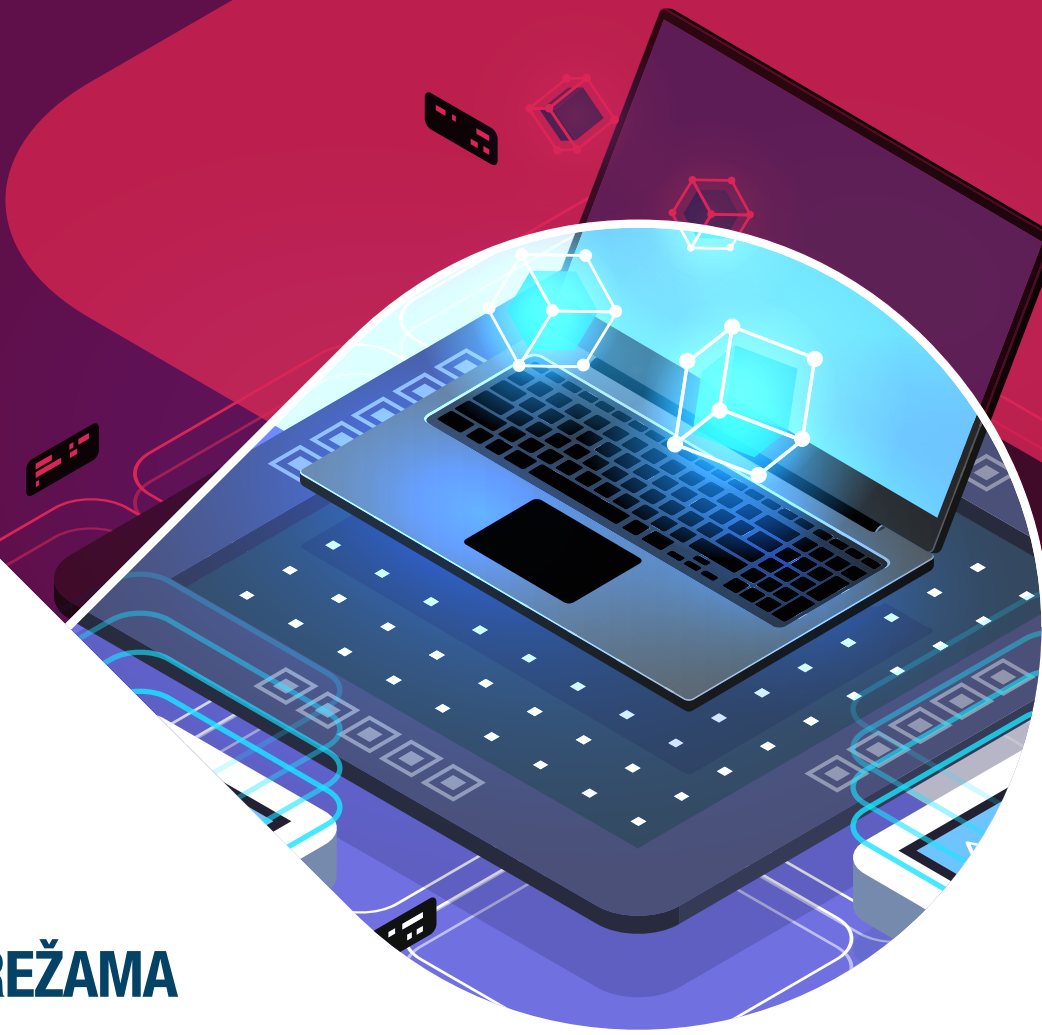
DFC
DIGITALNI FORENZIČKI CENTAR



Mart, 2023.

BEZBJEDNOST NA INTERNETU I DRUŠTVENIM MREŽAMA

mr Jakša Backović

Rukovodilac Grupe za suzbijanje krivičnih djela viskotehnološkog kriminala,
Uprava policije Crne Gore.

I PROBLEM

U ovom radu analiziraćemo bazične bezbjednosne propuste korisnika prilikom korišćenja interneta i društvenih mreža. Posebna pažnja biće usmjerena na neke od zamki kojima su izloženi crnogorski građani u sajber prostoru, te opasnosti po njihove lične podatke. Nadalje, autor upućuje kako zloupotreba ličnih podataka može rezultirati sajber incidentom, koji ultimativno predstavlja prijetnju po ličnost korisnika, funkcionalnost njegove radne okoline ili eventualni finansijski gubitak. Takođe, u radu se teži edukaciji o efikasnim mjerama zaštite prilikom korišćenja interneta i društvenih mreža i upućuje se apel da se jača informatička osvještenost crnogorskog društva u cjelini u sferi moderne digitalne tehnologije.

II UVOD

Sajber bezbjednost – terminološko rješenje koje i dalje teži demistifikaciji i čije značenje treba približiti građanima Crne Gore. Definicija *ITU*-u (*International Telecommunication Union*

Ovaj projekat finansira Ambasada SAD u Podgorici. Mišljenja, nalazi, zaključci ili preporuke koji su ovdje izneseni su stav autora i ne odražavaju nužno stav Stejt dipartmenta/Vlade SAD.

– Internacionalna Komunikaciona Unija) kaže da sajber bezbjednost uključuje skup alata, bezbjednosnih koncepata, zaštitnih mjera kao i obuke i tehnologije koje se mogu koristiti za zaštitu sajber okruženja.[1] To već govori da je pojam sajber bezbjednost ili bezbjednost na internetu veoma opširan koncept i apsolutno obuhvata sigurnost svakog segmenta tehnologije. Upravo tako, svaki dio tehnologije koji je *konektovan* na mrežu, predstavlja potencijalno ugroženi digitalni uređaj, a zaštita korisnika digitalnih uređaja i samih uređaja predstavlja dodatni izazov. Ukoliko uzmemo u obzir da je internet sistem umreženih digitalnih uređaja koji komuniciraju međusobno, imaćemo jasniju sliku da je sve u našem okruženju tehnološki povezano, te svakodnevno *komunicira*.

