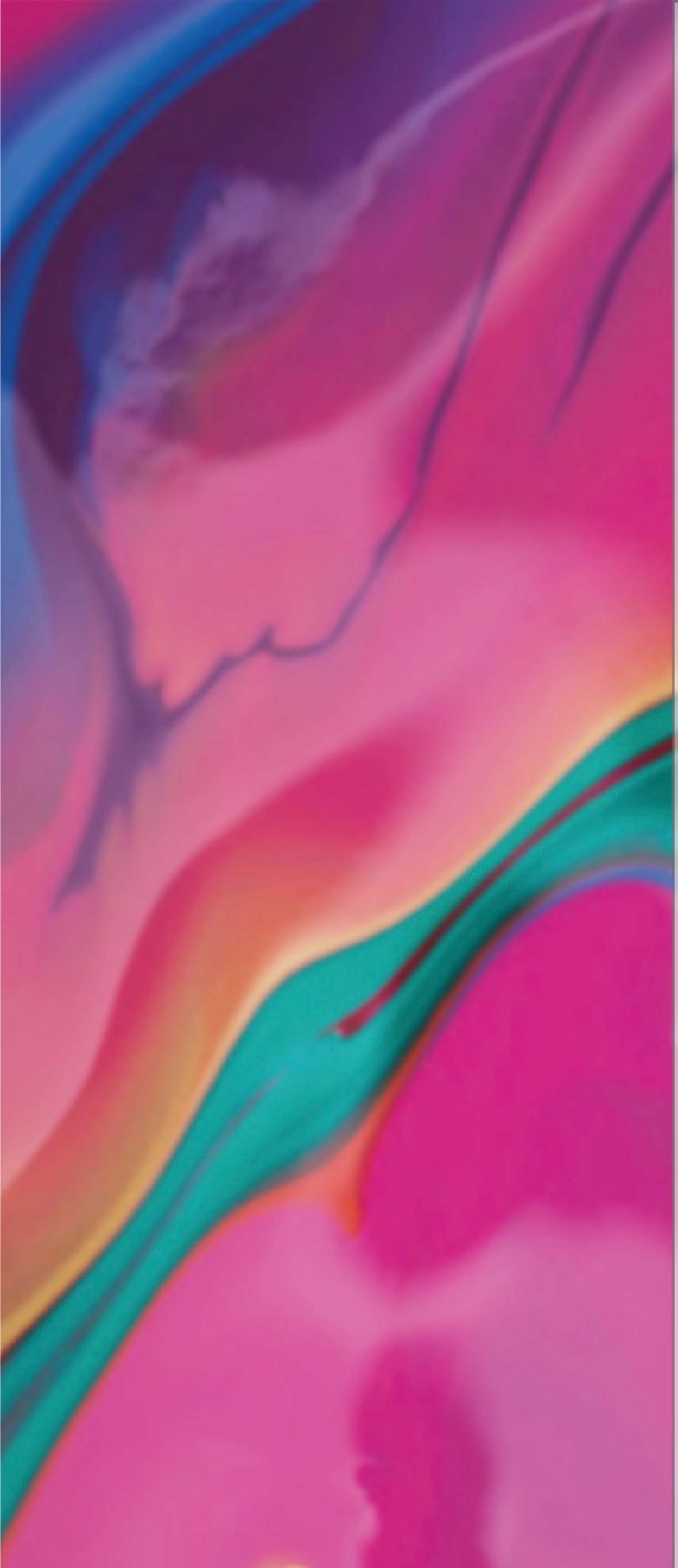

UNIVERZITET U BEOGRADU
FAKULTET ZA SPECIJALNU
EDUKACIJU I REHABILITACIJU

UNIVERSITY OF BELGRADE
FACULTY OF SPECIAL EDUCATION
AND REHABILITATION

# 11.

# MEĐUNARODNI NAUČNI SKUP „SPECIJALNA EDUKACIJA I REHABILITACIJA DANAS”

# 11th

# INTERNATIONAL SCIENTIFIC CONFERENCE “SPECIAL EDUCATION AND REHABILITATION TODAY”

## ZBORNIK RADOVA

## PROCEEDINGS

Beograd, Srbija
29-30. oktobar 2021.

