PROFESSIONAL PAPER

UDK: 004.491
DOI: 10.59245/ps.32.3.4
Received for publication: May 2023

BERNARD VUKELIĆ*, ALIDA DINA ZVONARIĆ**, NIKOLA PROTRKA***

The Recognition of an E-Mail Phishing Cyberattack in Business Organizations

Abstract

Phishing is a form of social engineering and cybercrime which entails theft of confidential information (personal or official) for financial gain. That is one of the oldest cyber threats. There is a wide range of phishing attack techniques, and the most frequent one is performed via electronic mail. Due to major changes in conducting business in the last pandemic, which entail remote work, fast digital transformation and the increase of ICT technologies, the statistics show that phishing attacks are on the rise. Employees who lack developed awareness of phishing attacks, responsibility and knowledge represent a potential danger to the entire organisation. This paper describes the research on e-mail phishing recognition in business organisations in Primorje-Gorski kotar County. The research showed that employees are not aware of phishing attacks to a sufficient extent and that all the habits contributing to the IT security level regarding these attacks are not satisfying. To protect against such attacks, organisations should, in addition to implementing safety technical measures, actively educate employees and periodically implement testing.

Keywords: *phishing, cybercrime, cyber threat, social engineering, cybersecurity.*

1. INTRODUCTION

Phishing continues to be a significant issue and is considered the number one threat in the online world. As the last few pandemic years have seen major changes in how business is done, the use of new technologies and remote work created new phishing opportunities

* Polytechnic of Rijeka, Vukovarska 58, 51000 Rijeka, Croatia.

** Polytechnic of Rijeka, Vukovarska 58, 51000 Rijeka, Croatia.

*** University of Applied Sciences in Criminal Investigation and Public Security, Av. Gojka Šuška 1, 10000 Zagreb, Croatia.

and increased phishing attacks in business organisations (Jain & Gupta, 2022). To protect against phishing attacks, business organisations must implement a large number of protective measures. However, despite the implemented technical measures, forged mail often reaches the employee. Then, the further business of the organisation depends on the actions they will take regarding that. Humans are easier to deceive than computer systems and networks, so exploiting employees as the weakest link of any institution or business organisation is a fundamental characteristic of phishing attacks. Phishing has increased in sophistication over the past 20 years, and deceptive e-mails which persuade users to take dangerous activities are increasingly difficult to recognise (Lain et al., 2022). Therefore, the key to protecting against phishing attacks is the knowledge and awareness of employees. Although many papers and research on phishing defence techniques have been published in recent years (CCERT, 2022), the human factor remains a problem (Aleroud & Zhou, 2017).

For these reasons, this research focused on employees in organisations and their knowledge about phishing. The target group is the working population that performs office work and uses a computer in their daily work. The research was conducted on e-mail phishing recognition in business organisations in Primorje-Gorski kotar County. The main objective of the research is to examine how many employees who use e-mails daily are familiar with e-mail phishing scams. Such phishing attacks are carried out through fraudulent electronic communications, which prompt the user to click on a specific link which takes them to the malicious web server's website and requires them to enter confidential information. At the same time, it is difficult to detect fraud because such e-mail messages and web pages often appear legitimate. One effective way of protection is using tools for simulating phishing attacks (Khonji et al., 2013). Such tools help examine employees' vulnerability to such attacks by creating fake e-mail campaigns and fake websites sent to employees and monitoring their reactions and activity (RISKIQ, 2023). Although various simulation tools can be used, we decided on a different and broader approach for this research. Instead of just carrying out an automated phishing campaign, we wanted to find out which elements and habits of employees are crucial to protection against phishing. In order to get answers to such questions, a survey was conducted. The survey is divided into four parts, each representing demographic data, phishing recognition, habits and training and awareness - all related to human factors of phishing.