O visokoj pozicioniranosti teme bezbjednosti na internetu, naročito u okrilju država NATO-a, govori i činjenica da su 2016. godine države članice na Samitu NATO u Varšavi prepoznali sajber prostor kao četvrti domen operacija unutar kojeg se države moraju braniti na efekasan način, isto onako kako to čine u vazduhu, na zemlji i moru. To je takođe prepoznala i naša država Crna Gora, pa je Programom rada Vlade za 2021. godinu kao peti ključni prioritet postavila digitalnu transformaciju, a u okviru nje aktivnosti na podizanju nivoa svjesti, pripremljenosti i reagovanja u cilju jačanja informacione bezbjednosti.[2]

Prema izvještajima Uprave za statistiku Crne Gore (Monstat) o upotrebi informaciono-komunikacionih tehnologija u preduzećima i domaćinstvima za 2022. godinu, utvrđeno je da u Crnoj Gori 81% anketiranih građana ima pristup internetu iz kuće, 98,9% građana ima pristup internetu sa svog mobilnog telefona, a 68,4% pristup sa svog laptop uređaja. Dolazimo do zaključka da su digitalne tehnologije značajno zastupljene među stanovništvom Crne Gore, te da je potencijalna ugroženost naših građana na temu sajber bezbjednosti veoma velika[3].

Tabela 1. Pristup internetu kod kuće, u %

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Pristup internetu kod kuće	51,4	55,0	55,8	63,6	67,5	69,8	70,6	72,2	74,3	80,3	80,8	81,0

Tabela 2. Uređaji pomoću kojih se u domaćinstvu pristupa internetu, u %

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Personalni računar (PC)	72,6	75,3	77,9	75,1	74,1	68,9	56,4	46,6	42,1	34,8	34,2	33,9
Laptop	49,9	52,0	56,7	57,6	56,4	58,4	64,0	65,0	65,9	67,8	67,9	68,4
Mobilni telefon	41,1	24,2	29,7	38,5	46,9	55,2	68,9	79,2	86,4	96,9	98,7	98,9

Nacrt Zakona o informacionoj bezbjednosti Crne Gore definiše incident kao svaki događaj koji ugrožava povjerljivost, cjelovitost i dostupnost skladištenih, prenesenih ili obrađenih podataka ili usluga koje mrežni i informacioni sistemi nude ili kojima omogućavaju pristup.[4] Rasprostranjena upotreba društvenih mreža dodatno otežava situaciju po pitanju bezbjednosti, pa se broj incidenata višestruko uvećava kao posljedica needukovanosti i neinformisanosti korisnika interneta. Po statistici *Dataportal*-a blizu 516 hiljada stanovnika Crne Gore koristi neke od društvenih mreža čak i ne znajući da su one, pored korišćenja elektronske pošte, jedan od glavnih krivaca za nastanak incidenata u sajber prostoru.[5]

U osnovnim i srednjim školama postoje predmeti tehničkog i informacionog karaktera, ali nema konkretne edukacije o tome kako bezbjedno koristiti digitalne uređaje među ovom populacijom. Podaci iz Strategije sajber bezbjednosti Crne Gore 2022-2026 govore da je samo 1% državnih službenika prošlo osnovnu obuku na temu sajber bezbjednosti, te ostaje utisak da se pored svih pomenutih napora ipak nedovoljno pažnje posvećuje sajber bezbjednosti crnogorske informatičke infrastrukture u javnoj upravi, a samim tim i građana. U nastavku ćemo predočiti kojim su to ključnim opasnostima građani Crne Gore izloženi korišćenjem društvenih mreža na internetu.

III RAZRADA

Prijetnje na internetu možemo vezati za neke od ključnih oblasti, a to su oblast: politike, ekonomije, proizvodnje i distribucije štetnih sadržaja i povrede privatnosti. Svaka od navedenih oblasti predstavlja veliku opasnost *per se*, u zavisnosti od ciljnog auditorijuma. Primjera radi, politika je segment u kojem su sajber špijunaže i sabotaže, hibridno ratovanje i sajber terorizam jedan od ključnih faktora na koji treba obratiti pažnju. Domen ekonomije u Crnoj Gori karakterišu kompjuterske prevare i prevare počinjene uz pomoć informacionih sistema. Nadalje, sociološki aspekt društva najviše ugrožavaju oblast proizvodnje i stavljanja u promet dječije pornografije na internetu, dok se krađa ličnih podataka, nadgledanje elektronske pošte, fišing i sl. svrstavaju u grupu prijetnji koje se tiču pitanja povrede privatnosti.

Kada se nađe u sajber prostoru, prvo o čemu jedan građanin treba da brine jeste bezbjednost ličnih podataka, tj. kako ih čuvati, kome ih otkrivati, gdje ih ostavljati dostupnim i kako oni nadalje mogu biti zloupotrijebljeni. Po Zakonu o zaštiti podataka o ličnosti Crne Gore (2020)[6], lični podaci su sve informacije koje se odnose na fizičko lice čiji je identitet utvrđen ili se može utvrditi. Navedenim Zakonom je definisano i čuvanje ili način čuvanja zbirki navedenih podataka. Međutim, problem nastaje šta raditi ukoliko nesavjesno, sasvim slučajno ili vođeni nekim drugim motivom, sami predamo lične podatke ili neki drugi dokument od važnosti nepoznatoj osobi na internetu uz pomoć kojeg bi nam to lice moglo pričiniti duševnu bol ili materijalna štetu. Napominjem da se još uvijek u Crnoj Gori lični podaci (ime i prezime, JMBG i dr.) ne mogu direktno zloupotrijebiti u cilju sticanja protivpravne imovinske koristi, mada postoji mogućnost da pomenuti podaci mogu indirektno dovesti u zabludu treća lica.

