ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Vulnerability of Students of Masaryk University to Two Different Types of Phishing

Klara Dubovecka | Department of Political Science, Faculty of Social Studies, Masaryk University, Czech Republic | ORCID: 0009-0003-9679-5767

Abstract

According to the European Union Agency for Cybersecurity's (ENISA) Threat Landscape (ETL) report 2020, phishing is the most commonly used type of cyberattack. Phishing is the technique of delivering false communications that appear to be from a real and respectable source, typically via e-mail or text message. The attacker aims to steal money, obtain access to sensitive data, and login information, or install malware on the victim's device. Data from the same report shows that during the COVID-19 pandemic, phishing attacks increased by 667% in one month. Simultaneously, warnings about expected waves of phishing e-mails at Masaryk University in Czechia were encountered more often. However, at the time this article was written, there was *de facto* no anti-phishing research dealing with the problem of phishing attacks on Czech universities. The present article focuses on unintentional human error on the side of students of Masaryk University. The main aim of this article is to uncover the profile of the user who is most prone to victimisation of phishing in the university setting. These results were achieved by performing two real-life phishing simulations. Data suggests that female students are more prone to crash for targeted e-mails. At the same time, all students are more susceptible to spear-phishing attacks than to the generic ones. Findings are explained by analysing the empirical results of the two real-life phishing attacks conducted.

Received: 4.11.2023

Accepted: 20.06.2024

Published: 24.07.2024

Cite this article as:
K. Dubovecka "Vulnerability of students of Masaryk University to two different types of phishing," ACIG, vol. 4, no. 2, 2024, DOI: 10.60097/ACIG/190268.

Corresponding author:
Klara Dubovecka, Department of Political Science, Faculty of Social Studies, Masaryk University, Czech Republic; E-mail: dubovecka.klara@gmail.com;
0009-0003-9679-5767

Keywords
phishing, university students, social engineering, the human factor, unintentional threat

1. Introduction

We live in the information age, where connected devices and end-users increase daily [1]. The number has significantly risen with the COVID-19 pandemic because of home offices, online education, and entertainment via platforms during leisure time [2]. However, cybersecurity education rarely preceded this shift, which exposed a big group of end-users to cyberattacks daily. Different devices and technologies are used in people's personal lives, the companies they work for, the universities they study at, and the political institutions that govern them. Nevertheless, institutions cannot solely rely on a technological aspect of cybersecurity because of its interdependence. The importance of the human factor is still present, and the threat is growing simultaneously with the number of institutions that undergo speeded digital transformation, which is more than ordinary during these strange times of the COVID-19 pandemic. Institutions try to maintain the quality of virtual communication and, simultaneously, assure security in cyberspace while the shift has increased remote activities on the Internet. Human error continues to be the weakest link of cybersecurity – intentionally or unintentionally [3]. This vulnerability creates many opportunities for cybercriminals to attack human perception, rather than security measures through social engineering. Social engineering techniques trick individuals or organisations into accomplishing actions that benefit attackers or provide them with sensitive data [4]. The 2021 Data Breach Investigations Report (DBIR) states that social engineering has been responsible for 37% of all breaches in 2021 [5].

Notably successful were phishing attacks. A phishing attack is a cyberattack that exploits human vulnerability by disguising oneself as a trustworthy entity to influence or gain private information by sending an e-mail [6]. According to social engineers, 90% of all sent e-mails (294 billion each day) are spam and viruses, which means that e-mail is a significant vulnerability. The Anti-Phishing Working Group reported that phishing attacks hit an all-time high in December 2021 (316,747 attacks per month), meaning that phishing attacks have tripled since the early 2020 [7, p. 2]. Data from last year shows us that phishing aimed at the education sector is

increasing [5]. Universities are often a target, mainly because they store private and financial information and academic records of thousands of students and members of faculties. One disadvantage is their transient nature, which makes education about cybersecurity malpractices more complicated [8]. The vulnerability posed by phishing is often used effectively to the largest extent. Therefore, universities have a significant interest in protecting themselves from malicious cyberattacks. At a time when phishing is still in the limelight and the success rate of attacks on universities is increasing, there is virtually no research in the academic environment of the Czech Republic that focuses on the vulnerability of students and their ability to guess whether an email is legitimate or fraudulent.

