FBIM Transactions
DOI 10.12709/fbim.07.07.02.15

PREVARE PUTEM INTERNETA: SAJBER ZABAVA KOJA „PRAZNI" RAČUNE ŠIROM SVETA

INTERNET FRAUD: CYBER ENTERTAINMENT THAT "CLEANS" BANK ACCOUNTS WORLDWIDE

Vida M. Vilić
Klinika za stomatologiju Niš, Niš, Srbija

JEL Kategorija rada: **L86**

Apstrakt

Postoje različiti oblici prevara putem Interneta, a kako najveći broj izvršilaca ovog dela pripada mlađoj populaciji, stiče se utisak da je ova vrsta kriminalne aktivnosti postala sve češća zabava mlađih ljudi koji su vešti u poznavanju informaciono-komunikacionih tehnologija. Pojavni oblici prevara su mnogobrojni i zbog različitih načina njihovog izvršenja nemoguće ih je u potpunosti sagledati. U praksi se javljaju kako primitivne i grube prevare tako i one prevare kod kojih učinioci ispoljavaju visok stepen veštine. Kao česti oblici Internet prevara javljaju se „Valentino" prevare, „lančana pisma", piramidalne šeme, „lutajući" trgovci, transfer novca u dobrotvorne svrhe i lutrijske prevare, dok je svakako jedan od najčešće viđenih oblika sa kojim se svako od nas susreo u svom poštanskom sandučetu tzv. "Nigerijska prevara". Prevare putem Interneta u Republici Srbiji još uvek nisu pravno regulisane. U toku 2008. i 2009. godine na teritoriji Republike Srbije prijavljeno je devet krivičnih dela prevare sa elementima „nigerijskih" prevara protiv nepoznatih učinilaca, dok je na svetskom nivou procena da su Internet prevare dostigle svoj vrhunac 2009. godine. Pored definisanja i klasifikacije najčešćih pojavnih oblika prevara putem Interneta, u radu su dati i neki praktični saveti kako sprečiti viktimizaciju od prevarnog ponašanja na Internetu.

Ključne reči: *Prevare putem Interneta, računarske prevare, nigerijska prevara, krivično delo prevare*

Abstract

There are various forms of Internet frauds, and since most of the perpetrators belong to the younger population, it seems that this type of criminal activity has become even more and more fun for younger people with great knowledge and practical skills in the field of information and communication technologies. There are many forms of this act, because of the many different modus operandi, so it is almost impossible to

Adresa autora:
Vida M. Vilić
e-mail: vila979@gmail.com

fully understand and to explain them, or even harder to prevent them. Common forms of Internet scams include so-called "Valentine" scams, "chain letters", pyramidal schemes, "wandering" merchants, charity transfers and lottery scams, while certainly one of the most commonly seen form we've encountered are so-called "Nigerian scams". In the Republic of Serbia, Internet fraud is not yet legally regulated as criminal acts. During 2008 and 2009, nine criminal offenses with elements of "Nigerian scam" were reported in the territory of the Republic of Serbia against unknown perpetrators, while at the global level, it is estimated that this particular kind of Internet fraud reached its top in 2009. In addition to defining and classifying the most common forms of Internet frauds, this paper also provides some practical tips on how to prevent victimization from fraudulent behavior on the Internet.

***Keywords**: Internet scams, computer fraud, Nigerian scam, fraud*

1 UVOD

Dosadašnja proučavanja i postojeća zakonska regulativa na međunarodnom i nacionalnom planu odnose se uglavnom na zloupotrebu računarskog hardvera i softvera, koji prilikom izvršenja krivičnih dela mogu da budu sredstvo izvršenja ili objekat napada (npr. kompjuterske krađe, prevare, oštećenje računarskih podataka i programa, sabotaža, pravljenje i unošenje računarskih virusa). Jedan od oblika devijantnog ponašanja koje još uvek nije regulisano krivičnim zakonodavstvom Republike Srbije jesu prevare putem Interneta. Transnacionalno posmatrano, ovaj fenomen je sve više prisutan u sajber prostoru, njegove žrtve su sve brojnije a pretrpljene materijalne štete sežu i do nezamisliih razmera. Postoje različiti oblici prevara putem Interneta, a kako najveći broj izvršilaca ovog dela pripada mlađoj populaciji, stiče se utisak da je ova vrsta kriminalne aktivnosti postala sve češća zabava mlađih ljudi koji su vešti u poznavanju informaciono-komunikacionih tehnologija.

2 ŠTA SU PREVARE PUTEM INTERNETA

Prevara, kao krivično delo, stara je koliko I ljudski rod, i za sve vreme nisu se promenili ni pojam prevare ni efekat koji prevara ima na žrtvu (Koong, Liu & Wei, 2012: 442). Prevare putem Interneta predstavljaju najrašireniji oblik sajber kriminaliteta, o kome se prvi put govori još 1996. godine ali sa veoma malo konkretnih detalja o pojavnim oblicima. Ova dela treba razlikovati od računarskih prevara kada se u računar unose netačni podaci ili se propušta unošenje tačnih podataka ili se na bilo koji drugi način računar koristi za ostvarivanje prevare putem prikrivanja ili lažnog prikaza podataka, a sve u cilju sticanja protivpravne materijalne koristi kojom se drugome prouzrokuje imovinska šteta (Vilić, 2016, str. 203).