Prethodni period posebno su obilježile *krađe* ličnih podataka na način što su od strane nepoznatih lica organizovane nagradne igre na društvenim mrežama, pa su građani Crne Gore dobijali novčane poklone ili vaučere u zamjenu za lične identifikacione podatke tipa slika lične karte, pasoš i dr. Tom prilikom prikupljani su lični podaci od strane većeg broja građana te postoji velika vjerovatnoća da se tako prikupljeni podaci mogu koristiti za neke nedozvoljene aktivnosti socijalnog inženjeringa u narednom periodu, iako to do sada nije bio slučaj. S tim u vezi, nije još uvijek poznato koja su to sve dokumenta prikupljena na ovaj način, te da li su ona negdje već zloupotrijebljena, ali je crnogorska policija postupala po sličnim predmetnim prijavama i podnosila krivične prijave[7] zbog krivičnih djela falsifikovanje i zloupotreba kreditnih kartica i kartica za bezgotovinsko plaćanje.[8] To su najčešći slučajevi kada su crnogorski građani nesavjesno odavali brojeve svojih kreditnih kartica i time postajali žrtve sajber kriminalaca, ostavši bez sredstava na bankovnom računu.

Organizovanje *lanaca sreće* tj. piramidalnih prevara na internetu, uz korišćenje raznih metoda i manipulativnih trikova kako bi se došlo do ličnih ili nekih drugih osjetljivih podataka od potencijalne žrtve, jeste samo jedan od *modusa operandi* socijalnog inženjeringa. Radi se o procesu dobrovoljnog davanja informacija *meti* kako bi ona preduzela željenu akciju (koja može biti štetna po nju).[9] Socijalni inženjering je fokusiran na ljudsku prirodu i emocije žrtve i s tim u vezi, sajber kriminalci osmišljavaju brojne načine kako da prevare svoju metu u digitalnom prostoru. Često možemo čuti izraze kao što su: ***bejting, fišing, preteksting, quid pro quo, spir fišing, višing, smišing, hanting, farming*** što predstavlja različite oblike socijalnog inženjeringa i svaka od navedenih vrsta

je jedan od načina kako se žrtva dovodi u zabludu da kriminalcima dostavi svoje lične ili druge kompromitujuće podatke. Prema podacima SOCTA (*Serious and Organized Crime Threat Assessment* – Procjena opasnosti od teškog i organizovanog kriminala u Crnoj Gori) 2021. godine crnogorski građani su najčešće bili žrtve zloupotreba malvera, profila na društvenim mrežama i drugih prevara putem interneta.[10]

BROJ RAZLIČITIH OBLIKA SAJBER KRIMINALA PO GODINAMA

Godina	Napad na web sajtove i IS	Prevare putem Interneta	Zloupotreba profila na društvenim mrežama	Neprikladan sadržaj na Internetu	Malver	Ostali (Uznemiravanje, ucjene, krađa identiteta...)	Ukupno
2011	1	-	-	-	-	-	1
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018	13	68	50	6	363	37	537
2019	19	70	79	11	387	38	604
2020	25	84	90	15	383	44	641
2021	21	75	86	9	430	51	672

SOCTA statistika

Takođe, nijesu zanemarljive prevare koje uključuju zloupotrebu brojeva bankovnih kartica koje građani svjesno ili nesvjesno daju kriminalcima na internetu, a čemu je prethodila neka od tehnika socijalnog inženjeringa. Sasvim je sigurno da je jedan od primarnih ciljeva ovih kriminalnih radnji sticanje protivpravne imovinske koristi, jer kada je treće lice u posjedu brojeva tuđe kreditne kartice, mogućnosti zloupotrebe postaju neograničene. Samo neke od njih uključuju registrovanje na sajtove za onlajn kockanje, trgovinu proizvodima koji naknadno mogu biti unovčeni ili neki drugi preferentni modalitet sajber krminalaca. Najpoznatije i najposjećenije tržište za ovu vrstu nelegalne trgovine jeste *Darknet*, gdje se setovi ličnih podatka prodaju trećim licima.[11]

Društvene mreže, odnosno komunikacije kroz direktne poruke (*direct messaging – DM*) na njima, jedan je od načina kako sajber kriminalci, koristeći provjerene tehnike socijalnog inženjeringa, mogu doći do podataka o svojim potencijalnim žrtvama. Proces socijalnog inženjeringa može biti izuzetno jednostavan ili znatno komplikovaniji pa može zahtjevati duži vremenski period u svrhu dostizanja željenog cilja. Kao šta je već prethodno rečeno, tu značajno ulogu imaju karakter i *modusa operandi* kriminalca, kroz primjenu odabrane tehnike manipulacije, kao i lakovjernost same žrtve.