This article focuses on unintentional human error and its threat to institutional cybersecurity by conducting real-life phishing simulations. The research goal of this experiment is to assess the profile of a student who is most susceptible to phishing and to provide the foundation for understanding how vulnerable students of the Faculty of Social Studies (FSS) at Masaryk University are. Phishing vulnerability is compared in two categories of e-mails – one generic and another targeted (spear-phishing). The research is limited to the Faculty of Social Studies at Masaryk University in Brno due to limited resources for this research. At the same time, this research provides a basis for similar research on a larger scale in the future.

The remainder of this article is organised as follows. Section 2 provides a literature review summarizing previous studies; Section 3 describes the methodology employed; Section 4 presents the results and analysis of data; and the final section discusses the implications of the findings.

2. Literature Review

The first phishing e-mail was sent in 1990 [9]. Fast forward 20 years, and it is the most commonly used tool for compromising an institution [10]. Many information security scholars have found phishing in a university community a research area of interest. Although studies have been performed before also, the most significant momentum has occurred in the past decade. Researchers have begun exploring what could be the user profile of a person most likely to react to phishing. Because of this, studies to capture demographics connected to phishing susceptibility have been administered in different universities worldwide. In the following section, related studies are discussed.

2.1. Phishing in General

Jerry Felix and Chris Hauck first outlined phishing as a strategy in which a third party imitates a genuine source to undertake a malicious operation at an Interex Conference in 1987. However, there does not appear to be a definite understanding of phishing techniques. Phishing has its own set of terminology that appears regularly in the literature. Mass, spam, and blanket phishing are examples of such words. They all have characteristics in common, such as many messages sent, misleading targeted individuals, impersonation of a sender, and data collection via social engineering [11–13].

Studies on phishing attacks' occurrence and success rate are conducted regularly. Overall, they all show an increasing tendency of phishing attacks [5, 7, 11, 14].

Previous studies have suggested that users are more prone to phishing if they are solicited by known entities in more targeted e-mails [14–17].

2.2. Phishing Susceptibility and Demography

Studies have been conducted to measure the relationship between demographic factors and phishing susceptibilities [14, 17–19] and to identify factors that predict phishing susceptibility [20].

Younger students presented themselves as more vulnerable in Jagatic et al.'s study, in which females became victims in 77% of cases, while males' proportion was 65% [14]. This study was performed on 487 selected students from Indiana University aged 18–24 years. On the other hand, this study was unique because it used personal information acquired from social media to send phishing messages to a target pretending to be a known friend.

Sheng et al. performed a role-play survey shared with 1001 respondents (only 29% of them were students) to learn more about the relationship between demographics and phishing susceptibility. Their results showed that females were more prone to phishing than males [18]. This is because females had less technical training and technical knowledge than males. Another finding was that participants aged 18–25 years were more susceptible than other groups. The age category of 18–25 years corresponds to the approximate age of university students.

Researchers from Carnegie Mellon University explored different age groups in their empirical phishing experiment. The study was based on the sending of phishing e-mails to a group of 515 participants. Results showed that 62.3% of the users in the age group of 18–25 years fell prey to the phishing e-mail, while 41.1% of the users in the age group of 26 years or older were tricked similarly [21].

Hong et al. explored the behavioural, cognitive, and perceptual attributes that make individuals more vulnerable to phishing. Of 53 respondents, over 92% were somewhat defenceless towards phishing [22]. In this experiment, it was revealed that females were less likely to uncover phishing e-mails.

Diaz et al.'s study conducted in 2019, where phishing e-mails were sent to 450 uninformed students at the University of Maryland, resulted in 60% of participants clicking on the phished e-mail; however, the study discovered no significant correlation between gender and susceptibility [19].

In Broadhurst et al.'s quasi-experimental study, 138 students were exposed to fake e-mails to connect demographic factors to phishing susceptibility. However, no correlation was found. All the variables indicated that international and first-year students were deceived more significantly than domestic and later-year students [17].