Belgrade, Serbia
October, 29-30th, 2021

UNIVERZITET U BEOGRADU – FAKULTET ZA SPECIJALNU EDUKACIJU I REHABILITACIJU

UNIVERSITY OF BELGRADE – FACULTY OF SPECIAL EDUCATION AND REHABILITATION

11. MEĐUNARODNI NAUČNI SKUP
SPECIJALNA EDUKACIJA I REHABILITACIJA DANAS
Beograd, 29–30. oktobar 2021. godine

# Zbornik radova

11th INTERNATIONAL SCIENTIFIC CONFERENCE
SPECIAL EDUCATION AND REHABILITATION TODAY
Belgrade, October, 29–30th, 2021

# Proceedings

Beograd, 2021.
Belgrade, 2021

11. MEĐUNARODNI NAUČNI SKUP
SPECIJALNA EDUKACIJA I REHABILITACIJA DANAS
Beograd, 29–30. oktobar 2021. godine
Zbornik radova

11th INTERNATIONAL SCIENTIFIC CONFERENCE
SPECIAL EDUCATION AND REHABILITATION TODAY
Belgrade, October, 29–30th, 2021
Proceedings

IZDAVAČ / PUBLISHER
Univerzitet u Beogradu – Fakultet za specijalnu edukaciju i rehabilitaciju
University of Belgrade – Faculty of Special Education and Rehabilitation

ZA IZDAVAČA / FOR PUBLISHER
Prof. dr Gordana Odović, v.d. dekana

GLAVNI I ODGOVORNI UREDNIK / EDITOR-IN-CHIEF
Prof. dr Branka Jablan

UREDNICI / EDITORS
Prof. dr Irena Stojković
Doc. dr Bojan Dučić
Doc. dr Ksenija Stanimirov

RECENZENTI / REVIEWERS
Prof. dr Sonja Alimović
Sveučilište u Zagrebu – Edukacijsko rehabilitacijski fakultet, Zagreb, Hrvatska
Doc. dr Ingrid Žolgar Jerković
Univerzitet u Ljubljani – Pedagoški fakultet Ljubljana, Slovenija
Prof. dr Vesna Vučinić, prof. dr Goran Jovanić, doc. dr Aleksandra Pavlović
Univerzitet u Beogradu – Fakultet za specijalnu edukaciju i rehabilitaciju

LEKTURA I KOREKTURA / PROOFREADING AND CORRECTION
Maja Ivančević Otanjac, predavač

DIZAJN I OBRADA / DESIGN AND PROCESSING
Biljana Krasić
Mr Boris Petrović
Zoran Jovanković

Zbornik radova biće publikovan u elektronskom obliku

Proceedings will be published in electronic format

Tiraž / Circulation: 200

ISBN 978-86-6203-150-1

UDK 343.533::004
616.98:578.834

# SAJBER KRIMINAL – OZBILJAN IZAZOV TOKOM KOVID-19 PANDEMIJE

Danka Radulović**, Nikola Milosavljević

*Univerzitet u Beogradu – Fakultet za specijalnu edukaciju i rehabilitaciju, Srbija*

**Uvod:** *Sajber kriminal se odnosi na svako nezakonito delo izvršeno korišćenjem računara, računarskih mreža ili drugog oblika informacionih i komunikacionih tehnologija. U zavisnosti od toga da li je tehnologija meta ili sredstvo izvršenja, možemo razlikovati krivična dela koja podrazumevaju napade usmerene na uređaje i računarske mreže i različite oblike „tradicionalnih" krivičnih dela čiji se obim i domet povećavaju upotrebom digitalnih tehnologija. Usled KOVID-19 pandemije ljudi su prisiljeni da ostaju kod kuće i da se, više nego ikada pre, oslone na računare, telefone i internet, kako bi mogli da rade, uče na daljinu, kupuju, informišu se i komuniciraju sa drugima. Premeštanje svakodnevnih i poslovnih aktivnosti iz fizičke u digitalnu sferu otvara i mogućnost nastanka novih oblika pretnji i rizika u sajber prostoru.*

