PERCEPTION OF THE INCREASED RISK OF PHISHING ATTACKS DURING THE COVID-19 CRISIS

Jana HANDRIKOVÁ, Darina STACHOVÁ
Department of Technical Science and Informatics, Faculty of Security Engineering,
University of Žilina, Univerzitná 8215/1, Slovak Republic,
E-mails: jana.handrikova@fbi.uniza.sk, darina.stachova@fbi.uniza.sk

ABSTRACT

Measures in connection with the COVID-19 crisis have forced a change in the processes taking place in individual organizations - whether in education, state administration or the commercial sphere. CEOs and full-time employees have been forced to ensure that the organization's goals are met in an ever-changing legislative environment, outside the standard work environment, with increased time pressure, in times of financial security concerns, and in times of heightened health or even life concerns. These factors have weakened concerns about one's own security - including the protection of one's own identity or the protection of the employer's assets in cyberspace. The presented research was attended by students, some of them, especially external students, are employees of the public or commercial sphere. The aim of the research was to find out whether students noticed an increased incidence of phishing attacks during the COVID-19 crisis, how they responded to this fact as individuals and how the organizations in which they are employed reacted. Based on the results of this survey, it can be estimated whether users with the development of Internet services are aware that they are an integral part of the cybersecurity system and, based on this fact, adjust their behavior in cyberspace.

Keywords: *COVID-19, Cyber security, Phishing*

1. INTRODUCTION

Every user of information and communication technologies is exposed to various types of threats that can potentially damage these systems. Knowledge of cyber security should therefore become part of the body of knowledge acquired during university studies. Basic tools and methods for increasing the level of cyber security of the user are also described in book publications [1]. Vulnerabilities of the system are not only the properties, errors or settings of technical means, but also an insufficiently educated and trained user. Despite the use of technical means and methods to protect them, such as steganography or cryptography, user error can cause the loss of an organization's assets, especially information.

The aim of a phishing attack is to obtain data from a user, which the attacker will use to gain his financial advantage by misusing this data for extortion, identity theft, unauthorized access, etc.

According to Verizon's 2020 Data Breach Investigations Report (DBIR) [2], the main types of compromised data are:

- Authentication data (passwords, usernames, PIN numbers).
- Personal data (name, address, e-mail address).
- Internal data (sales information, product plans).
- Medical data (information on treatment, insurance claims).
- Data related to banking operations (account numbers, credit card information).

In the event of a successful attack by the organization, there will be direct and indirect losses. The website [3] states that these losses can be divided into the following files:

- Lost hours from employees.
- Rehabilitation.
- Incident response.
- Damaged reputation.
- Loss of intellectual property.
- Direct cash losses.
- Fines for compliance.
- Loss of income.
- Legal fees.

Phishing is considered one of the forms of attacks using social engineering methods. One of the most detailed taxonomies of phishing attacks can be found at [4]. Attackers use different communication media, different types of target devices of the victim, different attack codes. Types of phishing attacks, vectors and technical approaches are described in [5]. Although there are technical means that can help reduce the risk of not detecting a phishing attack, setting up the security processes of organizations involving an electronic service user can decide whether an attack was successful and therefore a loss on the victim's side. Technical means, such as digital certificates, electronic signatures, or the use of machine learning tools to detect anomalies, can help detect attacks, not ensure that an individual or organization become a victim. The state of current research on automated phishing detection on the web and evaluation of its performance can be found in [6]. In general, a phishing attack vector can be described:

- Attack planning.
- Obtaining victim data.
- Fraud.

In the attack planning phase, the attacker selects the victim, obtains the victim's contact information, and selects the phishing method. The choice of victim can be random or targeted. The attacker obtains contact information on the black market, from a list of addresses in spam, from social media, from poorly secured legitimate websites, etc.

In the data acquisition phase, the victim is convinced that he or she is providing the data to an authorized user for a specific purpose with which he or she agrees. The attacker convinces the victim that it is necessary to confirm the service (login to the website, confirmation of delivery), obtain a profit (financial bonus, win, avoid the fine), help a

close person (the attacker obtains data on close persons from electronic communication or from social networks) or convince the victim of his false identity (the attacker pretends to be an official provider, a researcher, etc.). An attacker would create a fake Web page by abusing an existing legitimate Web site, provide a user with a misleading URL, domain, or HTTPS certificate, or deliver a malicious attachment to the victim.

