ISBN: 978-99955-45-38-3
UDK: 343.222.2:004.738.5

Datum prijema rada: 07.06.2022.
Datum prihvatanja rada: 16.06.2022.
Pregledni naučni rad

OTKRIVANJA PREVARE PRILIKOM PRODAJE PROIZVODA PREKO INTERNETA

DETECTION OF FRAUD WHEN SELLING PRODUCTS ONLINE

Predrag Katanić
Univerzitet u Istočnom Sarajevu, Fakultet poslovne ekonomije Bijeljina,
Republika Srpska, Bosna i Hercegovina
predrag.katanic@fpe.ues.rs.ba
ORCID: 0000-0002-6476-809X

Srđan Damjanović
Univerzitet u Istočnom Sarajevu, Fakultet poslovne ekonomije Bijeljina,
Republika Srpska, Bosna i Hercegovina
srdjan.damjanovic@fpe.ues.rs.ba
ORCID: 0000-0003-4807-5311

Apstrakt: *U posljednje vrijeme intenzivirane su internet prevare usmjerene na korisnike platformi za e-trgovinu. Reč je o prevari koja je usmjerena na ljude koji žele putem interneta da prodaju neki svoj proizvod. Komunikacija se najčešće odvija putem poruka preko mobilnih telefona. Brojevi telefona koji se koriste su najčešće iz inostranstva. Navodni kupac komunikaciju počinje pitanjem da li je proizvod i dalje dostupan i da li kupoprodaju mogu da obave elektronskim putem. Kupac obično odmah prihvaća ponuđenu cijenu i traži od prodavca da klikne na link, koji vodi na stranicu na kojoj se zahtjeva da unese u određena polja podatke sa bankarske kartice, kako bi mu se navodno izvršila uplata. Izgled poruke za većinu ljudi djeluju vjerodostojno i pouzdano. Žrtva popunjava formular i time prosljeđuje svoje podatke napadaču, koji koristi te podatke kako bi ukrao novac sa računa žrtve. Mi smu u radu opisali praktičan primjer u kome smo prikazali jedan ovakav napada na sajtu za oglašavanje prodaje preko interneta u Bosni i Hercegovini. Cilj rada je da upoznamo ljude, koji prodaju proizvode preko interneta, sa velikom opastnosti, kojoj mogu biti izloženi, ako nisu dovoljno pažljivi i ako olako prihvate da daju svoje lične podatke neprovjerenim osobama.*

Ključne riječi: *prevara, prodaja, proizvod, internet, otkrivanje, plaćanje*

JEL klasifikacija: *K24*

Abstract: *Recently, internet fraud aimed at users of e-commerce platforms have*

intensified. It is a fraud that is aimed at people who want to sell some of their products online. Communication usually takes place via messages via mobile phones. The phone numbers used are mostly from abroad. The alleged buyer begins the communication by asking whether the product is still available and whether they can make the purchase electronically. The buyer usually immediately accepts the agreed price and asks the seller to click on the link, which leads to the page where he is required to enter in certain fields the data from the bank card, in order to allegedly make a payment. The look of the message seems credible and reliable to most people. The victim fills out a form and thus forwards his data to the attacker, who uses this data to steal money from the victim's account. In this paper, we have described a practical example in which we presented one such attack on an online advertising site in Bosnia and Herzegovina. The aim of this paper is to acquaint people who sell products online with great danger, which they can be exposed to if they are not careful enough and if they readily accept to give their personal data to unverified persons.

Key Words: *fraud, sales, product, internet, detection, payment comparison*

JEL classification: *K24*

1. UVOD

Većina ljudi kod nas ali i širom svijeta svakodnevno na poslu ali i kući provode dosta vremena koristeći internet na raznim uređajima. Ljudi u internetu uglavnom vide njegove pozitivne strane, a da često nisu ni svjesni da im na internetu danas prijete razne opsnosti od raznih kriminalaca, koji se nalaze širom svijeta. Većina kriminalaca na internetu se oslanja na propuste u bezbjednosti žrtava i njihove slabosti na koje prevaranti računaju, a koje možemo podvesti pod društveni inženjering. Svaka internet prevara obično počinje sa kontoktom napadača sa žrtvom putem društvenih mreža, email poruka ili pozivima preko telefona. Ljudske osobine koje predstavljaju i vlastite slabosti internet korisnika na onovu kojih najčešće postaju žrtve raznih internet prevara su:

- požuda;
- pohlepa;
- lakovjernost;
- lijenost;
- brzopletost i
- saosjećajnost.

