Metode prijevara na internetu

Goljački, Matea

Undergraduate thesis / Završni rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:372132

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2021./2022.

Matea Goljački

Metode prijevara na internetu

Završni rad

Mentorica: dr.sc. Vjera Lopina

Zagreb, srpanj 2022.

Izjava o akademskoj čestitosti

Izjavljujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Sadržaj

1. Uvod

Pojava interneta sa sobom donijela je mnogobrojne dobrobiti čovječanstvu, poput pretvaranja svijeta u jedno veliko globalno selo te olakšavanja komunikacije i dijeljenja sadržaja u veoma kratkom vremenu. Zahvaljujući tome, možemo saznati što se događa u skoro svakom kutku svijeta i na koji način to utječe na nas i našu okolinu. Isto tako, internet nam je omogućio pregledavanje različitih baza podataka i kreativnih sadržaja preko mnogobrojnih platformi koje su često besplatno dostupne svima. Ta svrha potaknula je ljude da nastave nadograđivati i poboljšavati dijelove interneta kako bi svi u njima mogli sudjelovati i uživati. Razvoj komunikacijskih kanala poput e-pošte ili društvenih mreža doveo je do zbližavanja potpunih stranaca, kao što je i uvelike pojednostavio proces komunikacije poslovnih partnera i korporacija diljem svijeta.

Iako je prvotna svrha interneta možda upravo bila spajanje čovječanstva, u današnje vrijeme ne koriste svi tu tehnologiju na pozitivan način nego neki rade gotovo potpuno suprotno. Društvenim mrežama šire se lažne vijesti, šalju se materijali upitnog kredibiliteta u svrhu obmane i širenja političke propagande, a broj novih prijevara raste s porastom digitalnih noviteta. Zbog ekstremno brzog razvoja ovog izuma, zakoni većine država kaskaju u pravnoj regulaciji i kažnjavanju počinitelja prijevara putem interneta, što oni rado iskorištavaju.

Uzimajući u obzir da je velik udio starije populacije zabrinjavajuće tehnološki i informacijski nepismen, ne začuđuje niti činjenica da su upravo oni najčešće i „najlakše“ žrtve ove vrste zločina. S druge strane, mlađa populacija češće teži donošenju impulzivnih odluka koje im se prezentiraju kao mogućnost brzih i lakih zarada te stoga oni pak čine veći udio žrtava novijih vrsta prijevara poput lažnih kriptovaluta ili krađe nezamjenjivih tokena koje ipak zahtijevaju određenu vrstu znanja i svijesti o korištenju interneta i povezane tehnologije.

Stoga korisnici interneta imaju odgovornost da se samoinicijativno trude i ulažu u vlastitu edukaciju o opasnostima interneta kako bi izbjegli situacije u kojima postaju žrtve računalnih zločina jer zbog nemogućnosti i premalih resursa policijskih službi kao i pravnih sustava mnogih država, ovakav kriminal ostaje uvelike nekažnjen te počinitelji nemaju razloga stati s takvim ilegalnim radnjama.

2. Računalne prijevare

2.1. Definicija računalne prijevare

Vuletić i Nedić (2014) objašnjavaju da se u definiciju računalnih zločina podrazumijevaju „sva kaznena djela koja se tiču računalnih podataka“ te nadalje upozoravaju kako ugrožavanje računalnih mreža u bilo kojem obliku mogu „dovesti do kolapsa egzistencijalno važnih područja, poput komunikacijskog, vojnog, proizvodnog, financijskog, poreznog itd.“. Isto tako, glavna karakteristika ove vrste kriminaliteta jest „nematerijalna priroda računalnih podataka kao objekta ovih kaznenih djela“, a u slučajevima gdje ne postoje posebni propisi, „primjenjuju se opća načela kaznenog prava“ (Vuletić i Nedić, 2014).

Zbog brzog razvoja interneta i tehnologije te sve veće umreženosti ljudi, ovaj tip zločina je u konstantnom porastu, čemu svjedoči i reguliranje međunarodnih dokumenata o ovoj temi. Hrvatska zakonska regulativa temu računalnih zločina do sad je zapostavljala zbog toga što je tradicionalno kazneno pravo uglavnom orijentirano na „povredu materijalnih pravnih dobara koja egzistiraju u stvarnom okružju“ (Vuletić i Nedić, 2014). Ipak, 2004. godine unesena je u Kazneni zakon, a 2011. godine u posebnu glavu pod imenom „Kaznena djela protiv računalnih sustava, programa i podataka“, a „ostvaruje ju tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome“ (Sokanović i Orlović, 2017).

2.2. Izravne i neizravne računalne prijevare

Prema Vuletić i Nedić (2014), računalna prijevara može se podijeliti u dvije vrste – izravnu i neizravnu; kada je riječ o izravnoj računalnoj prijevari, ona se „sastoji u tome da počinitelj dovodi u zabludu ili održava u zabludi drugu osobu, koristeći pritom računalni sustav kao sredstvo obmane“. Drugim riječima, govori se o zločinu prijevare za koji je specifična upotreba računala. U slučajevima ovakvih zločina, zakonodavac ima dva izbora: „Može predvidjeti poseban oblik prijevare ili može ostaviti praksi da ovakva ponašanja razmatra u okviru općeg kaznenog djela prijevare. Potonje rješenje, međutim, u sebi sadrži opasnost da se pojedini oblici prijevare, zbog svojih specifičnosti, ne mogu podvesti pod klasično kazneno djelo prijevare, a kao primjer ovakve vrste zločina navode prijevare putem e-pošte, za koje objašnjavaju da „najčešće imaju međunarodni predznak, s obzirom na to da počinitelji i žrtve dolaze iz različitih država pa to može stvoriti i probleme oko uspostavljanja kaznene vlasti i nadležnosti pojedinih

država, posebno ako se imaju u vidu velike različitosti između kaznenopravnih sustava u raznim dijelovima svijeta“ (Vuletić i Nedić, 2014).

Ako je u pitanju neizravna računalna prijevara, onda se radi o varanju računalnih sustava, tj. „računalni sustav je objekt kaznenog djela“, tijekom kojeg „počinitelj manipulira računalnim podacima ili programima s namjerom stjecanja protupravne imovinske koristi“, a kada su u pitanju takve manipulacije, „računalni sustav više ne može raspoznati pristupa li mu ovlaštena ili neovlaštena osoba“ (Vuletić i Nedić, 2014).

2.3. Poteškoće u kažnjavanju računalnih prijevara

Kao mogući razlog zbog kojih počinitelji ovakvih zločina uvelike ostaju nekažnjeni Cross (2014) navodi činjenicu da vrste prijevara koje se događaju preko interneta jednostavno nisu nikad bile viđene kao prioritet policiji niti je ona dobila odgovarajuće resurse kako bi se bavila tim tipom kriminala. Nadalje, problemi s nedovoljnom izobrazbom i sposobnošću pronalaska i razumijevanja računalnih prijevara samo nadodaju policijskoj nemogućnosti da na iste djeluje. Isto tako, budući da se počinitelji ovih zločina nalaze u državama diljem svijeta i često ne žive u državama njihovih žrtava, policiji je nadodan problem istraživanja, uhićenja i kaznenog progona mogućih prijestupnika zato što se ne mogu pozivati na autoritet ili legitimnu nadležnost koja bi im to dopustila, jer „dok kriminalci mogu djelovati preko pravnih granica svih država, policija ne može“ (Cross, 2019).

Uz navedeno, Dinarević i Softić (2021) navode sljedeće poteškoće: „Pored izazova anonimizacije i prikrivanja, država koja je domaćin kriminalca i njegove aktivnosti možda njegovu radnju ne definira kao kazneno djelo, te stoga možda neće biti u mogućnosti da ga kazneno goni ili surađuje u njegovom izručenju za kazneno gonjenje drugdje; država domaćin možda nema važeće ugovore sa državom u kojoj je djelo počinjeno, koji bi je obvezivali da pomogne u prikupljanju dokaza koji se mogu koristiti protiv počinilaca.“

2.4. Profil prevaranata i žrtava

2.4.1. Počinitelji računalnih prijevara

Prema Rotenberg (2019), profilu ljudi koji se bave prijevarama preko interneta uglavnom odgovaraju mlađi muškarci koji imaju delinkventne prijatelje, uhićeni su u ranoj dobi, dolaze iz siromašnih područja s visokim stopama kriminala i čiji su roditelji već počinili nekakva

kaznena dijela. Online prijevare pogotovo čine ljudi iz siromašnih država s osobama na vlasti koje njihov narod smatra korumpiranima. Također, počinitelji ovih zločina iskazuju neka svojstva psihopatskih i antisocijalnih poremećaja osobnosti. Zbog toga što ove sheme često zahtijevaju planiranje unaprijed i sposobnost rukovanja i snalaženja na različitim tehnologijama, ovakvi ljudi posjeduju i povećane kognitivne sposobnosti.