If the attack was successful, the data obtained by the attacker are used to steal the identity of the victim or sold on the Internet black market.

2. PHISHING DURING COVID-19 CRISES

Attackers used the following COVID-19 factors to deceive the victim during the crisis:

- Increased intensity of external and internal stressors and the resulting reduction in the mental well-being of users of electronic services (attackers use social engineering methods).
- Transfer of resources of organizations (material and human) designed to ensure cyber security and ensure the basic tasks of the organization through remote access (work of employees from home, provision of virtual services, electronic communication with clients, etc.).
- Use of new applications, users unfamiliar with software alerts, error messages, etc. (Fraudulent e-mail issued to report used software).
- Delayed updates and changes to email and web server settings.
- Reduce the organization's costs of managing the organization's risks (including cybersecurity management).

According to the information provided by Member States and private partners in the "COVID-19 Cybercrime Analysis Report - August 2020 Cybercrime: COVID-19 Impact" [7], the main topics of phishing using COVID 19 are:

- e-mails from national or world health authorities,
- government orders and financial support companies,
  fake payment and refund requests,
- offers of medicines and medical supplies,
- COVID-19 tracking applications for mobile phones,
- investments and share offers,
- charity and donations related to COVID-19.

Typical phrases used by attackers to worry, scare the victim were:

- quarantine,
- virus escalation,
- public safety and health concerns,
- the unpredictable nature of the outbreak,
- inability to return home,
- local hospital,
- the need for testing.

In its monthly report from March 2020, the CSIRT [8] draws attention to the spread of malicious software, mainly through emails (phishing) aimed at paralyzing the activities of organizations in the first line of the fight against the spread of SARS COV-2. Interpol is also assisting in the investigation of these targeted attacks on hospitals and medical facilities. [9]. Interpol report of 04.08.2020 [10] points to the alarming increase of cybernetic attacks in member countries. About two-thirds of member countries that responded to the Global Cybercrime Survey reported significant use of COVID-19 topics for phishing and online fraud.

According to Interpol reports from 04.08.2020, the prediction of future cybernetic attacks is as follows: [10]

- A further increase in cybercrime in the near future is highly likely. Work-related vulnerabilities and the potential for increased financial benefits will cause cybercriminals to continue to intensify their activities and develop more advanced and sophisticated practices.
- Active threats are likely to further spread online coronavirus fraud and phishing campaigns to raise public concerns about the pandemic.
- The number of compromised business e-mails is also likely to result from the economic downturn and the shift in the business environment, which identifies new opportunities for crime.
- If vaccination against the COVID-19 virus is available, it is highly likely that there is a further increase in phishing associated with these medical manufacturers, as well as network disruptions and cybernetic attacks to obtain victim data.

3. METHODS

The aim of the research was to find out whether students, whose work will be security management in the organization, recorded an increased incidence of phishing attacks during the COVID 19 crisis, how they reacted to this fact as individuals, how individual organizations responded. Emphasis on linking the content of teaching with practice is a strong motivating factor that increases students' involvement in the process of acquiring knowledge and increases the likelihood that a student will pass the exam successfully. The use of online teaching poses new challenges for both teacher and student [11].

Two main hypotheses have been established:

Hypothesis 1: Students have encountered the concept of phishing in the past, they know the goals of the attacker.

Hypothesis 2: Due to the increased level of electronic communication and the increased risk of phishing attacks, schools, public and commercial organizations provided additional training to employees on ways to prevent phishing attacks.

The questionnaire method was chosen. The questionnaire was anonymous, students' answers were not evaluated, the time to complete the questionnaire was not limited. The questionnaire was filled in at the class (with the exception of one student), so students did not have the opportunity to search for data additionally during the completion of the questionnaire.