Većina od nabrojanih ljudskih osobina su loše i u svakodnevnom životu i upravo to žele da iskoriste i potencijalni predatori na internetu.

Požuda predstavlja ljudsku osobinu koja je dosta česta, jer većina ljudi u svakodnevnom životu želi da živi, radi i sarađuje sa lijepim i atraktivnim ženama ili muškarcima. Emocije koje ljudi imaju prema lijepom suprotnom polu se teško mogu kontrolisati. Upravo zato napadači na internetu kradu tuđi identitet i lažno se

predstavljaju kao lijepe i atraktivne žene ili muškarci. Prevara počinje kao jedan mali i običan bezopasan flert. Obično se počinje sa slanjem romantičnih poruka, slika, videa i linkova sa svojih profila na društvenim mrežana. Ali ti profili na društvenim mrežama su obično lažni jer su i fotografije na njima najčešće lažne. Međutim ovaj započeti flert preko interneta, zamišljen kao romansa sa nepoznatom osobom najčešće na kraju nije romantičan, već se obično završi kao neka prevara.

Pohlepa spada u jednu vrlo lošu ljudsku osobinu, koja je prikrivena kod dosta ljudi. Ljudi jednostavno vole da dobijaju razne poklone, a većina ljudi teško može da odoli i da odbije nešto što joj se nudi kao besplati poklon. Međutim kada vam neko nudi neki primamljiv besplatan poklon preko interneta, trebalo bi da prvo dobro posumnjate zašto ste baš vi izabrani da dobijete taj besplatni poklon. Samo ako ste dobro provjerili pošiljaoca poklona tek onda bi eventualno trebali da prihvatite takav poklon. Većina ovih prevaranata kada stupi u početni kontakt sa vama, u narednom koraku traži da joj pošaljete broja vašeg računa u banci. Zatim slijedi izvršenje same prevare, a to je najčešće krađa novca sa vašeg bankarskog računa.

Lakovernost predstavlja ljudsku osobinu, koju smo svi bar nekada imali u životu. Prevaranti na internetu se obično lažno predstavljaju da su poznanici ili prijatelji vaših prijatelja ili da su promoteri nekih poznatih firmi ili robnih marki, koje vam nude proizvode po povoljnoj cijeni. Za ovu vrstu napada se koristi lažni identitet i dokumenti, najčešće u vidu lažne akreditacije ili preporuke kako bi stupili u početni kontakt sa vama. Najčešće žrtve ove vrste sajber napada su starije osobe koje žive same.

Lijenjost je osobina koju ljudi imaju često u svakodnevnom životu jer živimo i radimo sve brže. Ova osobina dolazi posebno do izražaja kada ljudi koriste računar ili mobilni telefon jer preko ovih uređaja svakodnevno dobijaju veliki broj raznoraznih poruka putem meila ili društvenih mreža. Napadači upravo računaju na to da vi nećete detaljno da provjerite prvo adresu sa koje ste dobili poruku, a zatim i da detaljno pročitate cijelu poruku. Prevaranti računaju na to da vi nećete da provjerite cijeli tekst pristiglog linka u poruci, preko koga se ovično započinje napad. Odlazak na ove pogrešne linkove najčešće vodi do opcije za slanje vašeg računa u banci i unosa lozinke, a zatim slijedi prevara. Zato moramo biti oprezni i dobro pročitati i provjeriti svaku poruku koju dobijemo od banke ili nekoga ko želi da vam nešto plati. Nemojte biti lijeni jer prevaranti upravo na internetu računaju na tu vašu osobinu.

