CIVITAS, 2022, 12(1), 351-363
www.civitas.rs

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

UDC 004.738.5:343.54:[616.98:578.834
Professional paper
Received: 06. 01. 2022.
Accepted: 27. 01. 2022.

TYPES OF CYBER FRAUD DURING THE COVID-19 VIRUS PANDEMIC

Abstract: The pandemic caused by the COVID-19 virus shook the whole world and caused numerous consequences and great loss of human lives. The subject of the research refers to types of fraud encountered in cyberspace during the pandemic. The research found that some of the most common types of fraud are related to e-mail phishing, theft of user credentials, SMS phishing, malware distribution, as well as communication via social platforms. It is evident that cyber hygiene measures during the COVID-19 pandemic must be improved and implemented more efficiently. Also, the research showed that it is necessary to improve the current legislation not only at the national level, but also at the international level. The research made use of the normative method, induction and deduction.

Key words: law, security, cyber space, COVID-19, phishing

1. Introduction

The pandemic caused by the COVID-19 virus shook the whole world and resulted in numerous dire consequences and great loss of human lives. In addition to all the problems caused by the COVID-19

[1*] Associate Professor, Senior Research Fellow, Educons University, Faculty of Security Studies, Vojvode Putnika 87, Sremska Kamenica, Serbia, e-mail: sdomazetns@gmail.com ORCID iD: https://orcid.org/0000-0002-5964-2249

[2**] Full Professor, Faculty of Law and Business Studies Lazar Vrkatić, Novi Sad, Union University, Belgrade, Serbia, e-mail: zskakavac@useens.net

pandemic, we will focus on the problems in cyberspace, which have reached significant proportions. True, cyberspace problems are nothing new: they have existed since the rise of the Internet and information and communication technologies. Accelerated digitalization and the ever-widening application of modern technologies have further increased the level of risk to the population, the economy and the public sector around the world.

In this regard, the current COVID-19 pandemic brings not only health risks, but also risks of fraud and misuse of personal data. According to Đukić (2017, p. 99), "these include violation of information confidentiality, interference with their functionality through disruption of operations, usurpation and theft of intellectual property, various types of other theft and fraud, as well as a multitude of other frauds that differ in motives, goals, methods and techniques". As Petrović states (2004), "the notion of theft related to information and communication technologies, in addition to theft performed by stealing information and communication devices and their components, includes theft of various goods, theft of computer services, data theft, theft of codes, passwords and identification numbers and identity theft" (p. 133).

During the COVID-19 pandemic, a large number of different types of cyber fraud were registered, such as types of fraud related to e-mail phishing, theft of user credentials, SMS phishing, malware distribution, and communication platforms such as the ZOOM application. Social networks in particular proved to be a fertile ground for various cyber scams. According to Skakavac (2020) "the negative consequences of using various social networks, especially by minors, should not be overlooked. Although the users of many social networks are diverse when it comes to gender, age, education, etc., these networks have the greatest impact on young people. Young people are curious, eager for new challenges and all the latest types of information technologies, and they very easily become their constant companions and clients" (p. 85).

Phishing as a type of cyber fraud has been particularly prevalent during the pandemic. As Graydon (2006) explains, the term "phishing" "comes from the analogy that fraudsters use e-mail as bait for fish for profitable personal data from the unsuspecting sea of Internet users"

(p. 335-337). According to Domazet & Skakavac (2019), "in the early stages of phishing, perpetrators used relatively simple methods of fraud, so that phishing emails were relatively easily recognizable (for example, they contained numerous grammatical and spelling errors), while today phishing has evolved and become much more complex and sophisticated, including numerous advanced concealment software solutions to obtain sensitive (personal) data" (p. 191).

The damage from phishing attacks is constantly increasing. According to Đukić (2017, p. 110) "in 2015 alone, about 147 million phishing attacks were registered in the world, of which Russia suffered the most attacks (17.8%), while the United States was the best "host" to attackers and the most attacks were carried out from its territory (15.2%). By target, phishing attacks were mostly targeted at online financial institutions (banks, payment systems and online stores)". As Gudkova at al. (2018) state, "in 2016, over 154 million phishing attacks were registered, with Brazil suffering the most attacks, and over 12% of attacks originated in the United States. In 2017, over 246 million attacks were recorded, and the largest source of attacks this year remained the United States (with a share of 13.21%). The most widely used malware is called *Trojan-Downloader.JS.Sload*". According to the 2021 European Union Agency for Cybersecurity (ENISA) Report, "COVID-19 created opportunities for cybercriminals. Social engineering remains the most prevalent attack technique. During the pandemic, cybercriminals have been exploiting people's interest, concern, curiosity, and fear by using phishing lures related to COVID-19 for financial gain".

This research deals with the types of cyberspace fraud during the pandemic. In the sections that follow, we will first discuss the phishing-related legislation in the European Union and then analyze some of the typical examples of cyberfraud during the COVID-19 pandemic. The normative method will be used in the research, as well as the methods of induction and deduction.

