koji omogućava efikasniju prevenciju i suzbijanje *online* prevara. Unapređenjem propisa, usklađivanjem domaćeg zakonodavstva s evropskim standardima i osiguravanjem adekvatnih institucionalnih kapaciteta, moguće je stvoriti uslove za efikasniju zaštitu građana/ki i odgovornije djelovanje digitalnih platformi.

- **Uspostavljanje jasnijeg regulatornog okvira za odgovornost *online* platformi**

Bosna i Hercegovina treba što prije početi razvijati regulatorni okvir kojim bi se uspostavili efikasniji mehanizmi za sprečavanje i uklanjanje *online* prevara s digitalnih platformi te zaštitu korisnika/ca u okviru aktivnosti usmjerenih na usklađivanje s Aktom o digitalnim uslugama Evropske unije.

Takav regulatorni okvir trebao bi:

- uspostaviti zakonsku obavezu platformama da uvedu mehanizme za prijavljivanje nezakonitog sadržaja. Takvi bi mehanizmi korisnicima/ama omogućili da na jednostavan način prijave sadržaj i aktivnosti koje krše relevantne zakone Bosne i Hercegovine, što trenutno nije moguće uraditi. Osim toga, platforme bi trebale osigurati transparentnost u postupanju po prijavama, uz obavezu pružanja povratnih informacija korisnicima/ama o odlukama i poduzetim mjerama, kao i mogućnost žalbe.
- osigurati veću transparentnost digitalnog oglašavanja. Platformama je potrebno propisati obavezu jasnog označavanja plaćenih oglasa, tako da korisnicima/ama bude jasno ko je oglas platio, u čije se ime prikazuje i odakle oglašivač djeluje. Platforme bi također trebale osigurati da javno dostupni repozitoriji oglasa obuhvate i oglase koji se prikazuju korisnicima/ama u Bosni i Hercegovini te sadrže ključne informacije o oglašivaču, periodu prikazivanja oglasa, doseg i drugim relevantnim podacima. Takvi bi repozitoriji mogli značajno doprinijeti identifikovanju organizovanih kampanja *online* prevara, povezanih oglašivača i obrazaca njihovog djelovanja.

- **Uspostavljanje odgovarajućeg institucionalnog okvira i jačanje kapaciteta**

Usvajanje pravila za *online* platforme treba biti praćeno uspostavljanjem jasnog institucionalnog okvira za njihovo provođenje. Potrebno je jasno propisati nadležnosti pojedinačnih institucija u provođenju regulatornog okvira za *online* platforme, kao i njihovu međusobnu koordinaciju i mehanizme saradnje. Također je neophodno donijeti zakonska rješenja koja će nadležnim institucijama osigurati adekvatne ljudske i tehničke resurse te specifična stručna znanja i alate potrebne za efikasno provođenje njihovih nadležnosti u digitalnom okruženju.

- **Propisati efikasnije sankcije za organizatore *online* prevara**

Postojeći pravni okvir ne prepoznaje uvijek dovoljno jasno specifične oblike *online* prevara niti omogućava efikasno procesuiranje njihovih organizatora. Razvoj digitalnih tehnologija doveo je do novih modela kriminalnih aktivnosti, koje zahtijevaju odgovarajuća zakonska rješenja.

Potrebno je unaprijediti krivičnopravni okvir tako da jasno definiše različite oblike digitalnih prevara, uključujući prevare putem društvenih mreža, lažnih internet-trgovina, *phishing* kampanja, zloupotrebe identiteta i drugih oblika internet-kriminala. Istovremeno, potrebno je propisati odvraćajuće i proporcionalne sankcije koje će omogućiti efikasnije procesuiranje odgovornih osoba i doprinijeti smanjenju broja ovakvih krivičnih djela.

- **Pooštriti regulativu o informisanju korisnika/ca o uslugama naplate putem telekom-operatera**

Veliki broj *online* prevara zasniva se na naplati različitih digitalnih usluga putem računa mobilnih operatera, pri čemu korisnici/e često nisu dovoljno jasno informisani o tome da unosom broja telefona daju saglasnost za aktivaciju usluge koja se naplaćuje.

Potrebno je unaprijediti regulatorni okvir kojim bi telekom-operaterima i pružaocima usluga bila propisana obaveza jasnog, vidljivog i nedvosmislenog informisanja korisnika/ca prije aktivacije bilo koje usluge koja podrazumijeva naplatu putem telefonskog računa. Informacije o cijeni, učestalosti naplate, načinu otkazivanja usluge i identitetu pružaoca usluge trebale bi biti istaknute na jasan i lako uočljiv način, umjesto da budu skrivene u općim uslovima korištenja ili teško uočljivim napomenama. Takav pristup značajno bi smanjio broj slučajeva u kojima građani/ke nenamjerno aktiviraju usluge koje se kasnije naplaćuju putem njihovog mobilnog računa.