Krivični zakonik Republike Srbije (2005) sadrži propise materijalnopravnog karaktera, koji se odnose na kompjuterski kriminalitet, predviđajući krivična dela protiv bezbednosti računarskih podataka, ali i druga krivična dela koja se na osnovu Konvencije o visokotehnološkom kriminalu (čl. 8) i pozitivnopravnih zakonskih propisa smatraju krivičnim delima kompjuterskog kriminaliteta (Vilić, 2017, str 118). U okviru krivičnih dela kompjuterskog kriminaliteta koja se odnose na bezbednost računarskih podataka (Glava XXVII), predviđeno je krivično delo "računarska prevara" (čl. 301).

Radnje izvršenja ovog krivičnog dela sastoje se svakom umišljajno učinjenom delu unošenja, menjanja, brisanja ili prikrivanja kompjuterskih podataka ili ometanju funkcionisanja kompjuterskih sistema kojim se drugim licima nanosi veća imovinska šteta, a u nameri pribavljanja veće imovinske koristi sebi ili drugom licu. Za pravilnu kvalifikaciju krivičnog dela i dokazivanje računarske prevare potrebno je, pored ostalog, tačno utvrditi radnju koja je preduzeta, način unošenja neistinitog podatka, u čemu se neistinitost ogleda i kakav je bio uticaj na rezultat elektronske obrade i prenosa podataka.[1]

[1] U domaćoj sudskoj praksi zabeleženo je nekoliko slučajeva procesuiranja krivičnog dela računarske prevare. Tužilaštvo za borbu protiv visokotehnološkog kriminala pokrenulo je istragu protiv osumnjičenog Č. A. zbog osnovane sumnje da je tokom 2007. i 2008. godine u dva navrata koristeći računar ulazio u sisteme banaka u Australiji i Švajcarskoj i izdavao lažne naloge za transfer sredstava, čime je pribavio protivpravnu

Krivično delo računarske prevare treba razlikovati od klasičnog krivčnog dela prevare (čl. 208 KZ RS) koje pripada imovinskom kriminalitetu, odnosno grupi krivičnih dela protiv imovine. Iako u zakonu nije izričito naglašeno, krivično delo prevare može se izvršiti i korišćenjem računarskih tehnologija. Pojava Interneta otvorila je široke mogućnosti za vršenje krivičnog dela prevare, povećala broj potencijalnih žrtava i skoro sasvim otklonila troškove potrebne za izvršenje krivičnog dela. Načini izvršenja prevara korišćenjem kompjutera i Interneta su različiti, izvršioci su potpuno anonimni, a žrtva može da postane svako ko koristi računarsku tehnologiju.

Prevara putem Interneta nije uvek i obavezno računarska prevara, jer neke Internet prevare odgovaraju klasičnim prevarama koje za sredstvo izvršenja imaju Internet bez nekog posebnog uticaja na elektronsku obradu podataka ili rad računara. Prevarom putem Interneta obmanjuju se ljudi, dok se računarskom prevarom „obmanjuje“ računar i elektronska obrada navodi na pogrešan rezultat koji je usmeren na sticanje protivpravne imovinske koristi (Babović, 2004, str. 749-750).

Prevara putem Interneta ili Internet prevara odnosi se na bilo koju prevaru pri čijem izvršenju lice koje u nameri pribavljanja protivpravne imovinske koristi za sebe i drugoga, iskoristi jednu ili više komponenti Interneta, kao što su sobe za ćaskanje, veb stranice ili elektronska pošta, da bi se stvorili uslovi za lažno prikazivanje ili prikrivanje činjenica kojim bi se neko lice dovelo u zabludu ili u njoj održavalo, da bi to lice učinilo nešto na štetu svoje ili tuđe imovine (sprovođenje finansijske transakcije, prenošenje podatka finansijskoj instituciji koja je meta napada i sl.) (Matijašević, Spalević & Ignjatijević, 2012, str. 563).

3 NAJČEŠĆI POJAVNI OBLICI INTERNET PREVARA

Raznolikost i obim različitih vrsta mrežnih prevara teško je odrediti iz više razloga. Pojavni oblici prevara su mnogobrojni, zbog različitih načina njihovog izvršenja nemoguće ih je u potpunosti sve sagledati jer se u praksi javljaju kako primitivne i grube prevare tako i one prevare kod kojih učinioci ispoljavaju visok stepen veštine. Takođe, prevare putem Interneta se retko prijavljuju, a mnoge prevare putem Interneta koriste kombiacije različitih vrsta krivičnih dela (Button, McNaughton Nicholl, Kerr.& Owen, 2014, str. 396).

Kao čest oblik Internet prevara javljaju se: „valentino“ prevare, „lančana pisma“, piramidalne šeme, „lutajući“ trgovci, transfer novca u dobrotvorne svrhe i lutrijske prevare.

- „Valentino“ prevare su povezane sa „uslugama“ koje se pružaju usamljenim osobama koje žele da sklope brak ili da stupe u kontakt sa nekom osobom radi druženja. Posle određene pripreme, koja obuhvata komuniciranje mejlovima i razmenu fotografija, prevarant predlaže lični kontakt sa žrtvom pod uslovom da mu uplati određenu sumu novca kako bi doputovao do mesta susreta. Posle transfera novca, svaki kontakt sa žrtvom prestaje.
- „Lančana pisma“ sadrže zahtev upućen mejlom da se dobijeni mejl prosledi određenom broju prijatelja i ukoliko se to ne učini, osobu će zadesiti neka nesreća. Ovakva pisma sadrže kriptovane informacije, koje će licu koje je poslalo lančano pismo omogućiti da sazna lične podatke velikog broja lica i da ih zloupotrebi.
- Piramidalne šeme predstavljaju takvu vrstu prevara kod kojih se žrtvi obećava isplata određene svote novca za „privlačenje“ određenog broja ljudi i uključivanje u rad „piramide“.
- „Lutajući trgovci“ se bave prodajom nepostojeće robe, robe lažnog kvaliteta, koja može biti opasna po zdravlje, traže mejlovima isplatu novca, ali nikad ne izvrše isporuku.
- Kod prevare transferom novca u dobrotvorne svrhe od žrtve se traži da za određenu proviziju primi na svoj bankovni račun

