CIVITAS, 2022, 12(1), 338-350
www.civitas.rs

Siniša Domazet[1*]
Zdravko Skakavac[2**]

UDC 004.738.5:343.54:[616.98:578.834
Stručni rad
Primljen: 06. 01. 2022.
Prihvaćen: 27. 01. 2022.

KARAKTERISTIČNI OBLICI ZLOUPOTREBA U SAJBER PROSTORU TOKOM PANDEMIJE VIRUSA COVID-19

Sažetak: Predmet istraživanja odnosi se na karakteristične oblike zloupotreba u sajber prostoru za vreme pandemije. U radu je ustanovljeno da su neki od najčešćih oblika zloupotreba povezani sa fišingom u vezi s elektronskom poštom, krađom kredencijala korisnika, fišingom preko sms poruka, distribucijom malvera, kao i sa komunikacionim platformama. Utvrđeno je da mere sajber higijene za vreme pandemije COVID-19 moraju biti unapređene i efikasnije sprovođene. Takođe, istraživanje je pokazalo da je neophodno unapređenje važeće pravne regulative ne samo na nacionalnom nivou već i na međunarodnom nivou. U radu su korišćeni normativni metod, kao i pravno-logički metodi indukcije i dedukcije.

Ključne reči: pravo, bezbednost, sajber prostor, COVID-19, fišing

1. Uvod

Pandemija izazvana virusom COVID-19 potresla je ceo svet i izazvala brojne posledice i veliki gubitak ljudskih života. Pored svih problema izazvanih pandemijom COVID-19, treba istaći i probleme u saj-

[1*] Vanredni profesor, viši naučni saradnik, Univerzitet Edukons, Fakultet za studije bezbednosti, Vojvode Putnika 87, Sremska Kamenica, Srbija, e-mail: sdomazetns@gmail.com ORCID iD: https://orcid.org/0000-0002-5964-2249

[2**] Redovni profesor, Fakultet za pravne i poslovne studije dr Lazar Vrkatić, Novi Sad, Univerzitet Union, Beograd, Srbija, e-mail: zskakavac@useens.net

ber prostoru, koji poprimaju sve ozbiljnije razmere. Istina, problemi u sajber prostoru nisu nova stvar, oni postoje od samog početka razvoja interneta i informaciono-komunikacionih tehnologija. Ubrzana digitalizacija i sve šira primena savremenih tehnologija dodatno su povećale nivo opasnosti po stanovništvo, privredu i javni sektor širom sveta.

S tim u vezi, aktuelna pandemija izazvana virusom COVID-19 sa sobom nosi ne samo zdravstvene izazove već i zloupotrebe u vezi sa zaštitom ličnih podataka. Prema Đukiću (2017, str. 99), one se „ogledaju u narušavanju poverljivosti informacija, ometanju njihove funkcionalnosti kroz narušavanje poslovanja između njih, uzurpaciji i krađi intelektualne svojine, raznim vrstama drugih krađa i prevara, kao i brojnim zloupotrebama koje se razlikuju po motivima, ciljevima, metodama i načinima postizanja". Kako navodi Petrović (2004), „pojam krađe u vezi sa informaciono-komunikacionim tehnologijama, pored krađe koja se vrši krađom informaciono-komunikacionih uređaja i njihovih komponenti, obuhvata krađu različite robe, krađu računarskih usluga, krađu podataka, krađu kodova, lozinki i identifikacionih brojeva i identiteta" (str. 133).

Tokom pandemije izazvane virusom COVID-19, registrovan je veliki broj različitih vrsta sajber prevara, kao što su oblici zloupotrebe vezani za fišing e-pošte, krađu korisničkih kredencijala, fišing uz pomoć SMS-a, distribuciju malvera i komunikacione platforme, kao što je Zoom aplikacija. Poseban problem predstavljale su društvene mreže koje su se pokazale kao plodno tlo za razne sajber prevare. Prema T. Skakavac (2020) „ne treba zanemariti negativne posledice korišćenja različitih društvenih mreža, posebno od strane maloletnika. Iako su korisnici mnogih društvenih mreža različiti po polu, godinama, obrazovanju i sl., ove mreže imaju najveći uticaj na mlade. Mladi su radoznali, željni novih izazova i svih savremenih modaliteta razvoja informacionih tehnologija i vrlo lako postaju njihovi stalni saputnici i klijenti" (str. 85).