Zahvaljujući navedenim karakteristikama, zločinci se koriste i tehnikama socijalnog inženjeringa (eng. *social engineering)* kako bi lakše primamili žrtvu pod krinkom službenosti i povjerljivosti. „Socijalni je inženjering niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca kako bi ga naveo da učini nešto što nije u njegovom interesu. Socijalni se inženjering najčešće koristi u svrhu otkrivanja njihovih povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći“ (CARNET, 2022). Ovakve trikove upotrebljavaju tijekom slanja neželjene e-pošte na masovnoj razini kada u svaku poruku ubace jedan privatan detalj iz žrtvinog života, poput njezinog imena, adrese, datuma rođenja i slično. Žrtva zbog nedostatka sumnjičavosti i prevelikog povjerenja smatra da bilo koja osoba koja ju kontaktira s njezinim osobnim informacijama mora biti nekakav službeni entitet koji je te podatke dobio pravilnim i legalnim putem, stoga nema razloga za brigu.

Proces socijalnog inženjeringa može se podijeliti u sljedeća četiri koraka: „sakupljanje informacija o žrtvi, uspostavljanje veze sa žrtvom, pristupanje žrtvi te realizacija napada“ (CARNET, 2022). Nakon ovakvog napada, žrtva u većini slučajeva trpi materijalnu štetu, kompromitiranost osobnih podataka i ugleda, a ponekad doživljava i daljnje napade čime se žrtvi stvara emocionalni pritisak.

2.4.2. Žrtve računalnih prijevara

Prema Button et al. (2014), razlozi zbog kojih žrtve nasjedaju na ovakve prijevare su urgentnost ponude, zatim maleni, isprva nebitni žrtvini postupci koji na kraju vode do prihvaćanja ponude, nerazmjerne proporcije nagrade, tj. obećavanje velikih i brzih nagrada za ulaganje malo novca, kao i nesposobnost kontroliranja emocija zbog koje su žrtve sklonije donositi impulzivne odluke. Isto tako, ono što je specifično za žrtve romantičnih prijevara jest njihovo vjerovanje u ostvarivanje duboke povezanosti s prevarantom nakon samo nekoliko razmijenjenih poruka u kojima on namjerno sebe lažno predstavlja karakteristikama za koje zna da će se svidjeti njegovim žrtvama.

3. Vrste računalnih prijevara

3.1. Nigerijska prijevara ili „Prijevara 419“

Jedna od najpoznatijih i najuspješnijih internetskih prijevara jest pismo, odnosno e-pošta, koje navodno šalje princ iz Nigerije po čemu je i dobila naziv. Dodatno ime „Prijevara 419“ (eng. *Scam 419*) odnosi se na činjenicu da je ova prijevara prvi put opisana u nigerijskom kaznenom zakonu u članku 419. U poruci je često navedeno kako pošiljatelj prolazi kroz tešku životnu situaciju, npr. rat ili nekakvi problemi s bankom, te zbog tih okolnosti želi prokrijumčariti ogromnu svotu novca izvan države i za to upravo treba pomoć osobe koja zaprima takvu poruku. Sve što primatelj treba učiniti jest poslati svoj broj bankovnog računa i određenu količinu novca kako bi se taj tobožnji princ izbavio iz svojih problema, a za što zauzvrat obećava pozamašnu novčanu nagradu (Cummins, 2020).

Iako je prvotno ovakav oblik prijevare započeo u Nigeriji, sada postoje mnogobrojni oblici ovog pisma, poput onih koje naizgled šalje službena vlada Sirije ili pak osoba koja želi stupiti s nekime u kontakt tvrdeći da je njihov davno izgubljeni član obitelji i da joj je potrebna financijska pomoć kako bi se s njima upoznala uživo. Još neki od primjera takvog tipa poruka su i obavijesti u kojima piše da je osoba osvojila vrijednu nagradu te u svrhu slanja iste mora napisati svoje osobne podatke i broj kartice kako bi uspješno zaprimila nagradu, a šalju se i poruke iz nepostojećih banaka obavještavajući kako je nečiji član obitelji preminuo te mu ostavio veliko nasljedstvo. Naravno, ako netko povjeruje ovakvim porukama i pošalje novac, neće vidjeti nikakvu bogatu isplatu nego će postati jednom od mnogobrojnih žrtava prijevara preko interneta.

Razlog zašto je ovakav tip prijevara najuspješniji je upravo zato što je velik broj ljudi još uvijek informacijski nepismen, a starije populacije koje uglavnom budu žrtve ovakvih zločina često su naivne i ne vjeruju da bi ih netko mogao novčano prevariti preko interneta. Iako su većina takvih prevaranata zapravo siromašni studenti ili ljudi s nisko plaćenim poslovima, novac koji uspiju dobiti iz ovakvih prijevara je i više nego dovoljan za ugodan život. Oni najuporniji uspiju zaraditi skoro pola milijuna kuna godišnje, a „najisplativije“ žrtve su često umirovljenici ili muškarci i žene udovice u starosti od 45 do 75 godina zbog toga što je takva demografija statistički najvjerojatnije usamljena i dobrostojeća - stoga kada netko s njima stupi u kontakt u svrhu komunikacije veoma su otvoreni i pristupačni, tj. lake su mete ovakvoj vrsti prijevare (Schlesinger i Day, 2017). To dokazuje da se neke vrste kompjuterskih zločina ne događaju nužno zbog propusta u sigurnosti sustava, već zbog ljudske potrebe za socijalizacijom i

stvaranjem veza. S obzirom na to da ovakve prijevare funkcioniraju i djelomice zbog tzv. „zakona velikih brojeva“, što više e-mailova prevaranti pošalju, to je veća mogućnost da će se netko javiti i postati žrtvom.

Osim što ovakve prijevare mogu uzrokovati financijsku štetu, neželjene e-poruke (eng. *spam*) u isto vrijeme imaju sposobnost i zaraze računala virusom prilikom otvaranja poveznica koje se nalaze u poruci (Hrvatska udruga banaka, n.d.). Takvi virusi mogu biti neprimjetni, poput trojanskih virusa, no zato mogu slati osobne podatke i datoteke sa zaraženog računala na udaljeno računalo. Stoga od ovakvih prijevara najjednostavniju zaštitu pružaju filteri protiv neželjene e-pošte (eng. *spam filters*) koji su u zadnje vrijeme sve uspješniji u pronalasku i izolaciji takvih poruka, a preporučena je i dovoljna opreznost i doza skeptičnosti pri čitanju e-pošte.

3.2. Prijevare putem internetskih oglasnika

Prijevare putem interneta su sve češće, a u zadnje vrijeme učestalijim postaju prijevare putem internetskih oglasnika (Ministarstvo unutarnjih poslova, 2022). U ovakvim slučajevima, prevaranti na oglasnike stavljaju objave o proizvodima s puno nižim cijenama nego što je očekivano kako bi privukli pažnju što više kupaca. Najčešći proizvodi koji se reklamiraju u ovakvim prijevarama su automobili, odjeća i obuća poznatih marki, autogrami poznatih osoba, skupocjeni mobiteli itd., a od osobe se traži uplata na tekući račun prevaranta. U većini slučajeva, navedeni proizvodi nikada ne budu dostavljeni ili se dostavljaju prazne kutije ili pak u potpunosti drugačiji predmeti s malom vrijednosti.

Ovakve prijevare teško je identificirati i kazneno goniti zbog toga što se na internetskim oglasnicima lako mogu stvoriti profili s lažnim podacima koji se nakon uspješnih prijevara brzo brišu. Uz to, problem može predstavljati i dokazivanje namjere za prijevaru jer uvijek postoji mogućnost o gubitku paketa dostavne službe kada je riječ o međunarodnim dostavama. Također, ono što je još karakteristično za ovaj tip prijevara jest požurivanje osobe od strane prevaranta da uplatu obavi u što kraćem vremenu zbog moguće rasprodanosti traženih artikala čime se vrši pritisak na osobu kako bi donijela impulzivnu odluku i postala žrtvom internetske prijevare (Ministarstvo unutarnjih poslova, 2022).

Uz navedeno, oni smjeliji prevaranti koriste se i lažnim internetskim stranicama koje nalikuju na službene stranice dostavnih službi kako bi izgledali što pouzdanije te koriste domene nalik službenim uslugama, npr. www.posta-hr.site ili www.postahr.shop umjesto www.posta.hr

(Ministarstvo unutarnjih poslova, 2022). Na takvim stranicama otvaraju se uvjerljiva sučelja u koja osoba zatim upisuje svoje osobne podatke i broj kreditne kartice kao i CVV/CVC broj na njezinom začelju, usprkos tome što je jedini potreban podatak prilikom slanja novca nekome njihov IBAN, odnosno broj računa. Nakon unosa navedenih podataka, žrtva sa svojeg računa uplaćuje prevarantu količinu novca koju je naveo u oglasu za određeni predmet.

U svrhu zaštite mogućih kupaca, najkorišteniji hrvatski internetski oglasnik na kojem su se već dogodile slične prijevare, Njuškalo.hr, upozorava na potrebu provjeravanja sadržaja pristigle e-pošte jer, kako navode, u njihovoj službenoj e-pošti nikada ne traže: upisivanje osobnih podataka, brojeva kartica, preslike dokumenata u svrhu utvrđivanja identiteta, niti upisivanja limita na karticama ili autoriziranja iste radi izvršavanja uplata; a sama e-pošta mora biti napisana u skladu s hrvatskom gramatikom i pravopisom umjesto velikim tiskanim slovima i brojnim greškama u pisanju (Njuškalo.hr, 2022).