imovinsku korist u iznosu od 51.990 CHF, odnosno da je pokušao da iz jedne švajcarske banke neovlašćeno izvrši transfer sredstava u iznosu od 19.000 USD. Takođe je zabeleženo više slučajeva zloupotrebe računarskih sistema računarskih mreža u sportskim kladionicama. Izvršioci na različite načine pokušavaju da utiču na rezultat elektronske obrade podataka i koristeći softverska rešenja falsifikuju odigrane tikete. Više o tome: Nikolić, K. i dr., 2010, str.102-103 i Prlja, D., Ivanović, Z. & Reljanović, M., 2011, str. 173.

određenu sumu novca, podigne ga sa računa i uplati na neki račun u inostranstvu, sa obrazloženjem da će novac biti iskorišćen u dobrotvorne svrhe. Provizija za ovakvu transakciju se ne dobija, a ovakvim transferom se prikriva poreklo novca („pranje novca“).

- Lutrijske prevare se sastoje u tome što žrtvi stiže obaveštenje da je dobitnik neke premije i da pošalje određenu svotu novca u cilju dobijanja te nagrade ili se traži da žrtva navede broj svog bankovnog računa i određene lične podatke, što će svakako biti zloupotrebljeno.

Prema istraživanju Američkog udruženja za zaštitu potrošača za otkrivanje najčešćih Internet prevara (National consumers league – NCL), koje je sprovedeno 2006. godine (The top 10 Internet Frauds, 2017, *n.d.*), najčešće Internet prevare su navedene u tabeli 1.

Tabela 1. Vrste i frekvencija pojave Internet prevara

Mesto / zastupljenost u ukupnom broju	Internet prevare		
	Naziv prevare	**% žalbi u odnosu na ukupan broj**	**Prosečan gubitak u USD**
1.	Internet aukcije	34%	1.331
2.	Prodaja preko Interneta	33%	1.197
3.	Plaćanje lažnim čekovima	11%	4.053
4.	„Nigerijske prevare“	7%	3.741
5.	Lažne lutrije	4%	1.750
6.	Lažni zajmovi	3%	1.515
7.	Fišing	2%	/
8.	Nagradne igre	1%	2.447
9.	Prevare provajdera	1%	920
10.	Investicije	1%	4.759

Isto udruženje je i narednih godina analiziralo vrste najčešćih Internet prevara, a 2019.godine je u okviru projekta „Fraud.org“ objavilo podatke koje su bile najzabeleženije vrste Internet prevara tokom 2018. godine (Top ten scams of 2018, 2019, *n.d.*), Tabela 2.

Tabela 2. Najčešćih 10 Internet prevara tokom 2018. godine

Mesto / zastupljenost u ukupnom broju	Internet prevare	
	Naziv prevare	**% žalbi u odnosu na ukupan broj**
1.	Prodaja preko Interneta	31,25%
2.	Nagradne igre i besplatne stvari	16,97%
3.	Plaćanje lažnim čekovima	13,09%
4.	Lažni zajmovi koji se daju pravnim licima	7,63%
5.	Lažni zajmovi i krediti	7,37%
6.	Fišing/Spufing	4,84%
7.	Prevare iskorišćavanjem virtuelnih prijateljstava	2,81%
8.	Oprema za kompjutere i kompjuterski softver	2,23%
9.	Stipendije i donacije	1,63%
10.	Iznuđivanje i ucenjivanje porodice ili prijatelja	1,41%

Prevare prilikom različitih Internet prodaja postale su tokom 2018. godine najčešće vršene Internet prevare, čija se radnja izvršenja dela sastoji u tome da žrtva naruči i plati robu koja mu/joj nikada ne bude isporučena. Primećen je porast prevara koje su zasnovane na zloupotrebi ličnih odnosa žrtve i učinioca (rođački odnosi, prijateljski ili intimno partnerski odnosi), pri čemu se radnja izvršenja sastoji u zadobijanju nečijeg poverenja, razvijanju veze između žrtve i učinioca i ubeđivanju žrtve da učiniocu pošalje novac. Ipak, najveći porast je primećen u broju slučajeva fišinga. Krađa identiteta putem elektronske pošte (fišing, eng. phishing) sastoji se u slanju e-mail poruke korisniku u kojoj se navodi da poruku šalje legitimno pravno lice ili ovlašćena osoba tražeći lične podatke i privatne informacije (Vilić, 2019, str. 46). Navodi u poruci su lažni, a ukoliko primalac napiše podatke koji se traže, oni će kasnije biti iskorišćeni za krađu identiteta.

U najčešće vršene Internet prevare spadaju i prevare putem Internet promocija, kreditnih kartica, piramidalne novčane prevare putem multi level marketinga, poslovne ponude i pogotovo rad od kuće, investicione prevarne šeme poput „kako se lako obogatiti”, prevare sa putovanjima kao i prevare korišćenjem tuđih brojeva zdravstvenog osiguranja (Computer Crime Research Center: Fraud in the Internet, 2005). Među često vršene

prevare spadaju prevare prilikom Internet kupovine automobila i aukcijske i maloprodajne novčane prevare preko Interneta.