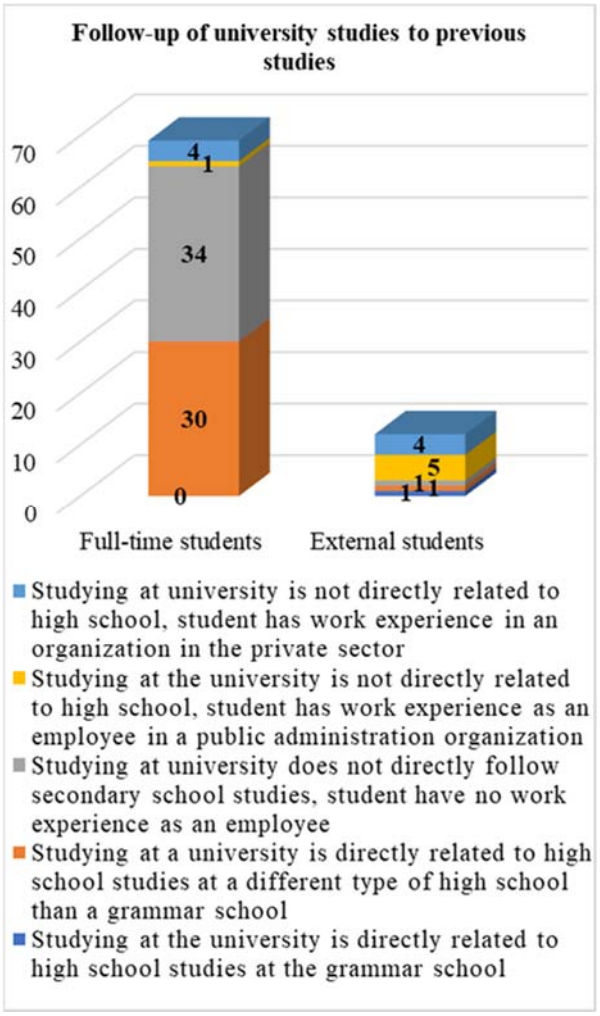

Fig. 1 Composition of the group of respondents

4. RESULTS

Although the sample, especially of external students, is too small to confirm or refute the hypothesis that computer and cyber security, its various aspects are becoming part of users' computer literacy, the fact that users are aware of cyber security risks at an ever younger age, at lower levels of schools can be assessed positively.

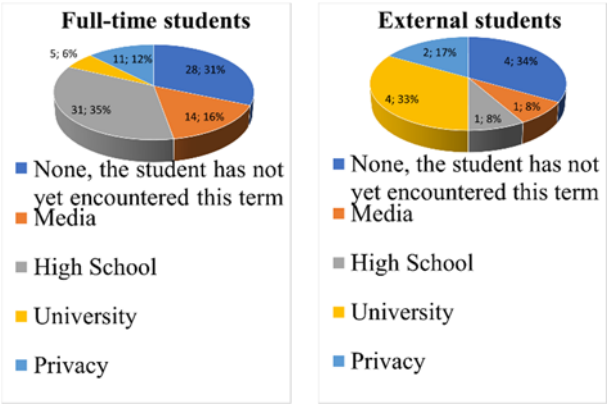

Fig. 2 The place where students first meet the term phishing

The question of focusing on knowledge of the targets of phishing attacks was asked to students as an open question.

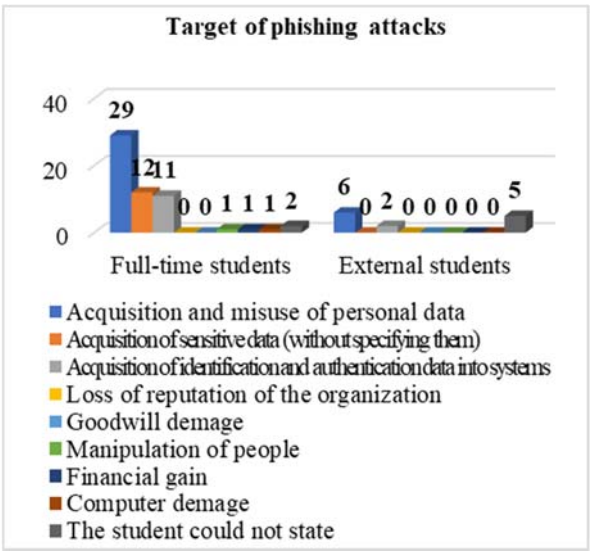

Fig. 3 Target of a phishing attack

Full-time students identified six areas of phishing targets, external students identified two areas. Neither full-time nor external students identified that the goal of the phishing attack could be to lose the organization's reputation. This is especially surprising for students who are already involved in the work process, are employees in the public or commercial sphere.