Brzopletost je ljudska osobina karakteristična danas posebno zbog sve bržeg životnog tempa u kome živimo i radima. Ova osobina je najčešće povezana sa lijenosti. Prevaranti prilikom izvođenja napada vam šalju poruku u kojoj morate vrlo brzo da odreagujete. Oni vas pri tome požuruju riječima da vam brzo ističe vrijeme za djelovanje i odgovor. Zbog želje da se posao uradi na vrijeme i da ne bi bili kritikovani za lijenost ljudi onda brzopleto reaguju. Zato ljudi ali i zaposleni greškom pošalju podatke i dokumente prevarantu. Da bi izbjegli ovakve vidove prevara potrebno je da i na internetu tražimo dovoljno vremena da bi nešto uradili i da dobro razmislimo prije nego što odreagujemo na dobijeni zahtjev, kao i u realnom životu.

Jer kada se jednom pošalje pogrešni podatak ili dokument onda je često već kasno, a kajanje nam neće pomoći da vratimo izgubljeni novac.

Za razliku od svih prethodno opisanih ljudskih osobina saosjećanje se može smatrati ponekad i kao dobra ljudska osobina u svakodnevnom životu. Kako u realnom svijetu tako i na internetu postoje prevaranti, koji žele upravo da vas prevare zahvaljujući ovoj ljudskoj osobini. Dok ste na internetu i dok pregledate poruke na društvenim mrežama saosjećanje može biti vrlo opasno posebno danas u vrijeme pandemije COVID-19. Ima veliki broj primjera lažnih ili preotetih naloga na društvenim mrežama ili email adresa sa kojih se upućuju razni pozivi za pomoć. Česte su poruke od vaših prijatelja ili poslovnih partnera koji su negdje na putu i izgubili su novčanik sa novcem i karticama, pa nemaju novca da se vrati kući. Od vas se obično traži da im pošaljete novac za kupovinu karte, plaćanje hotela ili dopunu računa na mobilnom telefonu. Postoje poruke od lažnih neprofitnih i nevladinih organizacija, koje skupljaju pomoć za oboljelu djecu, socijalno ugrožene porodice, izbjeglice ili postradale stanovnike u slučaju elementarnih nepogoda ili ratnih dejstava. Mnogi dobri i saosjećajni pojedinci i kompanije su prevareni na ovakav način, a prevaranti su skupili milionske iznose novca na svoje račune od ovakvih zahtjeva za pomoć.

Phishing (pecanje) napadi su oblik krađe identiteta koji se oslanja na e-poštu i web. Kada se govori o phishingu, misli se na pokušaj zavaravanja korisnika da se radi o ispravnoj poruci, a koja treba da dovede do krađe identiteta. Primjer ove vrste prevare je e-pošta, čiji je sadržaj sličan onome koji obično šalje banka ili bilo koja druga popularna usluga (poput Paypala, Ebaya, Facebooka itd.). U takvim mejl porukama je obično jedan link koji, na prvi pogled, otvara zvaničnu stranicu. Međutim iza tog linka se krije druga stranica, na koju se korisnik prevarom pokušava navesti. Otvorena stranica obično estetski izgleda poput zvanične stranice ili je veoma slična njoj, ali postoji razlika u linku, koji je naveden u adresnoj traci, odnosno u IP adresi stranice. Na primjer, iako je službena web stranica Paypal usluge www.paypal.com, korisnici će vidjeti stranicu koja je estetski ista, ali samo će se njena web adresa malo razlikovati i možda će biti teško uočljiva razlika, poput www.paypol.com ili sl. Kada korisnik posjeti lažnu stranicu od njega se traži da unese svoje lične podatke i lozinke, tako da prevarant na taj način krade mrežni identitet korisnika. Prevareni korisnik tada daje kreatoru lažne web stranice priliku da koristi novac na Paypal računu prevarenog korisnika. Sličan scenarij se primjenjuje i sa bankama, gdje će korisnik dobiti email u kojemu se traži „provjera ispravnosti“ kreditne kartice, na način da upiše svoje lične podatke, uključujući i broj kartice. Ukoliko tvorac lažne stranice dođe do takvih podataka, velika je vjerovatnoća da će kroz samo par minuta vlasniku kartice biti ukradena veća svota novca sa njegovog bankarskog računa. Phishing se smatra društvenim inženjeringom bez obzira što se radi o tehničkom napadu. Zbog medija kojim se širi i na kojem se njegov rad bazira, glavna komponenta tog krivičnog djela je nesavjestan ili neupućen korisnik, koji svojom voljom pristaje da bude meta napada. Na računarima se ovakva vrsta napada može djelimično lakše predvidjeti, u odnosu na napade kada korisnik koristi mobilni telefon. Kod monitora računara se lakše čita link lažne internet stranice, zbog činjenice da je adresna traka kod internet