Many studies have been conducted over the past few years, mostly based on role-play investigations. This setup allows researchers to assess the effectiveness of phishing attacks without undertaking real-world phishing tests. Users respond to questions using role-playing to examine a possible security situation. The preliminary findings are analysed and summarised to identify potential phishing victims [14, 18].

A controlled phishing experiment was also used, in which individuals were sent an actual phishing e-mail that directed them to a phishing website. The phishing website does not capture or keep any personal data. On the other hand, this website keeps track of the number of victims and perhaps their usernames. The information gathered can be used to measure user security awareness and, in the future, to improve security training [15, 19, 21, 23].

Although all previous studies focused on demography and susceptibility, they used different methods to find out results. None of the above studies explicitly focused on the gender of students and

susceptibility to phishing by using phishing simulation. The current study uses the latter technique and concentrates on finding whether females or males in a university setting are more prone to opening a phishing e-mail, and which type of e-mail is opened more often by sending a decoy e-mail to registered participants to help understand the current vulnerability of students of social studies.

3. Methods

In this section, details of the methodology of this research are presented.

3.1. Structural Overview

The aim is to create conditions similar to a real-life environment while maintaining secure surroundings for collaboration, privacy, and dignity in research. We opted for a phishing simulation campaign in which realistic decoy e-mails were sent to students. At the same time, Google Analytics and SalesHandy helped us gather accurate data on the dangers of phishing on social studies faculty – two phishing e-mails were used – one generic, although adjusted to the current situation, and another targeted (spear). The first phase comprised obtaining a list of target identities to experiment on; and the second phase comprised preparing a technical background for an experiment. This was followed by sending decoy phishing e-mails and gathering data.

3.2. Data Collection

The first step was to assemble participants. Participants were not chosen randomly, as mentioned in the literature, but voluntarily through a registration form. The registration form consisted of questions on demographic information (age, gender, studies, year of studies, and language of their studies) and an informed consent. With this, participants had the chance to learn the purpose, benefits, and risks before deciding or declining to participate in the study. Crucial to the experiment was soliciting university e-mail, which was later used as an entrance to complete research. Students were approached in November 2021 through the social network Facebook and Discord; they were able to register until the end of the year. Responses were collected through Enalyzer, a data-gathering and processing platform. Initially, 101 students registered. The number reduced to 68 due to incomplete data in some cases. After collection of all data, participants were assigned numbers to anonymise their identity and keep an overview

of the results. The Faculty of Social Studies at Masaryk University had 2804 students. With standard statistical technique [24], it was determined that a sample size of 68 students was applicable for a confidence level of 95% and with ±11.33% margin of error. For characteristics of the whole tested group, see Table 1.

3.3. Phishing Web Creation

The following step was to prepare a technological background to capture all feedback. To execute practical experiments, a functional website was needed, ideally similar to a faculty website that somehow counts the activity. For that purpose, the decision was to use the framework Django, a tool developed in the programming language Python. Because the only functionality requested of

Table 1. Characteristics of Sample.

Characteristic	Participants (N = 68)
Gender	
Male	44%
Female	54%
Others	1.5%
Age (years)	
<21	31
21–25	60
26–31	6
>31	3
Studies	
Environmental Studies	1.5
International Relations	40
Media Studies	7
Political Science	9
Psychology	7
Social Policy and Social Work	7
Sociology	7
Language	
Czech	90
English	10

the website was to appear legitimately and measure visits, a default Django project was created.

The consequent step was obtaining the visual side – which was achieved by using a web browser tool to view the HTML source code of the MUNI newsletter. This source code was copied, slightly adjusted, and set as a visual for the homepage of the Django project. We created one more page to count the hits of a targeted e-mail. The appearance of this page was not significant, so it contained just some simple HTML structures with the statement announcing that the visitor has been phished, it was a part of the experiment, and two useful links to relevant sources: one for the NÚKIB[1] website, and another for MUNI security.

1———NÚKIB is National Cyber and Information Security Agency in Czech Republic.