Kada je reč o fišingu, može se reći da je ova vrsta sajber prevara posebno aktuelna tokom pandemije. Kako Grejdon (2006) navodi, termin „fišing" „dolazi iz analogije da prevaranti koriste e-poštu kao mamac za ribu za profitabilne lične podatke iz nesvesnog mora internet korisnika" (str. 335, 337). Prema Domazetu i Skakavcu (2019) „u ranim fazama fišinga, izvršioci su koristili relativno jednostavne metode prevare, tako da su fišing mejlovi bili relativno lako prepoznatljivi (na primer, sadržali su brojne gramatičke i

pravopisne greške), dok je danas fišing evoluirao i postao mnogo složeniji i sofisticiraniji, uključujući brojna napredna softverska rešenja za prikrivanje za dobijanje osetljivih (ličnih) podataka" (str. 191).

Šteta od fišing napada stalno se povećava. Prema Đukiću (2017, str. 110) „samo u 2015. godini u svetu je registrovano oko 147 miliona fišing napada, od kojih je Rusija pretrpela najviše napada (17,8%), dok su SAD bile najbolji 'domaćin' napadačima, a najviše napada izvršeno je sa njene teritorije (15,2%). Po meti, fišing napadi su uglavnom bili usmereni na onlajn finansijske institucije (banke, sisteme plaćanja i onlajn prodavnice)". Kako su izjavili Gudkova, Vergelis, Shcherbakova (2018) „u 2016. registrovano je preko 154 miliona fišing napada, pri čemu je Brazil pretrpeo najviše napada, a preko 12% napada potiče iz Sjedinjenih Država. U 2017. zabeleženo je preko 246 miliona napada, a najveći izvor napada ostale su ove godine Sjedinjene Američke Države (sa učešćem od 13,21%). Malver koji se najčešće koristi zove se *Trojan-Downloader. JS.Sload*". Prema Izveštaju Agencije Evropske unije za sajber bezbednost (ENISA) iz 2021, „COVID-19 je stvorio prilike za sajber kriminalce". Društveni inženjering ostaje najrasprostranjenija tehnika napada. Sajber kriminalci su iskorišćavali interese, zabrinutost, radoznalost i strah ljudi koristeći mamce za krađu identiteta tokom pandemije COVID-19 i u vezi sa njom za finansijsku dobit.

Predmet istraživanja odnosi se na karakteristične oblike zlostavljanja u sajber prostoru tokom pandemije. U tekstu koji sledi prvo ćemo govoriti o pravnoj regulativi Evropske unije u oblasti fišinga, a zatim analizirati karakteristične primere zloupotrebe u sajber prostoru tokom pandemije COVID-19. U istraživanju će se koristiti normativni metod, kao i pravno-logički metodi indukcije i dedukcije.

2. Pravna regulativa u pogledu fišinga u Evropskoj uniji

U oblasti sajber bezbednosti na nivou Evropske unije još uvek ne postoji „krovni" propis koji bi regulisao ovu materiju, pa se zakonodavstvo u ovoj oblasti sastoji od više različitih pravnih akata. Prema Domazetu (2019), najvažniji propisi koji se tiču sajber bezbednosti u Evropskoj uniji jesu: Okvirna odluka Saveta 2001/413/JHA od 28. maja

