The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2023

Volume 24, Pages 21-28

IConTech 2023: International Conference on Technology

Exploring Social Engineering Attacks Using Spear Phishing in a University

Trust Tshepo Mapoka
University of Botswana

Keneilwe Zuva
University of Botswana

Gaedupe Kylian Kukumara
University of Botswana

Tebogo Seipone
University of Botswana

Tranos Zuva
Vaal University of Technology

Abstract: A thorough investigation of social engineering attacks was performed on the lab environment. Numerous users can be easily attacked through the use of illegitimate emails that may come from trusted users. Organizations often try to implement security measures but they remain susceptible to these attacks. The purpose of this study was to show that university students are at risk of being attacked. The deployment of a dedicated lab environment and the susceptibility of the network to countless social engineering attacks were completely assessed in a controlled lab environment. The targeted audience, students, showed that they were more vulnerable. The findings of these investigations revealed that the network is vulnerable to social engineering attacks, specifically spear phishing attempts. Recommendations were made that included that universities should invest in educating students, staff members, and the faculty at large about certain threats and how to avoid falling prey to them.

Keywords: Cyber vigilant, Deployment, Spear phishing, Vulnerability

Introduction

The continuous use of the internet by the current generation, especially university students, has placed them at huge risk of being prone to social engineering attacks even if they are not aware (Hatfield, 2018). Social engineering is, in most cases, described as the art of convincing individuals to reveal sensitive information in order to perform certain malicious tasks. In most cases, it is often described with the theory of gaining something in exchange for a loss to someone (Helminem, 2021). The best security measures and practices do not guarantee that a certain organization is safeguarded against these attempts. The majority of students and staff members are mostly affected by Spear Phishing attempts. Spear Phishing is the attack on certain users under the pretense of a candid individual that is mostly trusted through the use of any electronic medium. This attack is directed to specific individuals. Vast information regarding users is first collected; for example, all emails about targeted users will be known. Spear phishing attempts are the most triumphant, as information about users has already been studied (Chilisa & Preece, 2005).

This paper is arranged as follows: Section 1 specifies the introduction; Section II unravels the problem statement; section III shows the main aim of this research paper; Section IV shows the related studies in the form of a literature review. Section V shows the methodological approaches, and Section VI outputs the results and findings of the study. The last section shows conclusions and future recommendations.

Problem Statement

Social engineering attacks have the potential to seriously jeopardize the confidentiality, integrity, and availability of most university's computing resources (Bongiovanni, 2019). Despite the potential harm that social engineering attacks can inflict, the various social engineering techniques and the efficacy of the current security measures in preventing or reducing them are not fully understood. In order to uncover potential flaws and provide practical solutions to protect against these threats, a systematic evaluation of some university network vulnerability to social engineering attacks is explored.

Aim of Study

- To identify potential weaknesses in the network's security controls.
- To explore effective countermeasures to protect against social engineering attacks.

Literature Review

The social engineering attacks on university computer networks are a growing concern, and their effects cannot be magnified. These attacks have been used to gain unauthorized access to delicate data and even compromise network security (Omoyiola, 2020). Human behavior plays a crucial role in this type of attack, as people can easily succumb to social engineering attacks due to their lack of awareness of this type of attack (Eltahir & Ahmed, 2023). It is the onus of Universities to educate students and staff members about the repercussions of these attacks and their impact at large. Firewalls and antivirus applications are ways that universities can try to mitigate against this type of attack; however, the human factor must not be neglected in addressing these cybersecurity breaches. According to the University of Botswana Computer Science important, as it outlines and provides backing for efforts aimed at improving information security practices across various units in the department (Annamalai et al.,2021). Access controls and monitoring systems are technology control measures that can Department, there is a great need to execute comprehensive training programs that may help raise awareness about cybersecurity complications (Harris, 2019).