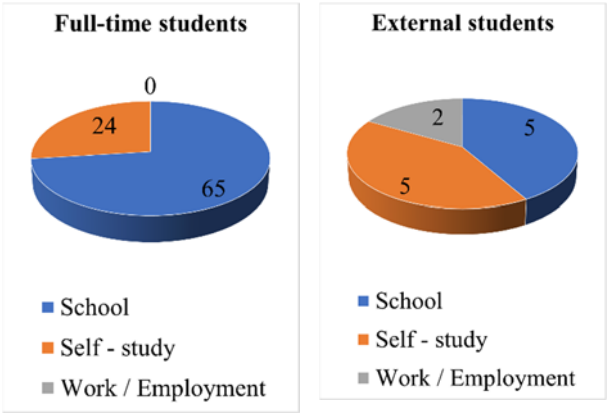

Fig. 4 The main source of information about phishing

For full-time students, school is the main source of information about phishing. Surprisingly, school is the dominant source of information also for external students. In both groups of students, self-study is an important source of information. This points to the danger and frequency of this type of attack, students consider this type of threat to be a real threat, their proactive approach can detect such an attack and prevent them from becoming a victim. Employment is an important source of information for external students - up to 17 percent cite work as the main source of information about phishing

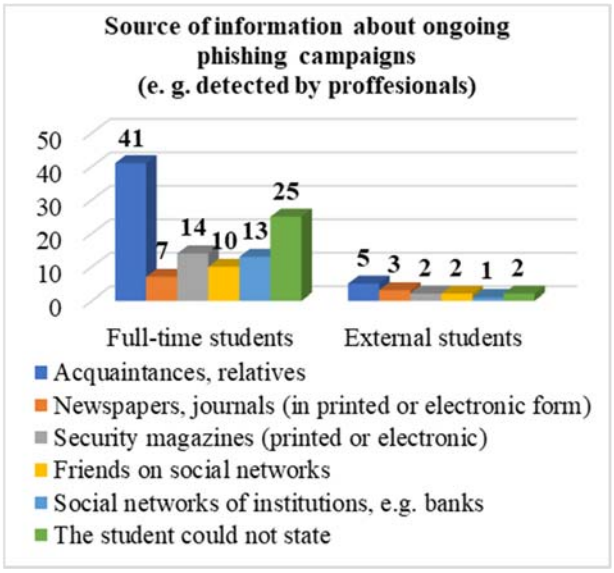

Fig. 5 Source of information about ongoing phishing campaigns

Up to 46 % of full-time and 42 external students do not actively seek information about ongoing phishing campaigns. Among the sources of information about ongoing phishing campaigns, there are several sources that are not significantly dominant. According to the results of answers to another question, approximately 80% of respondents (79 % daily and 83 % external) are aware that the Police of the Slovak Republic publishes information on fraud and phishing campaigns on their social networking sites.

Approximately 73 % of full-time students and 92 % of external students communicate with the bank electronically. Almost a third (30%) and even 50% of external students do not know that banks publish information on their websites aimed at increasing the security of their electronic services, including procedures that reduce the likelihood of a client falling victim to a phishing attack..

Surprisingly, although more than half of students are actively seeking information on ongoing phishing campaigns, as many as 52 % of full-time and 50% of external students have not seen an increased incidence of campaigns during the COVID-19 crisis. Only about 8 % of students (7.87 full-time and 8.33 external students) are actively looking for additional information. In the survey, any of the external students did not record the active approach of the organization (employer), supplementing the information of the employer's employees.