The paper and research resulted in several contributions. First, it investigated the impact of phishing on business organisations. Second, in addition to analysing recent literature and research on phishing, the situation of phishing attacks in the Republic of Croatia was also investigated. Finally, the research provided in business organisations in Primorje-Gorski kotar County answers such as whether younger employees recognise phishing better than older ones, whether they recognise the key indicators that an e-mail is fake and what their security habits are when working with usual office tools, and whether employees have sufficient knowledge and awareness about phishing. Likewise, the research has shown which employees are the most vulnerable to phishing in organisations and how organisations can help their employees in phishing prevention.

2. PHISHING DEFINITION

The term phishing comes from the term fishing, which has the letters ph instead of f, and in accordance with the original meaning of the word fishing, usernames, passwords and other sensitive information are "fished on boat" in the "river" of users (Gupta, 2018). The term phishing was first mentioned on 2 January 1996 in a group called AoHell (Sharma et al., 2017). Phishing is a type of social engineering. Social engineering has two goals: stealing confidential information for financial gain or sabotage, which refers to damaging data by stealing confidential information. Since this type of attack focuses on exploiting human psychology, attackers often exploit psychological states such as heightened emotions (fear, excitement, curiosity, anger, or guilt) by creating a sense of urgency to do a job or by creating trust. The attacker carefully selects the victim to carry out the attack, and the selection begins with the preliminary collection of information about them. Every successful attack based on social engineering methods is based on four steps, which include selecting the victim of the attack and collecting information about them, developing trust with the victim, exploiting the collected information and carrying out the attack. The choice of attack method and tools for its implementation is determined by the purpose of the attack, the level of knowledge of the social engineer, the available resources and the difficulty of exploiting the victim. It should also be pointed out that collecting information about the victim is considered the most demanding step in the attack. However, today, in the internet and social networks age, it is simpler than before. The methods used to collect data are divided into computer-assisted, which does not require direct contact with the victim, and physical, which is collected through physical communication with the victim on the spot. It is easy to persuade employees to talk; most often, they are unaware of the information they are sharing with the attackers. Extracting data through conversation is very effective, and attack victims are usually unaware they have discovered information. Using technical, computer-aided methods, personal and company websites are searched to profile the victim. By searching data on search engines, social networks, company websites, etc., it is possible to collect a lot of information about the victim's employment, family, hobbies, and attitudes, as well as many other useful information for the attacker.

There are different types of phishing attacks, characterised using different social engineering techniques or different ways in which the attacker communicates with the victim. The most common types of attacks are listed below.

2.1. E-mail phishing

The most common form of phishing attack uses fake links in fake e-mails. Attackers often impersonate e-mails from organisations like Google and Microsoft or alternatively impersonate a fellow employee's e-mail address and send thousands of generic requests. The links usually lead to malicious websites which steal credentials.

2.2. Malware phishing

It refers to scams which involve installing or running malicious code, known as malware, on victim users' devices. Malware can also be hidden in an attachment file (e.g., an MS Word document).

2.3. Spear phishing

When attackers want to "catch" a certain individual, they do so by exploiting data collected through research about that individual's habits and social and business life. They then take advantage of this through fake messages using real names and job roles to make the victim think the e-mail came from a known, legitimate source.

2.4. Whaling

Attackers use social media or company websites to find the names of an organisation's CEO or other members of senior management. They then impersonate someone using a similar e-mail address. E-mail messages may request money transfers or require the recipient to review documents. The whale attack is also known as the CEO scam.

2.5. Smishing

Smishing is the process of sending text messages to the victim asking them to take some action (e.g. click on a link in the SMS), which, when done, installs malware on the user's device. Employees are sensitive to SMS scams because they do not expect this type of attack.

2.6. Vishing

Vishing is short for voice phishing, which consists of tricking employees on the phone into giving away sensitive information.

3. THE IMPACT OF PHISHING ATTACKS ON THE ORGANISATIONS

Every year, there are more and more phishing attacks on different organisations, regardless of whether they are small businesses or those on a global scale. Global organisations receive up to 1,000 such attacks per month (Packetlabs, 2020). The impact of a successful phishing attack on organisations depends on a variety of factors, such as the size of the business and the amount of information at risk. Potential undesirable outcomes for the organisation are financial losses, loss of intellectual property, reputational loss, and business disruption.