2001. o borbi protiv prevare i falsifikovanja bezgotovinskih sredstava plaćanja, Direktiva (EU) 2016/1148 Evropskog parlamenta i Saveta od 6. jula 2016. o merama za visoki zajednički nivo bezbednosti mrežnih i informacionih sistema širom Unije, Direktiva 2013/40/EU Evropskog parlamenta i Saveta od 12. avgusta 2013. o napadima na informacione sisteme i zameni Okvirne odluke Saveta 2005/222/JHA, Uredba (EU) br. 526/2013 Evropskog parlamenta i Saveta od 21. maja 2013. godine u vezi sa Agencijom Evropske unije za mrežnu i informacionu bezbednost (ENISA) i ukidanjem Uredbe (EZ) br. 460/2004 (Tekst od značaja za EEA), Direktiva 2009/136/EC Evropskog parlamenta i Saveta od 25. novembra 2009. o izmenama i dopunama Direktive 2002/22/EC o univerzalnim uslugama i pravima korisnika u vezi sa elektronskim komunikacionim mrežama i uslugama, Direktiva 2002/58/EC o obradi ličnih podataka i zaštiti privatnosti u sektoru elektronskih komunikacija, Uredba (EC) br. 2006/2004 o saradnji između nacionalnih organa nadležnih za sprovođenje zakona o zaštiti potrošača, Saopštenje Komisije od 15. novembra 2006. Evropskom parlamentu, Savetu, Evropskom ekonomskom i socijalnom komitetu i Komitetu regiona za borbu protiv neželjene pošte, špijunskog softvera i zlonamernog softvera, Direktiva 2005/29/EC Evropskog parlamenta i Saveta od 11. maja 2005. godine o nepoštenoj poslovnoj praksi između preduzeća i potrošača na unutrašnjem tržištu i o izmenama i dopunama Direktive Saveta 84/450/EEC, Direktiva 97/7/EC, 98/ 27/EC i 2002/65/EC Evropskog parlamenta i Saveta i Uredba (EZ) br. 2006/2004 Evropskog parlamenta i Saveta („Direktiva o nepoštenoj poslovnoj praksi"), Direktiva 2002/58/EC Evropskog parlamenta i Saveta od 12. jula 2002. u vezi sa obradom ličnih podataka i zaštitom privatnosti u sektoru elektronskih komunikacija (Direktiva o privatnosti i elektronskim komunikacijama), Uredba (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. o zaštiti fizičkih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju takvih podataka i stavljanju van snage Direktive 95/46/EC (Opšta uredba o zaštiti podataka – dalje: GDPR). U vezi sa pandemijom izazvanom virusom COVID-19, Evropska unija je donela čitav set novih akata, nastojeći da što efikasnije pravno reguliše izazove, a ova sveobuhvatna baza propisa se redovno ažurira.[3]

[3] Spisak propisa Evropske unije u vezi sa pandemijom izazvanom virusom

Međutim, treba napomenuti da je specifična situacija sa pandemijom dovela do nekih zakonskih rešenja koja bi mogla da naruše normalno funkcionisanje demokratskog sistema i ostvarivanje sloboda i prava građana.

Prema Savetu Evrope (2020), na primer, države članice EU koje su potpisnice Konvencije za zaštitu pojedinaca u pogledu obrade ličnih podataka (u daljem tekstu: Konvencija 108+) usvojile su odredbe kojima se ograničavaju određene slobode i prava. U skladu sa Izveštajem Saveta Evrope o zaštiti podataka iz 2020. godine, mogu se identifikovati tri glavna pristupa: 1) usvajanje opštih hitnih mera dajući vladi posebna ovlašćenja (posebno na osnovu zakona ili uredbi, u primeni ustavnog zakona); 2) donošenje hitnih mera u određenim sektorima, često zasnovanih na propisima javnog zdravlja ili pandemije; 3) donošenje hitnih mera bez posebne zakonske osnove. Ovi različiti pristupi doveli su do mnoštva odredbi u 55 zemalja potpisnica Konvencije 108. Većina odredaba daje velika ovlašćenja vladama, iako obično samo u ograničenom vremenskom periodu. U istom izveštaju se navodi da, iako takve mere mogu biti veoma invazivne i predstavljaju važna ograničenja za osnovna prava (privatnost, zaštita podataka, ali i sloboda kretanja i okupljanja, a u nekim slučajevima i sloboda govora), neophodan je nadzor nadzornih organa, parlamenata, a sudovi su ponekad nedostajali. Neki ustavni sudovi su već doneli odluke o pojedinim merama. Ostali sudovi su bili sprečeni da ispune svoju ulogu (Council of Europe, 2020).