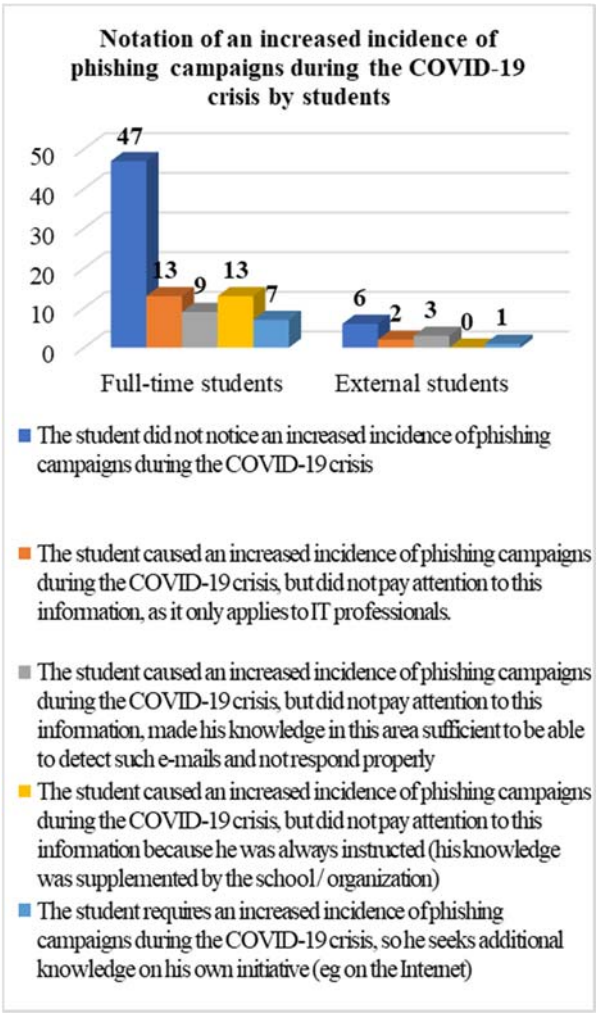

Fig. 6 Notation of an increaseincidence of phishing campaignsduring the COVID-19 crisis by students

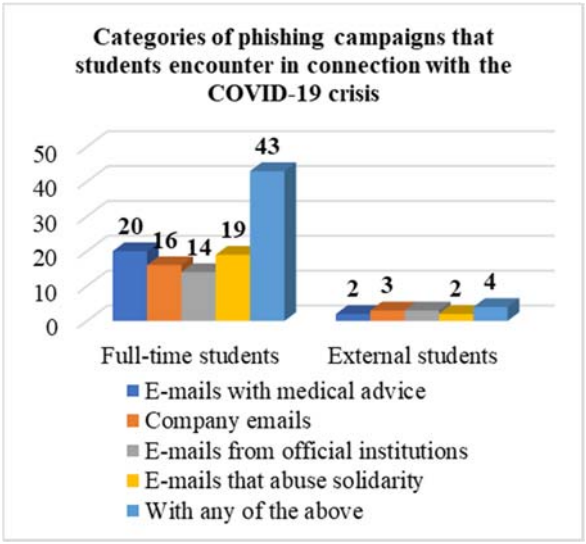

Fig. 7 Categories of phishing campaigns that students encounter in connection with the COVID-19 crisis