**Cilj:** *Cilj rada bio je da se eksplorativnim istraživanjem ustanove zastupljenost, raširenost i oblici ispoljavanja sajber kriminala tokom KOVID-19 pandemije.*

**Metod:** *Korišćena je metoda pretraživanja i analize velikog broja primarnih i sekundarnih izvora informacija (desk research), proučavanjem različitih naučnih baza podataka i sprovedenih istraživanja o zastupljenosti i različitim oblicima sajber kriminala tokom pandemije.*

**Rezultati:** *Podaci pokazuju da je tokom KOVID-19 pandemije došlo do povećanja stope raširenosti i sofisticiranosti sajber kriminala. Mete sajber napada su pored pojedinaca i malih preduzeća, sve više velike korporacije i institucije koje imaju ključnu ulogu u odgovoru na izbijanje bolesti. Pored rapidnog rasta sajber napada na računare i računarske mreže, došlo je i do povećanja broja „tradicionalnih" krivičnih dela u sajber prostoru, uz iskorišćavanje bezbednosne ranjivosti rada od kuće i straha i neizvesnosti zbog pandemije.*

**Zaključak:** *Enormni rast sajber kriminala tokom KOVID-19 pandemije predstavlja ozbiljan izazov za državne strukture. Državno reagovanje na krupan porast sajber kriminala prvenstveno bi trebalo da se usmeri na sprovođenje preventivnih mera kroz edukacije i kampanje podizanja svesti, jer je najveći bezbednosni rizik potcenjivanje ili nedostatak svesti o pretnjama u sajber prostoru.*

**Ključne reči:** *sajber kriminal, KOVID-19, državno reagovanje*

** dankamr@gmail.com

## UVOD

Savremena informatička i komunikaciona tehnologija česta je meta sajber napada ili je pak sredstvo za ostvarivanje kriminalnih ciljeva u okviru već ozbiljno strukturiranog sajber kriminala određenog kao „svako nezakonito delo koje je olakšano ili izvršeno pomoću računara, računarske mreže ili hardverskog uređaja“ (Gordon & Ford, 2006, p. 14). Tokom pandemije koronavirusa digitalna eksponiranost svetske populacije se višestruko povećala, jer je ogroman broj ljudi bio primoran da radi, uči, kupuje i realizuje brojne druge aktivnosti u virtuelnom prostoru, iako nedovoljno tehnički pripremljen, u atmosferi straha od zaraze i realnih zdravstvenih problema. To je obezbedilo izuzetne pogodnosti za širenje sajber kriminala, dodatno olakšanog dostupnošću i ranjivošću postojećih sistema kao i nove generacije uređaja za prenos informacija.

## CILJ

Cilj rada bio je da se na bazi detaljne analize relevantnih izvora istraži da li je pandemija koronavirusa uticala na stopu raširenosti sajber kriminala i da se razmotre oblici i mete sajber napada, prvenstveno pojedinaca i organizacija koje su tokom pandemije ispoljile posebnu vulnerabilnost.

## METOD

U radu je korišćena metoda pretraživanja i eksplorativne analize većeg broja primarnih i sekundarnih izvora informacija (desk research), uključujući izveštaje kredibilnih međunarodnih organizacija i rezultate novijih empirijskih istraživanja dostupne u naučnim bazama podataka.

## Sajber kriminal u periodu pandemije – rasprostranjenost, oblici napada i mete

Dobijeni rezultati potvrđuju da je trend višegodišnjeg povećanja stopa sajber kriminala tokom pandemije koronavirusa obeležen naglim skokom, uz učestalije, sofisticiranije, neretko kombinovane napade, teže za otkrivanje, realizovane različitim i povezanim digitalnim sistemima (EUROPOL, 2020). Progresivno raste i broj prijava sajber kriminala, a prema podacima FBI (FBI Internet Crime Complaint Center – IC3) u 2020. je za 69% veći u odnosu na 2019. god. (IC3, 2021), što značajno prevazilazi očekivan rast na osnovu ranijih trendova (Tabela 1) i ukazuje da je pandemija znatno uticala na povećanje stopa sajber kriminala (IC3, 2021), koje su inače neuporedivo veće jer delikti najčešće ostaju neprijavljeni i neotkriveni.

