Navigacija kroz pejzaž internet prevara

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Andrijana Bosiljčić
mi231031@alas.matf.bg.ac.rs

Anđela Damnjanović
mi19059@alas.matf.bg.ac.rs

Igor Paunović
mi231040@alas.matf.bg.ac.rs

Luka Radanović
mi231010@alas.matf.bg.ac.rs

17. decembar 2023.

Sažetak

Pojava interneta omogućila je nikad lakše dolaženje do informacija i znanja, brže povezivanje ljudi koji dele slična interesovanja i još mnogo toga. Sa druge strane, ljudi su upravo u tim novim mogućnostima uvideli prostor za prevaru. Stoga su u ovom radu opisane najčešće vrste internet prevara, kao i načini na koje se one realizuju jer da bi se došlo do rešenja problema potrebno je dobro poznavati taj problem. Zatim je ukratko izloženo kako se zaštititi od prevara, kao i profili koji su podložniji da upadnu u zamku. Dodatno, navedeni su poznati primeri nekih internet prevara.

Ključne reči — internet prevare, fišing, farming, krađa identiteta, lažno predstavljanje, romantične prevare, lažne internet prodavnice, nigerijska prevara, prevare starijih lica, prevare sa putovanjima, lutrijske prevare, prevare sa preplaćivanjem, prevare sa nasleđivanjem, prevare sa kriptovalutama, prevare sa kreditnim karticama, prevare pri konkurisanju za posao

Sadržaj

1 Uvod

Pojava interneta donela je izuzetan napredak u komunikaciji, trgovini i razmeni informacija, ali i potencijalne opasnosti kao što su internet prevare koje predstavljaju rizik ne samo za pojedinca, već i za firme i društvo u celini. Uporedo sa razvojem tehnologije, sajber kriminalci upotrebljavaju sve sofisticiranije tehnike sa ciljem da ukradu nečiji identitet, lične podatke ili novac. Stoga će u ovom radu biti prikazano koje sve vrste internet prevara postoje, kako se sprovode, kako se zaštiti od njih, kao i ko su najčešće žrtve.

2 Internet prevara — pojam i vrste

2.1 Internet prevara — pojam

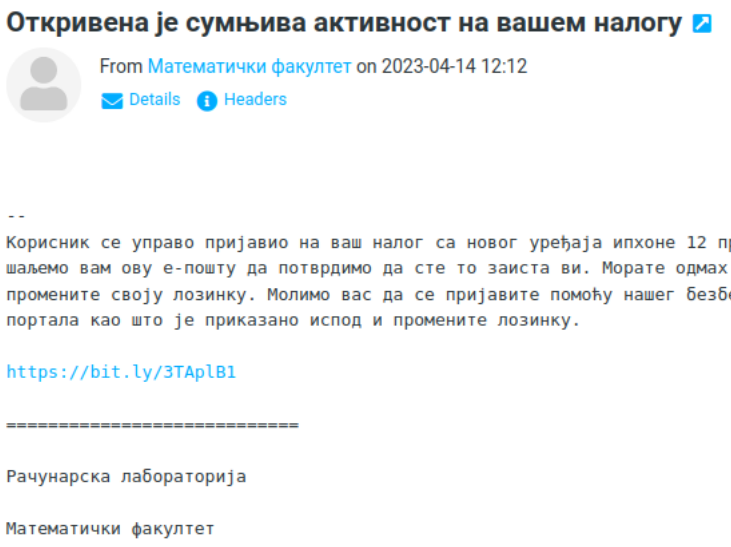
Internet prevara predstavlja korišćenje internet usluga ili softvera sa internet pristupom s ciljem da se obmane pojedinac, organizacija ili firma radi finansijske dobiti ili nanošenja štete. Ovakve prevare predstavljaju najrasprostranjeniji oblik visokotehnološkog kriminala. U nastavku teksta biće navedene neke od najčešćih vrsta internet prevara [1].

2.2 Internet prevare — vrste i način na koji se sprovode

Fišing (eng. *phishing*) je vrsta internet prevare u kojoj zlonamerni akteri pokušavaju da otkriju osetljive podatke pojedinca ili organizacije kao što su lični podaci, kredencijali za prijavljivanje na neki nalog, informacije o platnim karticama ili računu u banci [13, 31]. Prema podacima Federalnog istražnog biroa (eng. *Federal Bureau of Investigation*), 300.497 ljudi je postalo žrtva fišing prevara u 2022. godini. Zajedno su izgubili 52,1 milion dolara [17].

Fišing napadi se najčešće sprovode tako što napadači kreiraju lažnu veb-stranicu, nakon čega pošalju žrtvama poruku elektronskom poštom sa adrese koja liči na legitimnu adresu kao što je adresa neke banke, društvene mreže ili internet prodavnice. U poruci se obično navodi da će žrtvi uskoro biti blokiran internet nalog ili platna kartica, pa čak i da će im sa računa biti skinuta određena suma novca, ali da je to moguće sprečiti klikom na link koji se nalazi u nastavku poruke. Upravo zbog načina na koji su ove poruke napisane žrtva često, ne želeći da joj se blokira nalog ili kartica, klikne na link koji je zatim vodi do pomenute lažne veb-stranice (čiji URL veoma liči na URL stranice banke ili internet prodavnice, ali se obično razlikuje u nekom karakteru), gde će biti zatraženo korisničko ime i lozinka. Kada dobiju tražene podatke, napadači mogu pristupiti nalozima svojih žrtava, ukrasti dodatne podatke ili čak pristupiti uređajima na koje su žrtve bile povezane, što im omogućava da izvrše prevare još većih razmera [17, 25, 26]. Na slici 1 može se videti sadržaj elektronske poruke koju su studenti dobili tokom pokušaja sprovođenja fišing napada na Matematičkom fakultetu u Beogradu.