3.1. Financial loss

If an organisation becomes a victim of identity theft, the first and most important repercussion is financial costs, which can be direct and indirect. Indirect costs are those that result from "violations" of the regulations of legal acts such as the Personal Data Protection Act and others, as well as compensation to affected clients. Total costs can easily reach extremely high figures (Packetlabs, 2023).

3.2. Loss of intellectual property

The most devastating loss for an organisation is the theft of intellectual property, i.e. customer data, trade secrets, research, information about upcoming product launches or new partnerships, especially if we are talking about organisations whose activities include

technology, defence, pharmacy and the like. For example, the theft of a drug patent can cause millions of damage, which also affects the competitive advantage in the market.

3.3. Damage to reputation

Organisations have been building and investing in customer trust for years because the company's long-term success ultimately depends on it. Studies show that trust is the second most important factor because a customer will choose a company they trust. By trusting customers, the company succeeds in creating a brand from its product and gains a reputation. Both items result from the trust of customers, as well as the trust itself, not only of customers but also of the entire chain of employees on whom the organisation depends (suppliers, investors, employees) is lost if the information that a phishing attack was successfully carried out on it is revealed to the public. Unfortunately, such a newly formed opinion is challenging to change in the public. This is why cyber security is essential in all phases of project development. Research shows that about 41% of consumers would no longer use products from a company successfully targeted by a phishing attack (CybSafe, 2021).

3.4. Business disruption

A successful phishing attack on a company leads to business disruption, especially if it involves attacks involving malicious software. It takes some time to recover for the organisation to function as it did before the attack. Recovery involves shutting down the system, which results in reduced productivity and, thus, monetary losses. If the operations of organisations which provide services such as transportation, technology, waste disposal and other critical infrastructures are interrupted, economic and social disruptions result (CSBS, 2020).

4. PHISHING CAMPAIGNS IN THE REPUBLIC OF CROATIA AIMED AT BUSINESS ORGANISATIONS

A significant number of peer-reviewed academic papers have been published in the last five years that focus on phishing research (Alkhalil, 2021). According to a literature review of these papers, phishing attacks have increased from 76% in 2017 to 83% in 2018. Thus, Microsoft's New Future of Work 2021 report (Teevan, 2021) states that 80% of security professionals have experienced an increase in security threats since moving to remote work and of that 80%, 62% state that phishing attacks have increased more than any other type of threat. A report by security company RiskIQ found that cyberattacks related to the COVID-19 disease increased to an unprecedented level in March 2020 and that most of these scams took the form of fake websites with information about the COVID-19 disease (RISKIQ, 2023). It is significant that even before the start of the pandemic, an increase in phishing attacks was noticed. APWG Annual Reports also show that in the third quarter of 2019, the number of phishing attacks rose to 266,387, the highest level in three years since the end of 2016 (APWG, 2020). This is a 46% increase from 182,465 in the second quarter and nearly double the 138,328 seen in the fourth quarter of 2018. The number of phishing e-mails reported to the APWG in the same quarter was 118,260.

From 2017 to 2022, phishing e-mail messages were sent to a wide range of business organisations in the Republic of Croatia. Over the years, some message scenarios were repeated or were very similar, and at the same time, their appearance became more and more credible. Although the most famous case of phishing fraud from 2010 is the client of OTP Bank, the first major recorded attack, which took place in 2017, was when the attackers presented themselves as the Tax Administration asking the recipient to download a document for a new legal act on tax profits if they belonged to the company's accounting department, when in fact it was about downloading a malicious file (Poslovni dnevnik, 2022). Also, in 2019, recipients of corporations received e-mails with malicious content whose "sender" is the Tax Administration. In 2018, the head of finance of the city of Đakovo paid 50,000 euros to John Smith's account based on a fake phishing message (Svijet sigurnosti, 2018). In 2018, educational institutions were selected with the aim of compromising the user accounts of employees in order to obtain confidential data.