Communication in an organization is salient as it helps employees understand how crucial information security is. Support from management is also be implemented before issues get out of hand (Alzahrani & Alfouzan, 2022). Cybercriminals use various tactics to gain unauthorized access to sensitive information in the University Of Botswana Computer science networks. The review conducted on this study shows that attackers often use baiting tactics such as leaving an infected USB around or sending malicious emails with links to targeted users. Pretexting and creating false identities may also be used to manipulate users into divulging certain information (Salahdine & Kaabouch, 2019). Accomplished social engineers often use tailgating tactics, which involve following the victim through secured areas without permission and gaining access to secured places in order to loot data. This attack can lead to loss of clients, reputation, and even financial losses, which may affect organizations (Mbereki & Doss, 2021). Most university students are still unaware that password guessing is still one of the key components of their data that is easily exposed. Most social networking sites are built with basic settings that do not prioritize data acceptance mandates, making them prone to attacks (Kikerpill & Siibak, 2021). The same university is prone to vulnerabilities because of where students' data is stored. Hackers often find ways to access the students' data when attacking them (Xiangyu et al., 2017). They can also be disguised as technical staff by asking users their passwords while masquerading as the help center team (Ryck et al., 2013). There has been an increased number of publications since 2010 due to curiosity about the research topic; therefore, awareness about cyber-attack risks has been raised, making Universities around to be keen-eyed. There has been various review studies on social engineering attacks. The selected few are described below.

According to Kharrazi (2018), his article titled "Social Engineering Attacks and Countermeasures: Review" highlighted the significance of social engineering attacks. This study has a limited focus on specific social engineering tactics and countermeasures. The "The Psychology of Social Engineering" article by Hadnag (2010) emphasizes the role of human behavior in social engineering attacks, but it did not focus specifically on the role

of human factors in successful social engineering attacks. Yet in another by D'Angelo (2019) titled "Social Engineering Attacks: A Survey", a survey investigated the prevalence of social engineering attacks in organizations and identified the most common tactics used. Its limitation was that its general overview, lacked in depth analysis of specific tactics. Finally, Ross (2020) compared the effectiveness of different social engineering techniques and identified the most successful ones in the article "Social Engineering Techniques: An Analysis and Comparison" but used a limited sample size and his findings lacked real-world application.

Methodology

A lab environment was set up, deployed, and configured as shown in Figure 1 below.