Takođe, postoje nemoralni ljudi koji koriste prilike i sprovode prevare u slučajevima kada se desi neka prirodna katastrofa. Oni šalju poruke elektronskom poštom predstavljajući se kao legitimne dobrotvorne ili vladine organizacije i pokušavaju da ubede žrtvu da donira novac. Oni mogu da koriste kreditnu karticu i lične podatke žrtve u razne svrhe [11, 25].



Slika 1: Primer pokušaja fišinga na Matematičkom fakultetu

Farming (eng. *pharming*) je vrsta internet prevare koja podseća na fišing, ali ih ne treba mešati[1]. U nastavku su date dve vrste farming napada [2, 18].

- **Farming zasnovan na zlonamernom softveru** javlja se jer korisnici interneta često nesvesno preuzimaju zlonamerni softver (eng. *malware software*) putem poruke elektronske pošte poslate sa lažne adrese ili prilikom preuzimanja nekog drugog softvera. Nakon preuzimanja zlonamernog softvera, korisnik biva trajno preusmeren na lažnu veb-adresu koju je napadač prethodno kreirao. Svaki put kada neko od korisnika pristupi toj adresi, napadači vide sve podatke koje korisnik unosi. Ovde se mogu ubrajati i prevare tehničke prirode gde žrtva dobija iskačuće upozorenje na veb stranici koja je u vlasništvu napadača i koji ukazuju na to da im je računar zaražen. Sprovodi se tako što napadači traže od žrtve da preuzme aplikaciju koja im omogućava da daljinski kontrolišu računar žrtve kako bi rešili problem. Oni zatim preuzimaju stvarni virus ili žrtvu na neki drugi način navode da veruje da još nešto nije u redu, ističući da mogu da reše problem uz novčanu nadoknadu [17, 2]. Jedan od najpoznatijih slučajeva farminga zasnovan je upravo na ovom metodu. Naime, 2007. godine, lažirani su sajtovi više od 50 svetskih banaka. Svaki put kada bi neki korsnik odlučio da poseti stranicu neke od ovih banaka i greškom naišao na lažni sajt, sa njega bi nesvesno preuzeo zlonamerni softver. Takođe, njihovi kredencijali za prijavljivanje bili su ukradeni [20].
- **Trovanje DNS servera** uključuje manipulacije DNS-om (eng. *Domain name system*, sistem imena domena) kako bi se posetioci veb-

[1]Farming podrazumeva automatsko preusmeravanje korisnika na lažne veb-sajtove, dok se u slučaju fišinga preusmeravanje vrši klikom na link. Stoga je farming prevara znatno većeg obima.

adrese preusmerili na lažne veb-lokacije. Za razliku od napada zasnovanim na zlonamernom softveru, ovi napadi utiču na širu publiku manipulisanjem infrastrukture interneta (napadači manipulišu DNS tabelama koje žrtve zatim preusmeravaju na lažne adrese), što znači da i korisnici koji unesu tačnu adresu veb-lokacije u svojim pretraživačima mogu biti preusmereni na lažnu veb-adresu bez njihovog znanja [2].

Lažne internet prodavnice predstavljaju dosta čestu internet prevaru. Kupovina preko interneta donela je razne pogodnosti kao što je kupovina u bilo koje doba dana, lako upoređivanje cena [28], ali je sa sobom donela i rizik od prevara. Napadači koji se odluče da izvrše ovakve prevare kreiraju lažne veb-sajtove za kupovinu koji ili izgledaju originalno ili repliciraju postojeće veb-sajtove prodavaca. Imaju URL adrese slične brendovima koje pokušavaju da oponašaju (npr. Amaz0n.net). Obično sadrže ponude koje su previše dobre da bi bile istinite, npr. ponude popularnih brendova po veoma niskim cenama. Napadači to koriste da prevare žrtve i zabeleže podatke o bankovnom računu u trenutku kupovine [17].

Romantične prevare predstavljaju internet prevaru koja podrazumeva da napadači kreiraju lažne naloge na sajtovima za upoznavanje preko kojih u relativno kratkom vremenskom periodu izražavaju snažne emocije prema žrtvi, uz predlog da komunikaciju nastave preko elektronske pošte, SMS poruka ili slično. Nakon određenog vremena, napadač traži novac, poklone, ili čak lične informacije od žrtve [8, 10, 26].

Lažno predstavljanje (eng. *catfishing*) je vrsta internet prevare gde napadač stvara lažni identitet na nekoj od društvenih mreža, obično ciljajući određenu žrtvu, sa željom da od nje iznudi novac [27].

Jedan od najpoznatijih primera lažnog predstavljanja desio se 2012. godine kada je Mantaj Teo, istaknuti univerzitetski igrač američkog fudbala, dospeo u javnost nakon što je otkriveno da je naseo na prevaru od strane Lenej Kekue, ličnosti koju je izmislio Ronaja Tuisusopo, koji je koristio lažni profil na društvenim mrežama kako bi uspostavio vezu sa Teom. Ronaja je čak izmislio i njenu smrt kako bi stekao Teove simpatije. Po ovom događaju je snimljen film „Devojka koja nije postojala“ [27].

Još jedan primer lažnog predstavljanja jeste romantična prevara 2.2. Kada napadači steknu poverenje žrtve, od nje traže poklone, novac, podatke o bankovnom računu, često izmišljajući razloge za to (npr. trenutno su u lošoj finansijskoj situaciji, imaju porodičnih problema, treba im pozajmica, žele da prenesu novac van zemlje, ali im je za to potreban novac za plaćanje poreza ili taksi...)[27].