U Izveštaju se s pravom navodi da, iako obrada podataka u kontekstu borbe protiv pandemije može da nađe svoj legitimitet u Konvenciji, izuzetne okolnosti vezane za vitalnu pretnju i javni interes zahtevaju na nacionalnom nivou dodatnu i konkretniju regulativu da se obezbedi poštovanje principa pravne sigurnosti. Takvi propisi treba da definišu obim i svrhu nameravane obrade podataka (Council of Europe, 2020). Takođe, u Izveštaju se posebno ističe da je zaštita podataka od nezakonitog pristupa tim važnija s obzirom na osetljiv karakter većine podataka prikupljenih kao odgovor na zdravstvenu krizu. Organi za zaštitu podataka i civilno društvo odigrali su ključnu ulogu u verifikaciji i jačanju

COVID-19 nalazi se na sledećem linku: https://eur-lex.europa.eu/content/news/Covid19.html (15.11.2021)

bezbednosti predloženih digitalnih rešenja. Na primer, istaknute su slabosti u zaštiti ličnih podataka: bezbednosne slabosti na veb-lokaciji koja obrađuje samoprijavljene zdravstvene podatke, a posebno nedostatak odgovarajuće enkripcije ili slabosti u vezi sa izvornim kodom aplikacije za praćenje kontakata (Council of Europe, 2020).

Pored Konvencije 108+, da bismo zaštitili podatke od fišing napada tokom pandemije COVID-19, treba pomenuti i GDPR. Prema GDPR-u, (član 7) „kada se obrada zasniva na pristanku, rukovalac će moći da dokaže da je subjekt podataka dao saglasnost na obradu njegovih ili njenih ličnih podataka. Ako je pristanak subjekta podataka dat u kontekstu pisane izjave koja se odnosi i na druga pitanja, zahtev za pristanak će biti predstavljen na način koji se jasno razlikuje od drugih pitanja, u razumljivom i lako dostupnom obliku, koristeći jasan i običan jezik. Bilo koji deo takve izjave koji predstavlja povredu ove uredbe neće biti obavezujući. Subjekat podataka ima pravo da povuče svoju saglasnost u bilo kom trenutku. Povlačenje saglasnosti neće uticati na zakonitost obrade na osnovu saglasnosti pre njenog povlačenja. Pre davanja saglasnosti, subjekt podataka će biti obavešten o tome. Biće lako povući, kao i dati saglasnost. Prilikom procene da li je pristanak slobodno dat, najviše se vodi računa o tome da li je, između ostalog, izvršenje ugovora, uključujući pružanje usluge, uslovljeno pristankom na obradu ličnih podataka koja nije neophodna za izvršenje tog ugovora."