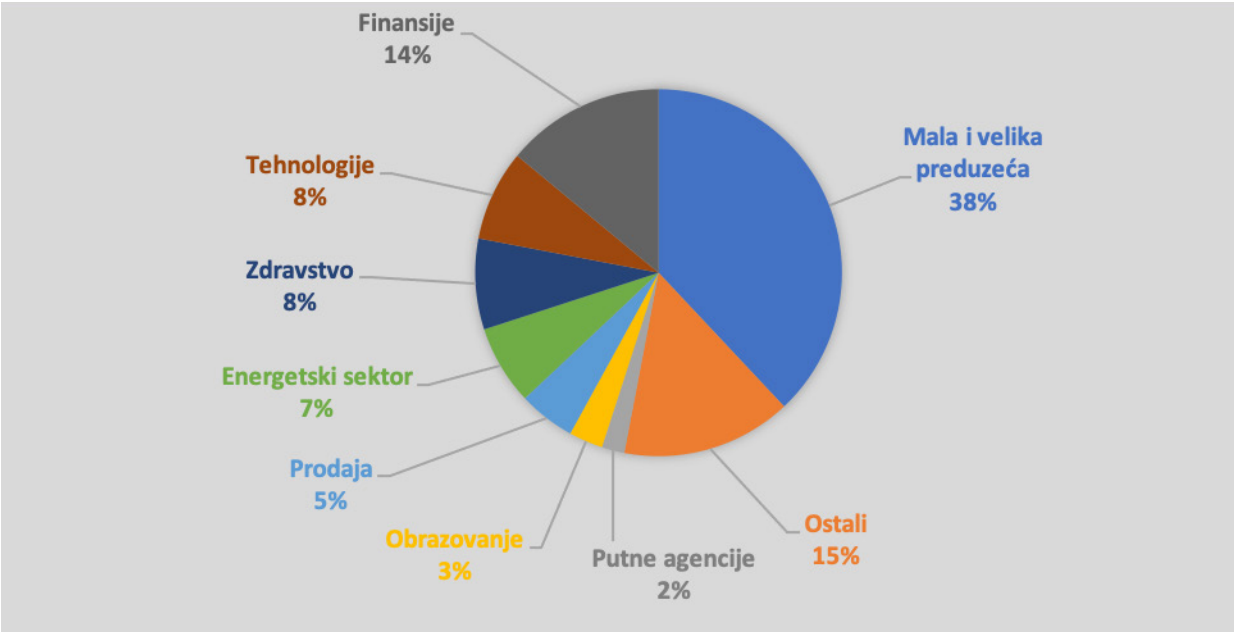
Albert Ajnštajn je s pravom rekao: *Samo su dvije stvari beskonačne: ljudska glupost i Univerzum, samo što kod ove druge nisam baš sasvim siguran*. U sajber prostoru to bi značilo da vašu naivnost možete vrlo skupo platiti. Naime, u velikom broju slučajeva, prvi kontakt sa žrtvom ostvaruje se promptno posredstvom društvenih mreža ili elektronske pošte. Zbog toga potrebno je dobro razmisliti o činjenici da nalog na društvenoj mreži korisnika bude privatan, odnosno da informacije na profilu ne budu vidljive za sva lica, te da se u startu izaberu opcije šta drugi učesnici u sajber prostoru mogu da vide od ličnih podataka, a šta baš i ne. Posjedovanje privatnog naloga ujedno pruža mogućnost korisniku za gledanje sadržine drugih javnih profila, bez bojazni da privatne informacije budu vidljive tim drugim korisnicima

društvene mreže. Sve prethodno nabrojano čini pitanje sigurnosti na društvenim mrežama, tj. problematiku koja se tiče korišćenja konkretne društvene mreže; zaštite ličnih podataka; odabira prijatelja itd. dodatno kompleksnijim.

Još jedna činjenica koju treba imati u vidu prilikom korišćenja društvenih mreža jeste objavljivanje imena i prezimena korisnika registrovanog na mreži. Ovaj podatak je javan i isti će biti objavljen na svaki postavljeni komentar ili drugu interakciju na društvenim mrežama. To posebno u situacijama kada se korisniku sviđa neka fotografija, komentar ili status, koji može slobodno da citira ili podijeli na svom profilu i na ovaj način učestvuje u široj konverzaciji, što je u jednu ruku i glavna poenta društvenih mreža i umrežavanja. Takođe, postoji i mogućnost korišćenja nadimka na mrežama, koji ljudi češće koriste prilikom oslovljavanja, a sve radi lakšeg pronalaženja na društvenim mrežama. O svemu ovome treba dobro voditi računa zarad lične zaštite na društvenim mrežama. Društvene mreže poput *Fejsbuka i Instagrama* omogućavaju da navedete još ličnih podataka poput: škole koju ste pohađali; firme u kojoj radite, brojeve telefona i sl. Dodatno treba razmisliti o tome da li su to podaci koje želite da podijelite sa svim vašim onlajn prijateljima i pratiocima. Možda bi bila dobra ideja izostaviti sve nepotrebne informacije na društvenim mrežama, jer upravo one nas čine pogodnom metom za socijalni inženjering, kroz lažno predstavljanje sajber kriminalaca.

U nastavku, nastojaćemo da sumiramo najčešće sajber incidente u sferi digitalnih tehnologija, kojima su izloženi građani Crne Gore.

BEC prevare (*Business Email Compromise* – kompromitacija poslovne elektronske pošte) ili *CEO* prevare (*Chief Executive Officer – direktorske prevare*) su vrsta prevara koje pričinjavaju najveću finansijsku štetu kompanijama širom svijeta. U pitanju su prevare gdje zaposleni dobijaju lažne mejlove od svog rukovodioca, u kojima se zahtijeva transfer velikih suma novca. Kako bi sajber kriminalci izvršili ovu vrstu prevare, moraju imati impozantno znanje iz oblasti informacionih tehnologija. Prema podacima kompanije *Symantec*[12], najčešća meta sajber kriminalaca su mala i srednja preduzeća (38%), u kojima je nivo sajber kulture na veoma niskom nivou te nemaju standardne operativne procedure (SOP) u slučaju potencijalnog sajber incidenta.



Mala i velika preduzeća su najviše ciljana grupe za BEC prevare

BEC prevarama pretežno prethodi *hakovanje* elektronske pošte neke kompanije, kada sajber kriminalci, koristeći već pomenute tehnike socijalnog inženjeringa, dođu u posjed informacija o pristupu elektronskoj pošti i vrše nadgledanje komunikacija koju firme ostvaruju sa dobavljačima ili klijentima. Kada zaposleni u kompaniji (žrtva prevare) želi da izvrši uplatu prema dobavljaču ili klijentu, sajber kriminalci izvrše presrijetanje i blokiranje komunikacije tj. mejla, izmjene postojeći broj žiro računa i tako dovedu u zabludu obje strane da je novac pošao na ispravan broj žiro računa. Obično su ove vrste prevara toliko uvjerljive, a sva dokumentacija toliko autentična da žrtva i ne posumnja da novac šalje na žiro račun koji nije u vlasništvu kompanije sa kojom ima ostvarenu saradnju. Najbolji način zaštite od ovih vrsta prevara je dodatni oprez tj. sumnjičavost prema zahtjevima ovog tipa dobijenim posredstvom informaciono-komunikacionih tehnologija, a posebno onima koji nisu u skladu sa pravilima i procedurama kompanije. Potrebno je poštovati SOP-ove svoje kompanije, provjeriti legitimnost izvora podataka te koristiti dvostruki faktor autentifikacije prilikom komunikacije sa klijentima[1].