**Tabela 1**
*Broj prijava sajber kriminala u periodu od 2016. do 2020. god.*

| Broj prijava sajber kriminala | 2016. | 2017. | 2018. | 2019. | 2020. |
|---|---|---|---|---|---|
| | 298728 | 301580 | 351937 | 467361 | 791790 |

*Izvor:* FBI Internet Crime Complaint Center, 2021

Kada je reč o vrsti krivičnih dela, najveći porast broja prijava u 2020. je u poređenju sa 2019. godinom, prema FBI Centru za žalbe, vezan za krađe identiteta (2,7 puta više), phishing napade (1,87 puta više) i iznude (1,78 puta više) (IC3, 2021). Istraživači takođe izveštavaju o značajanom porastu hakovanja sa iznudom, ali i hakovanja društvenih mreža i mejla i drugih oblika kriminala zavisnog od sajber prostora, pogotovu upotrebe zlonamernih softvera (Buil-Gil et al., 2020; Buil-Gil et al., 2021; Kemp et al., 2021). Tokom pandemije registrovano je šest puta više malicioznih domena u odnosu na 2019. godinu (EUROPOL, 2020).

Postoji konsenzus oficijelnih izvora o znatnom povećanju obima i sofisticiranosti phishing napada i socijalnog inženjeringa (EUROPOL, 2020; IC3, 2021; INTERPOL, 2020) modelovanih tako da koriste strah od zaraze i neinformisanost da šire neistine i paniku, a da pretnje učine težim za otkrivanje, a efikasnijim u navođenju žrtve da podeli svoje lične podatke ili da preduzme po nju štetne digitalne operacije. Pojedinci ili organizovane grupe sajber prestupnika su, lažno se prikazujući kao predstavnici državnih ili zdravstvenih institucija, dobijali lične podatke žrtava, nudeći informacije o koronavirusu sa sakrivenim malverom, prodajući medicinski netestirane proizvode za navodnu „zaštitu ili lečenje" od koronavirusa; pa i elektronski izdajući falsifikate potvrda o negativnom testu na koronavirus uz novčanu nadoknadu. INTERPOL (2020), pored phishing napada u kriznom periodu evidentira i značajno povećanje upotrebe malvera i ransomver softvera (koji se prevarno infiltrira u sistem, zaključava fajlove računara i pokreće iznudu otkupnine, bez garantovanja obećanog vraćanja podataka), kao i DDoS napada uskraćivanja usluga preopterećenjem mreže. Agencija za sajber bezbednost EU (ENISA, 2020) za period januar 2019 – april 2020. god., osim o phishing i ransomver napadima, izveštava o značajanom porastu: krađa identiteta, neovlašćenog pristupa računarskim podacima (data breach), povreda tajnosti podataka i curenja informacija, zlonamerne spam aktivnosti (neželjene pošte), insajderskih pretnji, ali i neovlašćenog korišćenja kompjutera, mobilnih telefona i svih povezanih uređaja za rudarenje kriptovaluta, a takođe i napada usmerenih na pametne senzore, dronove i dr. sisteme nadzora u vezi sa sajber špijunažom (ENISA, 2020).

U sagledavanju meta sajber kriminala upoređivane su prijave pojedinaca i organizacija za elektonski kriminal tokom pandemije koronavirusa. Britanski istraživači nalaze da je u slučaju kriminala omogućenog sajber prostorom tokom aprila i maja 2020. god., potvrđeno značajno povećanje broja prijava podnetih i od pojedinaca i od strane pravnih subjekata u odnosu na isti period 2019. god. (Buil-Gil et al., 2020); dok je u oblasti kriminala zavisnog od sajber prostora veći broj prijava podnet od strane fizičkih u odnosu na pravna lica (Buil-Gil et al., 2020), a u maju 2020. u odnosu na maj 2019. nije porastao broj podnetih prijava drugo pomenutih, delom zato što je poslovanje bilo onemogućeno i redukovano, ali i zbog ranije uočenog trenda da se mnogo više sajber delikata realizuje, nego što mala i srednja preduzeća, pa i velike

korporacije prijave policiji (Bidgoli & Grossklags, 2016). Oni upade u svoje računarske sisteme ne prijaljuju i prikrivaju od javnosti čuvajući ugled kompanije (Bilodeau et al., 2019; Smith et al., 2011).