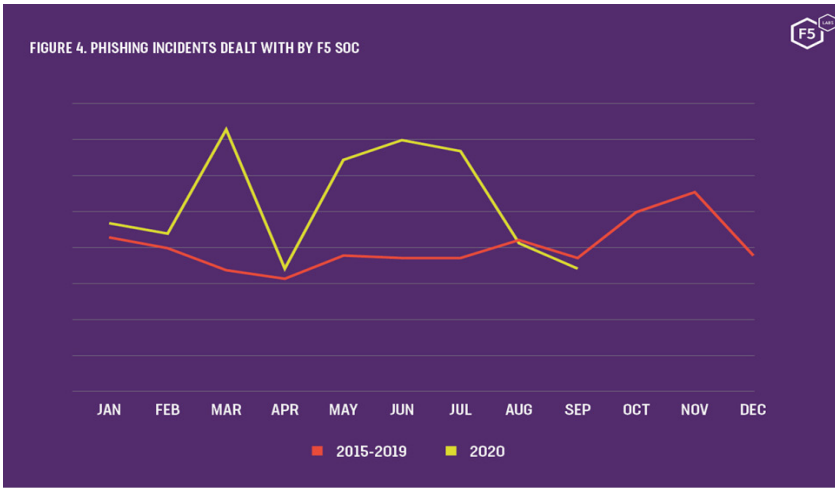
Dalje, u članovima 25 i 32 GDPR-a navodi se da „uzimajući u obzir stanje tehnike, troškove implementacije i prirodu, obim, kontekst i svrhu obrade, kao i rizike različite verovatnoće i ozbiljnosti za prava i slobode fizičkih lica izazvanih obradom, rukovalac će, kako u trenutku određivanja sredstava za obradu, tako i u trenutku same obrade, primeniti odgovarajuće tehničke i organizacione mere, kao što je pseudonimizacija, koje su osmišljene za sprovođenje podataka, principe zaštite, kao što je minimizacija podataka, na efikasan način i da integriše neophodne mere zaštite u obradu kako bi se ispunili zahtevi ove uredbe i zaštitila prava subjekata podataka. Rukovalac će primeniti odgovarajuće tehničke i organizacione mere kako bi obezbedio da se podrazumevano obrađuju samo lični podaci koji su neophodni za svaku konkretnu svrhu obrade."

Prema članu 33 GDPR-a, „u slučaju povrede ličnih podataka, rukovalac će bez nepotrebnog odlaganja obavestiti o povredi ličnih podataka nadležni nadzorni organ, osim ako je malo verovatno da će povreda ličnih podataka dovesti do rizika po prava i slobode fizičkih lica. Dalje, kada je verovatno da će povreda ličnih podataka dovesti do visokog rizika po prava i slobode fizičkih lica, rukovalac će obavestiti o povredi ličnih podataka subjekta podataka bez nepotrebnog odlaganja. Rukovalac će dokumentovati svaku povredu podataka o ličnim podacima, uključujući činjenice koje se odnose na povredu ličnih podataka, njene posledice i preduzete korektivne mere. Ta dokumentacija omogućava nadzornom organu da proveri poštovanje ovog člana."

Stoga su sve navedene odredbe od velikog značaja za zaštitu ličnih podataka u vreme pandemije COVID-19. S obzirom na zdravstvenu krizu, države članice Evropske unije usvojile su odgovarajuće akte sekundarnog (nacionalnog) zakonodavstva u cilju prevazilaženja problema u vezi sa zaštitom podataka o ličnosti. Prema Savetu Evrope (2020), Izveštaj pominje sledeće mere: a) korišćenje aplikacija za mobilne telefone, u različite svrhe; b) korišćenje podataka o saobraćaju i lokaciji sa mobilnih telefona i aplikacija; c) korišćenje drugih tehničkih alata (elektronske narukvice, pametne kamere koje omogućavaju prepoznavanje lica, termalna skeniranja, daljinsko upravljanje dronovima i robotima, obavezno testiranje).

3. Primeri zloupotreba u sajber prostoru tokom pandemije COVID-19

Od početka pandemije izazvane virusom COVID-19, zabeleženi su brojni slučajevi zloupotrebe u sajber prostoru. Pokazalo se da je COVID-19 izvanredna prilika za sajber kriminalce, a fišing prevare su bile među najrasprostranjenijima i na njih će biti stavljen akcenat. Prema Varburtonu (2020), broj fišing napada širom sveta u stalnom je porastu, posebno tokom 2019. i 2020. godine, što se može videti na slici 1:



Slika 1: Incidenti phishinga kojima se bavi F5 SOC
Izvor: (Varburton, 2020)