Poslednjih godina, unošenje malicioznih programa u računar žrtve ili ransomver napadi (*ransomware*)[2] su jedan od najopasnijih i najzlonamjernijih oblika sajber napada. Posljedice ovog napada su obično velike i veoma ih je teško otkloniti nakon što računar bude zaražen. Zbog toga, prevencija sajber napada ove vrste je najbolja i najefikasnija strategija koja postoji. Ransomver se obično širi kroz fišing mejlove koji sadrže štetne priloge, a koje treba preuzeti i instalirati na računaru. Sajber kriminalci koriste tehnike socijalnog inženjeringa kako bi natjerali žrtvu da otvori mejl, nakon čega ransomver šifrira sve podatke u računaru i ostavlja poruku žrtvi da je neophodno da se uplate novčana sredstva kako bi računar ponovo bio u funkciji. Postoji nekoliko oblika ransomvera kao što su *Locker, Scareware* i *Doxware.* ***Locker*** uglavnom ne bira šta zaključava na žrtvinom računaru i kada se jednom nađe u sistemu, vrši šifriranje svih mogućih podataka. Ukoliko žrtva ne može koristiti računar i njegove osnovne funkcije, a da se stalno ne prikazuje poruka u kojoj se zahtijeva novac, postoji velika vjerovatnoća da je sistem zaražen ovom vrstom malicioznog programa. ***Scareware*** takođe radi po principu da zaključava pristup svim funkcijama sistema, odnosno onemogućava njegov rad, a razlika u odnosu na prethodne je da se na računaru sa ograničenim funkcijama pojavljuje prozor**čić** koji navodno *skenira* žrtvin kompjuter u potrazi za problemima u sistemu i prilikom čega će žrtva dobiti obavještenje da se na računaru nalazi štetan program, te da ukoliko se ne plati određana suma novca, računarski sistem će biti nedostupan. ***Doxware*** je vrsta štetnog programa koji briše sadržaj koji se nalazi na računarskom sistemu. Obično nakon inficiranja računara, žrtva dobija poruku da će sadržaj biti objavljen na internetu kao i svi žrtvini osjetljivi podaci ukoliko ne plati traženi iznos. Drugi način na koji ransomver može doći u računarski sitem žrtve je *upadom* hakera u sistem kroz tzv. rupe u odbrambenom sistemu kompjutera, odnosno korišćenjem *exploit* programa[3] koji iskorišćavaju ranjivosti ili greške u kodovima na kompjuterskom ili operativnom sistemu i na taj način unosi štetne programe. Kompanije koje se bave sigurnošću računarskih sistema u kontinuiteti traže ranjivosti u kodu koje mogu predstavljati probleme i nakon njihovog otkrivanja propusti se obično isprave, odnosno pomenute *rupe se zakrpe*. Najednostavniji način zaštite od ove vrste napada je opet prevencija kao i podizanje nivoa svijesti korisnika računarskih sistema o pravilnom načinu korišćenja informacionih tehnologija. Instaliranje antivirus i antimalver programa, redovno ažuriranje operativnih sistema kao i redovno pravljenje kopija podataka će dodatno spriječiti potencijalne sajber napade.

1 Proces dvostruke provjere koja služi za pristup nekim stranicama ili servisima, a koja podrazumjeva lozinku i dodatnu metodu provjere vjerodostojnosti.

2 Vrsta štetnog softvera koji korisniku uskraćuje pristup računarskim resursima i traži plaćanje otkupnine.

3 Sigurnosni propust ili slabost u kodu računarskog sistema koji iskorišćavaju sajber kriminalci.

Sextortion (ucjena seksualnim sadržajem) je imenička složenica nastala leksičkim spajanjem dva pojma *sex* i *extortion* – što bi u prijevodu značilo iznuda ili ucjena na temelju seksualnog sadržaja. *Modus operandi* seks ucjene je da napadači od žrtava traže usluge seksualne prirode, novac ili neke druge usluge kako ne bi objavili njihov lični intimni ili seksualno eksplicitni sadržaj tj. fotografije ili videa. Napominjemo da su upravo žrtve te koje u nekom trenutku počinitelju same šalju predmetne kompromitujuće materijale ili je pak takav materijal proizveden uz korišćenje raznih digitalnih alata za snimanje. Najčešće se prvi kontakti sa žrtvom ostvaruju korišćenjem društvenih mreža kao što su *Facebook* i *Instagram*, gdje se šalju direktne poruke (*DM*) sa zahtjevom za prijateljstvo. Uz primjenu raznih tehnika socijalnog inženjeringa, sajber kriminalci se predstavljaju kao usamljeni pojedinci kojima treba pažnja i intimnost i pritom nude video komunikaciju koja ima samo jedan cilj - doći do podataka koji bi kompromitovali žrtvu. Obično se do eksplicitnog materijala žrtve dolazi izgradnjom odnosa povjerenja kroz razne vrste manipulacija ili lažnim predstavljanjem. Takođe, još jedan od načina pribavljanja eksplicitnog materijala žrtve jeste hakovanje korisničkih naloga na društvenim mrežama i personalnih digitalnih uređaja žrtve. Na taj način sajber kriminalci dolaze u posjed fotografskog ili video materijala eksplicitne prirode i iniciraju ucjenjivačke poruke, korišćenjem društvenih mreža. Sajber kriminalci se umnogome oslanjaju na dominantan strah od osude okoline, koji će žrtvu nedvosmisleno motivisati da uplatiti traženu sumu novca, u trenutku kada je suočena sa situacijom javnog iznošenja ličnog eksplicitog materijala. Ovdje takođe napominjemo da Krivični Zakonik Crne Gore uvodi krivično djelo Ucjena u članu 251.[13]

Pojam *on-line* prodavnica predstavlja vrstu ponude usluga ili prodaje proizvoda na internetu. Onlajn prodavnica je mjesto gdje se vrši onlajn kupovina (*online shopping* – onlajn šoping). Navedena kupovina podrazumijeva proces u okviru koga korisnici interneta mogu da kupuju određene proizvode ili usluge i da iste plate najčešće upotrebom kreditnih kartica. Prema izvještajima Uprave za statistiku Crne Gore o upotrebi informaciono-komunikacionih tehnologija u svrhu onlajn kupovine, primjetićemo da 2018. godine čak 73% građana Crne Gore nikada nije koristilo ovu vrstu onlajn usluge, dok se taj procenat 2022. godine smanjio na 53%, što predstavlja značajan rast od 20%. Ovaj rast svakako da rezultira i rastom mogućnosti zloupotreba u domenu kupovine posredstvom interneta.