Brojna istraživanja ukazuju da su organizacije u zdravstvenom sektoru i institucije uključene u suzbijanje epidemije koronavirusa bile česta meta hakovanja, iznuđivačkih softvera ransomver i DDoS napada (Chigada & Madzinga, 2021; INTERPOL, 2020; Jalali et al., 2020; Pranggono & Arabo, 2021; Williams et al., 2020). Ovi napadi se povezuju sa velikim opterećenjem zdravstvenih ustanova, činjenicom da prikupljaju i čuvaju ogroman broj osetljivih podataka pacijenata i da sajber kriminalci pri iznudama od njih traže veće finansijske iznose (Jalali et al., 2020). Sajber napadi na Svetsku zdravstvenu organizaciju su samo u aprilu 2020. bili pet puta češći nego u istom periodu 2019. godine (WHO, 2020).

Registrovani su i napadi na obrazovne ustanove kao što je Kalifornijski Univerzitet u San Francisku (UCSF) koji je hakovan od strane sajberkriminalne grupe koja je zahtevala isplatu da ne obelodani njihove poverljive informacije (Jalali et al., 2020).

Kako je pandemija naterala većinu zaposlenih širom sveta da rade onlajn bez jasnih instrukcija i bezbednosnih vodilja, koristeći lične računare, mobilne telefone i linternet, njihovi uređaji, ali i datoteke njihovih organizacija bili su meta sajber napada, budući da su novi phishing websajtovi registrovani za svaku od vodećih komunikacionih aplikacija, uključujuću i one oficijelno korišćene u nastavi kao što su Microsoft Teams, Zoom i dr. (Chowdhury et al., 2020). Zaposleni su i zbog čuvanja poslovnih video zapisa na personalnim kompjuterima postajali ranjiviji na malvere (Chowdhury et al., 2020), a njihova sajber sigurnost je ugrožena i nezakonitim curenjem ličnih podataka za koje su odgovorne organizacije.

Povećan je broj žrtava klasičnih krivičnih dela u sajber prostoru, između ostalog različitih vrsta prevara na internetu, a posebno u vezi sa onlajn bankarstvom, kupovinom i plaćanjem (Buil-Gil et al., 2020; EUROPOL, 2020; IC3, 2021), delom jer su mere zatvaranja zbog zdravstvene krize primorale mnoge nedovoljno digitalno osposobljene osobe da kupovinu i druge aktivnosti obavljaju elektronski. Najčešće žrtve internet prevara su stariji od 50 god., impulsivnije, neurotičnije, više zabrinute za vlastito zdravlje i slabije obučene za onlajn funkcionisanje (Abdelhamid, 2020; Monteith et al., 2021; Payne, 2020; Whitty, 2020). Tokom 2020. god., od ukupnog broja prijava prevara na internetu, gotovo trećinu su podneli ljudi stariji od 60 god., koji su bili oštećeni za oko jednu milijardu dolara, što je skoro 40% više u odnosu na 2019. (IC3, 2021).

I deca su česta meta sajber napada, a posebno brine alarmantan porast broja slučajeva seksualnog zlostavljanja dece na internetu i onlajn distribucije dečje pornografije tokom pandemije koronavirusa (EUROPOL, 2020; IC3, 2021). Zbog mera zatvaranja veliki broj dece je, ostajući kod kuće svakodnevno, dugo vremena, zbog školskih obaveza i dosade provodio na laptopu, mobilnom telefonu, uz kamere, postajući lak plen seksualnih predatora koji su svoje kriminalne aktivnosti u većoj meri preusmerili u sajber prostor (ECPAT, 2020; UNICEF, 2020).