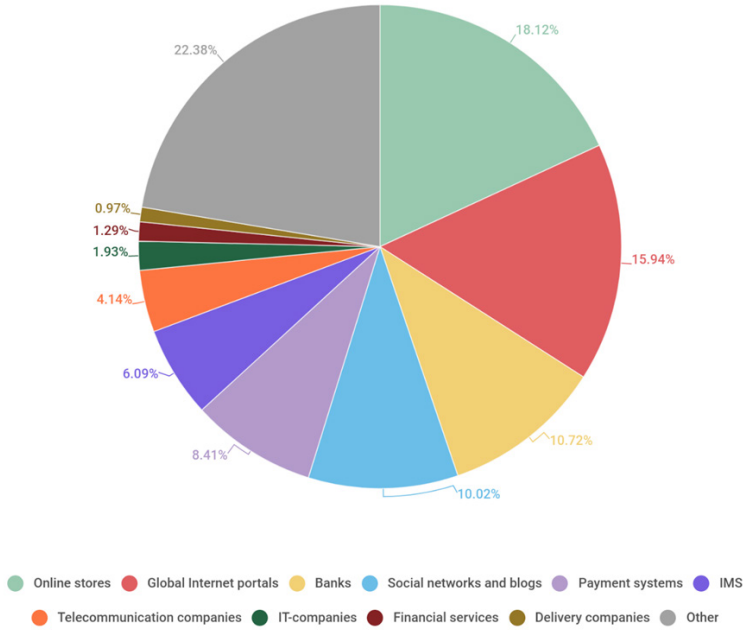
Tako su brojni primeri fišing napada bili napadi na naloge elektronske pošte širom sveta, pri čemu su elektronske poruke adresirane pod različitim imenima u vezi sa pandemijom COVID-19. Prema Izveštaju o fišingu i prevari iz 2020. (Varburton, 2020), dati su primeri elektronskih poruka sa različitim naslovima:

- Covid-19 in your area? Please confirm your address
- Click here for COVID-19 vaccinations
- Get your COVID-19 CARES Act relief check here
- Counterfeit Respirators, sanitizers, PPE
- Fake cures for COVID-19
- Message from the World Health Organization
- Message from the Centers for Disease Control and Prevention
- Click here for Coronavirus-related information
- Donate to these charitable organizations
- Message from Local hospital - Need patient data for COVID-19 testing

- COVID 19 Preparation Guidance
- 2019-nCoV: Coronavirus outbreak in your city (Emergency)
- HIGH-RISK: New confirmed cases in your city
- Coronavirus (2019-nCoV) Safety Measures.

Što se tiče SMS fišing prevara (tzv. smišing), takođe je prijavljen veliki broj pokušaja prevare. Prema Vatkinsu (2020), Simantec otkriva da jedna od dvadeset SMS poruka povezanih sa pandemijom COVID-19 sadrži pokušaje krađe identiteta ili drugi visokorizični sadržaj. Simantec je 24. januara 2020. prvi primetio visokorizični SMS fišing napad koristeći COVID-19 kao mamac, otprilike u istom periodu kada je virus počeo da dobija više medijske pokrivenosti. Svi kriminalci koji stoje iza ovih prevara koriste istu taktiku – iskorišćavanje strahova i finansijskih poteškoća ljudi tokom globalne pandemije kako bi ih namamili.

Istraživanje o fišing prevarama tokom pandemije COVID-19 sprovela je i poznata kompanija Kasperski. Prema relevantnom izveštaju ove kompanije u vezi sa fišing prevarama tokom 2020. godine, identifikovani su različiti oblici prevare, pri čemu se ističu „olakšanje javnosti" od strane spamera, zlonamerne veze (pominje se primer turskog Ministarstva zdravlja i lažne poruke koje obećavaju gotovinu), plaćanja ukoliko je instalirana zlonamerna aplikacija, praćena prevarama u vezi sa korporativnim sektorom (u jednom od mejlova je navedeno da je tehnička podrška napravila poseban sistem upozorenja kako bi se rizik od nove infekcije virusom minimizirao), čuvena nigerijska prevara i sl. (Kaspersky, 2021). Prema pomenutoj kompaniji, „prošlogodišnji događaji uticali su na distribuciju fišing napada po kategorijama ciljanih organizacija. Tri najveće kategorije ostale su nepromenjene nekoliko godina: banke, platni sistemi i globalni internet portali. Godina 2020. donela je promene. Internet prodavnice su postale najveća kategorija sa 18,12%, što se može dovesti u vezu sa rastom onlajn porudžbina zbog ograničenja vezanih za pandemiju. Globalni internet portali ostali su druga po veličini kategorija sa 15,94%, ali je njihov udeo opao za 5,18 p.p. u odnosu na 2019, a banke su bile treće sa „skromnih" 10,72%" (Kasperski, 2021). Ovi podaci su prikazani na Slici 2.