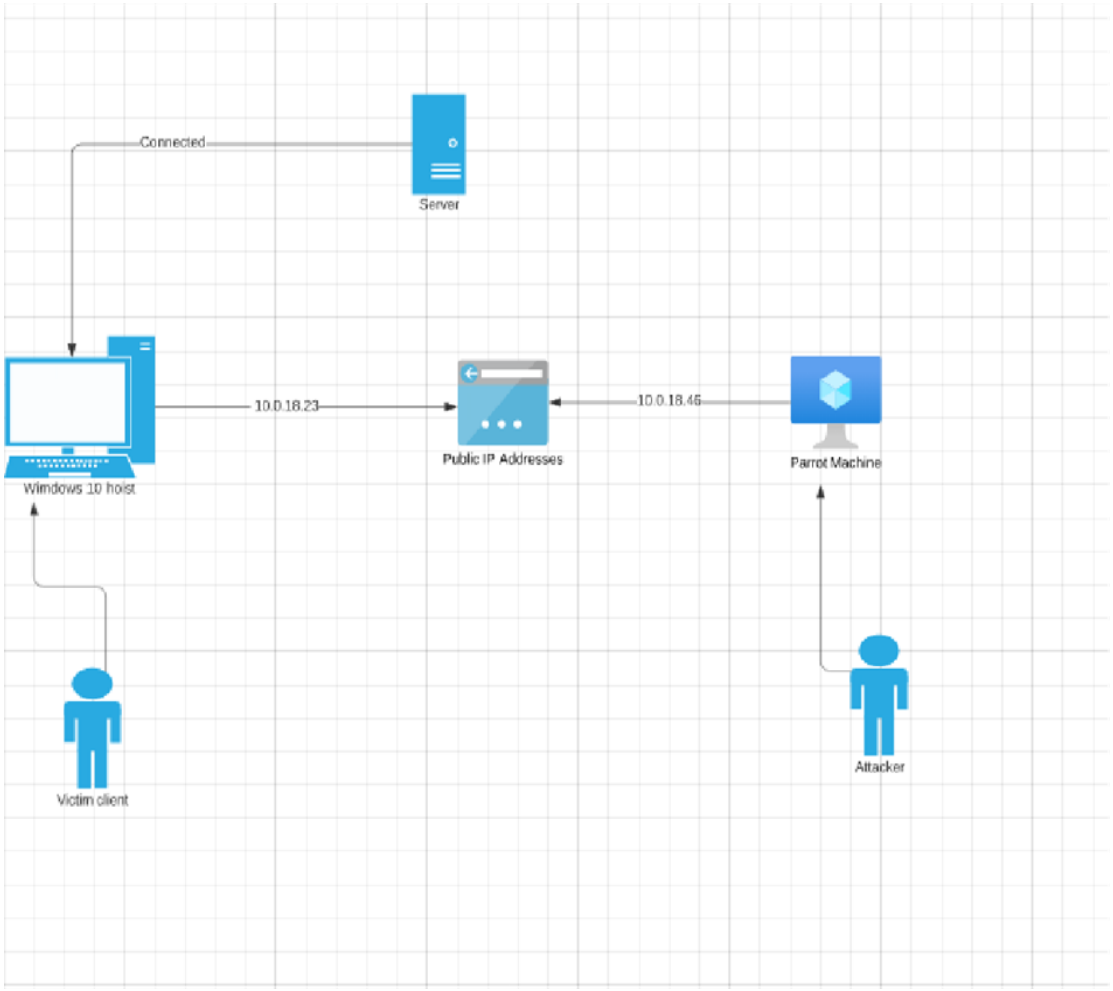

Figure 1. High level diagram showing how the attack was made

For the hardware components, lab environment was set up using Parrot Security Machine and a lab of thirty one (31) networked Windows 10 machines. The Parrot Security Machine served as the attacker machine, where the Social Engineer Toolkit was used to perform credential sniffing and cloned websites. The Windows 10 machines were used to serve as the victim machines, where the sniffing and cloned websites by the attacker machines was executed. As a control, lectures continued to take place within the lab in a controlled environment without the knowledge of the students or the lecturer. Three classes went in, therefore 90 students were subjected to the experiment.

The software components included Social Engineer Toolkit and Simple Mail Transfer Protocol (SMTP). The Simple Mail Transfer Protocol (SMTP) protocol was used to send an email to the victim machines. The new email will flash to lure the students to click on the link. The web browser on the victim machines was used to open a malicious website, which was used to steal sensitive information such as passwords. Both the Windows 10 machines and the Parrot OS machine had IP addresses assigned to their network interfaces. They had the same subnet to enable easier communication.

Social Engineering Toolkit

The Social Engineer Toolkit is an open-source penetration testing platform made to mimic social engineering assaults. It is often used to craft spear phishing emails. The Social Engineer Toolkit's main objective is to mimic actual social engineering attacks in order to assess an organization's security posture (Segovia et al., 2017). It allows security experts to evaluate how well their defenses work against social engineering strategies including phishing, pretexting, and impersonation. Using SET, testers may assess how vulnerable different employees are to these kinds of attacks, spot potential security holes, and create plans to improve security awareness.

Figure 2. Social Engineer toolkit

Experiments

A Demonstration Using the Social Engineer Toolkit on a Protected Lab Environment

Figure 3 shows how after logging into the parrot machine, the parrot (MATE) terminal was launched.