Zato je prilikom svake kupnje putem internetskih oglasnika potrebno: komunicirati preko službenih kanala, ignorirati molbe za otvaranjem poveznica i spajanja na druge servise, ne vjerovati u nerealno niske cijene popularnih marki proizvoda, izbjegavati donošenje impulzivnih odluka zbog velikih rasprodaja i ne upisivati podatke s platnih lista i kreditnih kartica, već isključivo IBAN. Isto tako, na internetskim oglasnicima koji pružaju takvu uslugu, potrebno je provjeriti i recenzije prodavača, a prilikom plaćanja važno je biti spojen na sigurnu internetsku vezu umjesto javno dostupnog WiFi-ja.

3.3. Investicijske prijevare

Do investicijskih prijevara dolazi kada „osoba, odnosno ulagatelj pretrpi financijski gubitak zbog ulaganja na temelju obmanjujućih, nepoštenih ili lažnih poslovnih praksi“ (Hrvatska agencija za nadzor financijskih usluga, 2021). Prilikom ovakvih prijevara često se koriste termini poput „velika zarada u budućnosti, visoki povrati na uloženi novac, laka zarada“ kako bi se osobu nagovorilo na preuzimanje financijskog rizika, a koriste se tehnike fantomskog bogatstva, oskudnosti, kredibiliteta izvora, društvenog konsenzusa i reciprociteta (Hrvatska agencija za nadzor financijskih usluga, 2021).

Fantomsko bogatstvo odnosi se na veliku količinu novaca koju kupac ima priliku dobiti nakon ulaganja u valutu prevaranta, dok se oskudnošću stvara lažan osjećaj nedostatka i ograničenosti zaliha valute kojom se trguje kao i vremena ulaganja čime se podupire ekskluzivnost i vrijednost same valute, a kupac je pod pritiskom donijeti impulzivnu odluku iz straha da ne

propusti dobru priliku (Hrvatska agencija za nadzor financijskih usluga, 2021). Izjave poput „ova je ponuda dostupna ograničenom broju ljudi“ ili „ovu ponudu možete iskoristiti još samo danas“ predstavljaju potencijalni gubitak i još više guraju kupca da uđe u financijski rizik kako bi si osigurao bolju budućnost (Hrvatska agencija za nadzor financijskih usluga, 2021). Kredibilitetom izvora smatra se „iskorištavanje sklonosti pojedinca da vjeruje osobama od autoriteta i organizacijama koje smatra legitimnima“ (Hrvatska agencija za nadzor financijskih usluga, 2021).

Taktike koje se koriste kako bi se stvorio lažan osjećaj sigurnosti u osobama autoriteta i takvim organizacijama su korištenje veoma stručnih i zbunjujućih termina za koje prosječna osoba ne zna, grafički dizajn nalik onima legitimnih organizacija, lažno predstavljanje i navođenje informacija u svrhu skretanja pažnje, poput govora o povijesti i uspješnosti poslovanja takve fiktivne kompanije (Hrvatska agencija za nadzor financijskih usluga, 2021). Zatim se socijalnim konsenzusom pokušava uvjeriti žrtvu da su mnogobrojni ljudi donijeli ispravnu odluku, tj. uložili u valutu, kako bi se i ona konformirala i pridružila tim ljudima, a zbog straha od isticanja, žrtvama je još teže usprotiviti se većini.

U ovakvim investicijskim prijevarama, prevaranti često govore kako je „velik broj osoba profitirao od njihove ponude ili pružaju lažne izjave 'sretnih dobitnika'“ (Hrvatska agencija za nadzor financijskih usluga, 2021). Reciprocitetom se prevaranti nadaju kako će potaknuti žrtvu na vraćanje usluge, odnosno investiranje u valutu zbog toga što se često ovakve investicijske prilike prezentiraju na besplatnim večerama tijekom kojih žrtve imaju priliku osvojiti nagrade poput popusta na određene proizvode. Ovakvim taktikama kod žrtve se stvara osjećaj da nešto duguje jer je dobila nešto vrijedno bez potrebe plaćanja čime se sklonost prema uzvraćanju usluge putem ulaganja pojačava.

Kada se radi o ulaganju u kriptovalute, na razini Europske Unije i Hrvatske još ne postoje zakoni koji bi regulirali takvo trgovanje, a propisi koji se njih tiču navode da je to jedino u svrhu sprječavanja pranja novca i financiranja terorizma. Kako takvo tržište nije zakonski uređeno zbog veoma brzog i promjenjivog razvoja, česti rizici nalaze se u asimetričnim i lažnim informacijama u svrhu očuvanja vrijednosti valute, što je zlouporaba tržišta koja se strogo nadzire u regularnim sustavima trgovanja te čiji se prekršaj smatra kaznenim i prekršajnim djelima i za koja postoje zatvorske kazne (Hrvatska agencija za nadzor financijskih usluga, 2021).

Najbolji način za zaštitu od investicijskih prijevara je prvotno oprez jer, iako je riječ o navodnim brzim i jednostavnim načinima zarade, od žrtve se očekuju veliki ulozi samo kako bi mogla dobiti informacije kako zaraditi. Također, prilikom ulaganja potrebno je napisati i držati se detaljnog plana ulaganja i ne postati žrtvom impulzivnog odlučivanja. Sredstva plaćanja treba pohranjivati na što sigurniji način, poput hardverskog novčanika u slučaju kriptovaluta, kako bi se izbjegla mogućnost krađe identiteta. Preporučljivo je uložiti minimalnu količinu novca tako da se u slučaju gubitka ne izgubi ekstremna količina novca, a prije samog ulaganja može se poslati i probna transakcija nakon koje postaje očito dolaze li sredstva na adresu primatelja ili ne (Hrvatska agencija za nadzor financijskih usluga, 2021).

Većina investicijskih prijevara vodi se dvama shemama: Ponzijevom shemom i piramidalnom shemom. Ponzijeva shema uključuje mamljenje ulagača obećanjima brzih i visokih zarada. Nakon osnutka ustanove koja se bavi prikupljanjem depozita, prevarant „poziva javnost da deponira novac kod institucije, nudeći velikodušne kamate“ (Hrvatska agencija za nadzor financijskih usluga, 2021) koje se isplaćuju iz fonda novca prikupljenog od novih deponenata, a prevarant uživa stare depozite i u isto vrijeme se obogaćuje od novih. Do propasti Ponzijeve sheme dolazi kada je broj novih deponenata premali da bi održavao isplate kamata starih depozita dok u međuvremenu prevarant bježi od kaznenog progona.

S druge strane, piramidalna shema zasniva se na zavaravanju ljudi obećanjima neizmjernih pogodnosti kako bi nastavili uplaćivati novac prevarantu. Glavna karakteristika ove sheme je, uz normalnu isplatu, davanje veće provizije onima koji dovuku što više ljudi u shemu čime se eksponencijalnim rastom povećava vrijednost za one na vrhu piramide. „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“ (Hrvatska agencija za nadzor financijskih usluga, 2021). Primjer piramidalne sheme u Hrvatskoj dolazi iz 2010. godine pri čemu su desetak samoprozvanih poduzetnika oštetili stotine građana za više stotina milijuna kuna lažnim predstavljanjem trgovanja devizama preko platforme Forex (Hrvatska agencija za nadzor financijskih usluga, 2021).

3.3.1. Kriptovalute

Kao posebnu vrstu investicijskih prijevara putem interneta čija popularnost u zadnjih nekoliko godina brzo raste, važno je spomenuti i prijevare koje uključuju kriptovalute i NFT tehnologiju.

Prema Stoica (2021), još uvijek ne postoji jedna univerzalna definicija oko koje se svi stručnjaci slažu jer ona varira od države do države zbog unikatnosti pravnih okvira koji ih se tiču, međutim navodi sljedeće: „Virtualne valute mogu se definirati kao digitalne reprezentacije vrijednosti koja nije garantirana centralnom bankom ili javnim autoritetom, nije nužno povezana s pravnim tijelom i nema legalan status valute, no pojedinci ili legalni entiteti ju mogu prihvatiti i koristiti kao medij razmjene, a isto tako može biti transferirana, pohranjena i razmijenjena elektronskim putem. Glavne funkcije virtualnih valuta su kao sredstvo plaćanja, razmjene, investicije, proizvoda s određenom vrijednošću ili proizvoda za uporabu u Internet kasinima“. Prva kriptovaluta koja je stvorena 2008. godine bio je „Bitcoin“ koji je nastao u svrhu zaštite investicija i osiguravanja slobodnog financiranja poslovanja bez potrebe uključivanja financijskih institucija poput banaka i koja se mogla koristiti izvan bilo kakvih regulacija i ograničenja, a danas postoji više od 10 tisuća različitih valuta koje se neprestano razmjenjuju preko virtualnih platformi (Stoica, 2021).

Ipak, s ovakvom tehnologijom postoje i određeni rizici, poput nesigurnih kripto-novčanika i anonimnosti prodavača koje zločinci iskorištavaju kako bi uspješno prevarili žrtve pomoću manjka službenih regulacija. Prema Bartoletti et al. (2021), sljedeće prijevare su najrasprostranjenije:

- Lažni kripto-novčanici preko kojih prodavači u nekim slučajevima kradu male količine novca, a neki uzimaju mali postotak dnevnog depozita,
- Lažne mjenjačnice koje prikazuju neistinite informacije o tržištu kriptovaluta tako da valutama koje imaju malu vrijednost daju krivu, tj. veliku vrijednost,
- Lažne kampanje donacija kojima prevaranti ciljaju na dobrotvorne ljude te zatim nestanu sa svim donacijama,
- Lažna obećanja o hardverskim potrebama računala koja stvaraju kriptovalute kako bi osobe investirale u kupnju bolje tehnologije, no novac se ustvari koristi u druge svrhe.