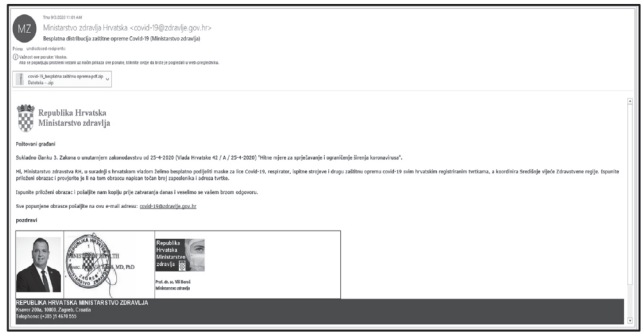

Figure 1 Phishing e-mail of the "Croatian Ministry of Health"

The sender presents themselves on behalf of the e-mail administrator, who warns about the storage quota being exceeded and instructs to click on the link and enter the user data and password so that the data can be updated and, thus, new e-mails can be received. In 2019, Croatian state bodies were targeted by a phishing campaign via electronic mail, which contained a malicious link imitating the official website of the Croatian Post (HP, 2019). The Institute for the Security of Information Systems identified two versions of the infected file, namely the Silent Trinity and Powershell Empire malicious programs, which enable taking control over the computer. In 2020, there was also an exceptional increase in phishing e-mails sent to legal and natural persons to extract material benefits by entering user data. In this way, an unknown perpetrator from abroad managed to defraud several rooms. In addition, hackers are using current events related to COVID-19. There are messages with the content and appearance of the Croatian Ministry of Health intended for Croatian organisations to "allocate" free face masks and other equipment against the pandemic. For this purpose, it is necessary to fill out the form (Vrbanus, 2020) and opening the attached form launches malicious content. In 2022, phishing messages related to events in Eastern Europe were also sent to many bodies in the European Union and Croatia. The text of the message mentions Ukrainian refugees or the payment of financial resources as donations and the like in order to induce the recipient to launch malicious content (Baretić & Protrka, 2021).

5. RESEARCH METHODOLOGY

Research on the recognition of e-mail phishing cyberattacks in business organisations was conducted using the survey method. According to the definition, a survey represents "the collection of opinions and data about a phenomenon among a large number of employees for the purpose of statistics, market research or public opinion or as a basis for some further study" (Anić et al., 2004). It was conducted in the mid-end of 2022 in the area of Primorje-Gorski kotar County. The survey was conducted online, and the LimeSurvey tool was used to create the survey.

The survey consists of 22 questions. The survey is divided into four parts, each of which represents the following:

1. demographic data,
2. phishing recognition,
3. employee security habits and
4. education and awarness.

All questions were multiple choice questions, except the third part questions, which have descriptive degrees of frequency, among which "never" and "sometimes" are classified as undesirable habits, and "often" and "always" are desirable habits.

Study Participants

The target group included employees who perform office work and use a computer in their daily work. The business organisations which were invited to participate in this study were informed that it is anonymous; that is, if they decide to be part of the research, their identity and the activity they are engaged in will not be revealed. Fifteen business organisations from different industries participated. A total of 214 employees took part in the questionnaire, and 190 (n = 190) answered it completely. Ten respondents have a high-level IT knowledge, and 119 respondents are self-taught. Forty-six respondents have some basic IT knowledge, and 11 have medium-level knowledge. Four respondents stated that they have low-level knowledge.

Age Distribution

A total of 2% of employees (3 respondents) belong to the group under 20 years of age, 9% of employees (18 respondents) belong to the group from 20 to 29 years of age, 23% of employees (43 respondents) to the group from 30 to 39, 30% of employees (58 respondents) to the group from 40 to 49, 24% of employees (45 respondents) to the group of 50 to 59, and 12% of employees (23 respondents) to the group of 60 and over. By age group, the respondents were divided into three categories:

– the younger group (up to 39 years of age) consists of 34% of employees (64 respondents),
– the mature group (from 40 to 59 years of age) consists of 54% of employees (103 respondents),
– the old group (60 years and older) consists of 12% of employees (23 respondents).