Slika 2: Distribucija organizacija koje su ciljane od strane napadača, po kategorijama u 2020.

Izvor: (Kasperski, 2021)

Prema CERT-u (2021), u pogledu krađe kredencijala, treba napomenuti da se ova vrsta prevare odvija na način da link vodi do lažne veb-stranice koja sadrži COVID-19 u nazivu, a za pristup informacijama sa stranice zahteva adresu e-pošte i lozinku. Ove veb-stranice izgledaju kao legitimne i izgledaju pouzdane, ali zlonamerni pokušaj se može utvrditi putem detaljnog pregleda URL-a. Unos kredencijala od strane korisnika omogućava napadaču da pristupi njegovoj elektronskoj pošti korisnika, koja obično sadrži lične i poverljive podatke (npr. izvode sa bankovnog računa), a takođe može da koristi imenik korisnika za dalje širenje phishing napada.

Pokazalo se da se komunikacione platforme, kao što je Zoom, takođe mogu koristiti za narušavanje sajber bezbednosti. Dakle, istraživači

bezbednosti su otkrili fišing napade koji se predstavljaju kao Zoom obaveštenja o sastancima. Prema Dejvisu (2020), imejl zahteva od korisnika da se pridruži sastanku o raskidanju posla, tražeći od korisnika da se prvo prijave na lažnu Zoom stranicu koja će zapravo ukrasti njihove kredencijale. Čini se da je zlonamerna odredišna stranica legitimna „kopija" Zoom stranice za prijavu. Imejl se maskira kao automatizovano obaveštenje za važan sastanak sa HR-om u vezi sa raskidom primaoca. Imejl sadrži vezu ka lažnoj Zoom stranici za prijavu koja se nalazi na „zoom-emergenci.miftp.org". Veze ka stranici za „pecanje" su skrivene u tekstu koji se koristi u automatskim obaveštenjima o sastancima. E-pošta se maskira kao podsetnik da primalac ima sastanak sa HR-om u vezi sa njihovim raskidom. Kada žrtva pročita mejl, uspaniće se, klikne na vezu za phishing i žurno pokuša da se prijavi na ovaj lažni sastanak. Ako primaoci postanu žrtve ovog napada, kredencijali za prijavu kao i sve druge informacije sačuvane na Zoom-u biće ugrožene.

4. Zaključak

Na osnovu navedenog, može se zaključiti da su sajber prevare bile veoma česte tokom pandemije izazvane virusom COVID-19. Sajber-kriminalci su pandemiju shvatili kao odličnu priliku za laku zaradu, a raznim metodama socijalnog inženjeringa (koristeći različite psihološke tehnike, uglavnom zasnovane na strahu od virusa COVID-19), uspeli su da prevare svoje žrtve širom sveta. Šteta od sajber napada tokom pandemije izazvane virusom COVID-19 raste. Ispostavilo se da žrtve sajber napada nisu bile samo privatne kompanije, već i privredni subjekti od javnog značaja, kao i javni sektor širom sveta.

Utvrđeno je da su neki od najčešćih oblika zloupotrebe vezani za fišing u vezi sa elektronskom poštom, krađom korisničkih kredencijala, fišing uz pomoć tekstualnih poruka, distribucija malvera, kao i komunikacione platforme poput aplikacije Zoom. Pomenute opasnosti u sajber prostoru mogu se sprečiti raznim merama tehničke, organizacione i pravne prirode. Pokazalo se da se mere sajber higijene tokom pandemije COVID-19 moraju unaprediti i efikasnije sprovoditi. Utvrđeno je da u Evropskoj uniji postoji zakonodavstvo u vezi sa fišingom, kako na nivou