Jedna od najvećih prijevara u povijesti kriptovaluta povezana je s tvrtkom „OneCoin“, a funkcionirala je kao Ponzijeva shema na značajnoj razini. Ovu prijevaru promovirala je Ruja Ignatova koju FBI sada smatra jednom od deset najtraženijih bjegunaca na svijetu zbog toga što je uspjela prevariti investitore u ulaganje u beznačajnu i nepostojeću kriptovalutu te na taj način od njih ukrala više od 4 milijarde dolara (Milmo, 2022).

3.3.2. Nezamjenjivi token (eng. non-fungible token) ili NFT

Osim kriptovaluta, na tržištu se nedavno pojavila nova tehnologija nezamjenjivih tokena (eng. *non-fungible token*), odnosno NFT. Prema Vrbanus (2021), radi se o kriptografski zaštićenim djelićima koji predstavljaju nešto unikatno, a koriste se u svrhu „čuvanja vrijednosti i kao lako provjerljivi dokaz vlasništva nad drugim jedinstvenim oblicima digitalne ili 'analogne' imovine, poput umjetničkih djela, kolekcionarskih predmeta i slično“. Razlika između kriptovaluta i NFT-a nalazi se upravo u jedinstvenosti svakog NFT-a zbog kojeg se on ne može zamijeniti drugim tokenom i koristiti se kao zamjena za novac ili druge kriptovalute koje imaju istu vrijednost.

Najčešća prijevara povezana s NFT tehnologijom je tzv. „rug pull“ prijevara, u kojima „prevaranti stvaraju veliko zanimanje za određenu NFT kolekciju, često plaćanjem influencera i nakon što postignu da određeni broj ljudi uloži, ugase web stranicu, zatvore sve račune po društvenim mrežama i nestanu“, a do problema dolazi u zakonskom dokazivanju prijevare jer kupci svejedno posjeduju kupljeni NFT, samo što je on izgubio svu vrijednost (Ivezić, 2022). Primjer navedene prijevare može se pronaći i u Hrvatskoj tijekom 2021. i 2022. godine kada su četvorica Hrvata pokrenula devet NFT projekata kojima su prevarili kupce za skoro 3 milijuna dolara.

3.4. Prijevara posrednika 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.“ (Hrvatska agencija za nadzor financijskih usluga, 2021). Novac je ukraden od drugih ljudi, a prevaranti putem e-pošte, oglasnika i sličnih usluga traže žrtve koje će taj novac prenositi uz nekakvu naknadu. Prevaranti će također tražiti od žrtve da policiji i banci ne otkrivaju razloge uplate i isplate novca, a najčešće vrebaju osobe lošijeg imovinskog stanja, imigrante, studente, nezaposlene, kao i sve ostale željne lake zarade.

Ovaj tip prijevare započinje varanjem ljudi o otvaranju nove firme zbog kojeg je potrebna pomoć za prijenos novca. Svaki razgovor i daljnji dogovor obavlja se online ili telefonski bez ikakvih susreta, a „jedini je zadatak „zaposlenika da u „nekoliko klikova“ u određeno vrijeme novac koji mu sjedne na račun proslijedi te uzme dogovoreni postotak“ čime se vrši kazneno

djelo pomaganja u pranju novca za što je moguća kazna zatvora u trajanju od šest mjeseci do pet godina (Hrvatska agencija za nadzor financijskih usluga, 2021).

3.5. CEO (Chief Executive Office) prijevara ili „Direktorska“ prijevara

„Direktorska prijevara događa se kada je zaposlenik koji je ovlašten za provođenje plaćanja prevaren na način da plati lažni račun ili provede neovlašteni prijenos s računa tvrtke“ (Europol, 2021). U najčešćim slučajevima događa se kada su osobe na visokim pozicijama u tvrtki izvan ureda ili na godišnjem odmoru i tada prevarant poziva na brzo djelovanje žrtve zbog hitnosti i osjetljivosti transakcije kako se ne bi prekinuo proces poslovanja. Počinitelji ovog zločina ne traže nužno uvijek novčanu naknadu; nekad postavljaju pitanja u svrhu saznavanja povjerljivih informacija kako bi kasnije mogli učiniti još veću štetu ciljanjem važnijih zaposlenika (Ministarstvo unutarnjih poslova, 2021).

Prevaranti šalju e-poštu zaposlenicima trgovačkih društava, računovodstvenim uredima, tijelima državne vlasti i pravnim osobama s javnim ovlastima, a lažno se predstavljaju kao direktori, članovi uprava trgovačkih društava ili kao neke druge osobe s višom pozicijom od žrtve. Tada traže osobu da što prije provede plaćanje lažne fakture ili izvrši neovlašteni prijenos sredstava s računa tvrtke, čime nakon kriminalističkog istraživanja počinitelj odgovara za kazneno djelovanje računalne prijevare i nedozvoljene uporabe osobnih podataka (Ministarstvo unutarnjih poslova, 2022).

Kako bi se tvrtke zaštitile od ovakvih napada, potrebno je informirati sve zaposlenike o načinu prijevare i zahtijevati opreznost pri svim transakcijama i bilo kakvim zahtjevima za plaćanje. Također, poželjno je i propisati službeni postupak kojim će se provjeravati legitimnost zahtjeva za plaćanje koji se šalju preko e-pošte, a svakako je potrebno i ažurirati sigurnosne sustave na službenim uredskim računalima (Ministarstvo unutarnjih poslova, 2022).

3.6. Prijevare u obliku zanimanja za romantičnu vezu

Prema Sorell i Whitty (2019), romantične prijevare (eng. *online dating scams*) jedne su od najčešćih i najunosnijih online prijevara u zadnjih nekoliko godina. Isprva su muškarci i žene predstavljali podjednak broj žrtava ove prijevare, no sada dominiraju žrtve ženskog spola. Osobe trpe financijske gubitke koje sežu i preko milijun kuna u ekstremnim slučajevima, no osim gubitka novca često dolazi i do psihološke povrede žrtava.

Nadalje, Sorell i Whitty (2019) objašnjavaju da romantična prijevara funkcionira tako da prevaranti naprave varljiv profil na stranicama za online upoznavanje pri čemu koriste slike drugih, često veoma atraktivnih ljudi i u opis profila stavljaju specifične ključne riječi i fraze kako bi pobudile interes od strane pomno odabrane žrtve. Na primjer, stvaraju lažne profile umirovljenih vojnika koji žive u inozemstvu kako bi privukli populaciju žena srednjih godina i ostvarili romantičnu vezu preko koje će tražiti sve više i više novca. Taj proces upoznavanja i stvaranja veze može trajati neki duži period tijekom kojeg će prevarant prvo slati brojne poruke na dnevnoj bazi, nakon čega prelazi u drugu fazu prijevare koja se sastoji od uvjeravanja žrtve u skorašnji susret uživo s lažnim profilom prevaranta. Takav susret uživo nikad se ne dogodi jer zločinac svaki put izmišlja nove izlike zbog kojih ne može stupiti u kontakt sa žrtvom, npr. nema novaca za let, treba podmiriti dugove u banci, iznenada se razbolio i treba platiti lijekove ili pak treba kupiti bolju odjeću da se ne osramoti itd.

Zbog ostvarene romantične veze, žrtva će imati osjećaj sažaljenja i ponudit će se da pomogne prevarantu u otplaćivanju dugova, na što prevarant pristaje i odmah šalje svoje bankovne podatke kako bi se uplata novaca uspješno obavila. Nakon nekoliko takvih transakcija, prevarant opetovano daje izlike kako mu treba još novaca prije susreta sa žrtvom, na što ona ili pristaje ili shvaća da je riječ o prijevari te odustaje od komunikacije s prevarantom. U nekim slučajevima komunikaciju je teže prekinuti ako je žrtva prevarantu slala kompromitirajući materijal koji on može koristiti za ucjenjivanje i financijsku iznudu (Sorell i Whitty, 2019).

U svrhu sprječavanja ovakve vrste prijevara, potrebno je izbjegavati objavljivanje osobnih informacija na društvenim mrežama, svaki profil s kojim osoba stupa u kontakt detaljno istražiti i tijekom dopisivanja postavljati puno pitanja, nikada ne razmjenjivati informacije koje prevarantu pružaju priliku za stvaranjem financijske štete i naposljetku ne slati eksplicitan sadržaj koji se kasnije može koristiti za ucjenu (CARNET, 2022).

3.7. Prijevare putem nagradnih igara

Ovakva vrsta prijevare započinje kada osoba zaprimi e-poštu u kojoj je obaviještena o velikom dobitku, npr. putovanje na tropski otok, novi auto ili pozamašna količina novca, iz neke nagradne igre ili drugih igara na sreću, iako se ta osoba nije prijavila u igru niti je sudjelovala u njoj. Sve što treba učiniti jest odgovoriti na poruku, a kada to učini osoba će dobivati još više e-pošte i u nekim slučajevima telefonske pozive.