pretraživača veća i može obično da se pročita u cjelini. Kod mobilnih telefona linkovi i adresne trake kod pretraživača nisu potpuno vidljivi, ili su slabo vidljivi.

Prema organizovanosti phishing napada, napadače je moguće razvrstati u dvije kategorije. Prvu kategoriju čine napadači koji rade potpuno samostalno. Jedna osoba kreira stranicu, šalje poruke i koristi dobijene podatke. Takvi napadači obično nemaju velike tehničke vještine, tako da napadi nisu sofisticirani, što je vidljivo i na realizaciji stranica i poruka. Osim toga, njihovi tekstovi često sadrže greške zbog upotrebe alata za automatsko prevođenje (u našem jeziku su to najčešće greške u padežima). Samostalni napadači nemaju fleksibilnost potrebnu za prikrivanje napada, pa često ni ne slute da određene službe prate sve njihove korake. U drugu kategoriju svrstavamo napadače koji rade u organizovanim grupama. Ti napadači su visokoorganizovani i svaki od njih dobro zna svoj posao, a osim toga svjesni su da policija pokušava pratiti njihove aktivnosti, te zbog toga ulažu velike napore u skrivanje vlastitih tragova.

U zadnjih pola godine u Bosni i Hercegovini je takođe aktuelna prevara sa lažnim donacijama lažnih islamskih humanitarnih organizacija. Prevaranti preko interneta su tražili da im potencijalne žrtve dostave brojeve svojih računa u banci, kako bi im se na taj račun uplatila humanitarna novčana pomoć. Nažalost prevarene osobe su ostale bez humanitarne pomoći, ali i bez novca koji su imali na svojim računima. Napominjemo da se ovde uglavnom radilo o osobama slabije materijalne situacije. To ove prevarante na internetu čini još okrutnijim.

2. POVEZANA LITERATURA

MacInnes (2005) je u svom radu utvrdio faktore koji doprinose prevari u elektronskoj trgovini. Predstavio je model koji identifikuje pet uzroka: podsticaji kriminalaca, karakteristike žrtava, uloga tehnologije, uloga sprovođenja i sistemski faktori. Internet je snizio barijere za izvršenje kriminalnih poduhvata. Analizom slučajeva prevara u elektronskoj trgovini autor je pokazao da većina krivičnih djela nije tehnološki sofisticirana i da će veća svijest i iskustvo sa ovom vrstom prevara dovesti do toga da ljudi izbjegnu da budu prevareni.

Još 2002. godine, Komisija Ujedinjenih nacija za međunarodno trgovinsko pravo (UNCITRAL) prvi put je razmotrila problem prevara, koje su imale značajan negativan ekonomski uticaj na svjetsku trgovinu i negativno uticale na legitimne komercijalne institucije. Kroz seriju konsultacija sa stručnjacima i državnim službenicima koji su se redovno susreli i borili protiv komercijalnih prevara i koji su predstavljali različite regione, perspektive i discipline, UNCITRAL je postao svjestan široko rasprostranjenog postojanja komercijalne prevare i njenog značajnog uticaja širom svijeta, bez obzira na stepen privrednog razvoja ili sistema vlasti. U razmatranju mogućih odgovora na ovu prijetnju, smatralo se da obrazovanje i obuka mogu da igraju značajnu ulogu u prevenciji prevara i da bi identifikacija uobičajenih znakova upozorenja i indikatora komercijalne prevare mogla biti posebno korisna u borbi protiv prevare. Dati su primjeri iz različitih oblasti pravne prakse i uključuju različite vrste žrtava.