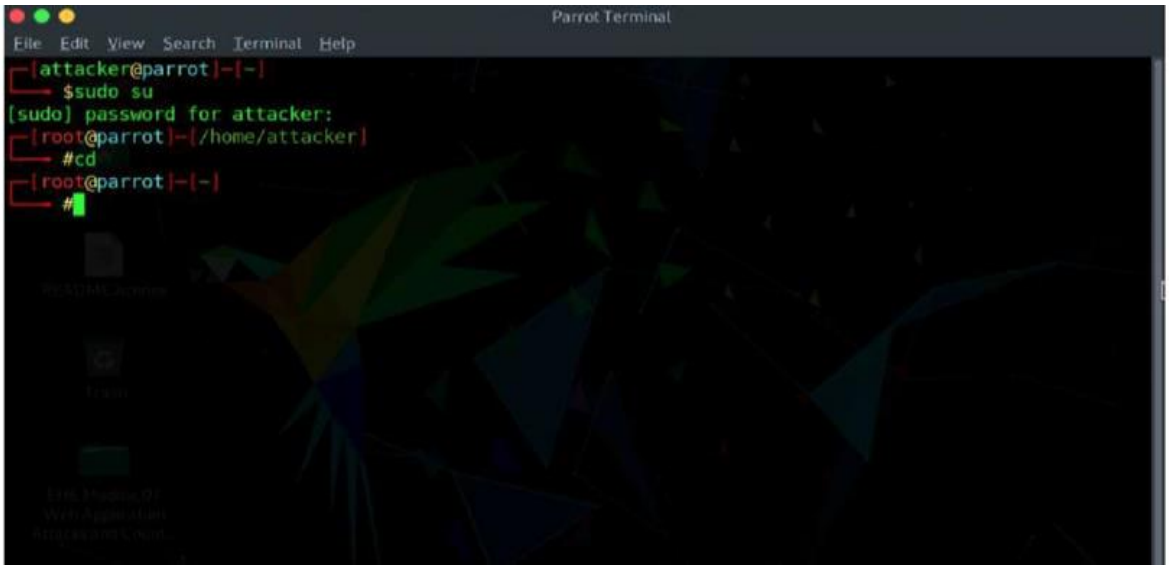

Figure 3. Launching parrot (MATE) terminal

To run the programs as a root user, sudo su command was used. To change to the root folder and navigate the SEtoolkit, the user may type cd social-engineer-toolkit. Then type chmod+x./setoolkit to execute the script and launch the social engineer toolkit as shown in Figure 4 below.