Ako osoba nastavi komunikaciju s prevarantom, primit će obavijest prema kojoj mora platiti određenu pristojbu pod krinkom pokrivanja administrativnih troškova kako bi joj se omogućilo zaprimanje glavne nagrade, tj. osvojene velike svote novca. Često će prevarant tražiti još i podatke bankovnih računa i kartica i uvjeravati žrtvu da je to zbog načina uplaćivanja nagrade, a isto tako će od osobe zahtijevati da nikome ne govori o dobitku kako bi ona i njena nagrada ostala sigurna.

U stvarnosti, prevarant na ovaj način pokušava spriječiti žrtvu od daljnjeg traženja savjeta ili informacija od drugih stranki. Ako mu osoba zaista napiše te podatke, on time uspješno vrši prijevaru. Ono što je zabrinjavajuće jest činjenica da ako je osoba već jednom bila žrtva ovakvih prijevara, ona biva stavljena na listu ljudi koji su nasjeli na takve sheme i počinje primati još više obmanjujućeg sadržaja (Griffiths, 2010).

Najlakši način za sprječavanje ovih prijevara je obraćanje pažnje na koje nagradne igre se osoba prijavljuje te sukladno s time imanje na umu od kojih igara na sreću osoba nije sposobna primiti nagradu zbog neprijavljivanja na njih. U slučaju bilo kakvog dobitka, poželjno je kontaktirati i utvrditi isti kod relevantnih organizacija putem telefonskih poziva dobivenih samostalnim istraživanjem na internetu, a ne se javljati na ponuđene kontakte u e-pošti i nikako slati osobne podatke niti brojeve kartica i bankovnih računa (Ministarstvo unutarnjih poslova, 2022).

3.8. Prijevare medicinskih proizvoda

Pod prijevare koje prodaju čudesne medicinske preparate spadaju proizvodi koji navodno preveniraju, tretiraju ili izlječuju bolesti ili druge zdravstvene tegobe, ali nisu dokazano sigurni niti efektivni za korištenje u takvu svrhu (U.S. Food & Drug Administration, 2022). Nadalje, osim što osoba zbog ovih lažnih proizvoda troši novce ni na što, također i odugovlači stvarne procese dijagnostike i tretmana bolesti. Ovakvi tobožnji lijekovi mogu uzrokovati još gore simptome od postojećih ali i smrt korisnika u najgorem slučaju.

Prodavači ovakvih preparata često koriste termine poput „drevni lijek“, „tajni sastojak“, „znanstveno otkriće“ ili „čudesni proizvod“ kako bi kupce uvjerili u veliki potencijal proizvoda. Isto tako, prevaranti tvrde da njihovi proizvodi garantiraju rezultate unutar 30 dana, liječe više vrsta biološki nepovezanih kroničnih bolesti, te da su dobitnici važnih znanstvenih nagrada čime pokušavaju nadodati prestižnost proizvodu (Federal Trade Commission, 2022).

Početak pandemije koronavirusa počinitelji ovakvih prijevara vidjeli su kao veliku šansu za brzim obogaćivanjem te krenuli s proizvodnjom i prodajom supstandardnih zaštitnih maski za lice, tzv. „korona sprejeva“ i ostalih čudotvornih lijekova koji suzbijaju bolest u potpunosti (Interpol, 2020).

Ovaj tip prijevara funkcionira zbog toga što prevaranti vrebaju ljude koji su izgubili nadu u medicinske postupke zbog oboljenja od neizlječivih bolesti te tragaju za bilo kojim drugim načinom tretiranja tegobe ili pak jednostavno žele doći do odličnog zdravlja u kratkom vremenu. Prije samostalnog tretiranja bolesti, svakako je potrebno prvo konzultirati se s doktorom, provjeriti više izvora i recenzija istog medicinskog preparata, pomnije razmisliti o upotrebi nedokazanih lijekova i tretmana te ne nasjedati na proizvode koji tvrde da posjeduju čarobne efekte i moć brzog iscjeljivanja (Federal Trade Commission, 2022).

3.9. Prijevare u svrhu krađe identiteta

Prema Vidas (2020) definicija krađe identiteta može se opisati „kao krađa tuđeg identiteta u kojoj netko želi biti netko drugi, najčešće radi stjecanja materijalne ili neke druge koristi. Krađa identiteta predstavlja otuđivanje identiteta druge osobe bez njezinog znanja ili pristanka.“ Također, prilikom ovakve prijevare, od žrtve se kradu osobni podaci koji su „sve informacije koje se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi“, a informacije iz različitih izvora koje „zajedno prikupljene mogu rezultirati utvrđivanjem identiteta određene osobe, također čine osobne podatke“.

Prijevare krađe identiteta mogu se podijeliti u tri kategorije ovisno o mediju koji se koriste prilikom prijevara: vishing, phishing i smishing. Sve tri mogu se smatrati vrstom socijalnog inženjeringa pomoću kojeg prevaranti nakon slanja lažnih poruka dobivaju zauzvrat osjetljive osobne podatke ciljanih žrtava. Počinitelji ovakvih napada također mogu dobiti zatvorsku kaznu u trajanju od minimalno godinu dana (Vidas, 2020).

3.9.1. Vishing

„Vishing (glas ili VoIP phishing) je elektronska prijevara u kojoj se pojedinci uvlače u otkrivanje kritičnih financijskih ili osobnih podataka neovlaštenim subjektima. Vishing djeluje poput krađe identiteta i provodi se pomoću govorne tehnologije.“ (Dinarević i Softić, 2021). Ovakvi napadi mogu se izvesti korištenjem glasovne e-pošte, fiksnim i mobilnim telefonima

ili VoIP-om (glas preko IP-a). Prevaranti koji uspješno koriste taktike vishinga uspiju prikupiti mnoštvo osobnih informacija od žrtava koje koriste kako bi ukrali njihov identitet i pomoću kojih mogu otvarati bankovne račune, stvarati dugove ili zloupotrebljavati kredite osoba od kojih su te informacije ukrali.

Također, ovakav tip prijevare ne zahtijeva korištenje komplicirane tehnologije i stoga je dostupan gotovo svima. Prevaranti zovu što više ljudi u danu te se predstavljaju kao službeni djelatnici banaka, sličnih financijskih institucija ili državnih agencija, a zatim od žrtve traže povjerljive informacije poput brojeva kreditnih kartica, lozinke važnih računa, odgovore na sigurnosna pitanja ili informacije prikazane na drugim važnim osobnim dokumentima preko kojih mogu preuzeti žrtvin identitet.

3.9.2. Phishing

„Pojam „phishing“ dolazi od engleske riječi „fishing“ kojom se metaforički opisuje postupak kojim neovlašteni korisnici mame korisnike interneta, kako bi dobrovoljno otkrili svoje povjerljive podatke. Lažno predstavljanje postaje sve opasnije razvijanjem u sofisticirane napade koji mogu manipulirati korisnicima putem prevarantskih web-stranica, ciljanih poruka e-pošte i lažnih telefonskih poziva.“ (Dinarević i Softić, 2021). Žrtvina motivacija kojom odaje osobne podatke često proizlazi iz obećanja prevaranta o različitim koristima ili pak prijetnjama i socijalnim inženjeringom. Žrtva pritom otkriva osobne informacije prevarantu kojeg smatra službenom osobom od povjerenja i to najčešće u obliku korisničkih imena i lozinki, podataka o bankovnim računima i slično čime počinitelj zločina dobiva detaljan uvid u žrtvin život.

Razvojem tehnologije ovakvi napadi su postali još sofisticiraniji te prema Dinarević i Softić (2021) danas postoji više vrsta phishing napada, poput „prijevarne krađe identiteta, krađe identiteta na zlonamjernom softwareu, Keyloggera i Screenloggera, hakiranja, trojanskih virusa, krađe identiteta u tražilicama, krađe identiteta u obliku injekcije, krađe identiteta na bazi DNS-a…“. Osim e-pošte, u phishing napadima mogu se koristiti i ostali web servisi kao što su razni forumi, platforme za online komunikaciju (Windows Messenger, ICQ, Skype, Google Talk itd.) i društvene mreže poput Facebook-a (CARNET, 2022).

Uobičajene phishing prijevare mogu se prepoznati po nestandardnim e-adresama s krivotvorenim porukama s naizgled službenih adresa, neformalnim pozdravima poput „Cijenjeni korisniče“ i osjetljivim pitanjima, neodloživim zahtjevima poput „Moramo potvrditi informacije o vašem računu“, lošem pravopisu i oblikovanju teksta, a ponekad sama e-poruka

može sadržavati samo neobičnu poveznicu koja prilikom otvaranja šalje žrtvu na stranicu s lažnim sučeljima i obrascima koje nakon upisa osobnih podataka te iste šalju prevarantu (Hrvatska udruga banaka, 2022).

3.9.3. Smishing

Prema Yeboah-Boaten i Mateko Amanor (2014), smishing je vrsta prijevare koja koristi SMS-ove ili druge servise za slanje poruka putem mobilnih uređaja u svrhu krađe identiteta. Dva glavna procesa koja se odvijaju prilikom ovakve prijevare su prvotno primanje poruke koja je pažljivo dizajnirana da izgleda kao da dolazi od službenog izvora, poput banke ili sistemskog administratora. Drugi dio sastoji se od žrtvinog zaprimanja poruke kako je njezin identitet otuđen i u kojoj se nalazi poveznica koja nakon otvaranja osobu šalje na lažnu stranicu gdje mora upisati svoje osobne podatke. Također, u nekim slučajevima, umjesto poveznice, u poruci se može poslati i prilog koji nakon preuzimanja datoteka instalira virus ili štetni program kako bi prevarant dobio pristup osjetljivim podacima. Nakon upisa povjerljivih informacija, te iste stižu prevarantima koji su poruke i poslali te ih oni zloupotrebljavaju u vlastite svrhe.