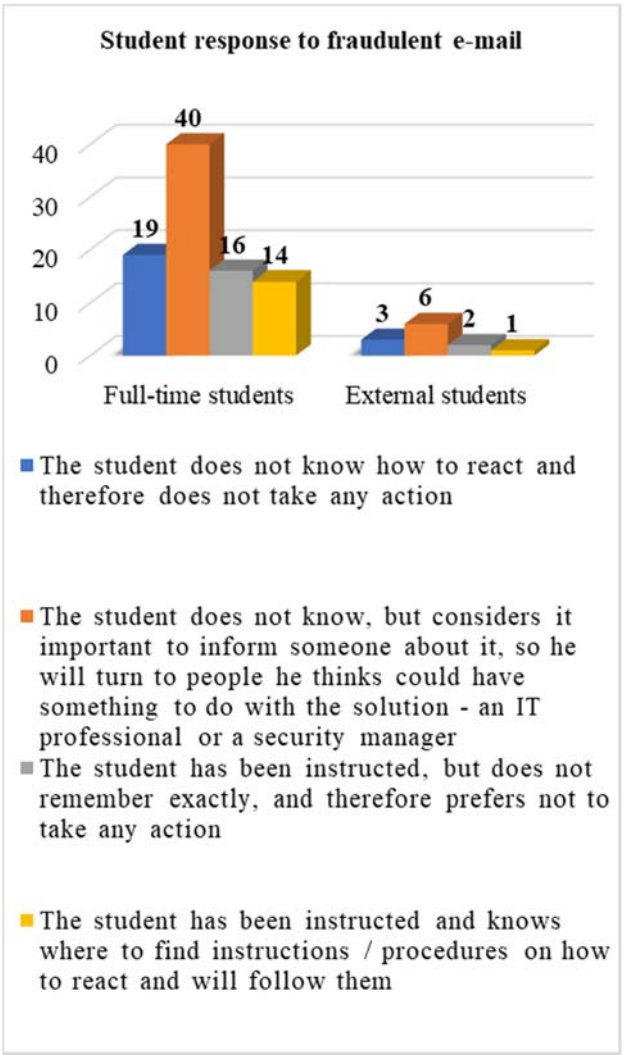

Fig. 8 Student response to fraudulent e-mail

Those who encountered fraudulent e-mails during the COVID-19 crisis which take advantage of this crisis encounter approximately the same extent with e-mails with health councils, with corporate e-mails, with e-mails from official institutions. In the survey, students also answered the question of whether they would know how to react if they identify an e-mail as fraudulent. 21.35 % of full-time and 25 % of external students do not know how to react and therefore do not take any action. Although 17.98 % of full-time and 16.67 % of external students were instructed on what steps to take after identifying a fraudulent e-mail, since they do not remember them exactly, they prefer not to do anything. Thus, about two-fifths of students would remain passive and did not contribute by taking an active approach to stopping the phishing attack. Three-fifths of students are proactively active - either mastering the steps needed to minimize the success of the attack, or at least have knowledge of who needs to be informed.

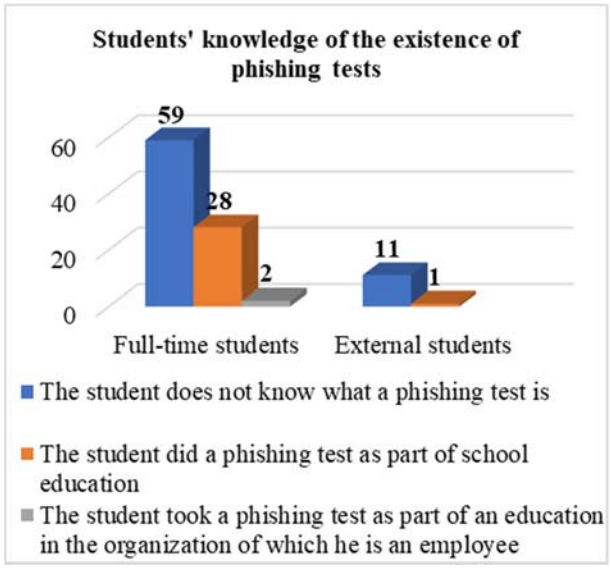

Fig. 9 Students' knowledge of the existence of phishing tests

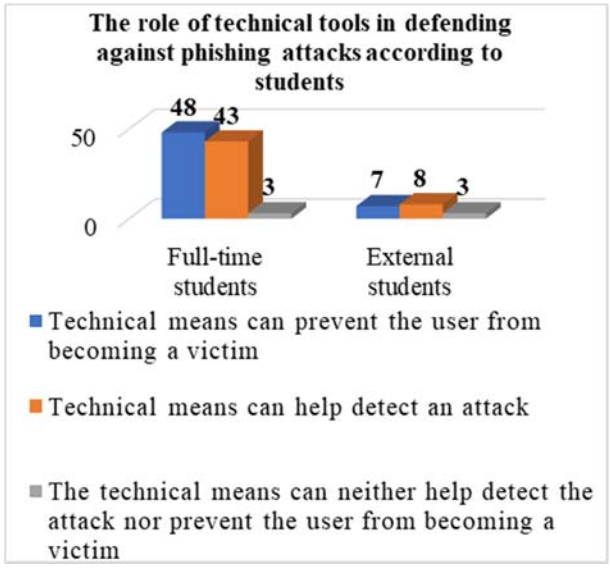

Fig. 10 The role of technical tools in defending against phishing attacks according to students

As many as 66.29 % of full-time students and even as many as 91.67 % of external students do not know what a phishing test is. A significant part of full-time students - 31.46 % encountered phishing tests during high school. The results show that training of employees in organizations includes training in the field of protection of employees against fraudulent e-mails only to a very small extent.

External students believe that technical means can prevent the user from becoming a victim. More than 40% of respondents believe that technical means can help detect an attack. Only 3.19 full-time students and 16.67 external students do not trust technical means.

The last two questions have shown the importance of including the topic of phishing in the subject aimed at acquiring basic knowledge in the field of informatics.

5. CONCLUSIONS

Hypothesis 1, that students have encountered the concept of phishing in the past, know the goals of the attacker, was only partially confirmed. Surprisingly, despite the current threat posed by the media, not all students are familiar with the concept of phishing.