Tabela 3. Kada ste posljednji put kupili ili naručili robu ili uslige preko Interneta u privatne svrhe, u %

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
U posljednja 3 mjeseca	6,1	7,0	10,1	11,1	10,8	11,3	15,7	19,5	19,9	20,5
Prije više od 3 mjeseca	3,0	4,6	3,9	5,5	6,2	4,9	5,1	9,8	12,3	9,4
Prije više od godinu dana	2,7	7,3	9,9	7,6	9,1	10,8	10,2	11,6	14,3	17,1
Nikada	88,2	81,0	76,1	75,8	73,9	73,0	69,0	59,1	53,5	53,0

Prema istom Izvještaju, crnogorski građani su u ovom domenu najviše poručivali odjeću, sportske proizvode, hranu i piće. Od početka pandemije virusa *COVID-19*, onlajn trgovima je doživjela nevjerovatnu ekspanziju, posebno u broju realizovanih onlajn transakcija, kao što se može vidjeti iz tabele u nastavku.

Tabela 4. Vrsta robe ili usluge koje su lica najčešće naručivala ili kupovala preko interneta su, u %

	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Odjeća, sportski proizvodi	38,6	73,4	82,9	84,5	77,7	68,2	73,5	77,7	81,4	80,4
Smještaj za odmor (hotel, itd.)	22,7	8,7	9,7	18,9	22,0	20,1				
Ostali putnički aranžmani (karte za prevoz, iznajmljivanje automobila, itd.)	23,0	5,4	5,3	14,8						
Igrice i dodaci za igrice	12,1									
Računarski softver i njegovi dodaci	9,8									
Filmovi, muzika	9,2	2,6	4,3	6,9	10,9	12,8	10,8	11,0	14,9	14,3

Farmaceutski proizvodi	9,1	2,7	3,1	11,6	7,5	6,7	11,0			
Video igrice, drugi računarski softveri i njihovi dodaci		8,3	9,3	6,4	5,3	5,5	5,5	8,4	11,3	10,3
Igračke, namještaj							17,2	19,0	19,1	21,1
Dostava hrane ili pića								27,5	28,5	34,6
Kozmetički proizvodi								17,2	20,5	17,5

Činjenica je da internet trgovina umnogome olakšava kupovinu proizvoda i usluga. U okviru većine internet prodavnica plaćanje je moguće izvršiti svim platnim karticama. S tim u vezi, često se može čuti pitanje vezano za sigurnost plaćanja ovim putem kao i mogućnost prevara prilikom ove vrste trgovine. Onlajn prevare možemo posmatrati kroz četiri koraka. Prvi korak je način na koji kriminalci dolaze do svojih žrtava; drugi predstavlja način dolaska do brojeva kreditnih kartica; treći korak se tiče mogućnosti zloupotrebe tih podataka, a četvrti je zaštita korisnika. Sajber kriminalci najčešće dolaze do brojeva bankovnih kartica žrtava korišćenjem već pomenute metode socijalnog inženjeringa, pretežno slanjem *SPAM*[4] mejlova koji sadrže internet adrese koje upućuju na onlan prodavnice koje simuliraju legitiman biznis za prodaju proizvoda ili pružanje servisa. Druga mogućnost je sponzorisanje baner[5] oglasa na nekom od veb sajtova. Obično su ponude ovim putem veoma unosne, izgledaju primamljivo te je prva pomisao kada ih ugledate da je to suviše dobro da biste propustili takvu ponudu. U većini slučajeva primamljiva ponuda pristiže nekoliko dana nakon što ste, koristeći vaš lap top ili pametni telefon, vršili *Google* pretragu baš tog proizvoda. Velike internet kompanije koriste *kolačiće* (*Cookies*)[6] kako bi identifikovale potrebe svojih posjetilaca i samim tim unaprijedile ponudu. Problem nastaje kada *kolačiće* otkupe sajber kriminalci i počnu slati ponude na mejl adrese ili ih objavljivati putem pomenutih banera. Lažni internet sajtovi ili fišing (*fishing*) stranice su napravljeni samo sa jednim ciljem, a to je krađa ličnih podataka i brojeva bankovnih kartica. Napominjemo da kreditna kartica može biti zloupotrijebljena samo u slučaju kada sajber kriminalci posjeduju: ime korisnika, broj kartice, datum njenog isteka kao i trocifreni broj koji se nalazi na poleđini kartice, odnosno podatke koje inače ostavljamo prilikom legitimne kupovine. Ukoliko se nalazimo na fišing internet stranici i želimo da obavimo trgovinu, ostavićemo navedene podatke i potom ćemo u većini slučajeva od fišing sajta dobiti odgovor da proizvod više nije dostupan i da se trgovina ne može obaviti ili ćemo dobiti odgovor da će paket biti dostavljen kroz nekoliko sedmica. U oba slučaja žrtve sajber kriminalaca nisu ni svjesne da su njihovi podaci otuđeni, sve dok ne saznaju da su zloupotrijebljeni, odnosno kada primijete da na njihovom bankovnom računu nedostaju novčana sredstva. Kada sajber kriminalci dođu u posjed podataka o bankovnim karticama svojih žrtvi, postoji nekoliko načina kako ih mogu zloupotrijebiti, a najčešće je to preprodajom brojeva kreditnih kartica na crnom tržištu ili kupovinom nekih proizvoda koji se naknadno mogu unovčiti. Najbolji način zaštite od fišing sajtova jeste dodatni oprez prilikom kupovine na sajtovima koji podrazumijeva istraživanje da li je već neko obavljao kupovinu na navedenim internet stranicama i kakva su iskustva s tim u vezi. Ukoliko ne možete naći informacije o prethodnim kupovinama na željenom sajtu, velika je vjerovatnoća da se radi o fišing internet stranici. Ukoliko je proizvod koji vas interesuje uz sve to i značajno jefitiniji od stvarne cijene na tržištu i ukoliko pomenutoj ponudi brzo ističe rok, onda postoji dodatna sumnja da se radi o internet fišing sajtu. Takođe, postoji mnogo smjernica kako se zaštititi[14] od onlajn prevara, a poštovanjem onih ključnih, vjerovatnoća da budete žrtva onlajn prevara je svedena na minimum. Sa druge strane, postoje i vrlo bezbjedne platforme za onlajn trgovinu. Primjera radi, crnogorskim građanima su dostupni *Amazon*, *Ebay* ili *AliExpress* koji svojim korisnicima garantuju (ujedno i prodavcu i kupcu) da će proizvod biti isporučen tj. da će novčana sredstva biti uplaćena na pravom mjestu.