Najbolji način zaštite protiv ovakvih prijevara jest prevencija jer krađe identiteta se u većini slučajeva primjećuju tek kada žrtva pretrpi neku vrstu financijskog gubitka. Stoga je potrebno strogo čuvati osobne podatke, pogotovo PIN-ove kartica i korisnička imena i lozinke, provjeravati jesu li stranice koje traže upis takvih podataka sigurne i službene, poželjno je korištenje složenih lozinki koje se sastoje od velikih i malih slova te brojeva s najmanje osam znakova i mijenjanje istih na godišnjoj razini, a za zaštitu podataka na računalima posebno je važno koristiti vatrozid (eng. *firewall*), antivirusne i antišpijunske programe te ih redovno ažurirati (Vidas, 2020).

4. „Deepfake“ tehnologija

4.1. Definicija „deepfake“ tehnologije

Naziv „deepfake“ vuče značenje iz engleskih pojmova „deep learning“ (duboko učenje) i „fake“ (lažno) što se odnosi na digitalno stvorene i krivotvorene video sadržaje koje postaje sve teže razaznati. Ukratko, ovakva tehnologija funkcionira „na nečemu što zovemo *generative adversarial networks* (GANs), odnosno „generativne suparničke mreže“ (Deepfake: tehnologija koja prijeti vjerodostojnosti medija, 2022). Algoritam GAN uključuje dvije odvojene umjetne inteligencije, jednu koja generira sadržaj – na primjer, fotografije lica ljudi

– i drugu, „protivničku“, koja pokušava prepoznati jesu li te fotografije stvarne ili su lažne, tj. radi li se o pravim licima ili ne“. Nadalje, prvotna umjetna inteligencija koja pomaže u proizvodnji ovakvog sadržaja isprve ne razumije izgled ljudskih lica, no s vježbanjem postaje vještija u stvaranju i skrivanju lažiranih videa: „Međutim, vremenom, oba AI-ja postaju sve bolja (uče), tako da prvi AI (zvani Generator) počinje generirati lica ljudi koja izgledaju tako uvjerljivo, da ovaj drugi (Diskriminator) sve teže može razlikovati ona prava od lažnih (kompjuterski generiranih) lica“ (Deepfake: tehnologija koja prijeti vjerodostojnosti medija, 2022).

4.2. Opasnosti i prednosti

Opasnost ovakve tehnologije krije se u činjenici da se u rukama pogrešnih ljudi može koristiti u svrhu zavaravanja javnosti događajima koji nisu istiniti, kao i mogućnost brzog širenja takvog sadržaja putem društvenih mreža. Time se ugrožavaju društveni, politički i poslovni procesi diljem svijeta, no uvođenjem pravnih regulacija, korporativnih politika, edukacijom i razvojem tehnologije koja ovakav sadržaj može prepoznati ovakav rizik se može znatno smanjiti (Westerlund, 2019). Iako širenje dezinformacija ne zahtijeva mnogo truda, borba protiv krivotvorenih sadržaja postaje sve teža pogotovo zbog toga što se ovo može smatrati relativno novom vrstom prijevara koja se pojavljuje tek 2017. godine i o kojoj ne postoji mnoštvo stručne literature (Westerlund, 2019).

Isto tako, Westerlund (2019) upozorava kako ovakav sadržaj predstavlja značajnu prijetnju čovječanstvu zbog toga što: stvara pritisak novinarima da raspoznaju stvarne od lažnih vijesti, ugrožavaju nacionalnu sigurnost širenjem propagande i miješanjem u demokratske procese, smanjuju povjerenje građana državnim vlastima, te stvaraju probleme sigurnosti računalnih sustava organizacija i pojedinaca. Nadalje, samim time što ih je teško uočiti znači da se mogu smatrati opasnijima od ostalih načina širenja lažnih vijesti jer tako ljudi lakše povjeruju da ono što je lažno zapravo jest istinito. Primjerice, tijekom incidenta masovnog pucanja u Christchurchu na Novom Zelandu 2019. godine, jedna medijska kompanija širila je video u kojem je zločinac vidno upucan od strane policije, no otkriveno je da je snimka zapravo krivotvoreni sadržaj drugog incidenta koji se dogodio u Sjedinjenim Američkim Državama i da stvarni počinitelj ustvari nije ubijen (Westerlund, 2019).

Uvjerljivo krivotvoreni video sadržaji u kojima su prikazane osobe na visokim funkcijama u državnim službama kako govore ili rade nešto što u stvarnosti nisu nikada učinili samo će

usporiti tehnološko opismenjavanje društva i stvoriti nepovjerenje između stanovništva i autoriteta. Ako dođe do širenja lažnog videa u kojem neki političar uzima mito, priznaje suučesništvo u zločinu ili objavljuje rat drugoj državi, ubrzo može doći i do nemira, prosvjeda i sprječavanja demokratskih procesa u slučaju da države koje se nađu u lažnoj ugrozi odluče reagirati na takve prijetnje i stvore međunarodne sukobe. Primjerice, pojava izmijenjenog videa američke političarke Nancy Pelosi na društvenim mrežama u kojem djeluje pijano i pogrešno izgovara riječi stvorilo je veliku pomutnju među američkim narodom. Tadašnji američki predsjednik, Donald J. Trump taj lažirani uradak je podijelio na svojem Twitter profilu kako bi širio dezinformacije i propagandu o svojoj protivnici. Video je pregledan i podijeljen preko 2,5 milijuna puta na Facebook-u i unatoč pozivima političkih stranaka da se taj sadržaj ukloni, glasnogovornik Facebook-a izjavio je da videozapis neće biti uklonjen jer platforma nema pravila koja nalažu uklanjanje lažnih informacija, što su mnoge svjetske vlade vidjele kao poticaj da pokušaju regulirati načine uporabe „deepfake“ tehnologije (Awah Buo, 2020). Učestalo širenje ovakvih videa može dovesti do urušavanja kredibiliteta svih informacija i kreiranja apatije društva prema stvarnosti, a najveća prijetnja bit će to što će ljudi smatrati sve prijevarom (Westerlund, 2019).

Još jedna od prijetnji „deepfake“ sadržaja koje Awah Buo (2020) navodi jest krivotvorenje dokaza u sudskim procesima, čime bi se stvorio pritisak na sudove koji bi iziskivao puno resursa i vremena u svrhu autentifikacije dokaza prije nego što se mogu upotrijebiti na sudu. Kao primjer daje slučaj iz Ujedinjenog Kraljevstva u kojem je majka tijekom suđenja za skrbništvom nad djetetom predstavila „deepfake“ audio datoteku u kojoj otac prijeti djetetu kako bi majka poduprla svoju tvrdnju da je on nasilan i ne smije imati pristup djeci. Međutim, nakon što je datoteka forenzički pregledana, dokazano je da je lažna i sud ju nije prihvatio kao dokaz.

Ipak, ovakva tehnologija danas se koristi i u pozitivne svrhe. Filmske i modne industrije, tvrtke koje se bave razvojem video igara ili drugih zabavnih sadržaja, zdravstveni i obrazovni sustavi mogu stvarati korisni i edukativni sadržaj pomoću „deepfake“ tehnologije. Primjerice, glumcima koji su izgubili sposobnost govora može se vratiti digitalni glas; u post-produkciji stvarati posebni efekti ili uređivati lica, kao i poboljšati kvaliteta amaterskih videa, a lica preminulih glumaca mogu se prenijeti na tijelo drugog čovjeka čime se postiže efekt kao da je taj glumac zaista u filmu (Westerlund, 2019). Awah Buo (2020) također objašnjava kako se ova tehnologija može koristiti u zdravstvene i socijalne svrhe tako da pomaže pojedincima preboljeti gubitak voljene osobe kroz stvaranje njihove digitalne verzije. Nadalje, postoji i

potencijal u asistiranju u rehabilitacijskim procesima ovisnicima, poput kroničnih pušača. Svjetska zdravstvena organizacija razvila je umjetnu inteligenciju zvanu „Florence“ s kojom ljudi mogu razgovarati kako bi razvili samopouzdanje u vlastitu sposobnost prestanka pušenja i stvaranja plana kojim bi pratili svoj napredak, a u medicini, znanstvenici istražuju mogućnost korištenja generativnih suparničkih mreža (GAN) kako bi detektirali abnormalnosti u X-zrakama i uočili rane stadije nekih bolesti čime bi spasili mnogobrojne živote (Awah Buo, 2020).