Takođe, često se dešava da žrtva želi da kupi neki artikal, npr. automobil i u tom cilju kontaktira osobu koja je postavila oglas. Ako je ta osoba prevarant, onda šalje žrtvi lažne lične podatke i lažni dokaz o vlasništvu automobila. Pod izgovorom da živi u inostranstvu, napadač govori da mu je lakše da komunikacija bude preko elektronske pošte ističući popularnost oglasa i da ako žrtva odmah uplati novac dobija popust, a sve sa ciljem da se žrtva brzo odluči za kupovinu [7].

Prevare starijih lica podrazumevaju iskorišćavanje naivnosti i ranjivosti starijih osoba kada je internet u pitanju [8].

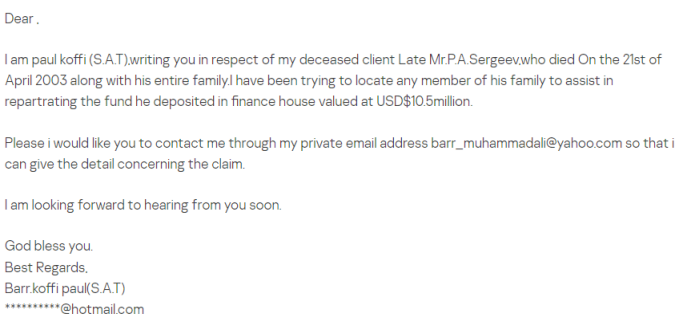
Postoje razni načini na koje se stariji mogu obmanuti. Jedan od njih su romantične prevare 2.2 koje podrazumevaju da se napadači predstavljaju kao potencijalni partneri starijim ljudima koji su u potrazi za životnim saputnikom da bi im na kraju tražili novac za različite svrhe.

Zatim, postoje i napadači koji se predstavljaju kao tehnička podrška i nude svoje usluge kako bi popravili nepostojeće kvarove na računaru [12].

Na ovaj način napadači dobijaju pristup ličnim podacima žrtava.

Ne treba izostaviti ni prevare u kojima napadači stupaju u kontakt sa starijima predstavljajući se kao član porodice da bi tražili da im se na račun uplati novac [8, 12, 17].

Nigerijska prevara poznata je i pod nazivom „Prevara 419“. „Nigerijska prevara“ najčešće počinje tako što žrtva dobija poruku elektronskom poštom, koja obično sadrži lažne informacije o dobicima u igrama na sreću, prikupljanju sredstva u dobrotvorne svrhe ili nasleđu imovine preminulih osoba, najčešće daljih rođaka. Zatim napadači ubeđuju žrtve da učestvuju u podeli novca, pri čemu žrtve moraju unapred da uplate određeni novčani iznos. Pošto je iznos koji treba uplatiti znatno manji od potencijalnog dobitka, žrtve se opredeljuju za ovaj korak. Nakon toga, elektronskom porukom (najčešće „spam“ (eng. *spam*) porukom (još jedna vrsta internet prevare) poslatom iz internet kafea) od primaoca poruke se traži pomoć pri transferu novčanih iznosa koji se kreću od par stotina hiljada do par desetina miliona dolara za koji će, nakon obavljenog transfera, žrtva dobiti određeni procenat kao nadoknadu (procenat zarade koji se obećava kreće se i do 40% od sume novca koja je predmet posla). Ukoliko žrtva odgovori na prvu poruku, napadači pokušavaju da je izmanipulišu da otkrije poverljive informacije o sebi tako što ubeđuju žrtvu da je baš njena pomoć neophodna da bi se posao završio. Kada žrtva uplati traženi iznos, napadači pod raznim izgovorima odlažu isplatu koju su obećali u zamenu za pomoć. Sa druge strane, oni nastavljaju da od žrtve traže novac pod izgovorom da i dalje postoje takse koje treba platiti da bi se pokrili dodatni administrativni troškovi, obećavajući opet da će žrtva dobiti svoj deo u najkraćem roku. Naravno, kada žrtva uplati i novi iznos, opet ulaze u isti začarani krug odlaganja isplate i traženja novca od žrtve [22]. Na slici 2 može se videti sadržaj elektronske poruke poslate žrtvi prilikom pokušaja sprovođenja Nigerijske prevare.



Dear ,

I am paul koffi (S.A.T),writing you in respect of my deceased client Late Mr.P.A.Sergeev,who died On the 21st of April 2003 along with his entire family.I have been trying to locate any member of his family to assist in repartrating the fund he deposited in finance house valued at USD$10.5million.

Please i would like you to contact me through my private email address barr_muhammadali@yahoo.com so that i can give the detail concerning the claim.

I am looking forward to hearing from you soon.

God bless you.
Best Regards,
Barr.koffi paul(S.A.T)
**********@hotmail.com

Slika 2: Primer poruke poslate žrtvi elektronskom poštom [19]

Putovanja predstavljaju vrstu internet prevare koja se uglavnom dešava na društvenim mrežama. Napadači kače primamljive slike predela na društvene mreže i navodno nude besplatne karte ili putovanja na te destinacije. Od potencijalnih žrtava se samo traži da popune anketu. Međutim, te ankete traže dosta ličnih podataka. Neki napadači čak i kreiraju lažne veb-sajtove (koji dosta podsećaju na prave, legitimne sajtove) na kojima je moguće izvršiti rezervacije. Takođe, moguće je i prodavanje lažnih polisa osiguranja [7].