Phishing recognition

Part 2 of the survey contained 11 common knowledge questions about phishing and questions with specific examples where respondents had to recognise phishing e-mails and login websites which are similar to their daily ones. An example of a question is shown in Figure 2 below. In that example, the question was: "Would you follow the instructions in the following e-mail?" The correct answer is: "No". 21% of employees (40 respondents) would follow the e-mail instructions, and 79% of employees (150 respondents) would not. It is also interesting that on the question "Can you identify phishing e-mails with ease?", 45% of employees (85 respondents) think they know how to recognise phishing scams, 11% of employees (21 respondents) think they don't know how to recognise them, and 44% of employees (84 respondents) are not sure. When it comes to the question, "Would you sign up on the Google page?" the correct answer is: "No." (Figure 3) 24% of employees (45 respondents) would log in to the website, and 76% of employees (145 respondents) would not.

Some examples of questions were the legitimate websites they use every day. In such questions, almost 65% of respondents did not recognise legitimate websites but marked them as phishing scams.

When asked to identify the elements of a phishing e-mail, such as a request for an urgent response or an e-mail containing spelling mistakes, 59% of employees (113 respondents) recognise the elements of a phishing e-mail, 16% of employees (30 respondents) do not, and 25% of employees (46 respondents) are not sure.

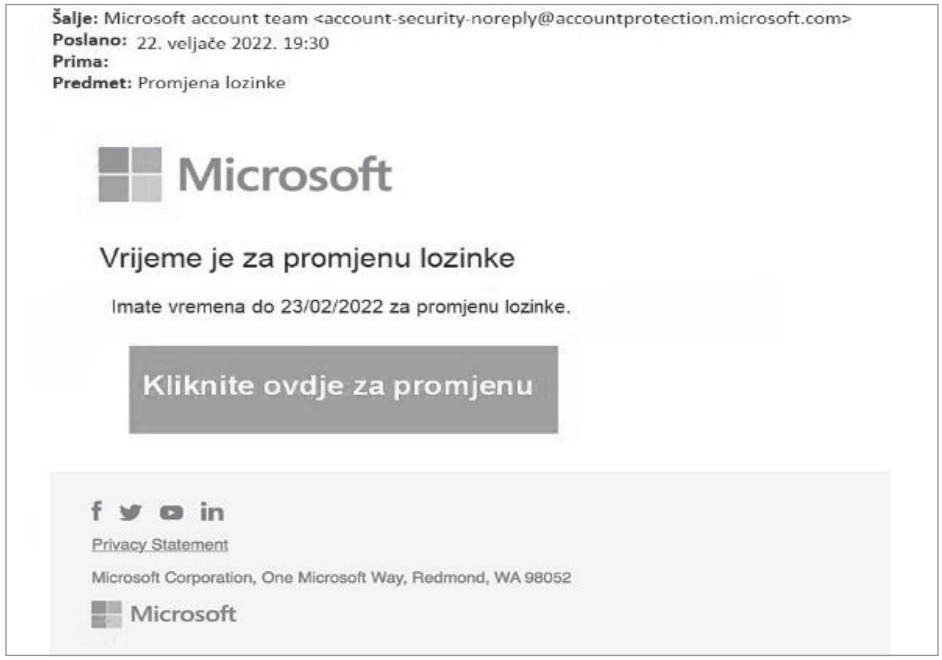

Figure 2 Phishing e-mail

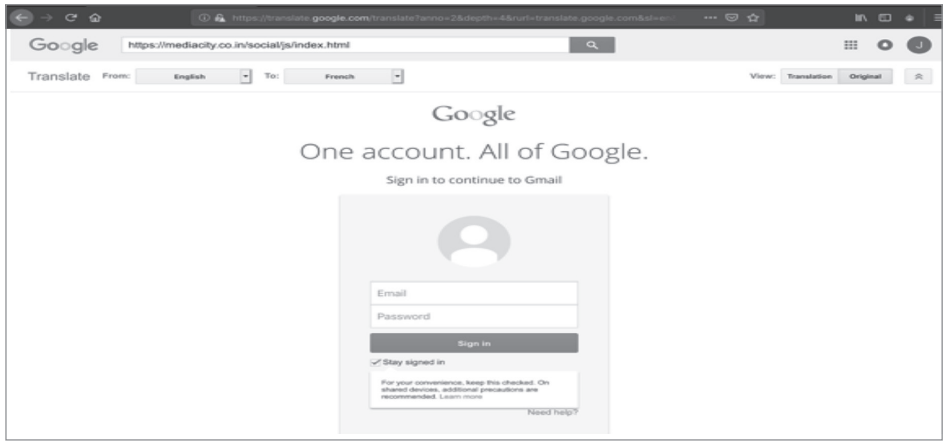

Figure 3 Phishing web page

Employee security habits

Part 4 of the survey contained 4 questions and 12 sub-questions. Question number 16 reads: "On a scale of 1 to 4, how often do you carry out the following activities ":

a) "You check whether the sender of the e-mail is the one they claim to be before you open the attached link (or link)."

Figure 4 shows that 53% of employees (91 respondents) have desirable habits for checking the sender of an e-mail before opening the attached link, and 47% of employees (89 respondents) have undesirable habits.