## ZAKLJUČAK

Globalna zdravstvena kriza COVID-19 stvorila je povoljne uslove za ubrzan eksponencijalni rast sajber kriminala, potvrđujući ranija predviđanja o njegovom supstancijalnom doprinosu globalnom epidemijskom širenju i usložnjavanju problema kriminala (Radulović, 2006). Povećan broj novih korisnika i intenzivirana digitalna aktivnost svih kategorija praćeni su rapidnim povećanjem kriminala zavisnog od sajber prostora, ali i tradicionalnih krivičnih dela izvršenih pomoću računara i računarskih mreža, pri čemu su žrtve pojedinci, organizacije i državne institucije. Zbog toga se, dugoročno gledano, nameće pitanje opravdanosti pritiska ubrzane digitalizacije, bez prethodnog rešavanja problema nekontrolisanog bujanja sajber kriminala, bitno osnaženog pandemijom; pogotovu ako se ima u vidu da su procene stručnjaka da će finansijska šteta od ovog vida kriminala samo za 2021. god. dostići šest triliona dolara. Sajber kriminal je ozbiljan izazov za sve kategorije digitalnih korisnika, ali i za državne strukture koje treba da preduprede njegovu dalju ubrzanu ekspanziju. Treba imati u vidu da empirijska istraživanja svedoče da do efikasne realizacije većine sajber napada dolazi manje zbog visoke sofisticiranosti, a pre zahvaljujući greškama ljudi (Jensen et al., 2017; Pfleeger et al., 2014) proisteklim iz nedovoljne svesti korisnika o pretnjama i nedostatka znanja o načinima zaštite u sajber prostoru. Na to ukazuje i olako deljenje osetljivih podataka od strane korisnika i preuzimanje malicioznih sadržaja (Lallie, 2021) koji omogućavaju izvršenje ostalih tipova sajber kriminala (EUROPOL, 2020), posebno u phishing napadima i socijalnom inženjeringu.

Iz tog razloga, kao nužan početni korak u neophodnom strateškom pristupu državnog reagovanja na krupan porast sajber kriminala, prvenstveno bi trebalo da bude usmeren na sprovođenje preventivnih mera kroz edukacije i kampanje podizanja svesti o različitim vrstama pretnji u sajber prostoru; jer je najveći bezbednosni rizik potcenjivanje ili nedostatak svesti ljudi o bezbednosnim izazovima i o posledicama sajber kriminala po pojedinca, organizacije i društvo. Preventivni programi bi morali obezbediti jasne smernice različitim kategorijama kako da prepoznaju sajber pretnje i bezbedno koristite digitalne uređaje; a u fokusu bi bile posebno vulnerabilne grupe: deca, stariji, potrošači i zaposleni, naročito u zdravstvenom sektoru za koje postoji empirijska potvrda o povećanoj verovatnoći da postanu žrtve phishing napada (Jalali, 2020).

## LITERATURA

Abdelhamid, M. (2020). The role of health concerns in phishing susceptibility: Survey design study. *Journal of Medical Internet Research*, *22*(5), e18394. http://doi.org/10.2196/18394

Bidgoli, M., & Grossklags, J. (2016, June 12-14). End user cybercrime reporting: what we know and what we can do to improve it. In B. Cartwright, G. Weir, & L. Y. C. Lau (Eds.), *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF),* (pp. 1-6). IEEE. http://doi.org/10.1109/ICCCF.2016.7740424

Bilodeau, H., Lari, M., & Uhrb, M. (2019). Cyber security and cybercrime challenges of Canadian businesses, 2017. *Juristat: Canadian Centre for Justice Statistics*, 1-18.

https://www150.statcan.gc.ca/n1/en/pub/85-002-x/2019001/article/00006-eng.pdf?st=Y21XDRqr

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Buil-Gil, D., Moneva, A., Kemp, S., Díaz-Castaño, N., & Miró-Llinares, F. (2020). Recorded cybercrime and fraud trends in UK during COVID-19. *Statistical Bulletin on Crime and COVID-19*, 6. University of Leeds. http://doi.org/10.5518/100/30

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management*, *23*(1), 1-11. http://dx.doi.org/10.4102/sajim.v23i1.1277

Chowdhury, S., Mujherjee, S., Roy, N. S., Mehdi, R., & Banerjee, R. (2020). An overview of cybersecurity risks during the COVID-19 pandemic period. *Scientific Voyage*, *1*(3), 47-54.