For the last requirement, counting visitors, Django extension called Django-hit count was used. This extension counts webpage hits by analysing the requests sent – website traffic. Later on, it was found that it did not work as needed, so this option was abandoned, and it was decided to look for other options.

The Google Analytics tool was used for the purpose of this experiment. A Google token was generated to make it operative, and HTML to the page's source code was added. Besides counting the visitors, Google Analytics provided us with much additional helpful information about them, such as operating system, whether participants used mobile or desktop access, and the browser.

The Django project was then ready to be deployed online. Heroku hosting was used for that purpose because it provided simple free hosting for projects written in Django. Heroku also allowed the use of custom domain names, which were essential for the success of this experiment. Because it allowed adjusting the domain, it looked more similar to the MUNI domain (*muni.cz*).

The domain name we chose for the experiment was muninewsletter.cz, for two simple reasons: it looks identical to MUNI, and it enabled the use of social engineering. The information was obtained to make it look like a credible institution. After doing market research online to find the best offer for this domain, we opted to go with godaddy.com. It simultaneously created an e-mail for this domain suited for the usage. After purchasing the domain name, the only thing remaining was to set it to redirect to Heroku. That was achieved by setting nameservers at godaddy.com to redirect to Heroku nameservers, which then directed the user to our project.

3.4. E-mail Setup

Creating a functionalised e-mail to store all responses was the next step when the website was set up and started working. For this purpose, a tool called SalesHandy was used. The e-mail address was chosen to be as similar as possible to the original. The e-mail address from which the university sends newsletter e-mails is studenti@newsletter.muni.cz. The e-mail address used for this experiment was studenti@newslettermuni.cz. The difference was in one dot. This method is called link manipulation; it is a technical disguise. The link is slightly altered to make the user believe it more and then redirects to the phisher's website.

After SalesHandy was connected to the e-mail address studenti@newslettermuni.cz, it enabled sending e-mails with tracking and planning the e-mail campaign. The most significant features of this tool were showing who opened, replied, and clicked on the link in the sent e-mail. This facilitated recording participants' behaviour after the decoy e-mail was sent.

3.5. Phishing E-mail Design

Phishing e-mails were inspired by the phishing archive of Berkeley University of California [25] to copy the usual visualities that real phishing e-mails in the university environment have. Social engineers use different techniques intending to be successful. Phishers are getting more sophisticated; phishing attacks incorporate greater details and context to become more effective and, therefore, more perilous for society [14]. Thus, both e-mails were written in the Czech language, because most registered respondents studied the Czech programme, and the main goal was to make it look real.

Because of that, with the first e-mail, we tried to be as precise as possible. For the first e-mail, the generic one, the decision was to copy the student's newsletter.

We used e-mail spoofing, where information from a section of the e-mail was falsified, making it appear as if it was coming from a legitimate source – Masaryk University. The second approach is website cloning; with this technique, we copied a legitimate website and an e-mail of the student newsletter and tried to deceive students into clicking on the link. These fake sites usually trick individuals into entering personally identifiable information (PII) or login credentials or attacking directly. For a higher click rate, the current situation was used. Specifically, students were presented

with an e-mail in which they could find more information on how Masaryk University is helping with the conflict in Ukraine. This topic was chosen because it is presently happening and attacks human emotions, which is one of the preconditions for successful phishing [9]. After clicking on the link, participants were redirected to the website, which looked like the webpage of Masaryk University but had spelling mistakes. This created space for conscious individuals to report this situation to MUNI IT team. The purpose of the second e-mail was to be more personal; hence, copying of an e-mail which announces the receiving of a document in the information system of Masaryk University. This e-mail was sent with spelling errors, and the link, http://www.newslettermuni.cz/outside/, did not match the e-mail's subject.

3.6. The Realisation of Experiments

Tryouts were executed before completing the first experiments to ensure that sent e-mails would not be delivered to spam.

The first e-mail was sent out on 2 March 2022. Two days later, the second e-mail type was sent on 4 March 2022. Two-month delay after collecting primary data was due to the waiting period, which was supposed to gain time to prepare the experiment's technical background and ensure that participants would not have a fresh memory of signing up for the experiment. E-mails were sent during the campaign, which ensured the delivery of e-mails at approximately the same time. Two days after the last e-mail was sent, the data was downloaded and converted to the .xlxs format for further analysis.