b) "You update the operating system immediately when the system provides you with this possibility."

57% of employees (109 respondents) have desirable habits for updating the operating system, and 43% (81 respondents) have undesirable habits.

c) "Monitor information about phishing attacks."

26% of employees (50 respondents) have desirable habits for monitoring information about phishing attacks, and 74% of employees (140 respondents) have undesirable habits.

d) "Check whether the website through which you enter confidential information uses the HTTPS protocol (the page starts with https:// instead of http://)."

A total of 41% of employees (78 respondents) have desirable habits for checking the HTTPS protocol of a website, and 59% of employees (112 respondents) have undesirable habits.

e) "You often change passwords."

Figure 5 shows that 29% of employees (56 respondents) have desirable habits for changing passwords, and 71% of employees (134 respondents) have undesirable habits.

Question number 17 reads: "Do you use the same passwords in several different online places (e-mail, social networks, entering the computer, accessing bank accounts, etc.)?"

48% of employees (92 respondents) use the same passwords for several online sites, and 52% (98 respondents) do not. Question number 18 reads: "What will you do as an employee if you suspect you have received a phishing e-mail?" A total of 68% of people (129 respondents) would report a suspicious message to the organisation, 15% of people (28 respondents) would ignore it, 13% of people (25 respondents) would show it to a colleague, and 4% of people (8 respondents) would do something else.

The last part of the survey referred to 4 questions related to the organisation's attitude towards phishing and the employee's attitudes about phishing awareness education. Only 26% of employees have received phishing awarness education. Question number 21 reads: "Would you like to attend education on phishing awarness?" 55% of employees (105 respondents) want to listen to a lecture on phishing attacks, and 45% of people (85 respondents) do not.