Prilikom kupovine automobila preko Interneta, prevarant oglašava da se po veoma pristupačnoj ili čak niskoj ceni prodaje nepostojeće vozilo, najčešće luksuzan ili skup sportski auto, čija regularna cena može da bude i nekoliko puta veća od tražene. Detalji o vozilu su najčešće preuzeti sa drugih sajtova koji se bave prodajom automobila preko Interneta i deluju vrlo primamljivo, pa zainteresovani kupci nadajući se povoljnoj kupovini kontaktiraju prevaranta, koji daje instrukcije žrtvi prevare da pošalje depozit ili celu uplatu preko elektronskog transfera kako bi pokrenuo proces „špedicije“, pošto se traženi automobil obično nalazi u inostranstvu. Prevarant može takođe da nabavi podatke o vozilu koje navodno pokušava da proda preko Interneta tako što će kontaktirati nekoga ko zaista pokušava da proda vozilo preko Interneta, pitajući ga za broj šasije vozila kako bi proverio zapise o nesrećama sa tim vozilom. Prevarant će zapravo taj broj iskoristiti da upotpuni sliku o vozilu koje navodno on prodaje.

Kod aukcijske i maloprodajne novčane prevare preko Interneta prevarant započinje prodaju po veoma povoljnoj ceni preko Interneta na sajtovima koji su za to specijalizovani. Najčešće su u pitanju skuplje i vrednije stvari ili ponekad i kolekcionarski primerci. Prevarant prihvata uplatu od pobednika virtuelne aukcije ili kupca u Internet prodavnici, ali mu uopšte ne isporučuje stvar za koju je dobio novac ili mu isporučuje predmet čija je realna vrednost znatno manja od one za koju je žrtva dala novac (npr. falsifikat ili korišćen predmet umesto novog).

Za izvršenje navedenih dela, prevaranti najčešće koriste fišing tehnike kako bi „oteli“ podatke sa naloga legitimnih korisnika ili naloge sa veoma pozitivnom reputacijum na Internetu i koriste ih da postave lažne virtuelne prodavnice. Prevarant ovakvim postupkom istovremeno sakuplja novac za sebe, a dok žrtva prevare shvati da nije dobila ono za šta je dala novac, za krivično delo prevare će biti optužen pravi nosilac naloga čiji je identitet prevarant preuzeo.

4 „NIGERIJSKA PREVARA” ILI „PREVARA 419”

Jedna od najpoznatijih svetskih, tzv. investicionih Internet prevara (engl. Advance-fee fraud) je „Nigerijska prevara” ili „Prevara 419”. Radnja ovog dela sastoji se u pribavljanju imovine putem prevarnih radnji, a koja može da podrazumeva ulaganje određene svote novca u određeni „posao“, uz obećanje da će se kao benefit ostvariti znatno veća suma novca od uložene (Matijašević, Spalević & Ignjatijević, 2012, str. 563).

Nekoliko nezaposlenih studenata sa nigerijskog univerziteta počelo je ranih osamdesetih godina XX veka da prevarom uzima novac od poslovnih ljudi sa zapada. Izraz „prevara 419” dobila je naziv po članu broj 419 Nigerijskog krivičnog zakona koji definiše i sankcioniše krivično delo prevare. Iako je po samom nazivu dela vezana za Nigeriju, ova vrsta prevare vezuje se i za sledeće zemlje iz kojih potiču izvršioci ovog dela: Togo, Burkina Faso, Gana, Benin, Obala Slonovače, ali i Južna Afrika, Španija, Holandija i Velika Britanija

Kriminalna aktivnost izvršilaca sastoji se u slanju elektronske poruke koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke, a počinje ubeđivanjem potencijalne žrtve prevare da učestvuje u podeli novčanih fondova ako unapred uplati određeni iznos koji je, u najvećem broju slučajeva, neuporedivo manji od onog iznosa koji bi trebalo da dobije kao korist od tog fonda. Elektronskom porukom se od potencijalne žrtve traži pomoć za transfer velikih novčanih iznosa, a ona će zauzvrat dobiti određeni procenat kao nagradu. U porukama se takođe navodi da je reč o izuzetno velikoj sumi novca, da je pošiljalac poruke član nigerijske vlade ili vojske, da je spreman da podeli novac sa osobom koja mu pomogne da se transfer izvrši i da je neophodno da ceo postupak ostane u najstrožijoj tajnosti. Ukoliko žrtva pristane da učestvuje u sprovođenju ove transakcije, dostavljaju joj se falsifikovani dokumenti, na osnovu kojih će žrtva uplatiti određeni novčani iznos prema instrukcijama koje je dobila. Nakon toga, počinje odlaganje novčanih transakcija, povećanje troškova transakcija, vrši se pritisak na žrtvu, koja posle dužeg vremena shvata da je prevarena.

Pisma sa elementima "Nigerijske prevare" su se 2016. godine u Srbiji pojavila i na lošem srpskom jeziku, pa čak i na ćiriličnom pismu, jer izvršioci ovog dela, korišćenjem usluge *Google translate,* pokušavaju da dođu do što šireg kruga ljudi koje bi prevarili, a koji ne poseduju dovoljno znanja engleskog jezika kako bi sledili postupak koji je u originalnom prevarnom pismu naveden. Kako ovaj alat za prevođenje tekstova nije baš najpouzdaniji i najprecizniji u prevodu na srpski jezik, moguće je lako uočiti da poruka nije verodostojna i da ima potencijalni prevarni karakter.

Model pisma „Nigerijske prevare“ (Model 1):

“INVESTMENT ASSISTANCE

Sir,

With due respect, trust and humility I write you this proposal which I believe would be of great interest to you. I am MRS TINA GOGO the wife of late DR. DONALD GOGO of blessed memory. Before my husband was killed by rebel forces loyal to Major JOHN PAUL KOROMAH. He was the Director General Gold and Diamond Mining Corporation (G.D.M.C.) of Sierra Leone.