4 Pod spemom obično podrazumijevamo poruke marketinškog karaktera putem elektronske pošte, gdje nepoznati pošiljalac nudi svoje usluge.

5 Baner predstavlja oglasni prostor koji je sastavni deo neke veb stranice.

6 Kolačići (Cookies) su mali tektualni programi u vašem računaru koje postavlja Web server kada posjetite neki sajt koji imaju namjenu da identifikuju korisnika koji posjećuje neku web stranu.

Država Crna Gora je 2005. godine potpisala Konvenciju o kompjuterskom kriminalu i time se obavezala da **će** sve preporuke iz pomenute Konvencije implementirati u svoje zakonodavstvo. U tom smislu možemo govoriti o legislativnoj harmonizaciji sa državama potpisnicama Konvencije.[15] Krivičnim zakonikom Crne Gore, 2006. godine, propisuju se krivična djela protiv bezbjednosti računarskih podataka. Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Uprave policije, otvara se radno mjesto čiji opis poslova obuhvata suzbijanje krivičnih djela iz oblasti kompjuterskog kriminala. Takođe, 2014. godine, Vlada Crne Gore nominuje kontakt tačku 24/7 Savjeta Evrope po pitanju kompjuterskog kriminala i time pristupa mreži eksperata bezbedonosnih službi, za brzu razmjenu i prezervaciju elektronskih dokaza. Zakon o informacionoj bezbjednosti Crne Gore objavljen je 2010. godine i u skladu sa njim formiran je *CIRT* tim (eng. *Computer Incident Response Team*) koji je zadužen za odgovor na računarsko-bezbjednosne incidente u sajber prostoru Crne Gore.[16] Navedeni tim je osnovan 2012. godine kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne telekomunikacione unije (*ITU*) i trenutno je pozicioniran u Direkciji za zaštitu tajnih podataka. Prvi Zakon o elektronskim komunikacijama je objavljen 2013. godine i on uređuje način upravljanja i korišćenja elektronskih komunikacionih mreža; uslove i način obavljanja djelatnosti u oblasti elektronskih komunikacija, kao i druga pitanja od značaja za elektronske komunikacije. Usvojene su ključne strategije: Strategija nacionalne bezbjednosti, Strategija odbrane Crne Gore, Strategija o sajber bezbjednosti za period 2022-2026. godine, Strategija sajber bezbjednosti Vojske Crne Gore 2019-2022. godine, što govori o ozbiljnosti pristupa i naporima države Crne Gore u cilju podizanja svijesti o datoj problematici kod službenika javne uprave i šire.

Pored legislativnog okvira u ovoj oblasti, Crna Gora je uspostavila i organizacionu strukturu u oblasti sajber bezbjednosti i prepoznala organe državne uprave nadležne za pomenutu oblast, kao što su: Savjet za informacionu bezbjednost, Tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore(CIRT) , Direkcija za zaštitu tajnih podataka, Agencija za nacionalnu bezbjednost, Ministarstvo odbrane, Ministarstvo javne uprave, Uprava policije i Forenzički centar, a njihova glavna funkcija jeste zaštita građana u sajber prostoru, svako iz domena svoje nadležnosti.

IV ZAKLJUČCI I PREPORUKE

Ovaj rad je imao za cilj da obuhvati najčešće prijetnje sa kojima se građani Crne Gore suočavaju prilikom interakcija u sajber prostoru. Opisani su različiti incidenti (*BEC/CEO* prevare; ransomver napadi; ucjene seksualnim sadržajem; prevare prilikom onlajn kupovine itd.) i predloženi su adekvatni načini postupanja. Kao izrazito efikasne mjere zaštite ličnosti i ličnih podataka prilikom korišćenja interneta i društvenih mreža izdvojene su sljedeće: edukacija korisnika interneta; prevencija sajber incidenata kroz uspostavljanje releventnih SOP-ova, dodatne mjere zaštite uređaja korišćenjem antivirus i antimalver programa kao i redovno ažuriranje korisničkog sistema. Sve ove aktivnosti neophodno je da prati kontinuirano podizanje nivoa svijesti i digitalne pismenosti građana Crne Gore, počev od ranog školskog uzrasta treće dobi korisnika modernih digitalnih tehnologija. Naročito su istaknuti napori države Crne Gore i njenih nadležnih institucijama u kreiranju čvrste legislativne osnove u ovom domenu i stavljanja digitalnih tehnologija u fokus budućih generacija.