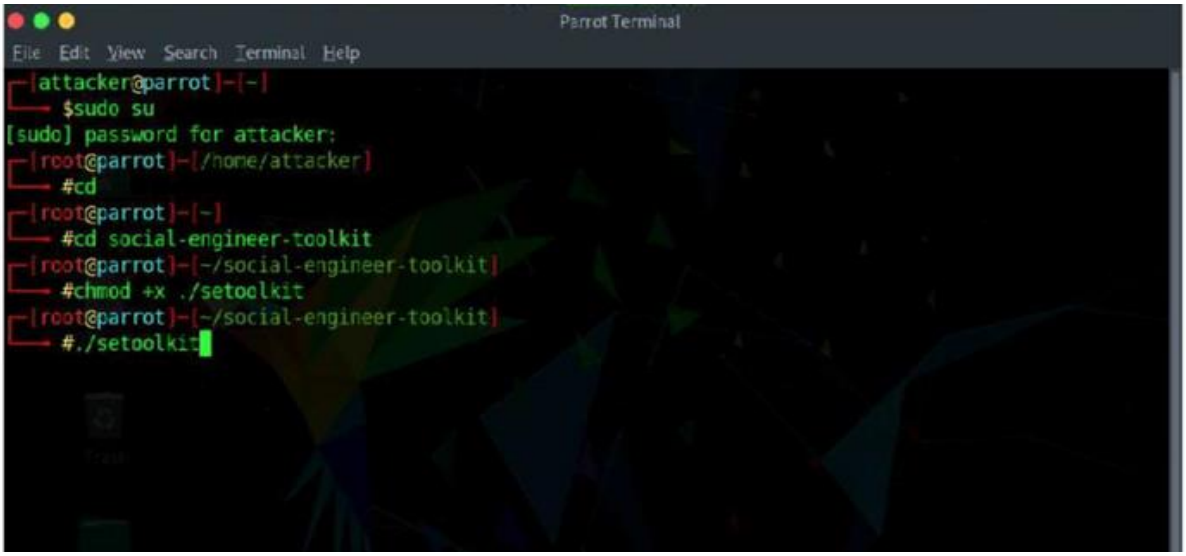

Figure 4.Generating malicious code using the Social Engineering toolkit

The social engineer toolkit was selected, then navigated to the credential harvester attacker. The IP address of the local machine was entered. In the case of the above scenario, it was 10.0.18.46 and then the URL to clone was entered. Then an email (see Figure 5) was sent to the victim machines, attaching both the URL link after the successful cloning of the website. Email flashed that made the students to quickly go to their emails and some students fell for the trap.

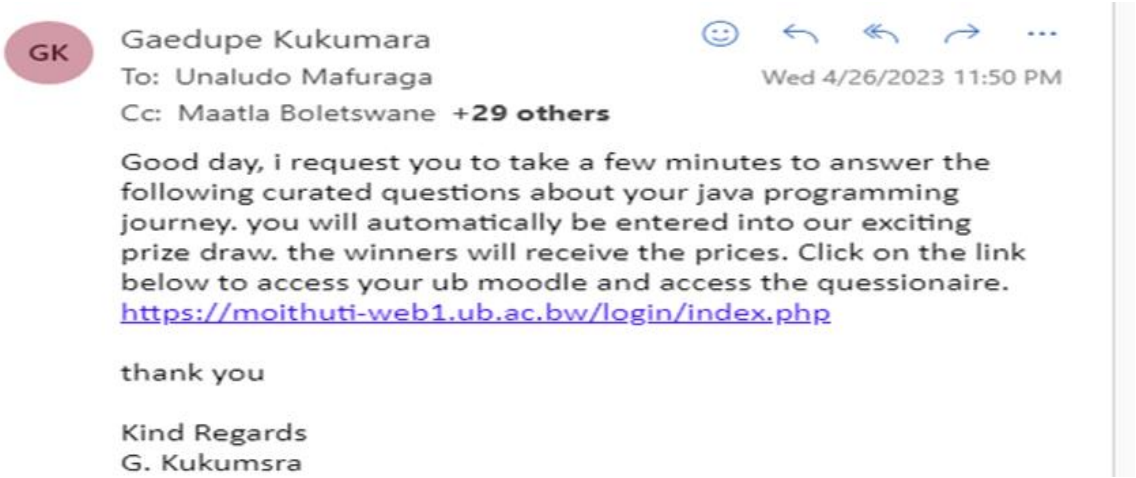

Figure 5. Malicious email

After email was sent, the victims fell for the trick and clicked the link they received and were prompted to enter their details on what looks like a real web page.

Lab Parameters

500 simulated spear phishing attempts were run in the lab environment

Results and Findings

The success rate of spear phishing attacks against students was examined. According to the findings. Data was gathered and examined on how quickly phishing emails were responded to. Students took an average of 2 hours to click on a phishing link, 60% of the recipients clicked on the phishing emails' dangerous links. 40% of these individuals went on to enter private data on the phony websites, including usernames and passwords. The screenshots on Figure 6 below shows the details that were captured from the cloned website. This was the well laid out results after students clicked on the link sent via an email.