Two days before his death, he managed to sneak a written message to me, explaining his condition and concerning trunk box of valuables containing money and diamonds, which he concealed under the roof. He instructed me to take our children and move out of Sierra Leone immediately to any neighbouring country. Eventually it resulted into full war, I became a widow overnight, helpless in this hopeless situation.

Daughter and I my son managed to escape to Abidjan, Ivory Coast through the help of my husband’s friend. The cash inside the box was USD $ 25.5 MILLION (TWENTY FIVE MILLION FIVE HUNDRED THOUSAND US DOLLARS), and DIAMOND, due to fear and limit right as a refugee I deposited the items with private security company with my son’s name MR. JOGO GOGO (JR). Be informed that the real content of the boxes were not disclosed to the security company as these were deposited as personal effects for security reasons. Meanwhile I want to travel out of Ivory Coast entirely with this money for investment in your country because of the unsuitable political situation and mostly for the future benefit of my children. I want you to assist us get the money out of the Security Company and transferred into your nominated private account in your country. You shall also source for good investment, so that we can invest the money wisely.

*Concerning the money, we are prepared to give you 20% of the total sum and 5% mapped out for expenses. For the interest of this business do not hesitate to call my son MR JOGO GOGO (JR) on telephone number ********** or email address: ********** immediately you receive this message for more information to enable us proceed in earnest towards concluding all arrangements, no other person knows about this money expect I, my son and you.*

Awaiting your most urgent response.
Thanks for your co-operation and GOD bless you.”

Model pisma „Nigerijske prevare“ (Model 2):

“Poštovani,

Treba mi hitna pomoć,

Dobar dan. Znam da vam ova pošta može doći kao iznenađenje. Molim vas, nemojte se ljuti na mene što ste primili moju poštu. Uzmite me kao svoju kćerku ili kao sestru. Videla vašu adresu e-pošte putem online poslovnog imenika tokom moje pretrage. Poštena sam osoba i kontaktirala sam te lično, jer sam ozbiljno trebala vašu pomoć.

Moje ime je Mari Frank. Ja imam 20 godina i jedina sam dete mojih pokojnih roditelja Mr. and Mrs Frank. Moj otac je dugi niz godina radio sa preduzećem za naftu i gas i deponovao je ukupno dva miliona evra u moje ime pre nego što je umro 2014. godine. Tokom ovog depozita, moj otac je imao saglasnost sa bankom da mi novac neće biti direktno dat sve do 25 godina ili više. Molim vas, hoćete da mi pomognete da prebacim ovaj novac na vaš bankovni račun za investicije i da vam pomognem da dođem u vašu zemlju da nastavim sa školovanjem, jer moj ujak želi da me ubije i sakupi moj novac za nasleđe, jer sam ja mala devojčica.

Prijavila sam ga u lokalnoj policiji moje zemlje, Obale Slonovače, ali policija nije učinila ništa da mi pomogne. Od tada i moj život je u velikom riziku ovde u mojoj zemlji. Pišem vam ovu poštu

iz lokalnog hotela u kome se trenutno krijem za moju sigurnost dok ne odem iz svoje zemlje nakon prenosa. Ja sam voljna da vam ponudim 20 odsto ukupnih sredstava kao nadoknadu za vašu pomoć nakon transfera i želim da mi hitno odgovorite ako prihvatite da mi pomognete da vam pošaljem više detalja.

Hvala i Bog blagoslovio,

Gospođica Mari Frank"

„Nigerijske prevare" dostigle su na globalnom nivou svoj vrhunac 2009. godine, kada su žrtve prevara, prema podacima holandske kompanije Ultrascan (Ultrascan Advanced Global Investigations, 2018, *n.d.*), izgubile gotovo 50% više novca nego 2008. godine. Prema izveštaju ove kompanije, koja je analizirala 8.503 slučaja u preko 152 zemlje u toku 2009. godine, žrtve su izgubile 9,3 milijarde dolara u odnosu na 6,3 milijarde dolara 2008. godine (*Ibid.*). Ukupno 51.761 prevara je počinjena iz 69 svetskih zemalja, dok je ostalih 250.000 prevara počinjeno iz Nigerije (*Ibid.)*.

U Srbiji je, prema podacima Tužilaštva za visokotehnološki kriminal, prvi slučaj jednog od oblika "Nigerijske prevare" prijavljen 2009. godine, kad je jedan građanin ostao bez 2.500 dolara (Brkić, 2017), dok je kasnije prijavljena i slična aktivnost, čija se radnja izvršenja dogodila 2008. godine. Ukupno, tokom 2008. i 2009. godine na teritoriji Republike Srbije izvršeno je i prijavljeno devet krivičnih dela prevare sa elementima „nigerijskih prevara" protiv nepoznatih učinilaca, pri čemu je ukupna imovinska šteta iznosila preko 60.000 evra (Urošević, 2009). Oštećena lica su novac izvršiocima krivičnih dela slala preko servisa Western Union i MoneyGram, uglavnom preko besplatnih naloga za elektronsku poštu koja je otvarana na Internet servisima koji omogućuju besplatne naloge elektronske pošte. Nakon što se prevara prijavi, neophodno je prikupiti sve elektronske dokaze koji ukazuju na ostvarenu komunikaciju između izvršilaca krivičnog dela i oštećenih, kao i podatke o finansijskim transakcijama koje je oštećeni izvršio prema instrukcijama koje je dobio od izvršilaca. Pokušava se da se pronađe IP adresa i locira server sa koga su izvršioci krivičnog dela slali elektronske poruke oštećenom, prikuplja se pregled celokupne elektronske pošte koju je oštećeni primio, a zatim se preko Interpola vrše provere korisnika kome je ova adresa bila dodeljena u trenutku vršenja krivičnog dela (*Ibid.)*. Korišćene su lažne Internet adrese, Internet portali, falsifikovana dokumentacija državnih organa i preduzeća Nigerije, Gane i drugih država sa teritorije Zapadne Afrike. Izvršioci su najčešće svu korespodenciju obavljali sa javnih mesta, kao što su Internet kafei, kako ne bi moglo da im se uđe u trag.