VI REFERENCE

1 *Definition of Cybersecurity*, *Međunarodna telekomunikaciona unija,* Dostupno na: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
2 Ministarstvo javne uprave, digitalnog društva i medija*, Strategija sajber bezbjednosti Crne Gore 2022-2026*, 15.06.2022, *Vlada Crne Gore*, Dostupno na: https://www.gov.me/dokumenta/85e2a9d0-0d3c-483a-9822-515d3b7798de
3 *Upotreba informaciono - komunikacionih tehnologija u domaćinstvima i od strane pojedinaca***,** 31.10.2022**,** *Uprava za statistiku Crne Gore – MONSTAT***,** Dostupno na**:** https://www.monstat.org/cg/page.php?id=1848&pageid=1846
4 Ministarstvo javne uprave, *Nacrt zakona o informacionoj bezbjednosti*, 01.03.2023, *Vlada Crne Gore*, Dostupno na: https://www.gov.me/dokumenta/e0bbdb63-8f15-4b79-8833-9390f286d7a1
5 *Digital 2022: Montenegro*, 16.02.2022, *DataReportal*, Dostupno na: https://datareportal.com/reports/digital-2022-montenegro
6 Ministarstvo unutrašnjih poslova, *Zakon o zaštiti podataka o ličnosti (Službeni list Crne Gore, br. 079/08 od 23.12.2008, 070/09 od 21.10.2009, 044/12 od 09.08.2012, 022/17 od 03.04.2017)*, 18.03.2020, *Vlada Crne Gore*, Dostupno na: https://www.gov.me/dokumenta/d65b84b4-14df-43e0-aeb2-aadf44149486
7 *Zakonik o krivičnom postupku, (Službeni list Crne Gore 028/18 od 27.04.2018),* Dostupno na: https://www.paragraf.me/propisi-crnegore/zakonik-o-krivicnom-postupku.html
8 *Krivični zakonik Crne Gore (Službeni list Crne Gore 003/20 od 23.01.2020. godine) – Član 260,* Dostupno na: https://www.paragraf.me/propisi-crnegore/krivicni-zakonik-crne-gore.html
9 *Šta je socijalni inženjering?*, 26.06.2018, *IT klinika*, Dostupno na: https://www.it-klinika.rs/blog/sta-je-socijalni-inzenjering
10 Ministarstvo unutrašnjih poslova, *Procjena opasnosti od teškog i organizovanog kriminala u Crnoj Gori (SOCTA2021)*, 16.04.2022, *Vlada Crne Gore*, Dostupno na: https://www.gov.me/dokumenta/cf105122-2c9b-4816-b152-8487b5f59063
11 Stamenković, Branko, Doc. dr. Adis Balota, Valentina Pavličić, Bojana Paunović, mr Jakša Backović, *Visokotehnološki kriminal, praktični vodič kroz savremeno krivično pravo i primjere iz prakse***,** 14.04.2014, *OEBS misija u Crnoj Gori***,** Dostupno na: https://www.osce.org/files/f/documents/5/6/117630.pdf
12 *Billion-dollar scams: The numbers behind BEC fraud***,** 12.07.2016, *Symantec*, Dostupno na: https://community.broadcom.com/symantecenterprise/viewdocument/billion-dollar-scams-the-numbers-b?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
13 *Krivični zakonik Crne Gore (Službeni list Crne Gore 003/20 od 23.01.2020. godine) – Član 251,* Dostupno na: https://www.paragraf.me/propisi-crnegore/krivicni-zakonik-crne-gore.html
14 Milosavljević, Milica, *Bezbedna online kupovina: opasnosti i zaštita (drugi deo)*, 07.05.2019, *SecuritySEE*, Dostupno na: https://www.securitysee.com/2019/05/bezbedna-online-kupovina-opasnosti-i-zastita-drugi-deo/
15 *Zakon o potvrđivanju Konvencije o računarskom kriminalu, (Službeni list Crne Gore - Međunarodni ugovori,br. 4/2009 od 20.10.2009. godine),* Dostupno na: https://wapi.gov.me/download/fe845b44-f208-444b-9ff1-3a96b6ce0983?version=1.0
16 *Zakon o informacionoj bezbjednosti (Službeni list Crne Gore, br. 14/2010, 40/2016, 74/2020 - drugi zakon i 67/2021. godine),* Dostupno na*: https://wapi.gov.me/download-preview/fbb730c5-8c62-47e3-863f-cfaae9631b8d?version=1.0*

O BRIFU

DFC *Policy Brief*-ovi analiziraju različite aspekte medijskog okruženja, borbu protiv dezinformacija, stranog malignog uticaja i drugih aktivnosti manipulacije informacijama, nudeći konkretne preporuke. *Briefovi* će biti kreirani u saradnji sa različitim stručnjacima iz zemlje i šireg regiona koji će pružiti dodatni uvid i perspektivu problematike, što će doprinijeti stvaranju i učvršćivaju mreže saradnika koja će održavati i širiti svijest o problemu. Novi broj će izlaziti na svaka 2 mjeseca u saradnji sa novim autorom.

Drugo izdanje ove publikacije analizira bezbjednosne propuste korisnika prilikom korišćenja interneta i društvenih mreža. Posebna pažnja je usmjerena na zamke kojima su izloženi građani u sajber prostoru, te opasnosti po njihove lične podatke. Brief teži da edukuje o efikasnim mjerama zaštite i upućuje na neophodnost snažnije informatičke osvještenosti crnogorskog društva u cjelini u sferi moderne digitalne tehnologije.

O AUTORU

Jakša Backović je zaposlen kao Rukovodilac Grupe za suzbijanje visokotehnološkog kriminala u Upravi policije i posjeduje više od 16 godina profesionalnog iskustva u borbi protiv ove vrste kriminala. Magistrirao je na prestižnom Univerzitetskom koledžu u Dablinu (UCD), čiji je i alumnista, na temu kompjuterskog kriminala i digitalne forenzike. Predavač je na Univerzitetu Mediteran u Podgorici, vanredni predavač na Policijskoj akademiji u Danilovgradu kao i kontakt osoba 24/7 Savjeta Evrope po pitanju kompjuterskog kriminala. Aktivno učestvuje u reformi crnogorskog zakonodavstva i eskpert je Savjeta Evrope i OEBS-a dugi niz godina.

DFC
DIGITALNI FORENZIČKI CENTAR

DFC Policy Brief izdaje Atlantski savez Crne Gore/Digitalni forenzički centar. Izneseni nalazi, stavovi i zaključci su stav autora i ne odražavaju nužno stav ASCG/DFC.