Istražni i pravosudni organi

Uloga istražnih i pravosudnih organa u otkrivanju i sankcionisanju organizatora *online* prevara u Bosni i Hercegovini od ključnog je značaja u slučajevima kada takve prevare prelaze iz sfere potrošačkih sporova u sferu krivičnopravne odgovornosti. Uzimajući u obzir postojeća ograničenja u pogledu ljudskih resursa i finansijskih kapaciteta, smatramo da su sljedeće preporuke realne i primjenjive u postojećem institucionalnom okviru.

- **Dugoročno jačanje kapaciteta za identifikaciju organizatora *online* prevara unutar policijskih agencija**

S obzirom na rast broja i složenosti *online* prevara, potrebno je dugoročno jačati kapacitete policijskih agencija za postupanje u ovim predmetima. To, prije svega, podrazumijeva povećanje broja službenika/ca koji/e se bave istragama *online* prevara. Osim toga, potrebno je kontinuirano ulagati u specijalizovanu obuku službenika/ca iz oblasti digitalnih istraga, *online* prevara i praćenja digitalnih finansijskih tokova, kao i osigurati adekvatne tehničke alate za prikupljanje i analizu elektronskih dokaza. Cilj je osigurati efikasniju identifikaciju organizatora prevara,

kvalitetnije dokumentovanje krivičnih djela i podnošenje utemeljenijih izvještaja o počinjenim krivičnim djelima nadležnim tužilaštvima.

- **Uvođenje kontakt-tački za prijavu *online* prevara u okviru nadležnih policijskih uprava Federacije BiH i RS**

Umjesto pokušaja da se sve *online* prevare tretiraju kao prioritet ravnopravan sa složenim *cyber* kriminalom, policijske agencije u BiH trebaju odrediti specijalizovane službenike/ce ili male timove koji bi se bavili isključivo prijavama *online* prevara, bilježenjem obrazaca i koordinacijom slučajeva. Cilj je omogućiti efikasnije istrage, a time i odgovor na izazov *online* prevara.

- **Unapređenje postupanja po prijavama**

Potrebno je razviti efikasniji sistem zaprimanja i obrade prijava *online* prevara, uključujući jedinstveni obrazac za prijavu kojim bi se od početka prikupljali ključni podaci i digitalni dokazi. Time bi policijske i pravosudne institucije lakše povezivale pojedinačne prijave protiv istih počinitelja, umjesto da ih posmatraju kao izolovane slučajeve male vrijednosti. Posebnu pažnju treba posvetiti organizovanim kampanjama koje mogu pogoditi veći broj građana/ki, što podrazumijeva razvijanje jasnih kriterija za prioritetno postupanje u takvim slučajevima.

- **Razvijanje specijalizovanih edukacija o *online* prevarama u okviru centara za edukaciju sudija i tužilaca FBiH i RS**

Potrebno je da centri za edukaciju sudija i tužilaca u Federaciji BiH i Republici Srpskoj, kao i advokatske komore, razviju specijalizovane programe edukacije posvećene *online* prevarama i izazovima njihovog procesuiranja. Edukacije ne bi trebale biti fokusirane na opšti pregled *cyber* kriminala, već na praktične aspekte postupanja u ovim predmetima, uključujući način dokazivanja postojanja lažnih *web* trgovina, povezivanja digitalnih tragova s počiniocima te korištenja podataka koje mogu dostaviti platforme, banke i telekom-operateri. Cilj je povećati efikasnost procesuiranja ovih slučajeva i izvršenje sankcija.

Platforme

Online platforme danas su jedan od glavnih kanala za širenje različitih oblika *online* prevara, zbog čega bi trebale imati proaktivniju ulogu u njihovom sprečavanju. U nedostatku regulatornog okvira koji bi im nametnuo odgovarajuće obaveze i uspostavio formalne mehanizme saradnje s nadležnim institucijama, primjena sljedećih preporuka već bi sad mogla doprinijeti boljoj zaštiti korisnika/ca i efikasnijem odgovoru na prevare:

- **Uspostavljanje funkcionalnih kanala komunikacije s nadležnim organima i institucijama u Bosni i Hercegovini**

Platforme bi trebale imenovati kontakt-tačke za saradnju s nadležnim policijskim i drugim institucijama u Bosni i Hercegovini kako bi se omogućila direktna razmjena informacija i

koordinacija u slučajevima *online* prevara, uključujući pružanje povratnih informacija koje trenutno u većini slučajeva izostaju. Takvi kanali trebali bi omogućiti nadležnim institucijama da platformama direktno dostavljaju prijave i zahtjeve za postupanje u vezi sa sadržajem koji krši zakone Bosne i Hercegovine ili nalogima koji učestvuju u prevarama, kao i da od platformi dobiju informacije potrebne za provođenje istraga.