ECPAT (2020). *Why children are at risk of sexual abuse and exploitation during COVID-19.* https://ecpat.org/story/why-children-are-at-risk-of-sexual-exploitation-during-covid-19/

European Union Agency for Cybersecurity (2020). *ENISA Threat Landscape – The year in review.* https://www.enisa.europa.eu/publications/year-in-review

Europol (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020.* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

FBI (2021). *Internet Crime Complaint Center 2020 Internet Crime Report.* https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20. https://doi.org/10.1007/s11416-006-0015-z

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research*, *22*(1), e16775. https://doi.org/10.2196/16775

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626. https://doi.org/10.1080/07421222.2017.1334499

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, 10439862211027986. https://doi.org/10.1177%2F10439862211027986

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports*, *23*(4), 1-9. https://dx.doi.org/10.1007%2Fs11920-021-01228-w

Payne, B. K. (2020). Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American*

*Journal of Criminal Justice*, *45*, 563-577. https://doi.org/10.1007/s12103-020-09532-6

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), 489–510. https://doi.org/10.1515/jhsem-2014-0035

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247

Radulović, D. (2006) *Psihologija kriminala-psihopatija i prestupništvo*. Univerzitet u Beogradu – Fakultet za specijalnu edukaciju i rehabilitaciju i Institut za kriminološka i sociološka istraživanja, 368-372.

Smith, K. T., Smith, M., & Smith, J. L. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*, 1-18. https://ssrn.com/abstract=1724815

UNICEF (2020). *COVID-19 and its implications for protecting children online.* https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research*, *26*(3), 399-409. http://doi.org/10.1007/s10610-020-09458-z

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), e23692. http://dx.doi.org/10.2196/23692

World Health Organization (2020). *WHO reports fivefold increase in cyber attacks, urges vigilance*. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

## CYBER CRIME – SERIOUS CHALLENGE DURING THE COVID-19 PANDEMIC

Danka Radulović, Nikola Milosavljević

*University of Belgrade – Faculty of Special Education and Rehabilitation, Serbia*

**Introduction:** *Cybercrime refers to any illegal act committed using computers, computer networks, or other forms of information and communication technologies. Depending on whether the technology is a target or a means of execution, we can distinguish between crimes that involve attacks aimed at devices and computer networks, and different forms of "traditional" crimes whose scope and reach increase with the use of digital technologies. As a result of the COVID-19 pandemic, people have to stay home, rely more than ever on computers, phones, and the Internet to telework, learn on distance, buy things, get information, and communicate with others. The shift of everyday and business activities from the physical to the digital sphere also opens the possibility of the emergence of new forms of threats and risks in cyberspace.*

**Aim:** *The paper aimed to explore the prevalence and forms of manifestation of cybercrime during the COVID-19 pandemic.*

**Method:** *Desk research was conducted by gathering and analyzing a plethora of primary and secondary sources of information, various scientific databases and research findings on the prevalence and various forms of cybercrime during the pandemic.*

**Results:** *The data show that during the COVID-19 pandemic, there was an increase in the prevalence, widespread presence, and sophistication of cybercrime. In addition to individuals and small businesses, the target of cyberattacks in greater amount is large corporations and institutions that play a crucial role in responding to the outbreak. Besides the rapid growth of cyber-attacks on computers and computer networks, the rate of “traditional” crimes in cyberspace has also increased by exploiting security vulnerabilities of teleworking and fear and uncertainty due to the pandemic.*

**Conclusion:** *The enormous growth of cybercrime during the COVID-19 pandemic poses a serious challenge to government structures. The state’s response to the huge rise of cybercrime should initially focus on implementing preventive measures in the form of education and awareness-raising campaigns, as the greatest security risk is underestimation or lack of awareness of cyber threats.*

**Keywords:** *cybercrime, COVID-19, state response*