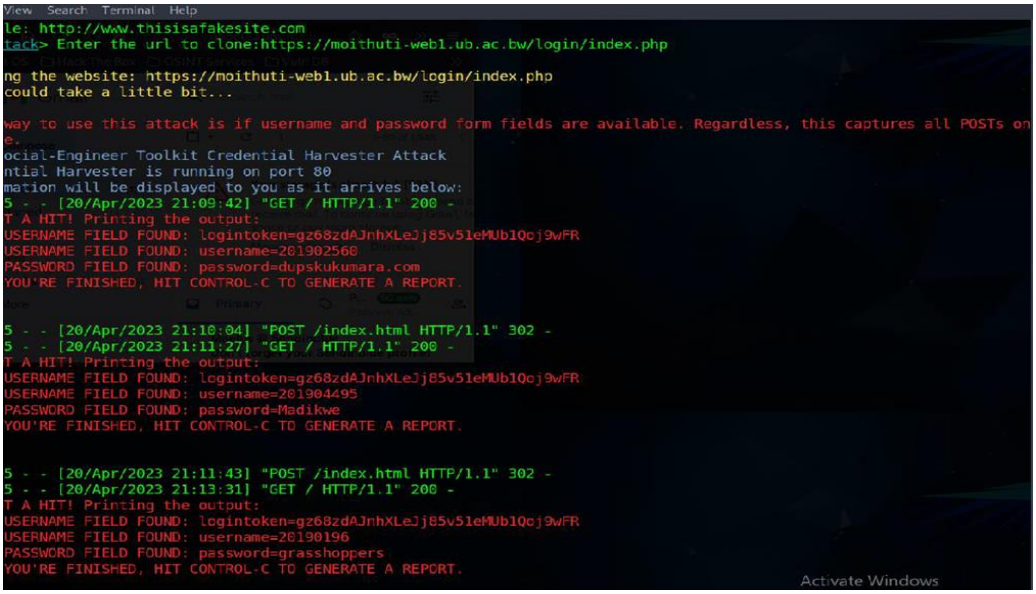

Figure 6.URL cloned and details captured

After certain details of students were captured, their student portals accounts were accessed, and certain details were exposed, as further clarified by the details following. Withdrawing student assignment, deleting of some files and many other malicious activities could be carried out easily.

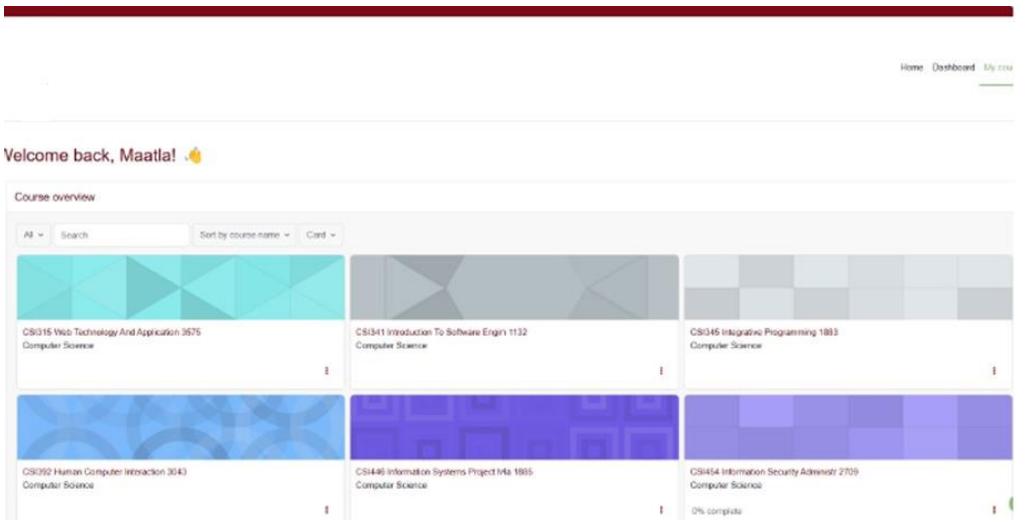

Figure 7. Student data in moodle

Conclusion

The results show that students do not use complex passwords and are easily tricked into clicking any link available. Some are just simple passwords with no complicated characters. This network was configured, tested, and final conclusions were drawn from the results obtained. Thus, the network was vulnerable to phishing attacks on their websites.