Lutrijske prevare podrazumevaju da napadači šalju lažne elektron-

ske ili tekstualne poruke kojima obaveštavaju žrtve da su osvojili nagradu na lutriji. Da bi dobili svoju nagradu, žrtvama se traži da uplate razne troškove ili da pošalju informacije o bankovnom računu. Ovo može biti vrsta fišing napada 2.2, jer se može desiti da žrtve budu upućene na lažne veb-lokacije ili da dostave lične i finansijske podatke [8, 24].

Prevare sa preplaćivanjem u svom najosnovnijem obliku podrazumevaju da napadači lažno tvrde da je žrtvi uplaćeno više novca nego što je trebalo, te se od žrtve zahteva da vrati razliku između uplaćenog novca i dogovrenog iznosa. Ova prevara može imati više oblika [8]. Dva najpoznatija oblika ove prevare navedena su u nastavku.

- **Prevara sa lažnim čekovima** je jedna vrsta prevare sa preplaćivanjem. Žrtve ove prevare mogu biti osobe koje prodaju artikle preko interneta ili nekog oglasa. Analogno osnovnom obliku prevare sa preplaćivanjem, napadač želi da kupi određeni proizvod dajući lažni ček na kome je napisan iznos veći od dogovorenog, nakon čega traži od žrtve da mu vrati preostali novac. Ubrzo nakon slanja novca, žrtva saznaje da je prevarena [8, 23].
- **Prevara sa povraćajem novca** je vrsta internet prevare u kojoj napadači zovu ljude nasumično dok ne nađu žrtvu koja će im poverovati. Oni se predstavljaju kao osobe iz firme koja žrtvi treba da vrati novac jer žrtva navodno nije dobila određeni proizvod. Napadač ubeđuje žrtvu kako će posao firme biti ugrožen ukoliko ne uplati višak novca. Kada žrtva pristane na obavljanje datog transfera, od nje se traži da napadačima omogući pristup svom računaru preko softvera i da se prijavi na veb-stranicu za internet bankarstvo. Nakon što dobije pristup žrtvinom računaru, napadač isprazni ekran pomoću softvera za udaljen pristup i korišćenjem alata za razvoj veba u pretraživaču žrtve privremeno uredi veb-stranicu za internet bankarstvo. Na lažno kreiranoj stranici, žrtvi se prikazuju podaci podaci o navodnoj transakciji koju je firma izvršila. Naravno, vrednost uplate koju žrtva vidi je veća od cene artikla koji je žrtva navodno naručila, pa se od nje očekuje da vrati nastalu razliku. Tek nakon određenog vremenskog perioda žrtva saznaje da je prevarena (obično nakon sto uđe ponovo na veb-stranicu internet bankarstva). Ovo je takođe i vrsta tehničke prevare jer napadač obično prati isti format povezivanja sa računarom žrtve (preko softvera za udaljeni pristup). Dešava se i da žrtva dobije poruku elektronskom poštom u kojoj napadač moli za pomoć prenosa ogromne količine novca u inostranstvo ili traži podatke o bankovnom računu žrtve kako bi obavio transakciju obećavajući im novac zauzvrat [8].

Prevara sa nasleđivanjem je vrsta internet prevare u kojoj napadači kontaktiraju žrtvu predstavljajući se kao advokati i obaveštavaju žrtvu da joj je ostavljeno veliko nasledstvo od rođaka ili nekog bogatog dobrotvora koji je preminuo u inostranstvu. Da bi prevara bila verodostojnija, napadači mogu da pristupe javnim podacima o žrtvi i da nađu informacije o preminulima u njenoj okolini, ali se dešava i da samo izmisle ime preminulog. Oni zatim ubeđuju žrtvu da je potrebno da plati razne vrste troškova i da popuni formular pun ličnih podataka kako bi dobila nasledstvo [8].

Konkurisanje za posao predstavlja internet prevaru koja se danas često sprovodi jer je u poslednjih nekoliko godina došlo do povećanja broja kandidata koji traže radna mesta koja nude rad od kuće. Prevara obično uključuje ubeđivanje žrtve da kupi neke stvari ili uplati naknadu (npr. ukoliko pozicija zahteva podnošenje početne takse za registraciju) uz obećanje

provizija ukoliko namame i druge osobe da se prijave. Napadači nude žrtvama „informativni materijal“ koji će im omogućiti da se pripreme i lako dobiju posao u određenoj kompaniji, a zauzvrat traže novac. Zatim se žrtva obaveštava da je izabrana kao jedan od finalista za određenu poziciju (obično žrtva nije ni konkurisala za posao). Kada dođe vreme za intervju, napadač otkriva da je to online intervju putem određene usluge za razmenu poruka, koja od žrtve traži da unese lične podatke kojima napadač tada može da pristupi [16].

Prevare sa kriptovalutama se sprovode [32] tako što napadači kreiraju lažne platforme za trgovanje kriptovalutama ili lažne verzije zvaničnih kripto-novčanika (koje izgledaju slično legitimnim sajtovima). Lažni kritposajtovi uglavnom rade na dva načina, kao fišing stranice i kao jednostavna prevara [17].

- **Fišing stranice** podrazumevaju upotrebu fišing stranica, gde prevaranti imaju mogućnost da vide sve podatke (lozinka kripto-novčanika, lični i finansijski podaci) koje žrtva unese [17].
- **Jednostavna prevara**, sa druge strane, u početku omogućava žrtvi da podigne malu količinu novca. Ako žrtva vidi da investicije imaju dobre rezultate ona ulaže dodatni novac, međutim kada posle određenog vremena pokuša da podigne novac sajt se ili gasi ili odbija zahtev [17].