Interesantan slučaj "Nigerijske prevare" dogodio se mladiću (23) iz Beograda, koji je 2012. godine na jednom Internet sajtu objavio oglas da prodaje kuću. Na oglas se javio navodno državljanin Velike Britanije, koji je rekao da želi da se preseli u Srbiju, da želi da dođe da pogleda svoj budući stambeni prostor i od prodavca je zahtevao da mu pošalje svoju adresu, kopiju lične karte i adresu na kojoj se nalazi kuća, kako bi od službenika carine dobio neophodna dokumenta, vizu i putne isprave za preseljenje i ocarinjenje svog pokućstva koje bi doneo u Srbiju prilikom navodnog preseljenja. Kupac je prodavcu slao svoje fotografije i fotografije svoje porodice, kako bi sa njim uspostavio prisnu prijateljsku vezu, autentične dokumente nadležnih institucija, troškovnike i različite sertifikate. Jednog dana, ovaj navodni kupac je prodavca obavestio da je kupio avionske karte, ali, da bi ocarinio svoje stvari, prodavac treba da reguliše plaćanje slanja i preuzimanja ovih stvari, kao i angažovanja carinika. Prodavac je to učinio na način na koji je od njega kupac tražio, uplaćujući na račune koje mu je takođe kupac davao, čime je izgubio oko 640.000 dinara. Sam prodavac je naveo kako mu ništa nije delovalo sumnjivo i kako je celokupan ovaj postupak trajao skoro dve godine. Shvatio je da je prevaren tek kada je shvatio da mu mejlove ne šalju nadležne službe na koje se kupac pozivao, kada se konačno obratio policiji i Upravi za visokotehnološki kriminal. Prijava je prosleđena Višem sudu u Beogradu, koji je pokrenuo pretkrivični postupak, dok Interpol dalje procesuira slučaj (Čuvajte se – Nigerijska prevara u Srbiji, 2014, *n.d.*).

Drugačija vrsta "Nigerijske prevare" zabeležena je 2018. godine u Kosjeriću, kada su se u ulozi žrtava našla dva oženjena muškarca iz Kosjerića, koji su, iako su bili dobro nasamareni i oštećeni

za 550 evra, ipak skupili hrabrosti i policiji prijavili šta im se dogodilo. Naime, obojica su preko društvenih mreža dobili zahteve za prijateljstvo od navodnih profila atraktivnih devojaka bele puti pod imenima Seli i Monika. Kako su obojica ušli sa njima u prepisku koja je prerasla u otvoreni flert i slanje nagih fotografija intimnih delova tela i video snimaka istih, ubrzo su im stigle poruke da ukoliko ne uplate po 1000 EUR, ove slike i video snimci će biti prosleđeni njihovim porodicama i prijateljima. Uz poruku je bila napisana i adresa za transfer novca, a zahtevani rok za isplatu bio je pola sata. Ova avantura je jednog od dvojice muškaraca koštala 300, a drugog 250 EUR, jer su im ucenjivači poverovali da nemaju više od toga da plate (Čuvena nigerijska prevara opet hara Srbijom, 2018).

Tokom 2016. godine, "Nigerijske prevare" su se u Srbiji raširile i na društvene mreže i na sajtove za masovnu trgovinu. Jedna od meta napada bio je i sajt za trgovinu *Limundo*, čiji su administratori odmah detektovali pokušaj prevare, obavestili regtistrovane članove ovog portala i dali im smernice o poželjnom ponašanju u slučaju viktimizacije od ove vrste Internet prevare (Divković, 2018). Radnje napada su se sastojale u pokušaju prevare prodavaca na ovom sajtu, ostavljanju ličnih poruka sa molbom da se uplati novac zbog neke nesreće koja je nastala, pokušaju dopisivanja radi ostvarivanja bliske I emotivne veze kako bi se zatim tražio novac, lažnim zahtevima za odobravanje kredita kojima bi se prikupljali detaljni lični podaci registrovanih korisnika sajta koji bi potom bili zloupotrebljeni u nekoj drugoj Internet prevari I sl. Tokom 2017. godine samo na sajtu *Limundo* zabeleženo je 28 pokušaja ovakvih prevara (Ibid.). Svi ti pokušaji su brzo detektovani, nalozi su suspendovani, pa oštećenih korisnika ovog sajta nije bilo.

Veliki broj prevara putem Interneta omogućen je društvenom interakcijom preko društvenih mreža (Vilić, 2013, str. 188), pri čemu svi oblici krivičnih dela i devijantnih ponašanja koja se na njima pojavljuju mogu da imaju oblik bilo kog tradicionalnog krivičnog dela. U istraživanju koje je sprovedeno 2014. godine u kome je učestvovalo 612 ispitanika i ispitanica starosti od 9 do 65 godina (Vilić, 2018, str. 16-17), korisnici društvenih mreža su prepoznali visok stepen rizika od Internet prevara ali je najveći broj (533 tj. 87,1%) izjavio da nije direktno bio/bila žrtva Internet prevare ili krađe (Vilić, 2016, str. 369).