Hypothesis 2, that due to the increased level of electronic communication and the increased risk of phishing attacks, schools, public and commercial organizations provided additional training to employees on ways to prevent phishing attacks, was not confirmed. According to the authors, the main reason was the time stress, the lack of experts in the field of cyber security, perhaps the underestimation of the possible effects of a successful phishing attack.

The role of the human factor in processes that reduce the likelihood of an individual or organization becoming a victim of phishing needs to be emphasized. These processes must involve not only IT specialists and security experts, but also all employees who use information and communication technologies. Due to its danger, the widespread possible consequences and damage, cyber security should become part of lifelong learning, whether non-formal self-study or formal education in schools and organizations. Phishing tests are one way to learn in this area.

REFERENCES

[1] LEVICKÝ, D.: „Základy kybernetickej bezpečnosti". Košice: elfa, 2020. ISBN 978-80-8086-280-0.

[2] Verizon, „2020 Data Breach Investigations Report," 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf. [Cit. 27 November 2020].

[3] ROSENTHAL, M.: "Must-Know Phishing Statistics: Updated 2020," 25 August 2020. [Online]. Available: https://www.tessian.com/blog/phishing-statistics-2020/. [Cit. 27 November 2020].

[4] ALEROUDA, A. – ZHOU, L.: "Phishing environments, techniques, and countermeasures: A survey", *Computers & Security,* vyd.68, pp. 160-196, July 2017.

[5] ALABDAN, R.: "Phishing attacks: Types, Vectors and Technical Approaches", Future Internet, Vol. 12, Assue 10 Available: https://www.mdpi.com/1999-5903/12/10/168 [Cit. 20 December 2020].

[6] VIJAYALAKSHMI, M. – MERCY SHALINIE, S. – MING HOUR, Y. – RAJA MEENAKSHI, U.: "Web phishing detection techniques: a survey on the state-of-the-art, taxonomy and future directions", IET Networks, 2020, 9, (5), p. 235-246, DOI: 10.1049/iet-net.2020.0078, IET Digital Library, Available: https://digital-library.theiet.org/content/journals/10.1049/iet-net.2020.0078 [Cit. 20 December 2020].

[7] Report – August 2020 Cybercrime: COVID-19 Impact, August 2020. [Online]. Available: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. [Cit. 25 November 2020].

[8] Mesačná správa CSIRT.sk Marec 2020, [Online]. Available: https://www.csirt.gov.sk/doc/MS2020-03verejnost.pdf. [Cit. 27 November 2020].

[9] INTERPOL: Cybercriminals targeting critical healthcare institutions with ransomware, [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware. [Cit. 27 November 2020].

[10] INTERPOL: INTERPOL report shows alarming rate of cyberattacks during COVID-19, 04 August 2020. [Online]. Available: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. [Cit. 27 November 2020].

[11] MADEJA, M. – PORUBÄN, J. – PEJOVIC, V. – GJORESKI, M.: "Observation of students behavior in programming courses with automated testing platform at differently geolocated universities: a case study". Acta Electrotechnica et Informatica, Vol. 20, No. 3, 2020.

Received December 12, 2020, accepted May 26, 2021

BIOGRAPHIES

Jana Handriková was graduated at the department of Computers and Informatics of the Faculty of Electrical Engineering and Informatics at Technical University in Košice. She worked as a university pedagogue, later as a programmer and information systems administrator. She completed her doctoral studies at the Armed Forces Academy of General Milan Rastislav Štefánik in Liptovský Mikuláš, field of study Military Communication and Information Systems. She currently works at the Department of Technical Sciences and Informatics of the University of Žilina.

Darina Stachová is a graduate of the Faculty of Natural Sciences of Comenius University in Bratislava, Department of Teaching Mathematics - Descriptive Geometry. Rigorous exam and obtaining the title of RNDr. performed at the Faculty of Mathematics and Physics, Comenius University in the subject of the theory of teaching mathematics. She completed her doctoral studies at UKF in Nitra and obtained a PhD degree in Theory of Teaching Mathematics. He currently works as an assistant professor at the Department of Technical Sciences and Informatics, FBI UNIZA. In his professional-scientific activity, he deals with mathematical modeling of some effects of vehicles on traffic structures and with the study of didactic problems in mathematics and geometry.