U svom radu Ranđelović (2017) obrađuje internet prodaju i analiza zakonske propise kojima se ona reguliše u Srbiji. Opisana su neka od najčešćih pitanja i problema sa kojima se suočavaju potrošači prilikom internet kupovine. U Srbiji je donijet niz zakona i drugih podzakonskih propisa kojima se reguliše internet prodaja i koji prate zahtjeve i standarde Evropske unije. Međutim, nije dovoljno donošenje zakonskih propisa, već njihova efikasna implementacija i primjena od strane građana i nadležnih organa, kao i obrazovanje trgovaca, ali i samih potrošača radi širenja svjesti o značaju i koristima elektronske trgovine.

Renjith (2017) je u svom radu pokazao da udio e-trgovine u globalnoj maloprodajnoj potrošnji pokazuje stabilan porast tokom godina. Posljednjih godina, onlajn tržišta su postala jedan od ključnih faktora koji doprinose ovom rastu. Kako poslovni model sazrijeva, broj i vrste prevara koje se prijavljuju u ovoj oblasti takođe rastu na dnevnoj bazi. Prevarni kupci e-trgovine i njihove transakcije se detaljno proučavaju i pripremaju strategije za njihovu kontrolu i sprečavanje. Roba/usluge koje se nude i prodaju po niskim cijenama, ali nikada nisu isporučene je jednostavan primjer ove vrste prevare. Ovaj rad pokušava da predloži modele za otkrivanje takvih lažnih prodavaca i upozoravanje kupaca uz pomoć tehnika mašinskog učenja.

Weng (2020) tvrdi da uz veliki uspeh e-trgovine, rastu i mnoge zlonamjerne promotivne usluge sa ciljem povećanja prodaje. Zlonamjerni trgovci pokušavaju da promovišu svoje ciljne artikle tako što nezakonito optimizuju rezultate pretrage koristeći lažne posjete, kupovine itd. U ovom radu je proučavan problem otkrivanja prevara na velikim platformama za e-trgovinu.

Prevare u transakcijama e-trgovine porasle su u posljednjoj deceniji, posebno sa sve većim brojem onlajn prodavnica. Pojava pandemije COVID-19 je primorala sve više ljudi da plaćaju usluge i namjernice na mreži koristeći svoje kreditne kartice (Alqethami 2021). Predloženo je nekoliko metoda mašinskog učenja za otkrivanje lažnih transakcija. Neuronske mreže su pokazale obećavajuće rezultate, ali imaju nekoliko nedostataka, koji se mogu prevazići korišćenjem metoda optimizacije.

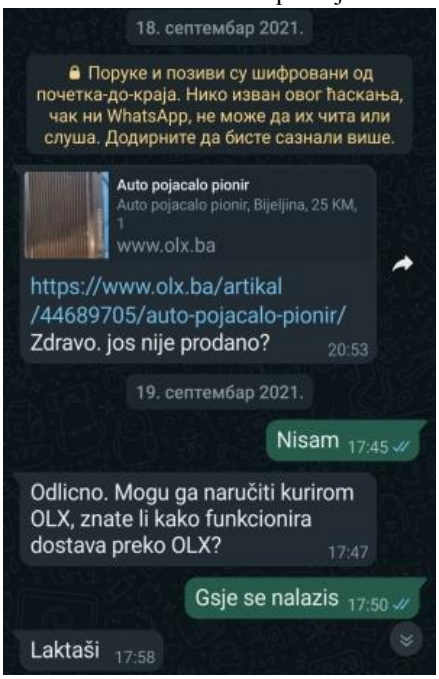
Alkhalil (2021) u svom radu pokazuje kako sa rastom upotrebe interneta, ljudi sve više dijele svoje lične podatke na mreži. Phishing je jedan od primjera visoko efikasnog oblika sajber kriminala, koji omogućava kriminalcima da obmanu korisnike i ukradu njihove važne podatke. Od prvog prijavljenog phising napada 1990 godine, ovi napadi su evoluirali u sofisticirani vektor napad. U radu su predloženi novi detalji anatomije phising napada, koja uključuje faze napada, tipove napadača, ranjivosti, prijetnje, mete, sredstva napada i tehnike napada. Istraživane su kontra mjere kao oblik predostrožnosti zaštite od ovog napada.