Krađa identiteta podrazumeva nezakonito pribavljanje i korišćenje tuđih ličnih podataka u razne svrhe (za dobijanje kredita ili novca, kupovinu proizvoda, sumnjive transakcije sa računa). Ova vrsta prevare dešava se uglavnom na društvenim mrežama, gde napadač kopira sliku profila i lične podatke žrtve koje su javno dostupne i pravi lažni nalog koji koristi u različite svrhe. Zatim, u cilju dolaženja do dodatnih informacija, šalje zahteve profilima koje žrtvin originalni profil prati [30].

Takođe se dešava da prevaranti pogode lozinku žrtve pomoću algoritama koji mogu da pogode milijarde lozinki u sekundi, čime dolaze do ličnih podataka žrtve. Nakon dobijanja podataka o identitetu, napadači mogu da koriste žrtvin račun u banci, prave nove račune na lažno ime, vrše transakcije na svoje račune i kupuju proizvode novcem žrtve.

Ovde takođe treba navesti i prevaru internet bankarstva koja je česta pojava. Napadači korišćenjem onlajn tehnologije nezakonito izvlače novac sa bankovnog računa žrtve i vrše transfer novca na svoj račun [17, 25].

Jedan poznati primer krađe identiteta desio se 2001. godine kada je Abraham Abdalah, koristeći mobilne telefone i usluge preko govorne pošte, uspeo da dođe do ličnih informacija i brojeva kreditnih kartica brojnih poznatih ličnosti. Procenjuje se da je za šest meseci, koliko su njegove obmane trajale, ukrao oko 22 milona dolara [21].

Prevara sa kreditnim karticama odnosi se na bilo kakvu neovlašćenu upotrebu kreditne, debitne kartice ili sličnog načina plaćanja za kupovinu proizvoda ili usluga bez ovlašćenja vlasnika kartice. Ovo ne zahteva fizičko posedovanje kartice žrtve i može se uraditi pristupom broju kreditne kartice, datumu isteka i CCV broju. Prevara sa kreditnim karticama se često dešava nakon uspešnog okončanja druge vrste internet prevare gde se dobijaju podaci o kartici [8].

3 Žrtve internet prevara

U ovoj sekciji biće reči o tome ko su najčešće žrtve internet prevara, koje osobine ličnosti su pozitivno a koje negativno korelisane sa verovat-

noćom da osoba postane žrtva neke od internet prevara, kao i o tome koliki su prosečni gubici nastali usled internet prevara.

Možda iznenađujuće, podaci Savezne trgovinske komisije (FTC) iz 2021. godine [6, 9] pokazuju da su u SAD-u osobe od 18 do 59 godina generalno češće prijavljene kao žrtve prevara nego one starije od 60. Ipak, pol i starosna dob žrtava znatno zavisi od vrste prevare. Na primer, mlađe osobe su bile znatno podložnije prevarama vezanim za internet kupovinu, zapošljavanje i investiranje (naročito u kriptovalute), dok su, sa druge strane, starije osobe češće bile žrtve nagradnih igara, lutrijskih prevara i prevara tehničke podrške (što se može dovesti u vezu sa njihovim obično znatno slabijim tehničkim znanjem). Iako su se starije osobe ređe javljale kao žrtve prevara, upravo oni su imali drastično veće središnje vrednosti gubitka, oko 800 dolara za one od 70 do 79 godina, čak 1500 dolara za one starije od 80, dok je za mlađe osobe središnja vrednost gubitka bila 500 dolara. Još jedna velika razlika je i u tome da li se prevare odvijaju preko društvenih mreža ili elektronske pošte. Tako su napadači češće stizali elektronskom poštom do starijih žrtava, dok su društvene mreže češće bile mesto prevara za mlađe osobe. U tabeli 3 su dati podaci o procentima ukupnih prevara za različite metode kontakta.

Tabela 1: Procenat prijava prevara za različite metode kontakata i starosne grupe

Metod kontakta	**Mlađi (18 - 59) %**	**Stariji (60 -) %**
Društvene mreže	31	15
Telefonski poziv	10	24
Vebsajt ili aplikacija	30	21
Elektronska pošta	7	11
Internet reklama	6	10
SMS poruka	4	5
Ostalo	12	13

S obzirom na to da veliki broj ljudi provodi dosta vremena na društvenim mrežama, koje se, kao što je napomenuto, često javljaju kao mesto prevara, može se postaviti pitanje koji faktori utiču na podložnost osoba na ove prevare [33].

Jedno istraživanje iz 2015. godine [33] se upravo bavilo uticajem navika i ponašanja studenata na Fejsbuku na rizik da budu prevareni fišing napadom. Pokazalo se da osobe koje su mnogo vremena provodile na Fejsbuku i nisu mogle da iskontrolišu dužinu provedenog vremena na internetu, imaju dosta veću verovatnoću da prihvataju zahteve za prijateljstvo od nepoznatih ljudi. Takođe, i osobe koje su osećale da su pod društvenim pritiskom da uzvrate zahtev za prijateljstvo su ga mnogo češće prihvatale, dok su osobe koje se više brinu za svoju privatnost bile pod manjim rizikom da prihvate zahtev nepoznatih osoba.