- **Uspostavljanje kontinuirane saradnje s lokalnim pouzdanim partnerima i *fact-checking* organizacijama**

Lokalne organizacije koje se bave provjerom činjenica i monitoringom kršenja digitalnih prava građana/ki često prve identifikuju nove obrasce *online* prevara i koordinisane kampanje. Platforme bi trebale uspostaviti strukturiranu saradnju s ovim organizacijama, omogućiti im posebne kanale za prijavu sadržaja i prioritetno postupati po njihovim prijavama.

Također, platforme bi trebale redovno saradivati s lokalnim organizacijama civilnog društva, *fact-checking* organizacijama, akademskom zajednicom i drugim stručnjacima/kinjama radi boljeg prepoznavanja novih obrazaca *online* prevara i procjene rizika specifičnih za lokalni kontekst.

Takva saradnja može pomoći u utvrđivanju načina na koji sistemi preporučivanja i oglašavanja, alati zasnovani na vještačkoj inteligenciji ili monetizacija sadržaja doprinose širenju prevara te omogućiti da se politike i mjere zaštite platformi bolje prilagode lokalnom kontekstu.

- **Provođenje internih istraga i jačanje mjera za sprečavanje ponavljanja prevara**

U saradnji s lokalnim pouzdanim partnerima i drugim relevantnim akterima, platforme bi trebale razviti sistematičniji pristup internim istragama *online* prevara. Pored pojedinačnih objava, interne istrage trebale bi obuhvatiti i povezane naloge, oglašivače i koordinisane mreže koje stoje iza prevara.

Uklanjanje pojedinačnih objava ili naloga često nije dovoljno, jer se isti organizatori prevara vrlo brzo vraćaju koristeći nove profile ili oglašivačke naloge. Platforme bi stoga trebale unaprijediti provjere oglašivača i uvesti mjere koje otežavaju ponovno otvaranje naloga, pokretanje novih oglašivačkih kampanja ili ponovnu monetizaciju onima koji su prethodno uklonjeni zbog učešća u *online* prevarama. Pri tome bi se trebale oslanjati i na informacije i saradnju s lokalnim partnerima kako bi lakše prepoznale povezane naloge i koordinisane mreže.

- **Pravovremeno i transparentno postupanje po prijavama korisnika/ca**

Platforme bi trebale u najkraćem mogućem roku razmatrati prijave korisnika/ca koje se odnose na *online* prevare i druge sadržaje zabranjene njihovim standardima zajednice i internim pravilima te poduzimati odgovarajuće mjere.

Korisnicima/ama bi trebale pružiti jasne povratne informacije o ishodu prijave i poduzetim mjerama, kao i obrazloženje u slučajevima kada procijene da prijavljeni sadržaj ne krši njihova pravila. Transparentnije postupanje po prijavama i dosljednije provođenje internih pravila doprinijeli bi većem povjerenju korisnika/ca i podstakli prijavljivanje *online* prevara.

Civilno društvo

- **Provoditi kontinuirane kampanje za podizanje svijesti građana/ki o online prevarama**

Prevenција predstavlja jedan od najvažnijih mehanizama zaštite građana/ki od online prevara. Zbog brzog razvoja digitalnih tehnologija i stalnog pojavljivanja novih oblika manipulacija, organizacije civilnog društva moraju kontinuirano provoditi javne kampanje kojima će se javnost upoznavati s najčešćim metodama obmane i načinima zaštite. Ove su kampanje ključne za osnaživanje građana/ki i njihovo pravovremeno informisanje.

- **Jačati digitalnu i medijsku pismenost različitih ciljnih grupa**

Organizovane mreže prevara koriste nizak nivo medijske i digitalne pismenosti građana/ki kako bi ostvarile finansijsku korist. Kako bi se ovaj trend usporio, neophodno je jačati digitalnu i medijsku pismenost različitih ciljnih grupa, uključujući praktične informacije o tome kako prepoznati i verifikovati različite oblike prevara. Poseban fokus u ovim edukacijama potrebno je usmjeriti na ranjive grupe, poput starijih osoba i korisnika/ca s nižim nivoom digitalnih kompetencija, kao i na praktične savjete.