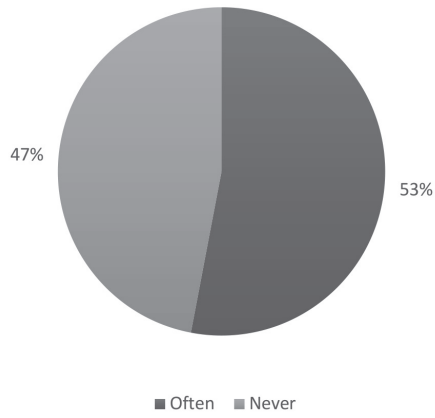

Figure 4 Checking the sender of an e-mail before opening the attached link

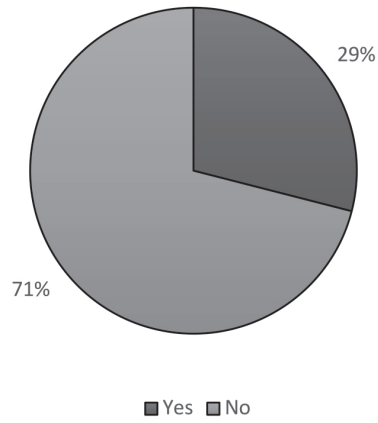

Figure 5 Changing passwords habit

6. CONCLUSION

Most employees in the survey part 2 have three or more mistakes in not recognising and knowing about phishing scams. The entire test was solved correctly by only one employee; one employee had one error, and 14 employees had two errors. So, 17 employees solved the test correctly, while 173 employees did not recognise phishing at a satisfactory level. Expressed as a percentage, 14% recognise phishing attacks, which is worrying. The younger group has an average result of the knowledge test of 74% (the best results). The mature group has an average result on the knowledge test of 63%, and the old group has an average knowledge test result of 51%. The younger group achieved the best results in the knowledge test, which can be linked to a better knowledge of information and communication technology. In addition, not all habits contributing to the IT security level are satisfactory.

The number of those who attended the education on phishing awareness (31 respondents) is too small to correlate it with recognition of phishing scams and more desirable habits. In addition, the sample of respondents with a higher level of IT education (10 respondents) is too small to correlate this with better recognition of phishing scams and more desirable habits.

Unfortunately, what the employer actively did in relation to the employees' phishing awareness in the survey (phishing awareness education) is negligible when looking at the entire survey sample (16%). Such results based on knowledge of phishing scams by employees are not unexpected. Employees who do not have a high IT education cannot be expected to be a protective factor that can respond to phishing scams because they are becoming more sophisticated and complex every day. In addition, the employer who does not recognise the potential dangers and does not take active measures to raise the level of IT protection has a big problem.

REFERENCES

1. Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006
2. Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *Conference: 2017 IEEE International Conference on Big Data (Big Data)*, 4458–4466. https://doi.org/10.1109/bigdata.2017.8258485
3. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060
4. Anić, V. et al. (2004). *Hrvatski enciklopedijski rječnik, drugo izdanje,* EPH d.o.o. Zagreb i Novi Liber d.o.o. Zagreb, svezak 1., p. 119.
5. Jain, A. K., & Gupta, B. B. (2021). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

6. APWG. APWG phishing attack trends reports. 2020 anti-phishing work Group, IncAvailable at: https://apwg.org/trendsreports/ [Online; accessed 18 January 2023]
7. APWG. (2018). Phishing activity trends report 3rd quarter 2018., https://docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf,., [Online; accessed 18th January 2023]
8. Baretić, M., & Protrka, N. (2021). Healthcare information technology. *International Journal of E-services and Mobile Applications*, *13*(4), 77–87. https://doi.org/10.4018/ijesma.2021100105
9. CCERT. (2021). Godišnji izvještaj nacionalnog CERT-a za 2021. godinu, https://www.cert.hr/wp-content/uploads/2022/03/CERT-godisnje-izvjesce-2021.pdf
10. Cyber Security Breaches Survey 2020; https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020, [Online; accessed 17th January 2023]
11. CybSafe. (2021). How can phishing affect a business?, https://www.cybsafe.com/community/blog/how-can-phishing-affect-a-business/, [Online; accessed 17th January 2023]
12. Lain, D., Kostiainen, K., & Capkun, S. (2022). Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. *2022 IEEE Symposium on Security and Privacy (SP)*. https://doi.org/10.1109/sp46214.2022.9833766
13. Gmail. (2021). Avoid and report phishing e-mails, https://support.google.com/ mail/answer/8253, [Online; accessed 18 January 2023].
14. Gupta, B. B., Arachchilage, N. a. G., & Psannis, K. E. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z
15. Sharma, H., Meenakshi, E., & Bhatia, S. K. (2017). A comparative analysis and awareness survey of phishing detection tools. *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*. 1437-1442. https://doi.org/10.1109/rteict.2017.8256835
16. Hrvatska pošta. Lažne poruke na društvenim mrežama, https://www.posta.hr/lazne-poruke-na-drustvenim-mrezama/7795, [Online; accessed 17th January 2023]
17. KnowBe4. (2021). Phishing. https://www.knowbe4.com/phishing, [Online; accessed 20th January 2023].
18. Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys and Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/surv.2013.032213.00009
19. Nacionalni CERT (2019). https://www.cert.hr/CUPOPOREZ, [Online; accessed 19th January 2023]
20. Packetlabs. Pandemic Impacting the Cost of a Data Breach https://www.packetlabs.net/posts/pandemic-cost-of-data-breach/, [Online; accessed 18 January 2023]
21. Packetlabs. (2020). What is the business impact of a Phishing Attack?, https://www.packetlabs.net/posts/impact-of-phishing-attack/, [Online; accessed 18 January 2023]