Gorepomenuto istraživanje je takođe pokazalo da za osobe naviknute da provode puno vremena na Fejsbuku postoji veća verovatnoća da odgovaraju na poruke od nepoznatih ljudi na Fejsbuku (u istraživanju su studenti dobijali poruku od osobe koja se predstavljala kao poznanik nekog kome su potrebni studenti za praksu i tražila određene lične informacije). Takođe, postoji mogućnost da su veliki broj prijatelja na Fejsbuku, kao i njegovo često korišćenje doprineli tome da osobe previde neke detalje poruke ili pomisle da je od prijatelja, ne razmišljajući odakle ga poznaju

i kako je došlo do toga da budu povezani na Fejsbuku, zbog čega često završe kao žrtve fišinga.

U prethodnom primeru, kao što se često dešava i u drugim fišing prevarama, dolazi do tzv. perifernog procesiranja informacija [33, 14], gde osoba iz dobijene poruke ne zaključuje o njoj prvenstveno na osnovu njenog sadržaja i činjenica, već na osnovu načina na koji je prezentovana. Stoga su vršena mnoga istraživanja u cilju ispitivanja koje osobine ličnosti utiču na to da će osoba verovatnije procesirati informacije iz fišing poruka na ovaj način i samim tim imati veći rizik da bude njegove žrtve [14]. Pokazalo se da su otvorenost, saradljivost i neuroticizam osobine koje imaju pozitivan uticaj i na periferno i na centralno procesiranje. Sa druge strane, pokazalo se da savesnost ima negativan uticaj na periferno procesiranje, pa se smatra da će savesne osobe lakše prepoznati fišing prevaru. Takođe, ispostavilo se da ekstraverzija nije imala statistički značajan uticaj ni na periferno ni na centralno procesiranje.

Još jedno anketiranje koje treba pomenuti bavilo se utvrđivanjem uticaja karakteristika osoba na njihovu podložnost internet prevarama je rađeno 2020. godine i obuhvatalo je preko 10.000 osoba sa područja Ujedinjenog Kraljevstva [34]. Ovo istraživanje pokazalo je da je lokus kontrole uticajan na podložnost prevarama. Naime, osobe koje veruju da imaju kontrolu nad tokom svog života su češće bile prevarene. To se može objasniti time što zbog sigurnosti u sebe zanemaruju uticaj koji napadači mogu imati na njihove odluke. Možda neočekivano, isto istraživanje je pokazalo da su muškarci i edukovane osobe češće bili žrtve. Takođe treba napomenuti da su žrtve prevara sa ulaganjem su češće bili stariji i muškarci, dok su žrtve prevare potrošača uglavnom bile žene i manje edukovane.

Sva ova istraživanja o žrtvama su veoma značajna, jer mogu dati značajne informacije koje se kasnije mogu koristiti za razumevanje mehanizama prevara u cilju borbe protiv njih, kao i u osmišljavanju programa obuke i edukacije osoba na temu internet bezbednosti [35, 9]. Zbog toga je važno da internet prevare budu prijavljene, kako bi mogla da se stekne što realnija slika o ovom problemu. Prema podacima iz različitih godina (2005, 2011, 2017) [4] oko 45% žrtava se žalilo nekome osim svoje porodice i prijatelja. Procenat prijavljenih prevara značajno zavisi od vrste prevare na koju su žrtve nasele: osobe kojima je naplaćen proizvod koji nisu pristali da kupe su se znatno češće žalile (60%) nego, na primer, osobe koje su platile lažnu popravku računara (20%). Žrtve su se najviše žalile prodavcu ili proizvođaču proizvoda (30%), manje njih banci ili pružaocu platnih usluga (12%), a državnim institucijama samo oko 3%.

4 Kako se ljudi mogu zaštititi od internet prevara?

Ova sekcija biće posvećena načinima na koje se ljudi mogu zaštititi od internet prevara. Postoje različiti načini da se spreče internet prevare, kao što su edukacija, razumevanje kako sajber napadi funkcionišu, kao i uvid u raznovrsnost internet prevara, a koji se vrlo često uzimaju zdravo za gotovo. Upravo su sami korisnici prva linija odbrane od internet prevara. Zato je važno imati određenu dozu sumnje i kritičkog mišljenja prilikom korišćenja interneta. U nastavku će biti opisani opšti saveti, kao i načini prevencije od specifičnih internet prevara, koje se često dešavaju.

Rezultati Jubiko ankete iz 2023. godine pokazuju da čak 39% ljudi koristi istu lozinku za veći broj naloga [36]. Jedan od opštih saveta jeste

da se za svaki nalog koristi jedinstvena lozinka. Na taj način, ako napadač dođe do lozinke jednog od naloga, to ga sprečava da ima pristup svim nalozima žrtve. Poželjno je često menjati lozinke i koristiti dvofaktorsku autentifikaciju, ukoliko je dostupna. Redovno ažuriranje veb pregledača pomaže u zaštiti od potencijalnih propusta koje starije verzije nose sa sobom. Takođe, dobra je praksa proveriti sigurnost konekcije veb-sajta, što se može lako uraditi, na primer, u Google Chrome pretraživaču postoji sivi katanac, ispred URL-a, koji označava sigurnu konekciju. Često nas veb pretraživač obavesti da konekcija nije sigurna, pa ovo obaveštenje ne treba ignorisati [29].

Pored opštih saveta, postoje i specifični načini zaštite od fišinga. Jedan od njih jeste detektovanje fišing sajtova. Oni se mogu blokirati i na taj način se ne mogu koristiti za prevaru. Iako je relativno lako manuelno proveriti da li je veb-sajt fišing ili ne, automatsko lociranje ovih veb-sajtova predstavlja znatno teži posao. Zato ljudi koji održavaju originalni veb-sajt često sprovode aktivnosti praćenja kako bi identifikovali potencijalne pretnje, poput neovlašćenih domena koji su slični njihovom (na primer, *www.1cbc.com.cn* može biti domen lažnog sajta, dok je domen originalnog veb-sajta *www.icbc.com.cn*). Praćenje se sprovodi putem provere baza registracije domena, izvršavanja DNS upita i korišćenja specijalizovanih alata.