4. Results

Susceptibility is not homogenous among internet users; many factors influence individuals' decision-making and online behaviour. The present study seeks to determine the profile of a student most vulnerable to phishing and, based on results from previous research, confirm whether male or female students of FSS MUNI SCI are more susceptible to be victimised by phishing e-mails [14, 17–19]. The following text presents general observations of this study, followed by a comparison of the results from phishing susceptibility to two types of e-mails. In this research, falling for phishing is defined as clicking on the link in the e-mail, according to the research which was published in 2021 [26]. The distinction is made between not opening an e-mail, opening an e-mail and clicking on the link in the e-mail. The phishing campaign and collection of the responses lasted the first forty-eight hours after delivering the e-mail.

4.1. General Observations

Altogether, 136 e-mails were sent. Participants were most susceptible to thespear-phishing e-mail, which announced the delivery of a document to the IS of MUNI. This e-mail was tailored for the students of Masaryk University because it informs the recipient from the second-person point of view. Of all participants, 74% opened this e-mail, and 96% of those who opened it also clicked on the link. This was noticeably different in the case of the first e-mail, which was opened by 34% of respondents, and on the link clicked by 52% of those who had opened the e-mail. Overall, there appeared to be an increasing trend concerning scam and scam susceptibility in normalised proportions, with increasing success for more individualised and tailored scam rather than the generic one.

4.2. The First E-mail

The first e-mail was not opened by 66% of respondents. 34% of participants opened the e-mail, and 52% also clicked on the link contained in the e-mail. This e-mail aimed to be general but slightly adjusted for the attention of university students, so the e-mail domain fits the perspective. Regarding the male–female ratio, of 45 people who did not open the e-mail, 18 were males, 26 were females and one other. While this first e-mail was mainly ignored by females, the ratio was equivalent when opening the e-mail. Of 23 people who opened the e-mail, 12 were males and 11 were females. More females clicked on the link, but the difference was minimal; the male–female ratio was 5:7. This thesis focuses on 'male's and 'female's susceptibility to phishing; however, participants marked other demographic information in the registration form.For the whole list of characteristics, see Table 2. Data that were insignificant due to the low number of responses captured are excluded from the table. The success rate of this first e-mail was 18%.

4.3. The Second E-mail

The second e-mail brought different results. Only 18 participants did not open the e-mail, while 50 users opened it. From that, 48 people clicked on the link in the e-mail, making for a 96% clicking rate. In the case of the second e-mail, two persons alerted the CSIRT[2] MUNI team. Of 18 people who did not open the e-mail, 7 were males, and 11 were females. The e-mail was opened by 19 male respondents, 30 female respondents and one other. Further, 17 male and 30 female respondents clicked on the link, showing higher susceptibility to phishing in females. The sample of

2——CSIRT stands for Computer Security Incident Response Team, and it handles security incidents on computer networks. This type of group is usually associated with a specific region or organisation; in this case, the Masaryk University.

Table 2. Characteristics of the First E-mail.

Characteristics	Didn't open the e-mail (N = 45)	Opened the e-mail (N = 23)	Clicked on the link (N = 12)
Males	18	12	5
Females	26	11	7
Others	1	0	0
International Relations	18	9	4
Psychology	11	8	5
Political Science	6	1	0
>21 years	14	7	2
21–25 years	26	15	10
2nd	12	3	1
3rd	12	7	5
4th	11	5	4

respondents consists of a more significant proportion of females than males, and the reason for this is that it reflects more female students at the FSS; the male–female ratio was 30:37. The success rate of the second e-mail was 71%.

After clicking on the link, participants were directed to the page announcing that they were phished and linked to useful links to learn more about phishing attacks from the NÚKIB or MUNI security team.

The last e-mail of this type was sent on 4 March 2022 at 22:15. Approximately 24 h later, on 5 March 2022, respondents numbered 16 and 54 started a debate on the suspicious e-mail on the FSS virtual campus on discord. Participants discussed whether it was part of a training or a real security threat. After exchange of short messages, they concluded that the best would be to report it to the CSIRT MUNI. And so they did; both participants communicated this information to the relevant team, who told them that this was part of a research for thesis. For further data concerning the second e-mail, see Table 3.