4.3. Kako prepoznati „deepfake“ sadržaj

Usprkos tome što se „deepfake“ tehnologija veoma brzo razvija, postaje široko dostupna i uvjerljivo krivotvorene videozapise je gotovo nemoguće prepoznati, Johansen (2020) preporuča obraćanje pažnje na sljedeće karakteristike potencijalnih lažiranih sadržaja kako bi se razaznalo što je istinito, a što ne:

- Zubi ili kosa ne izgledaju stvarno zbog nemogućnosti tehnologije da stvori detaljne individualne karakteristike lica,
- Neprirodne boje subjekta u vidu abnormalne boje kože, čudnog osvjetljenja, nelogično postavljenih sjena,
- Nedostatak emocija na licu i neprirodni izrazi lica koji ukazuju na preklapanje dviju slika na jednom subjektu,
- Neprirodni pokreti tijela i držanje subjekta mogu sugerirati na lažirani sadržaj jer se „deepfake“ tehnologija uglavnom fokusira na realan prikaz lica umjesto tijela,
- Zamagljenost i neusklađenost dijelova tijela na mjestima poput glave i vrata,
- Nekonzistentna buka i zvuk zbog toga što se stvaratelji „deepfake“ videa više trude oko slike umjesto zvuka, što može dovesti do loše sinkronizacije usana i govora, robotskih glasova, čudnog izgovora riječi, digitalne pozadinske buke ili odsutnosti zvuka.

4.4. Budućnost s „deepfake“ tehnologijom

Zbog široke rasprostranjenosti „deepfake“ sadržaja kao i jednostavnost same tehnologije potrebne u stvaranju istih, navedene svrhe korištenja ovakvih uradaka s vremenom će dovesti do još prirodnijeg izgleda i težeg uočavanja lažiranih videa, te je stoga potrebno razviti

specifične strategije u borbi protiv takve vrste dezinformacija. Neke od koraka koje Awah Buo (2020) predlaže su postavljanje zakonskih regulativa, korporativnih politika i dobrovoljno preventivno djelovanje, obrazovanje i obuka, te ulaganje u razvoj tehnologije koja ima sposobnost detektiranja „deepfake“ sadržaja. Iako bi se zakonskom regulativom moglo utjecati na stvaranje lažiranih videa u državama koje takve zakone i propise donesu, oni svejedno neće imati učinak na stvaratelje koji se nalaze izvan tih pravno reguliranih država. Zato se korporativnim politikama i dobrovoljnim moderiranjem sadržaja, kao i brzim uklanjanjem „deepfake“ sadržaja kojeg identificiraju korisnici društvenih platforma, uz obrazovanje i poboljšanje digitalne pismenosti stanovništva može spriječiti rapidno širenje lažiranih uradaka. Državna tijela, tvrtke, edukatori i novinari trebaju osvijestiti građane o opasnostima ovakve tehnologije i upozoriti na njezinu primjenu u svrhu propagande i širenja dezinformacija kako bi se očuvalo povjerenje javnosti u javne medije i vlast (Awah Buo, 2020).

5. Zaključak

Iako je internet uvelike pomogao ljudima u njihovom obavljanju svakodnevnih aktivnosti, ne smiju se zanemariti i njegovi određeni negativni aspekti. Od najjednostavnijih prijevara u svrhu krađe male ili značajne količine novca, sve do krađe identiteta koja, osim financijskih gubitaka, nosi sa sobom i emocionalne posljedice kod žrtava. Isto tako, ne smije se propustiti i činjenica da su ovakvi zločini imali vremena za usavršavanje skoro od samog početka razvoja interneta i stoga počinitelji točno znaju profile ljudi koji će najvjerojatnije „zagristi mamac“ i postati žrtvom, a samim time što populacije na koje se fokusiraju nisu dovoljno informacijski pismene, njihov posao je znatno olakšan.

Danas postoji velik broj računalnih prijevara i svaka od njih namami znatnu količinu žrtava, djelomice zbog toga što se zločinci trude dizajnirati prijevaru tako da izgleda što službenije, čime ujedno i smanjuju razinu propitkivanja i povećavaju povjerenje od strane žrtve. Isto tako, samim time što se u slučaju prijevara koje zahtijevaju slanje e-pošte, poruka ili telefonskih poziva takve radnje već uvelike automatiziraju i šalju na masovnoj razini, uvijek postoji barem mali dio populacije koji će u njih povjerovati i učiniti ono što od njih prevarant i očekuje; to je dovoljno da se takvi zločini nastave u nedogled.

Osim prijevara koje od žrtve iziskuju direktne uplate financijskih sredstava, postoje također i one koje se predstavljaju malo kompleksnijima te djeluju na profinjeniji način. Lažne mjenjačnice kriptovaluta ili sheme nezamjenjivih tokena u kojima njihov osnivač nakon sakupljanja dovoljne svote novca pobjegne sa svim investicijama samo rastu u broju i popularnosti, a financijski gubitci u ovim slučajevima često prelaze nekoliko milijuna kuna i ostavljaju neoprezne ljude na rubu siromaštva.

Također, bitno je imati na umu da isto kao što postoji i tehnologija za digitalno preuređivanje slika poput programa Photoshop, tako se razvijaju i tehnologije za mijenjanje videa i glasova kako bi se stvorio i širio neistinit sadržaj koji se nikada nije dogodio. Iako takva „deepfake“ tehnologija ima potencijala biti korištena u korisne svrhe poput medicine ili različitih industrija, postoji i značajna mogućnost njezine upotrebe za cilj stvaranja političke propagande. Ako države ne reagiraju dovoljno brzo i donesu pravne okvire i regulacije kojom bi se korištenje ovakve tehnologije ograničilo, posljedice „deepfake“ sadržaja mogu biti trajne i opasne za održavanje mira u čovječanstvu.

6. Literatura

Awah Buo, S., 2020. The Emerging Threats of Deepfake Attacks and Countermeasures. *Department of Computing & Informatics Bournemouth University, UK*. [online] Dostupno na: https://www.researchgate.net/publication/347096267_The_Emerging_Threats_of_Deepfake_Attacks_and_Countermeasures [Pristupano: 4.7.2022.].

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L. and Serusi, S., 2021. Cryptocurrency Scams: Analysis and Perspectives. *IEEE Access*, [online] 9, pp.148353-148373. Dostupno na: https://ieeexplore.ieee.org/abstract/document/9591634 [Pristupano: 4.7.2022.].

Button, M. *et al*., (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, [online] 47(3), pp.391-408. Dostupno na: https://journals.sagepub.com/doi/abs/10.1177/0004865814521224 [Pristupano: 20.6.2022.].

CARNET, 2022. *Dan zaljubljenih, a ne prevarenih*. [online] Dostupno na: https://www.cert.hr/dan-zaljubljenih-a-ne-prevarenih/ [Pristupano: 20.06.2022.].

CARNET, 2022. *O socijalnom inženjeringu*. [online] Dostupno na: https://www.cert.hr/socijalni_inzenjering/ [Pristupano 20.06.2022.].

CARNET, 2022. *Phishing*. [online] Dostupno na: https://www.cert.hr/phishing/ [Pristupano: 20.06.2022.].

Consumer Advice. 2022. *Common Health Scams*. [online] Dostupno na: https://consumer.ftc.gov/articles/common-health-scams [Pristupano: 20.06.2022.].

Cross, C. i Blackshaw, D., (2014). Improving the Police Response to Online Fraud. *Policing*, [online] 9(2), pp.119-128. Dostupno na: https://academic.oup.com/policing/article-abstract/9/2/119/1454984?redirectedFrom=fulltext [Pristupano: 20.06.2022.].

Cross, C., (2019). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, [online] 20(3), pp.358-375. Dostupno na: https://journals.sagepub.com/doi/10.1177/1748895819835910 [Pristupano: 20.06.2022.].

Cummins, E., 2020. *The Nigerian prince scam is still fooling people. Here's why.*. [online] Popular Science. Dostupno na: https://www.popsci.com/story/technology/nigerian-prince-scam-social-engineering/ [Pristupano: 20.06.2022.].

Dinarević, M. i Softić, L., (2021). Razvoj, pojam i oblici cyber kriminala / Development, Concept and Forms of Cyber Crime. *Pregled: časopis za društvena pitanja / Periodical for social issues*, [online] 62(2), pp.125-141. Dostupno na: https://www.pregled.unsa.ba/index.php/pregled/article/view/1057 [Pristupano: 20.6.2022.].

Europol, 2018. *Internet Organised Crime Threat Assessment (IOCTA)*. Luxembourg: Publications Office of the European Union, pp.16-64.

Europol, 2021. *Internet Organised Crime Threat Assessment (IOCTA)*. Luxembourg: Publications Office of the European Union, pp.29-39.

Federal Trade Commission, 2022. *Common Health Scams*. [online] Dostupno na: https://consumer.ftc.gov/articles/common-health-scams [Pristupano: 20.06.2022.].

Griffiths, M., (2010). Crime and gambling: a brief overview of gambling fraud on the Internet. *Internet Journal of Criminology*, [online] pp.1-5. Dostupno na: https://irep.ntu.ac.uk/id/eprint/23349/ [Pristupano: 20.06.2022.].

Hrvatska udruga banaka, 2021. *Vodič o financijskim prijevarama*. [online] Dostupno na: https://www.hanfa.hr/vijesti/objavljen-hanfin-vodi%C4%8D-o-financijskim-prijevarama/ [Pristupano: 20.06.2022.].

Hrvatska udruga banaka, 2022. *Neželjene promotivne e-poruke*. [online] Dostupno na: https://www.hub.hr/sigurnost-na-internetu/vrste-prijevara/nezeljene-promotivne-e-poruke [Pristupano: 20.06.2022.].