5 ZAKLJUČCI – KAKO SE ZAŠTITITI?

Kompjuterski kriminalitet je postao jedan od najvećih transnacionalnih problema koji se prostire daleko van granica samo jedne države, pa samim tim se i nameće zaključak da mehanizmi borbe protiv ovog vida kriminaliteta moraju da obuhvataju preduzimanje odgovarajućih mera tehničkog, strukturalnog i obrazovnog karaktera (Vilić, 2015, str. 12).

Preporuke Saveta ministara Evropskog saveta (Recommendations to the European Council “Europe and the global information society”, 1994) predstavljaju jedan od bitnih napora preventivnog delovanja međunarodne zajednice na suzbijanju komjuterskog kriminaiteta i prevarnog ponašanja u sajber prostoru, i koje se, između ostalog, odnose na poboljšanje tehničkih mogućnosti za autentifikaciju korisnika podataka, poboljšanje tehničkih mogućnosti praćenja komunikacija preko Interneta i poboljšanje tehnologija kojima bi se zaštitile novčane transakcije preko Interneta (Vilić & Žunić, 2018, str. 93).

Svako od korisnika Interneta, a posebno korisnika društvenih mreža, može da doprinese borbi prevarnog ponašanja na Internetu, kako bi se izbegla ovakva vrsta viktimizacije ili bar smanjila mogućnost da do nje dođe. Korisnicima se savetuje da (The FBI – Common Fraud Schemes: Internet Fraud, 2018):

- ukoliko učestvuju u Internet aukcijama, dobro prouče kako se aukcije zaista sprovode, koje su obaveze prodavaca pre nego što proda određenu stvar i koje su obaveze kupca; da se što bolje raspitaju i da saznaju sve o prodavcu i njegovom poslovanju, kao i o načinu dostave kupljene stvari;
- korisnici dobro provere da li prilikom Internet kupovine nema još nekih dodatnih i nepredviđenih troškova;
- nema potrebe da za ovakav vid transakcija nigde upisuju broj zdravstvenog osiguranja ili vozačke dozvole, jer su to podaci koji se mogu zloupotrebiti i za krađu identiteta i izvršenje različitih krivičnih dela;

- kako bi se izbegla zloupotreba kreditnih kartica, korisnik ne sme da ukucava njen broj ukoliko nije uveren da je sajt zaštićen i pod sigurnom vezom;
- prilikom Internet kupovine, neophodno je proveriti da li prodavac zaista postoji (proveriti pozivom na telefonski broj prodavca, poslati eletronsku poruku da se vidi da li je adresa aktivna i da li se zaista koristi i sl.);
- kada je reč o tzv. "nigerijskim prevarama", korisnici moraju da budu skeptični po pitanju svih osoba koji im se obraćaju kao zvaničnici iz Nigerije a traže pomoć u novcu koja mora da se uplati u neku stranu banku, da ne veruju obećanjima o velikim sumamam novca koje će im biti isplaćene i da veoma pažljivo čuvaju lozinku svog naloga kako ga neko ne bi zloupotrebio.

U svim ovim mogućim situacijama, od korisnika se očekuje da kontaktiraju administratora sajta preko koga su dobili sumnjivu poruku, kako bi sprečili da dođe do nastanka bilo kakve štete i eventualnog izvršenja krivičnog dela.

Pored preduzimanja odgovarajućih tehničkih mera koje bi umanjile mogućnost zloupotreba u virtuelnom svetu Interneta i korigovanja ponašanja samih korisnika, veoma je bitno i stvaranje međunarodnog pravnog okvira, kako bi se sprečilo vršenje krivičnih dela kompjuterskog kriminaliteta, otkrili i procesuirali izvršioci ovih krivičnih dela i kako bi se stvorili mehanizmi pomoću kojih bi se žrtvama ovih dela nadoknadila pretrpljena šteta, koja je kod dela Internet prevara velika i u materijalnom i u nematerijalnom smislu. Postojeće krivično zakonodavstvo u Republici Srbiji žrtvama prevare na Internetu omogućava pokretanje postupka podnošenjem prijave Odeljenju za visokotehnološki kriminal Ministarstva unutrašnjih poslova Republike Srbije ili Odeljenju za visokotehnološki kriminal javnog tužilaštva pred Višim sudom u Beogradu, ali i različitim udruženjima za zaštitu potrošača ili servisima koji se bave zaštitom na Internetu.

CITIRANI RADOVI

Babović, M. (2004). Hakerska subkultura i kompjuterski kriminal. *Pravni život – časopis za pravnu teoriju i praksu,* 9/2004, godina LIII, knjiga 485, 749-750, Udruženje pravnika Srbije, Beograd.

Brkic, M. (2017). *Nova Internet prevara u Srbiji.* Preuzeto na https://www.blic.rs/vesti/hronika/nova-Internet-prevara-u-srbiji-da-bi-vam-novac-legao-kao-i-meni-javite-se-ovom-coveku/lz1rpnm, dana 29.08.2019.

Button, M., McNaughton Nicholl, C.C., Kerr, J. & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology 47*(3):391-408, DOI: 10.1177/0004865814521224

Divković, A. (2018). *Nigerijska prevara – koje su vrste i kako ih prepoznati.* Preuzeto sa https://blog.limundograd.com/2018/01/nigerijska-prevara-vrste-i-kako-se-zastiti/, dana 26.08. 2019.

Koong, S. K., Liu, L.C. & Wei, J. (2012). *An Examination of Internet Fraud Occurrences,* Preuzeto sa https://www.researchgate.net/publication/228460925_An_Examination_of_Internet_Fraud_Occurrences, dana 30.08. 2019.