4.4. Comparison

From the results listed above, it is clear that the second targeted e-mail was more successful; however, what was the difference? We examined the effect of gender on participants to

Table 3. Characteristics of the Second E-mail.

Characteristics	Didn't open the e-mail (N = 18)	Opened the e-mail (N = 50)	Clicked on the link (N = 48)
Males	7	19	17
Females	11	30	30
Others	0	1	1
International Relations	8	19	18
Psychology	4	15	14
Political Science	2	5	5
<21 years	6	16	14
21–25 years	9	32	32
1st	4	10	9
2nd	4	11	10
3rd	4	15	15
4th	6	10	10

see whether gender differences exist in responding to phishing susceptibility.

In the case of the first e-mail, the opening of an e-mail was comparable between genders. The results showed that 12 males and 11 females opened it.

Numbers almost doubled when it came to the targeted e-mail. The second e-mail was opened more times by females, even though the number of participants in both groups was roughly the same (30 males and 37 females were registered for this study).

It was found that the first type of phishing attack equally deceived female and male subjects. However, in the second type of phishing, almost 63% were female compared to 36% male victims, which was in accordance with the study of Jagatic et al. [14] and Sheng et al. [18], where the authors found that females were more susceptible to the spear-phishing risk.

A low percentage of subjects clicking on the link (18%) suggests that the more targeted the e-mail, the more significant the threat. From the second e-mail, it was clear that males were less susceptible to falling prey to phishing attacks than females. The results also indicated that females were more likely to click on phishing links.

4.5. Google Analytics – Profile of the User

Google Analytics provides additional information about the operating system and the browser through which users accessed the phishing site. This information helped to more accurately define the user profile of those who were victimised by phishing in this research and provided a framework for developing a new hypothesis in future research related to the factors that make users vulnerable to phishing attacks.

Because the first e-mail demonstrated a success rate of 18% for susceptibility to phishing, to create a profile of a student of FSS susceptible to phishing, the data obtained by the second decoy e-mail was used.

Females clicked on the link in the e-mail with a ratio of 30:17, thus making them user's first attribute. The highest click rate was in the age category of 21–25 years. However, this may be negligible due to the disproportion of the sample in this category. Across different university year groups, the sample was divided comparably. Students reached the highest susceptibility in the third year. From the perspective of studies, the highest number occurred for students of International Relations, followed by students of Psychology. Provided by Google Analytics, most users used Windows as their operating system and entered the web page from their desktop, specifically from the Google Chrome browser. Table 4 summarises all the factors connected with susceptibility to phishing attacks in the present research.

5. Discussion

According to the literature review, the specificity of scams may influence phishing attack susceptibility; that is, people are more likely to be deceived by scams tailored to their specific circumstances

Table 4. Profile of a Highly Susceptible User.

	Highly susceptible
Age (years)	21–25
Gender	Females
Education	International relation
Year of studies	3rd
Operating system	Windows
Desktop/mobile	Desktop
Browser	Google chrome

than scams with generic content. We used two scam types – generic and spear-phishing – to check whether respondents were more vulnerable to spear-phishing attempts than generic ones. This logic was confirmed. More than twice as many people opened the more targeted e-mail; 23 participants opened the generic e-mail, while the targeted phishing e-mail was opened by 50.

In the present study, the success rate was 18% for the first e-mail and 71% for the second e-mail, which is considerably closer to the type of phishing where e-mails were constructed based on gathered information.

The high success rate in the second e-mail indicates that students are more susceptible to targeted phishing than the generic one. This number is alarming but not unusual among university students. The success rate was comparable to the results of a study done by Jagatic et al. [14], which had a success rate of 72%. However, this high number opens a space for discussing basic cybersecurity knowledge among university students because they represent a highly vulnerable group.

Results suggest that the more susceptible gender to targeted phishing e-mails is females because the clicking rate in their case was 81%, while 63% males clicked on the link in the second phishing e-mail.