Unije, tako i na nacionalnom nivou. Posebno treba istaći značaj Konvencije za zaštitu pojedinaca u pogledu obrade ličnih podataka (Konvencija 108+), kao i Uredbe (EU) 2016/679 Evropskog parlamenta i Saveta od 27. aprila 2016. godine o zaštiti fizičkih lica u vezi sa obradom ličnih podataka i o slobodnom kretanju tih podataka i stavljanju van snage Direktive 95/46/EC (Opšta uredba o zaštiti podataka). Analizirajući najvažnije odredbe ovih pravnih akata, stiče se utisak da je neophodno unaprediti postojeću zakonsku regulativu ne samo na nacionalnom nivou već i na međunarodnom. Jedna od mera koja može dati rezultate odnosi se na podizanje svesti građana i privrede o potencijalnim opasnostima koje vrebaju u sajber prostoru.

Bibliografija

CERT. (2021). Zloupotreba pandemije virusa COVID-19 u sajber prostoru. Beograd, Srbija. Retrieved Novembar 01, 2021, from https://www.cert.rs/files/shares/Zloupotreba%20COVID%20latinica.pdf

Council of Europe. (2020, October 12). *Digital solutions to fight against COVID-19 (2020 data protection report)*. Retrieved October 15, 2021, from Newsroom: https://www.coe.int/en/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020

Davis, J. (2020, April 27). *New COVID-19 Phishing Campaigns Target Zoom, Skype User Credentials*. Retrieved November 01, 2021, from HealthITSecurity: https://healthitsecurity.com/news/new-covid-19-phishing-campaigns-target-zoom-skype-user-credentials

Domazet, S. (2019). Phishing and pharming attacks aimed at identity theft of internet users. *Security nad Crisis management-theory and practice-SECMAN* (p. 12). Belgrade: BEKMEN. Retrieved October 3–4, 2019

Domazet, S., & Skakavac, Z. (2019). Fišing-izazov u zaštiti podataka korisnika interneta. *Srpska politička misao, 63*(1), 191. doi: https://doi.org/10.22182/spm.6312019.10

Đukić, A. (2017). Krađa identiteta – oblici, karakteristike i rasprostranjenost. *Vojno delo*, 99.

ENISA. (2021, October). *ENISA Threat Landscape 2021*. Retrieved October 15, 2021, from file:///C:/Users/SINIA~1/AppData/Local/Temp/ENISA%20Threat%20Landscape%202021.pdf

Graydon, S. (2006). Phishing and Pharming: The New Evolution of Identity Theft. *Financial Law quarterly Report*(60), 335,337.

Gudkova, D., Vergelis, M., Shcherbakova, T., & Demidova, N. (2018, February 15). *Spam and phishing in 2017 on February 15*. Retrieved October 15, 2021, from Securelist: https://securelist.com/spam-and-phishing-in-2017/83833/

Kaspersky. (2021). *Spam and phishing in 2020.* Retrieved January 11, 2022, from https://securelist.com/spam-and-phishing-in-2020/100512/

Petrović, S. (2004). *Kompjuterski kriminal.* Beograd: Vojnoizdavački zavod.

Skakavac, T. (2020). Uticaj društvenih mreža na pojavu maloletničke diskriminacije. *Civitas, 10*(1), 85. Preuzeto January 12, 2022 sa https://civitas.rs/wp-content/uploads/2020/10/UTICAJ-DRU%C5%A0TVENIH-MRE%C5%BDA-NA-POJAVU-MALOLETNI%C4%8CKE-DELINKVENCIJE.pdf

Warburton, D. (2020, November 11). *2020 Phishing and Fraud Report*. Retrieved November 01, 2021, from F5 Labs Application threat intelligence: https://www.f5.com/labs/articles/threat-intelligence/2020-phishing-and-fraud-report

Watkins, K. (2020, May 29). *SMS Phishing Campaigns Take Advantage of Coronavirus Pandemic*. Retrieved November 01, 2021, from Symantec Enterprise Blogs/Threat Intelligence: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/sms-phishing-coronavirus