- **Fact-checking platforme trebaju sistematski pratiti i dokumentovati nove obrasce online prevara**

Lokalne organizacije koje se bave provjerom činjenica često prve identifikuju nove obrasce online prevara i koordinisane kampanje. Zbog toga je od suštinske važnosti da fact-checking platforme nastave sistematski pratiti i dokumentovati ove obrasce, jer njihov rad direktno doprinosi razotkrivanju i evidentiranju novih tehnika obmane te predstavlja bazu za daljnje djelovanje drugih aktera u digitalnom prostoru.

- **Razvijati saradnju civilnog društva s online platformama**

S obzirom na to da su online platforme glavni kanal za širenje različitih oblika online prevara, civilno društvo mora uspostaviti direktnu i strukturiranu saradnju s njima. Platforme bi trebale redovno sarađivati s lokalnim organizacijama i stručnjacima/kinjama radi boljeg prepoznavanja novih obrazaca prevara i procjene rizika specifičnih za lokalni kontekst te im omogućiti posebne kanale za brzu prijavu problematičnog sadržaja.

- **Unaprijediti saradnju civilnog društva s akademskom zajednicom i drugim akterima s ciljem rada na istraživanjima u publikaciji podataka i nalaza**

Složenost fenomena online prevara zahtijeva dubinski pristup koji prevazilazi dnevni monitoring. Zbog toga je potrebno unaprijediti saradnju civilnog društva s akademskom zajednicom i drugim akterima kako bi se provodila zajednička istraživanja. Publikacija naučno utemeljenih podataka i nalaza ključna je za razumijevanje sofisticiranih tehnika koje prevaranti koriste te za kvalitetno kreiranje budućih edukativnih i zagovaračkih aktivnosti.

- **U saradnji sa svim navedenim akterima, razviti mehanizam i kreirati kanale komunikacije za brzu detekciju, obavješćavanje i reakciju na slučajeve online prevara**

S obzirom na to da se online prevare često šire velikom brzinom, pravovremena razmjena informacija presudna je za njihovo suzbijanje. Neophodno je uspostaviti sistem brzog upozoravanja i kreirati kanale komunikacije koji bi omogućili da informacije o novootkrivenim prevarama budu odmah dostupne svim relevantnim akterima. Ovakvim koordinisanim mehanizmom, biznisi mogu brzo upozoriti građane/ke putem svojih kanala, fact-checking organizacije mogu označiti sadržaj kao lažan, a regulatori mogu imati evidentiran slučaj, te time značajno smanjiti broj potencijalnih žrtava i doseg prevara.

- **Zagovarati unapređenje regulatornog okvira i usklađivanje s evropskim zakonodavstvom**

Organizacije civilnog društva imaju vitalnu ulogu u zagovaranju unapređenja javnih politika. Civilni sektor mora aktivno zagovarati donošenje propisa i usklađivanje s Aktom o digitalnim uslugama (DSA) Evropske unije, kako bi se uspostavili efikasniji mehanizmi za sprečavanje i uklanjanje online prevara te povećale transparentnost i odgovornost samih online platformi.

- **Razvijati partnerstva s regionalnim i međunarodnim organizacijama**

S obzirom na to da online prevare sve češće imaju prekogranični karakter i da se infrastruktura i finansijski tokovi nalaze u različitim državama, imperativ je razvijati snažna partnerstva s regionalnim i međunarodnim organizacijama. Razmjena dobrih praksi, operativnih saznanja i alata za rano upozoravanje na evropskom i regionalnom nivou ključna je za adekvatan odgovor na ove prijetnje.

Ova publikacija izrađena je u sklopu projekta "Adresiranje *online* prevara kroz odgovornost platformi i osnaživanje građana/ki", koji provodi UG "Zašto ne", uz podršku šireg programa "Media-Lit", koji vodi Centar za građansko obrazovanje (CCE/CGO) u partnerstvu s Helsinškim odborom za ljudska prava u Srbiji (HCHRS), Helsinškiot komitet za čovekovi prava u Sjevernoj Makedoniji (MHC), Tirana Centre for Journalism Excellence (TCJE) iz Albanije i Atlantskom inicijativom (AI) iz Bosne i Hercegovine, uz finansijsku podršku Evropske unije i sufinansiranje Ministarstva regionalno-investicionog razvoja i saradnje s nevladinim organizacijama Vlade Crne Gore. Sadržaj ove publikacije isključiva je odgovornost UG "Zašto ne" i ne odražava nužno stavove Evropske unije, Ministarstva regionalno-investicionog razvoja i saradnje s nevladinim organizacijama Vlade Crne Gore ni CGO-a i projektnih partnera.