3. PRIMJER POKUŠAJA PREVARE PRILIKOM KUPOVINE NA INTERNETU

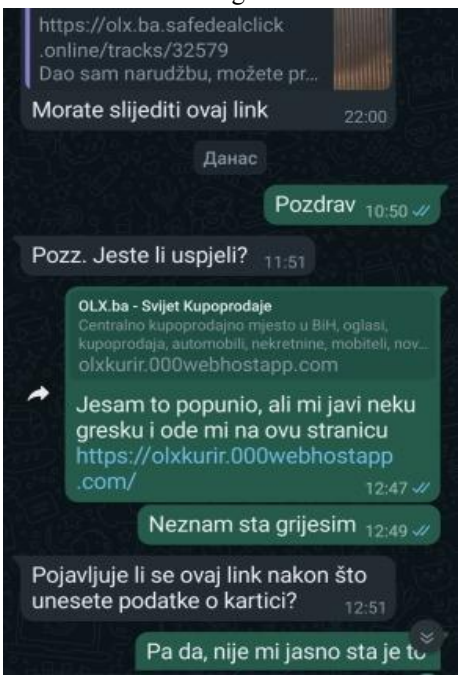
U ovom dijelu rada želimo da opišemo jedan primjer neuspjelog pokušaja prevare prilikom prodaje proizvoda preko interneta. Prodavac je želio da preko sajta www.olx.ba proda polovno pojačalo za automobil. Na slici 1 prikazan je početak

komunikacije između prodavca i potencijalnog kupca (koji je u ovom slučaju prevarant na internetu) preko *WhatsApp* aplikacije na mobilnom telefonu.

Slika 1. Početak prodaje



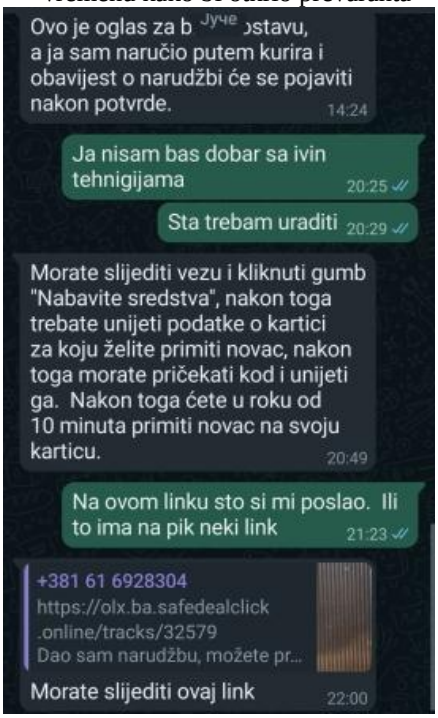
Slika 2. Pogrešan link



Suština pokušaja prevare se ogleda u tome, da osoba koja se predstavlja kao potencijalni kupac želi da dođe do broja bankarskog računa prodavca robe preko interneta. Ono što je prodavcu u ovom slučaju bilo odmah sumljivo, što je potencijalni kupac odmah pristao na početnu cijenu po kojoj je ponuđen proizvod za prodaju. Potencijalni kupac je insistirao da se roba preuzme uz pomoć kurirske službe, a da se plaćanje izvrši elektronski na tekući račun prodavca odmah. Zato je potencijalni kupac poslao prodavcu link, na kome je uputstvo za plaćanje preko interneta. U poslatom linku https://olx.ba.safedealclic.online/track32579 koji je prikazan na slici 2 je suština pokušaja prevare. Pomenuti link ne sadrži putanju do stvarnog uputstva za plaćanje preko interneta, koje je napravljeno na sajtu www.olx.ba, već se radi o lažnom linku, koji prestavlja klasičnu prevaru koja se zove fišing. Ovaj lažni link sadrži uputsvo koje treba da uputi prodavca da pošalje broj svoga računa u banci. Nakon toga bi preko lažne uplate i slanja potvrde u oplati prevarant došao i do sigurnosnog pina računa u banci, preko koga bi poslije ukrao kompletan novac sa računa prodavca. Potencijalni prodavac je u ovom slučaju odmah posumnjao u ovaj lažni link i odlučio je da se malo našali sa prevarantom. Želio je da dođe do njegove IP adrese sa koje je vršio ovu prevaru. Drugi korak je otkrivanje tipa mobilnog telefona, koji prevarant koristi u komunikaciju. Zadnji planirani korak je bio da se

prevarantu ponodu maska telefona za njegov mobilni telefon i da mu se na taj način kaže da je njegova prevara u potpunosti razotkrivena.