2. Phishing Legislation in the European Union

In the field of the EU cyber security, there is still no "umbrella" regulation that would regulate this matter, so the legislation in this area consists of several different legal acts. According to Domazet (2019), the most important regulations regarding cyber security in the European Union are: Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Directive 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Communication from the Commission of 15 November 2006 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on fighting spam, spyware and malicious software, Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in

the electronic communications sector (Directive on privacy and electronic communications), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation-further: GDPR Regulation). In connection with the the COVID-19 pandemic, the European Union has adopted a whole set of new acts, striving to legally regulate the challenges as efficiently as possible, and this comprehensive database of regulations is regularly updated.[3] However, it should be noted that the pandemic situation has led to adopting some legislation that could disrupt the normal functioning of the democratic system and the exercise of freedoms and rights of citizens.

According to Council of Europe (2020), for example, the EU member states that are signatories to the Convention for the Protection of Individuals with regard to the Processing of Personal Data (hereinafter: Convention 108+) have adopted provisions restricting certain freedoms and rights. According to the 2020 Council of Europe Report on Data Protection, three main approaches can be identified: 1) adoption of general emergency measures giving the government special powers (notably based on laws or decrees, in application of constitutional law); 2) adoption of emergency measures in specific sectors, often based on public health or pandemic regulations; 3) adoption of emergency measures without a specific legislative basis. These different approaches have led to a patchwork of provisions in the 55 countries parties to Convention 108. Most provisions give extensive power to the governments, though usually only for a limited period of time. The same report states that even though such measures can be highly invasive and constitute important limitations to fundamental rights (privacy, data protection but also freedom of movement and assembly, and in some cases freedom of speech), the necessary oversight by supervisory authorities, parliaments and courts has sometimes been missing. Some constitutional courts have already issued rulings on some measure. Other courts were prevented from fulfilling their role (Council of Europe, 2020).

[3] The list of EU documents related to the common EU response to the COVID-19 pandemic can be found at the following link: https://eur-lex.europa.eu/content/news/Covid19.html (15/11/2021)

The Report rightly states that although data processing in the context of combating the pandemic can find its legitimacy in the Convention, the exceptional circumstances related to the vital threat and the public interest call at national level for additional and more specific regulation to ensure compliance with the principle of legal certainty. Such regulations should define the scope and purpose of the intended data processing (Council of Europe, 2020). Also, the Report states that protecting data against unlawful access is all the more important considering the sensitive character of most of the data collected in response to the health crisis. Both data protection authorities and civil society have played a crucial role in verifying and reinforcing the security of the proposed digital solutions. For example, weaknesses in the protection of personal data were highlighted: security weaknesses on the website processing self-reported health data, and especially a lack of proper encryption or weaknesses related to the source code of the contact -tracing application (Council of Europe, 2020).

In addition to Convention 108+, the EU General Data Protection Regulation (GDPR) also serves to protect data from phishing attacks during the COVID-19 pandemic. According to the GDPR, (Article 7) where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Furthermore, the GDPR Articles 25 and 32 state that taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

According to the GDPR Article 33, in the case of a personal data breach, the controller shall without undue delay notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Further, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Therefore, all the above provisions are of great importance for the protection of personal data during the pandemic. In view of the health crisis, the Member States of the European Union have adopted appropriate acts of secondary (national) legislation in order to overcome the problems related to the protection of personal data. According to Council of Europe (2020), the Report mentions the following measures: a) use of mobile phone applications, for different purposes; b) use of traffic and location data from mobile phones and apps; c) use of other technical tools (eBracelets, smart cameras allowing for facial recognition, thermal scans, remote control by drones and robots, mandatory testing).

3. Examples of Cyberfraud During the COVID-19 Pandemic

Since the beginning of the COVID-19 pandemic numerous cases of cyberfraud have been recorded. The pandemic turned out to be an extraordinary opportunity for cybercriminals; since phishing scams were among the most widespread the following sections will focus on them. According to Warburton (2020), the number of phishing attacks across the world was constantly increasing, especially during 2019 and 2020, which can be seen in the Figure 1:

Figure 1: Phishing Incidents dealt with by F5 SOC
Source: (Warburton, 2020)

Thus, numerous examples of phishing attacks have been attacks on e-mail accounts around the world, with e-mails being addressed by different names referencing the pandemic. According to the Phishing and Fraud Report from 2020 (Warburton, 2020), examples of e-mails with different subject lines are given:

- 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.

With regard to SMS phishing scams (smishing), a large number of fraud attempts have also been reported. According to Watkins (2020), Symantec finds that 1 in 20 COVID-19 related SMS messages contain phishing attempts or other high-risk content. Symantec observed the first high-risk SMS phishing attack using COVID-19 as bait on January 24, 2020, roughly around the same time as the virus began to receive more media coverage. The criminals behind these scams all use the same tactic; taking advantage of people's fears and financial hardships during the global pandemic in order to lure them in.