Hrvatska udruga banaka, 2022. *Phishing*. [online] Dostupno na: <https://www.hub.hr/sigurnost-na-internetu/vrste-prijevara/phishing> [Pristupano: 20.06.2022.].

Interpol.int. 2020. *Global operation sees a rise in fake medical products related to COVID-19*. [online] Dostupno na: https://www.interpol.int/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19 [Pristupano: 20.06.2022.].

Ivezić, B., 2022. *Otkrivena prva velika hrvatska NFT prevara: Četiri mladića ukrala 2,8 mil. dolara*. [online] jutarnji.hr. Dostupno na: https://novac.jutarnji.hr/novac/aktualno/otkrivena-prva-velika-hrvatska-nft-prevara-cetiri-mladica-ukrala-2-8-mil-dolara-15189283 [Pristupano: 4.7.2022.].

Johansen, A., 2020. *What are deepfakes and how to spot them*. [online] us.norton.com. Dostupno na: https://us.norton.com/internetsecurity-emerging-threats-what-are-deepfakes.html#spot [Pristupano: 4.7.2022.].

Leonhardt, M., 2022. *'Nigerian prince' email scams still rake in over $700,000 a year—here's how to protect yourself*. [online] cnbc.com. Dostupno na: https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html [Pristupano: 20.06.2022.].

McAndrew, F., 2018. *Why We Still Fall for the "Nigerian Prince" Scam*. [online] Psychology Today. Dostupno na: https://www.psychologytoday.com/us/blog/out-the-ooze/201808/why-we-still-fall-the-nigerian-prince-scam [Pristupano: 20.06.2022.].

Milmo, D., 2022. *FBI offers $100,000 reward for help finding OneCoin 'Cryptoqueen'*. [online] theguardian.com. Dostupno na: https://www.theguardian.com/technology/2022/jul/01/fbi-offers-100000-reward-for-help-finding-onecoin-cryptoqueen-ruja-ignatova [Pristupano: 4.7.2022.].

Ministarstvo unutarnjih poslova, 2022. *Internet "CEO / direktorska" prijevara u Vinkovcima*. [online] Dostupno na: https://vukovarsko-srijemska-policija.gov.hr/vijesti/internet-ceo-direktorska-prijevara-u-vinkovcima/19067 [Pristupano: 20.06.2022.].

Ministarstvo unutarnjih poslova, 2022. *Internet prijevara*. [online] Dostupno na: https://mup.gov.hr/policijske-uprave/vijesti-1423/internet-prijevara-235768/232070 [Pristupano: 20.06.2022.].

Ministarstvo unutarnjih poslova, 2022. *Internetske prijevare - preventivni savjeti građanima*. [online] Dostupno na: https://zagrebacka-policija.gov.hr/vijesti/internetske-prijevare-preventivni-savjeti-gradjanima/89942 [Pristupano: 20.06.2022.].

Ministarstvo unutarnjih poslova, 2022. *Kako se zaštititi od računalnih prijevara?*. [online] Dostupno na: https://splitsko-dalmatinska-policija.gov.hr/prevencija-kriminaliteta-

32267/korisni-savjeti-32736/kako-se-zastititi-od-racunalnih-prijevara/37966 [Pristupano: 20.06.2022.].

Njuskalo.hr. 2022. *Općeniti savjeti - Njuškalo*. [online] Dostupno na: https://www.njuskalo.hr/index.php?ctl=help&content_id=119 [Pristupano: 20.06.2022.].

Psihologis. 2022. *Deepfake: tehnologija koja prijeti vjerodostojnosti medija*. [online] Dostupno na: https://psihologis.com/deepfake-tehnologija-koja-prijeti-vjerodostojnosti-medija/ [Pristupano: 4.7.2022.].

Rotenberg, K., 2019. *Inside the mind of the online scammer*. [online] The Conversation. Dostupno na: https://theconversation.com/inside-the-mind-of-the-online-scammer-127471 [Pristupano: 20.06.2022.].

Schlesinger, J. i Day, A., 2017. *Watch out, Nigerian con artists no longer hide behind princes in an attempt to steal your cash*. [online] cnbc.com. Dostupno na: https://www.cnbc.com/2017/10/18/nigerian-con-artists-have-new-ways-theyre-using-to-steal-your-cash.html [Pristupano: 20.06.2022.].

Sokanović, L., i Orlović, A. (2017). 'OBLICI PRIJEVARA U KAZNENOM ZAKONU', *Hrvatski ljetopis za kaznene znanosti i praksu*, 24(2), str. 583-615. Dostupno na: https://hrcak.srce.hr/196303 [Pristupano: 20.06.2022.].

Sorell, T., i Whitty, M., (2019). Online romance scams and victimhood. *Security Journal*, [online] 32(3), pp.342-361. Dostupno na: https://link.springer.com/article/10.1057/s41284-019-00166-w#citeas [Pristupano: 20.06.2022.].

Stoica, M., 2021. CRYPTOCURRENCY – DEFINITION, FUNCTIONS, ADVANTAGES AND RISKS. *Entrepreneurship and Trade*, [online] (30), pp.5-10. Dostupno na: http://www.journals-lute.lviv.ua/index.php/pidpr-torgi/article/view/935/886 [Pristupano: 4.7.2022.].

U.S. Food and Drug Administration. 2022. *Health Fraud Scams*. [online] Dostupno na: https://www.fda.gov/consumers/health-fraud-scams [Pristupano: 20.06.2022.].

Vidas, I., 2020. *Krađa identiteta - kako se zaštititi? | Zaštita osobnih podataka*. [online] Gdpr-2018.hr. Dostupno na: https://gdpr-2018.hr/33/kra-a-identiteta-kako-se-zastititi-uniqueidRCViWTptZHJrD63HGNzcj7rq1H43HBOkayX0xicUK50/ [Pristupano: 20.06.2022.].

Vrbanus, S., 2021. *Što su NFT-i i zašto ljudi za njih daju milijune?*. [online] Bug.hr. Dostupno na: https://www.bug.hr/blockchain/sto-su-nft-i-i-zasto-ljudi-za-njih-daju-milijune-19244 [Pristupano: 4.7.2022.].

Vuletić, I., i Nedić, T. (2014). 'Računalna prijevara u hrvatskom kaznenom pravu', *Zbornik Pravnog fakulteta Sveučilišta u Rijeci*, 35(2), str. 679-692. Dostupno na: https://hrcak.srce.hr/131272 [Pristupano: 20.06.2022.].

Westerlund, M., 2019. The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, 9(11), pp.39-52.

Yeboah-Boateng,, E. i Mateko Amanor, P., (2014). Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices. *Journal of Emerging Trends in Computing and Information Sciences*, [online] 5(4), pp.297-305. Dostupno na: https://www.semanticscholar.org/paper/Phishing%2C-SMiShing-%26-Vishing%3A-An-Assessment-of-Yeboah-Boateng-Amanor/7a271a3ff90b2a19d6b4f4ecc800e0aebdcda063 [Pristupano: 20.06.2022.].

zadarska-policija.gov.hr. 2021. *Internet prijevare - savjeti za građane*. [online] Dostupno na: https://zadarska-policija.gov.hr/vijesti/internet-prijevare-savjeti-za-gradjane/11115 [Pristupano: 20.06.2022.].

Metode prijevara na internetu

Sažetak

U radu se opisuju oblici prijevara na internetu, te kakvi se sve i na kakav način koriste razni tipovi dostupnih alata u takvim postupcima. U sklopu toga, objašnjavaju se najčešći primjeri takvih prijevara koje dolaze putem e-pošte ili drugih kanala, kao i zakonski okviri izvan kojih operiraju i pomoću kojih izbjegavaju kazne, a ujedno se skreće pažnja i na korake koje pojedinac može poduzeti kako bi takvo što spriječio. Također, ukazuje se na opasnost uporabe tzv. „deepfake“ tehnologije u svrhu obmane javnosti i širenja lažnih vijesti i propagande kao jedan od načina prevare korisnika interneta. Isto tako, opisuje se korištenje navedene tehnologije u političke svrhe, njezina primjena u budućnosti i sažetak najboljih načina kako raspoznati što je „deepfake“ video, a što nije. Kao još jedan od načina Internet prijevara u novije doba, spomenute su i neke kriptovalute i NFT-ovi koji u posljednje vrijeme rastu u popularnosti pod krinkom moguće „brze zarade“.

Ključne riječi: internet, prijevare, deepfake, kriptovalute, NFT

Methods of Internet Scams

Summary

This paper describes the various types of scams that exist on the Internet and how different tools are used to successfully commit crimes. Alongside this, the most common examples of such scams are mentioned, as well as the legal frameworks outside which criminals operate and avoid punishment. At the same time, an emphasis is put on the safety steps that individuals can take in order to avoid becoming victims of online fraud. Furthermore, the use of the so-called “deepfake” technology for the purpose of deceiving the public, spreading fake news and propaganda is explained. In addition, the paper also warns about the use of such technology for political purposes and its application in the future, with a description of the best ways how to recognize what is or is not a “deepfake” video. The subject of the rising popularity of cryptocurrency and NFTs, which appeared under the guise of “easy money” in more recent times, is mentioned as well.

Key words: internet, scams, deepfake, cryptocurrency, NFT