Slika 3. Prodavac želi da dobije na vremenu kako bi otkrio prevaranta



Slika 4. Prevarant je shvatio da je otkrivena njegova prevara

Zato je potencijalni prodavac u ovom slučaju izigravao osobu, koja nije dobar poznavalac informacionih tehnologija. Nizom poruka je obavještavao prevaranta da nije mogao da otvori proslijeđeni link i da nije u stanju da popuni potrebne podatke o broju svog bankarskog računa. Na taj način je želio da dobije na vremenu i da preko niza poruka otkrije IP adresu prevaranta. Primjer jedne ovakve prepiske prikazan je na slici 3. Nakon nekoliko dana prepiske potencijalni prodavac je uspio da dođe do IP adrese prevaranta i da čak otkrije i tip njegovog mobilnog telefona koji koristi za prevaru. Na slici 4 je prikazana poruka prodavca u kome se na kraju prevarantu nudi maska za njegov mobilni telefon, koji je koristio u komunikaciji. Tada prevarant obustavlja svaku dalju komunikaciju sa potencijalnim prodavcem, jer je shvatio da je njegova prevara otkrivena. Ovaj prevarant je koristio IP adresu koja se nalazila u Hrvatskoj, a koristio je da bi prevario ljude, koji su prodavali svoje proizvode u Bosni i Hrecegovini preko sajta www.olx.ba. Prevarant je odmah ugasio i domen na kome je postavljao lažno uputstvo za plaćanje preko interneta, jer se bojao da će biti prijavljen policiji. Potencijalni kupac u ovom slučaju prevaru nije prijavio policiji jer se radi o IP adresi iz druge države. Zahvaljujući malo sreći, ali i poznavanju informacionih tehnologija potencijalni prodavac pojačala u ovom slučaju nije bio finansijski oštećen. Međutim možemo reći da neki drugi prodavci u Bosni i Hercegovini nisu imalu tu sreću, već su njihovi računi u banci bili opljačkani pomoću opisane prevare.

ZAKLJUČAK

Nastojali smo kroz ovaj naš rad da ukažemo na opasnost, koja prijeti prilikom prodaje proizvoda na internetu. Razlog leži u činjenici da je kod nas uobičajeno mišljenje da se prevare na internetu dešavaju samo prilikom kupovine proizvoda, a ne i prilikom prodaje proizvoda. Ovaj naš primjer upravo pokazuje da do prevara na internetu može doći i prilikom prodaje proizvoda na internetu. Zato svim korisnicima interneta i društvenih mreža sugerišemo da dobro treba pregledati sve dobijene linkove prije njihovog otvaranja. Svaki dobijeni link koji od posjetioca traži da ostavi broj svoga računa u banci treba odmah izbjegavati jer se uglavnom radi o pokušaju prevare. Nijedan legalan sajt za prodaju preko interneta u Bosni i Hercegovini ne traži od prodavca da svakom kupci šalje broj svoga računa u banci. Tako da sve poruke ovog sadržaja treba izbjegavati, a posebno ne treba otvarati linkove koji se nalaze u ovim porukama. Na sličnom principu funkcionišu prevare u kojima se dobije lažna meil poruka od banke, da se ukuca svoj račun u banci, a zatim lozinka, kako bi se izvršila navodno redovna provjera stanje računa. Obično je u tim prukama riječ "HITNO" tako da žrtva misleći da radi ispravnu stvar i da ne bi zakasnila, postaje predmet prevare. Kada se prevara otkrije tada je obično već kasno jer je žrtva ostala bez svog novca na računu u banci. U zadnje vrijeme su u Bosni i Hercegovini takođe aktuelne prevare sa lažnim donacijama lažnih humanitarnih organizacija. Nažalost prevarene osobe su ostale bez humanitarne pomoći, ali i bez novca koji su imali na svojim računima. Napominjemo da se ovde uglavnom radilo o osobama slabije materijalne situacije. To ove prevarante na internetu čini još okrutnijim.