Krivični zakonik Republike Srbije („Službeni glasnik RS" br.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 i 104/2013)

Matijašević, J., Spalević, Ž. & Ignjatijević, S. (2012). *Vrste Internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice.* INFOTEH-JAHORINA Vol. 11, 562-565

n.d. (1994). *Recommendations to the European Council "Europe and the global information society".* Preuzeto sa http://channelingreality.com/Digital_Treason/Brussels_1995/Bangemann_report.pdf, dana 31.08.2019.

n.d. (2005). *Computer Crime Research Center: Fraud in the Internet.* Preuzeto sa http://www.crime-research.org/articles/Internet_fraud_0405/, dana 02. 09. 2019.

n.d. (2014). *Čuvajte se – Nigerijska prevara u Srbiji*. Preuzeto na https://srbin.info/pocetna/aktuelno/nigerijska-prevara-u-srbiji-hteo-da-proda-kuca-a-ostao-bez-para/, dana 12.08.2019.

n.d. (2017). *The top 10 Internet Frauds - National Fraud Information Center*. Preuzeto sa http://www.nclnet.org/, dana 14. 08. 2018.

n.d. (2018). *Čuvena nigerijska prevara opet hara Srbijom.* Preuzeto na https://www.kurir.rs/vesti/drustvo/3168527/cuvena-nigerijska-prevara-opet-hara-srbijom-ozenjeni-muskarac-iz-kosjerica-dobio-poruku-od-nepoznate-devojke-na-fejsbuku-tog-trenutka-pocela-je-njegova-nocna-mora-ovako-ga-je-opeljesila, dana 23.08.2019.

n.d. (2018). *Nigerijska prevara i dalje živi: Lažni naslednici lakoverne Srbe vrebaju i na ćirilici.* Preuzeto sa https://www.telegraf.rs/vesti/ekonomija/2986678-nigerijska-prevara-i-dalje-zivi-lazni-naslednici-lakoverne-srbe-vrebaju-i-na-cirilici, dana 23.08.2019.

n.d. (2018). *The FBI – Common Fraud Schemes: Internet Fraud.* Preuzeto sa http://www.fbi.gov/scams-safety/fraud/_fraud , dana 23. 01. 2018.

n.d. (2018). *Ultrascan Advanced Global Investigations.* Preuzeto sa http://www.ultrascan-agi.com/, dana 03.02. 2018.

n.d. (2019). *Top ten scams of 2018 – Fraud.org.* Preuzeto sa https://www.fraud.org/2018_top_ten, dana 31.08.2019.

Nikolić, K., Gvozdenović, L., Radulović, R., Milosavljević, S., Jerković, A., Živković, R., Živanović, V., Reljanović, M. & Aleksić, I. (2010). *Kratak prikaz razvoja pravne regulative o visokotehnološkom kriminalitetu na međunarodnom nivou.* Suzbijanje visokotehnološkog kriminala, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd.

Prlja, D., Ivanović, Z. & Reljanović, M. (2011). *Krivična dela visokotehnološkog kriminala*. Institut za uporedno pravo, Beograd.

Urošević, V. (2009). Nigerijska prevara u Republici Srbiji. *Časopis Bezbednost.* (3).

Vilić, V. (2013). *Possibilities of privacy rights abuses in social networks and practical protective measures.* International scientific and practical conference „Internet – Government – Politics“, Kemerovo, 2013, 187-192, ZAKAZ No.458

Vilić, V. (2015). *Mechanisms for Protecting the Right to Privacy and Personal Data on Social Networks.* INTERNATIONAL Scientific Conference of IT and Bussiness – Related Research Synthesis Univerzitet Singidunum Beograd 2015, 10-13. DOI: 10.15308/Synthesis-2015-10-13, ISBN 978-86-7912-595-8

Vilić, V. (2016). *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta, Doktorska disertacija,* Pravni fakultet Univerziteta u Nišu, 535. COBISS.SR-ID 1026747809

Vilić, V. (2017). *CYBERCRIME: Basic criminological characteristics and legislation.* LAP - LAMBERT Academic Publishing – International Book Market Service Ltd. member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5

Vilić, V. (2018). *Users' considerations about possibilities of self-protection on social networks.* Center for Open Access in Science - Open Journal for Legal Studies, 2018, 1(1), 9-24. ISSN (Online) 2620-0619 ▪ DOI: 00.00000/ojls.2017.00000a

Vilić, V. & Žunić, N. (2018). *Prevencija i mere zaštite od kompjuterskog kriminaliteta (Prevention and measures of protection against computer crime).* III međunarodna naučna konferencija „Društvene devijacije: NE NASILJU – jedinstven društveni odgovor“, Banja Luka 25-27.05.2018, Centar modernih znanja, Banja Luka, 92-100, UDK: 004,738,5:316,472,4, DOI: 10.7251/CMZ1803092V

Vilić, V. (2019). Phishing and pharming as forms of identity theft and identity abuse. *Balkan Social Science Review, 13*(13), 43-57.

Datum prve prijave: 08.09.2019.
Datum prijema korigovanog članka: 08.10.2019.
Datum prihvatanja članka: 11.10.2019.

Kako citirati ovaj rad? / How to cite this article?

Style – APA Sixth Edition:

Vilić, V. (2019, 10 15). Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 135-145. doi:10.12709/fbim.07.07.02.15

Style – Chicago Sixteenth Edition:

Vilić, Vida. 2019. "Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 135-145. doi:10.12709/fbim.07.07.02.15.

Style – GOST Name Sort:

Vilić Vida Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 135-145.

Style – Harvard Anglia:

Vilić, V., 2019. Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. *FBIM Transactions,* 15 10, 7(2), pp. 135-145.

Style – ISO 690 Numerical Reference:

Prevare putem Interneta: Sajber zabava koja „prazni" račune širom sveta. **Vilić, Vida.** [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 135-145.