Research on phishing scams during the COVID-19 pandemic was also conducted by the well-known company Kaspersky. According to the relevant report of this company regarding phishing fraud during 2020, various forms of fraud have been identified, highlighting "public relief" by spammers, malicious links (mention is made of the example of the Turkish Ministry of Health and false messages promising cash payments if a malicious application is installed), followed by fraud related to the corporate sector (one of the emails stated that technical support had created a special alert system to minimize the risk of a new virus infection), the famous Nigerian scam and the like (Kaspersky, 2021).

According to Kaspersky, "last year's events affected the distribution of phishing attacks across the categories of targeted organizations. The three largest categories had remained unchanged for several years: banks, payment systems and global Internet portals. The year 2020 brought change. Online stores became the largest category with 18.12%, which may be linked to a growth in online orders due to pandemic-related restrictions. Global Internet portals remained the second-largest category at 15.94%, but their share dropped by 5.18 p.p. as compared to 2019, and banks were third with a "modest" 10.72%"(Kaspersky, 2021). This data is shown in Figure 2.

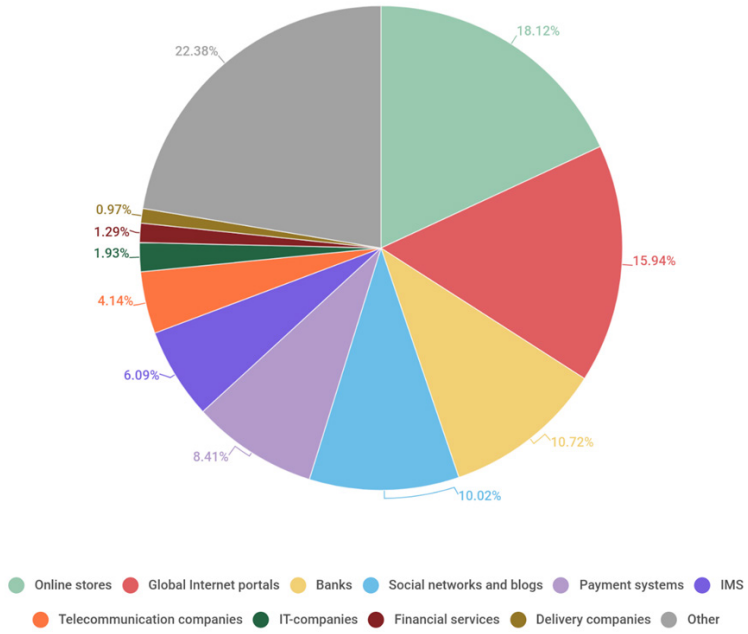

Figure 2: Distribution of organizations targeted by phishers, by category in 2020

Source: (Kaspersky, 2021)

According to CERT (2021), with regard to credential theft, it should be noted that this type of fraud takes place in such a way that Link leads to a fake website containing "COVID-19" in the name, and for access to

information from page requires an email address and password. These websites look like legitimate and seem reliable, but a malicious attempt can be determined by a detailed examination URL. The entry of credentials by the user allows the attacker to access his electronic user's mail, which usually contains personal and confidential data (eg bank account statements), and can also use the user's directory to further spread phishing attacks.

It has been shown that communication platforms such as ZOOM can also be used to disrupt cyber security. Abnormal security researchers detected phishing attacks posing as Zoom meeting notifications. According to Davis (2020), the email requests the user to join a meeting about their job termination, asking users to first log into a fake Zoom page that will actually steal their credentials. The malicious landing page appears to be a legitimate "carbon copy" of a Zoom login page. The email masquerades as an automated notification for an important meeting with HR regarding the recipient's termination. The email contains a link to a fake Zoom login page hosted on 'zoom-emergency.myftp.org.' Links to the phishing page are hidden in text used in automated meeting notifications. The email masquerades as a reminder that the recipient has a meeting with HR regarding their termination. When the victim reads the email they will panic, click on the phishing link, and hurriedly attempt to log into this fake meeting. Should recipients fall victim to this attack, login credentials as well as any other information stored on Zoom will be compromised.

4. Conclusion

Based on the above, it can be concluded that cyber scams were very common during the COVID-19 pandemic. Cybercriminals understood the pandemic as a great opportunity for easy gain, and with various methods of social engineering (using various psychological techniques, mostly based on the fear of the virus), succeeded in deceiving their victims worldwide. The damage from cyber-attacks during the COVID-19 pandemic is increasing. It turned out that the victims of the cyber-attack were not only private companies, but also public utilities, as well as the public sector around the world.

The research has shown that some of the most common types of cyberfraud are related to e-mail phishing, theft of user credentials, SMS phishing, malware distribution, as well as communication platforms such as the ZOOM application. These cyberspace risks can be prevented by various measures of technical, organizational and legal nature. It was determined that cyber hygiene measures during the COVID-19 pandemic must be improved and implemented more efficiently. It has been established that there is phishing-relelated legislation both at the EU level and at the national level. Some of the most important EU legislation includes the Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), as well as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Analyzing the most important provisions of these legal acts, one gets an impression that it is necessary to improve the current legal regulations not only at the national level, but also at the international level. One of the measures that can give results is related to raising the awareness of citizens and the economy about the potential dangers lurking in cyberspace.

Bibliography

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-SEC-MAN* (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