A real-life fraud experiment on human subjects was witnessed in this study, with highly valuable ethical implications. How can one learn about students' sensitivity to phishing without them knowing but keeping it in a natural setting? In this experiment, this was solved through a signed registration form. However, this ethical issue was at the expense of a more significant number of participants and also the moment of surprise, even though we waited for 2 months for the preparation of experiment post-registration.

This article, however, had several limitations. The first was the insufficiency of the sample size for generalisation. The final number of respondents was 68, as many had to be excluded because of insufficient information. Hence, a limitation in presenting the pattern of findings and analysis. Because of the small sample size, the scope of analysis was also limited. Even though it was not significant in the case of this study, this could be an opportunity for future researchers in this area because, as stated before, the number of clicking on the links was alarming. Statistics were partly collected manually, creating space for human error because of accidental occurence of miscounting.

One of the aspects which helped this research was the usage of its own domain. This raised the overall level of legitimacy of e-mails. It also allowed to measure users' susceptibility to higher-level phishing attacks, requiring higher understanding and awareness to fail victims.

Future research could apply a more extensive phishing simulation to determine the variables influencing students' scam susceptibility. Understanding the factors that influence phishing susceptibility could help with customised cybersecurity education, thereby protecting against phishing and other forms of cybercrime.

6. Conclusions

In conclusion, this article presented the design and results of two phishing campaigns conducted among students of the Faculty of Social Studies at Masaryk University. Through a phishing campaign simulation using e-mails, the practical study enabled a deeper investigation of the phenomenon of phishing at universities, providing insight into the susceptibility of different genders. Based on the obtained click rate percentage, more cybersecurity education and awareness are required.

Results from phishing simulations indicate that students are prone to be victims of targeted phishing to a much greater extent than generic phishing e-mail, which does not compel action. Females opened and clicked on the phishing e-mails almost twice as often as males. According to the findings, phishing assaults are still one of the most severe threats to individuals and institutions. The phishing cycle is mainly driven by human interaction. Phishers frequently exploit human weakness, increasing the possibility of victimisation by phishing. Despite the limitations of this work, we consider it beneficial for a better understanding of the issues and future research. Exploring phishing threats and vulnerabilities in a university setting is especially crucial because everyone, employees and students alike, is accountable for handling the institution's data. As the sophistication of phishing attempts enhances, the likelihood of a university being targeted also increases. We can personalise focused prevention for such groups if we conduct a study and determine the most vulnerable groups.

Acknowledgements

At this point, the author would like to thank the people without whom the motivation and creation of this article would not have been possible: her parents, her siblings, Emma and Daniel,

and her long-time friends, Lucie and Samuel, who have always remained by her side.

References

[1] M. Roser, H. Ritchie, E. Ortiz-Ospina. (2021). *Internet: Our world* in *data*. [Online]. Available: https://ourworldindata.org/internet. [Accessed: Mar. 28, 2022].

[2] S. Venkatesha, K.R. Reddy, B.R. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *SN Computer Science*, vol. 2, no. 2, p. 78, 2021, doi: 10.1007/s42979-020-00443-1.

[3] IBM. (2014). *IBM security services 2014 cyber security intelligence index: Analysis of cyber attack and incident data from IBM's worldwide security operations*. [Online]. Available: https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF. [Accessed: Apr. 26, 2022].

[4] F. Salahdine, N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019, doi: 10.3390/fi11040089.

[5] G. Bassett, C.D. Hylender, P. Langlois, A. Pinto, S. Widup. (2021). *Data breach investigations report*, DBIR. [Online]. Available: https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf. [Accessed: Mar. 28, 2022].

[6] P.W. Singer, A. Friedman, *Cybersecurity and cyberwar: What everyone needs to know*. New York, NY: Oxford University Press, 2014.

[7] Anti-Phishing Working Group. (2022). *Phishing activity trends report: Unifying the global response to cybercrime 4th quarter 2021*. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf. [Accessed: Mar. 28, 2022].