LITERATURA

[1] Alkhalil Z., Hewage C., Nawaf L., Khan I., Phishing attack: A Recent Comprenhensesive Study and a New Anatomy, Frontiers in Computer Science, 2021, Volume 3, str. 1-23.

[2] Alqethami S., Almutanni B., AlGhamdi M., Fraud Detection in E-Commerce, IJCSNS International Journal of Computer Science and Network Security, 2021, VOL. 21, No. 6, str. 200-206.

[3] MacInnes I., Musgrave D., Laska J., Electronic Commer onic Commerce Fraud: Towards an Understanding of the ds an Understanding of the Phenomenon, Proceedings of the 38th Hawaii International Conference on System Sciences - 2005, str. 1-11.

[4] Ranđelović D., Internet prodaja u Republici Srbiji, PRAVO – teorija i praksa Broj 1–3 / 2017, str. 13-24.

[5] Renjith S., Detection of Fraudulent Sellers in Online Marketplaces using Support Vector Machine, International Journal of Engineering Trends and Technology (IJETT) – Volume 57 Number 1, 2018, str. 48-53.

[6] United Nations, Recognizing and Preventing Commercial Fraud Indicators of Commercial Fraud Prepared by the UNCITRAL Secretariat, Publication 2013, str. 1-98.

[7] Wang S., Liu C., Gao X., Qu H., Xu W., Session-Based Fraud Detection in Online E-Commerce Transactions Using Recurrent Neural Networks, Book Machine Learning and Knowlwdge Discovery in Databases, str. 241-252.
[8] Weng H., Li Z., Ji S., Chu C., Lu H., Du T., He Q., Online E-Commerce Fraud: A Large-scale Detection and Analysis, College of Computer Science, Zhejiang University, Hangzhou, China, 2020, str. 1-6.

SUMMARY

Most people in our country and around the world spend a lot of time at work and at home every day using the Internet on various devices. People on the Internet mostly see its positive sides, and are often unaware that they are threatened on the Internet today by various dangers from various criminals around the world. Most criminals on the Internet rely on the shortcomings in the safety of victims and their weaknesses, which the fraudsters are counting on, which we can classify as social engineering. Every internet fraud usually starts with the attacker's contact with the victim via social networks, emails or phone calls. The human traits that represent the own weaknesses of Internet users to those who most often fall victim to various Internet fraud are: lust, greed, gullibility, laziness, haste and compassion. Starting flirting over the Internet, conceived as a romance with an unknown person and haste, is usually not romantic in the end, but usually ends up as a fraud. Internet fraud aimed at users of e-commerce platforms have recently intensified. Through this work, we have tried to point out the danger that threatens when selling products on the Internet. The reason lies in the fact that in our country it is a common opinion that frauds on the Internet happen only when buying products, and not when selling products. This paper of ours shows that fraud on the Internet can also occur when selling products on the Internet. It is a scam that is aimed at people who want to sell some of their products online. Communication usually takes place via messages via mobile phones, because due to the smaller screen size compared to a computer monitor, the victim is less likely to detect fraud. The phone numbers used are mostly from abroad. The alleged buyer begins the communication by asking whether the product is still available and whether they can make the purchase electronically. The buyer usually immediately accepts the agreed price and asks the seller to click on the link, which leads to a page where he is required to enter data from the bank card in certain fields, in order to allegedly make a payment. The look of the message for most people seems credible and reliable. Fraudsters usually count on the seller's lust if the offered price is immediately accepted at the time of sale. The victim fills in the offered fake form and thus forwards his data to the attacker, who uses this data to steal money from the victim's bank account. In this paper, we have described a practical example in which we presented one such attack on an online advertising site in Bosnia and Herzegovina. The aim of this paper is to acquaint people who sell products online with great danger, which they can be exposed to if they are not careful enough and if they readily accept to give their personal data to unverified persons, especially their bank account information.