Pored prethodno navedenog, takođe, ukoliko napadač želi da duplira sadržaj čitavog veb-sajta, on može koristiti i različite alate da automatski preuzme veb-stranice sa određenog sajta. Ovakva preuzimanja moguće je detektovati i pratiti, pa na taj način napadač može biti identifikovan. Oba pristupa imaju svoje nedostatke [5].

Sa druge strane, poslovni veb-sajtovi, poput veb-sajtova banaka, mogu pribeći nekoj od novih metoda za garanciju bezbednosti korisničkih informacija. Na primer, Barkli banka daje čitač kartica svojim korisnicima. Pre kupovine, korisnici moraju da ubace karticu u čitač i ukucaju svoj lični pin kod, nakon čega se generiše jednokratna šifra. Korisnik može obaviti transakciju jedino ako ukuca tačnu šifru. Još jedan od primera bio bi pokušaj kompanije Paypal da uz uobičajeno unošenje šifre dodatno uključi i prepoznavanje glasa, i na taj način dodatno unapredi bezbednost korisnika.

Sa ovim metodama, koje su primeri dvofaktorske autentifikacije, napadač ne može naneti štetu čak iako je došao do osetljivih podataka. Mana ovih pristupa je povećavanje troškova i usložnjavanje cele infrastrukture, te je potrebno još vremena da se ove tehnike šire prihvate [5].

Takođe, napadači često koriste slabost SMTP (eng. *Simple Mail Transfer Protocol*) protokola za slanje elektronske pošte. Kako njemu nedostaju mehanizmi autorizacije, informacije pošiljaoca, kao i rute preko kojih je poruka isporučena mogu biti lažirane u ovom protokolu. Iz tog razloga, napadači mogu poslati velike količine fišing poruka sa lažne adrese elektronske pošte. Učestalost fišing napada bi drastično opala, ukoliko bi antispam sistem mogao da utvrdi da li je poruka zaista poslata sa naznačene adrese. Tehnike koje sprečavaju pošiljaoca da falsifikuje poruku sastoje se iz proveravanja da li je poruka poslata sa servera koji je autorizovan da šalje poruke sa tog domena. Ukoliko to nije slučaj, poruka se označava kao spam. Iz ove perspektive, fišing poruke se mogu posmatrati kao tip spam poruka [5].

Kao i za fišing, i za farming postoje specifični načini zaštite. Jedan od njih je korišćenje antivirusa i antimalvera koji predstavljaju zaštitu od farminga koji se zasniva na zlonamernom softveru. Sa druge strane, od

trovanja DNS servera, pojedinac se može zaštititi korišćenjem VPN-a i povezivanjem na privatni DNS server koji koristi enkripciju sa kraja na kraj. On je bolje konfigurisan i otporniji je na trovanje DNS-a. Takođe, može se podesiti i DNSSEC, koji radi tako što dodeljuje digitalne potpise DNS podacima i analizira sertifikate korenog domena da bi se uverio da su svi odgovori autentični. Na taj način se osigurava da svaki DNS odgovor dolazi sa originalne veb-stranice. Nažalost, DNSSEC nije u široj upotrebi, pa DNS podaci često ostaju neenkriptovani. Takođe, češće brisanje DNS keša može pomoći da iskvareni podaci što manje vremena budu dostupni potencijalnim žrtvama [29].

I na kraju, specifični načini za zaštitu od lažnog predstavljanja mogu se koristiti servisi kao što su Information.com i Instant Checkmate. Oni mogu pomoći pri otkrivanju profila sumnjive osobe na društvenim mrežama, vesti i artikala gde se žrtva pominje, njenog radnog mesta, porekla, ili bilo kog drugog sadržaja koji sadrži njeno ime [3].

Čak i ako se ne upotrebi ova vrsta provere, treba znati da nikako ne treba deliti lične podatke sa nepoznatim osobama [15]. Iz tog razloga, ako napadač počne da se raspituje o ličnim podacima žrtve, kao što su adresa, detalji naloga ili podaci o životu, moguće je da je u pitanju prevara. Ukoliko napadač traži šifru zbog dodatne sigurnosti, uzbune ili nekakve potvrde, velika je verovatnoća da je u pitanju prevara [3].

Takođe, ukoliko je osoba sa kojom se žrtva dopisuje sumnjiva, dobra ideja je pretražiti slike koje ta osoba koristi, jer ih je relativno lako identifikovati. Alati koji omogućavaju ovakve pretrage, mogu potvrditi autentičnost slike, kao i nalaženje originalne verzije. Primer takvog alata je TinEye [3].

Na kraju, jedan od najbržih načina za detekciju lažnog predstavljanja jeste zahtevanje video poziva. Ukoliko ta osoba odbije poziv, pod izgovorom da nema kameru, trebalo bi odmah posumnjati u ispravnost identiteta [3].

5 Zaključak

Kao što je u radu i izloženo, postoji mnogo vrsta internet prevara, a još više načina na koje korisnici mogu biti obmanuti. Poražavajuća statistika pokazala je da nijedan korisnik interneta nije imun na prevare, tj. za svakoga, nezavisno od pola, godina i zrelosti postoji prevara na koju bi mogao da nasedne. Stoga se treba neprestano edukovati, biti veoma oprezan pri komunikaciji sa nepoznatim ljudima, menjati šifre redovno, te ne deliti lične podatke ni sa kim. Međutim, kako je tehnologija u stalnom razvoju, izvesno je da će prevaranti pronalaziti sve inovativnije načine da dođu do zarade. Upravo zbog toga, odbrana od internet prevara će biti izazov dok god se tehnologije i ljudski um razvijaju.