[8] M. Wagner. (2006). *Who's phishing for your students?* ZDNet. [Online]. Available: https://www.zdnet.com/article/whos-phishing-for-your-students/. [Accessed: Mar. 28, 2022].

[9] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, Mar. 2021, doi: 10.3389/fcomp.2021.563060.

[10] J.L. Bailey, B.K. Jensen, R.B. Mitchell, "Analysis of student vulnerabilities to phishing," Learning from the past & charting the future of the discipline. Proceedings of the fourteenth Americas conference on information systems, AMCIS 2008, Toronto, ON, Canada, Aug. 14–17, 2008. [Online]. Available: https://www.researchgate.net/publication/220891604_Analysis_of_Student_Vulnerabilities_to_Phishing. [Accessed: Apr. 03, 2022].

[11] R. Heartfield, G. Loukas, D. Gan, "You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks," *IEEE Access*, vol. 4, pp. 6910–6928, 2016, doi: 10.1109/ACCESS.2016.2616285.

[12] J. Hong, "The state of phishing attacks," *Communications of the ACM*, vol. 55, no. 1, pp. 74–81, 2012, doi: 10.1145/2063176.2063197.

[13] E.E.H. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science*, vol. 3, no. 1, pp. 1–10, 2014, doi: 10.1186/s40163-014-0009-y.

[14] T.N. Jagatic, N.A. Johnson, M. Jakobsson, F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007, doi: 10.1145/1290958.1290968.

[15] R.C. Dodge, C. Carver, A.J. Ferguson, "Phishing for user security awareness," vol. 26, no. 1, pp. 73–80, 2007, doi: 10.1016/j.cose.2006.10.009.

[16] E.D. Frauenstein, "An investigation into students responses to various phishing emails and other phishing-related behaviours," 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers (Communications in Computer and Information Science Book 973). New York, NY: Springer, 2019, pp. 44–59, doi: 10.1007/978-3-030-11407-7_4.

[17] R. Broadhurst, K. Skinner, N. Sifniotis, B. Matamoros-Macias, "Cybercrime risks in a university student community," *SSRN Electronic Journal*, vol. 2a, no. 1a, pp. 5–10, 2020, doi: 10.2139/ssrn.3176319.

[18] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, J. Downs, "Who falls for phish?," Proceedings of the 28th International Conference on Human Factors in Computing Systems, Atlanta, GA: ACM Press, USA, 2010, pp. 373–382, doi: 10.1145/1753326.1753383.

[19] A. Diaz, A.T. Sherman, A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia*, vol. 44, no. 1, pp. 53–67, 2020, doi: 10.1080/01611194.2019.1623343.

[20] M.K.K. Tornblad, K.S. Jones, A.S. Namin, J. Choi, "Characteristics that predict phishing susceptibility: Areview," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 65, no. 1, pp. 938–942, 2021, doi: 10.1177/1071181321651330.

[21] P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 1–31, 2010, doi: 10.1145/1754393.1754396.

[22] K.W. Hong, C.M. Kelley, R. Tembe, E. Murphy-Hill, C.B. Mayhorn, "Keeping up with the Joneses," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 57, no. 1, pp. 1012–1016, 2013, doi: 10.1177/1541931213571226.

[23] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M.A. Blair, T. Pham, "School of phish," Proceedings of the 5th symposium on usable privacy and security (SOUPS ,09). New York, NY: ACM, 2009, doi: 10.1145/1572532.1572536.

[24] R.V. Krejcie, D.W. Morgan, "Determining sample size for research activities," *Educational and Psychological Measurement*, vol. 30, no. 3, pp. 607–610, 1970, doi: 10.1177/001316447003000308.

[25] Berkeley Information Security Office. (2023). *Phishing examples archive* [Online]. Available: https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive. [Accessed: Apr. 04, 2023].

[26] A. Jayatilaka, N.A. Gamagedara Arachchilage, M.A. Babar, "Falling for phishing: an empirical investigation into people's email response behaviors," Proceedings of the 42nd international conference on information systems (ICIS), 2021, Austin, TX. Atlanta, GA: Association for Information Systems, pp. 1–6, 2021, doi: 10.48550/arXiv.2108.04766.