22. Poslovni dnevnik. Kruži lažni mail OTP banke, kradu se podaci, https://www.poslovni.hr/trzista/kruzi-lazni-mail-otp-banke-kradu-se-podaci-144835, [Online; accessed 23rd January 2023]
23. RISKIQ. COVID-19 cybercrime weekly update, https://www.riskiq.com/blog/analyst/covid19-cybercrime-update [Online; accessed 23rd January 2023]
24. Salloum, S. A., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using Natural Language Processing Techniques: A literature survey. *Procedia Computer Science*, *189*, 19–28. https://doi.org/10.1016/j.procs.2021.05.077
25. Svijet sigurnosti. Kako je iskusni šef financija grada Đakova nasjeo na stari hakerski trik?, https://www.svijetsigurnosti.com/kako-je-iskusni-sef-financija-grada-dakova-nasjeo-na-stari-hakerski-trik/, [Online; accessed 23rd January 2023]
26. Teevan, J. et al. (2021). New Future of Work Report 2021, https://www.microsoft.com/en-us/research/uploads/prod/2021/01/NewFutureOfWorkReport.pdf.
27. Tportal. (2017). Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka, https://www.tportal.hr/tehno/clanak/ne-nasjedajte-na-ovaj-lazni-mail-iz-porezne-mogli-biste-ostati-bez-podataka-20171201;
28. Volkamer, M., Sasse, M.A., Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. In: , et al. Computer Security. ESORICS 2020. Lecture Notes in Computer Science(), vol 12580. Springer, Cham. https://doi.org/10.1007/978-3-030-66504-3_19
29. Vrbanus, S. (2020). U Hrvatskoj aktivna phishing kampanja vezana uz COVID-19, *Bug.hr*, https://www.bug.hr/sigurnost/u-hrvatskoj-aktivna-phishing-kampanja-vezana-uz-covid-19-16426, [Online; accessed 17th January 2023]

Sažetak

Bernard Vukelić, Alida Dina Zvonarić, Nikola Protrka

Prepoznavanje phishing napada u poslovnim organizacijama

Phishing je oblik socijalnog inženjeringa i računalnog kriminaliteta koji podrazumijeva krađu povjerljivih podataka (osobnih ili službenih) radi financijske dobiti. To je jedna od najstarijih kibernetičkih prijetnji. Postoji širok raspon tehnika phishing napada, a najčešći se izvodi putem elektroničke pošte. Zbog znatnih promjena u vođenju poslovanja posljednjih pandemijskih godina, koje podrazumijevaju rad na daljinu, brzu digitalnu transformaciju i povećanje korištenja ICT tehnologija, statistika pokazuje kako su phishing napadi u porastu. Zaposlenici koji nemaju razvijenu svijest o phishing napadima predstavljaju potencijalnu opasnost za cijelu organizaciju. Ovaj rad opisuje istraživanje o prepoznavanju e-mail phishing napada u poslovnim organizacijama u Primorsko-goranskoj županiji. Istraživanje je pokazalo kako zaposlenici nisu dovoljno svjesni phishing napada te da njihove poslovne navike koje pridonose razini IT sigurnosti u odnosu na ove napade nisu zadovoljavajuće. Osim implementacije sigurnosnih tehničkih mjera, organizacije bi za zaštitu od phishing napada trebale aktivno educirati zaposlenike i periodično provoditi testiranje prepoznavanja takve vrste napada.

Ključne riječi: phishing, kibernetički kriminal, kibernetička prijetnja, socijalni inženjering, kibernetička sigurnost.