Literatura

[1] Sajber kriminal. on-line at: https://vokabezbedno.weebly.com/sajber-kriminal/internet-prevare.

[2] Abnormal. What Is Pharming? How DNS Spoofing and Malware Sends Users To Fake Websites? on-line at: https://abnormalsecurity.com/glossary/pharming.

[3] Cyber Management Alliance. 6 ways to protect yourself from online catfishing. on-line at: https://www.cm-alliance.com/cybersecurity-blog/6-ways-to-protect-yourself-from-online-catfishing.

[4] Keith B. Anderson. To whom do victims of mass-market consumer fraud complain? *Available at SSRN 3852323*, 2021.

[5] Mayur Bhati and Rashid Khan. Prevention approach of phishing on different websites. *International Journal of Engineering and Technology*, 2(7):1097–1098, 2015.

[6] Federal Trade Commission. Who experiences scams? a story for all ages - federal trade commission, 2022. on-line at: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/12/who-experiences-scams-story-all-ages.

[7] European consumer centre France. Online fraud. on-line at: https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams.html.

[8] Anti cybercrime group. COMMON TYPES OF INTERNET FRAUD SCAMS. on-line at: https://acg.pnp.gov.ph/main/cyber-security-bulletin/2-uncategorised/172-common-types-of-internet-fraud-scams.html.

[9] Marguerite DeLiema and Paul Witt. Profiling consumers who reported mass marketing scams: demographic characteristics and emotional sentiments associated with victimization. *Security Journal*, pages 1–44, 2023.

[10] FBI. Romance Scams, 2022. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/romance-scams.

[11] FBI. Charity and Disaster Fraud, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud.

[12] FBI. Elder Fraud, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/elder-fraud.

[13] FBI. Spoofing and Phishing, 2023. on-line at: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing.

[14] Edwin Donald Frauenstein and Stephen Flowerday. Susceptibility to phishing on social network sites: A personality information processing model. *Computers & security*, 94:101862, 2020.

[15] Draško Grbić, Brankica Jokić, and Tatjana Medarević. *Osnovi informatike za šesti razred osnovne škole*. Zavod za udžbenike i nastavna sredstva, Istočno Sarajevo, 2014.

[16] Indeed. 17 Common Job Scams and How To Protect Yourself. on-line at: https://www.indeed.com/career-advice/finding-a-job/job-scams.

[17] Investopedia. Watch Out for These Top Internet Scams. on-line at: https://www.investopedia.com/articles/personal-finance/040115/watch-out-these-top-internet-scams.asp.

[18] Kaspersky. What Is Pharming and How to Protect Yourself? on-line at: https://www.kaspersky.com/resource-center/definitions/pharming.

[19] Kaspersky. Your Nigerian inheritance is waiting. on-line at: https://securelist.com/your-nigerian-inheritance-is-waiting/36776/.

[20] Jeremy Kirk. Elaborate 'pharming' attack targeted 50 banks. *Computerworld*.

[21] Jory MacKay. The most unbelievable identity theft stories of all time. *Aura*.

[22] Jelena Matijašević, Žaklina Spalević, and Svetlana Ignjatijević. Vrste internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice. *INFOTEH-JAHORINA*, 2012.

[23] New Hampshire Department of Justice. Don't Cash That Check! Check Overpayment Scams, 2023. on-line at: https://www.doj.nh.gov/consumer/dont-cash-that-check/check-overpayment.htm.

[24] Office of the Attorney General for the District of Columbia. Consumer Alert: Sweepstakes and Lottery Scams. on-line at: https://oag.dc.gov/consumer-protection/consumer-alert-sweepstakes-and-lottery-scams.

[25] Australian Federal Police. Internet Fraud. on-line at: https://www.police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf.

[26] New Zealand Police. Scams and fraud. on-line at: https://www.police.govt.nz/advice/email-and-internet-safety/internet-scams-spam-and-fraud.

[27] Proofpoint. What Is Catfishing? on-line at: https://www.proofpoint.com/us/threat-reference/catfishing.

[28] Vaggelis Saprikis, Adamantia Chouliara, and Maro Vlachopoulou. Perceptions towards online shopping: Analyzing the greek university students' attitude. *Communications of the IBIMA*, 2010, 2010.

[29] Panda Security. What Is DNS Spoofing and How Can You Prevent It? on-line at: https://www.pandasecurity.com/en/mediacenter/dns-spoofing.

[30] Federal trade commission. IdentityTheft. on-line at: https://www.ftc.gov/news-events/topics/identity-theft.

[31] Federal trade commission. Phishing scams and how to spot them. on-line at: https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams.

[32] Federal trade commission. What To Know About Cryptocurrency and Scams, 2022. on-line at: https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams#scams.

[33] Arun Vishwanath. Habitual facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1):83–98, 2015.

[34] Monica Therese Whitty. Is there a scam for everyone? psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, 26(3):399–409, 2020.

[35] Emma J. Williams, Amy Beardmore, and Adam N Joinson. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72:412–421, 2017.

[36] Yubico. New Yubico Survey: Boomers Have Better Cybersecurity Habits Than Millennials and Gen Z. on-line at: https://www.yubico.com/press-releases/new-yubico-survey-boomers-have-better-cybersecurity-habits-than-millennials-and-gen-z/.