Future Recommendations

Most universities should invest in educating students, staff members, and the faculty at large about certain threats and how to avoid falling prey to them. Implementation of multi-factor authentication (MFA) systems, which may include facial recognition and fingerprint recognition, when accessing their websites at the university should be utilized. Implementing a phishing detection system specifically for the university is necessary, as it appears that human factors are the leading contributors to these attacks.

Limitations of Research

While the research has yielded valuable insights into social engineering attacks, particularly spear phishing attempts within university networks, it is essential to acknowledge certain limitations inherent in the study. These limitations, however, do not diminish the practical implications of the findings or their potential to contribute to enhanced security practices.

Lab Environment Constraints: The study was conducted within a controlled lab environment, which, by its nature, may not fully replicate the complexities of real-world university networks. While this controlled setting ensured the safety and privacy of the participants, it may not encompass all the intricacies of dynamic network behaviors.

Sample Size: We acknowledge that the study's sample size was limited due to resource constraints and the need for volunteer participants. As such, the findings may not be entirely representative of the entire university community.

Despite these limitations, the research holds significant practical implications for improving security within university networks:

Tailored Security Awareness Programs: The findings underscore the importance of targeted security awareness programs within academic institutions. By recognizing the specific vulnerabilities of students and staff to spear phishing attacks, universities can develop tailored training modules that empower users to identify and respond to such threats effectively.

User Behavior Analysis: The insights gained into user behavior when faced with spear phishing emails can inform the design of security controls. Universities can adapt their security measures to align with the typical responses of their users, enhancing the overall security posture.

Recommendations for Defense: The research provides actionable recommendations for strengthening network defenses against social engineering attacks. These recommendations encompass both technical measures, such as email filtering and authentication protocols, and non-technical strategies, such as user education and multi factor authentication implementation.

Building Cyber Vigilance: Beyond the technical aspects, these studies emphasize the role of user awareness and vigilance. By acknowledging the human element in cybersecurity, universities can cultivate a culture of cyber vigilance among students and staff, reducing the overall risk of social engineering attacks.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Technology (www.icontechno.net) held in Antalya/Turkey on November 16-19, 2023.

References

Alzahrani, N.M., &Alfouzan, F.A. (2022). Augmented reality (AR) and cyber-security for smart cities a systematic literature review. *Sensors, 22*(7), 2792.

Annamalai, A., Poonia, R. C., & Shanmugasundaram, S. (2021). A broach study on issues in social engineering attacks on social networking sites. *International Journal of Mechanical Engineering, 6*(2), 105.

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, *86*(1), 350-357.

Chilisa, B., & Preece, J. (Eds.). (2005). African perspectives on adult learning: Research methods for adult educators in Africa. *Adult Education Quarterly, 59*(1), 84-86.

De Ryck, N. P., Nikiforakis, L., & Desmet, J. W., (2013). Tabshots: Client-side detection of tabnabbing attacks. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*. Hangzhou, China.

Eltahir, M.E., & Ahmed, O.S. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Inf. Sci. Lett, 12*(1).

Harris, J.K. (2019). *Statistics with R: solving problems using real-world data*. SAGE Publications

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers and Security, 73*, 102-113.

Helminen, N. (2021). *Social Engineering: Introduction to social engineering through real-life hacking attempts*. Jamk University of Applied Sciences. Retrieved from https://www.theseus.fi/handle/10024/503239

Kalnins, R., Purins, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. *Applied Computer. Systems, 21*(1), 38–45.

Kikerpill, K., & Siibak, A., (2021). Mazephishing: The COVID-19 pandemic as credible social context for social engineering attacks. *Trames: A Journal of the Humanities and Social Sciences, 25*(4),371-393.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22,* 113-122.

Mbereki, K., & Doss, S. (2021). Investigating the Level of Awareness on Information Security amongst Users at Botho University. *International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE), 4*(9), 905-912.

Omoyiola, B.O. (2020). *Exploring strategies for enforcing cybersecurity policies*. Walden University.

Riquarts, K., (1987). Technology education: Science-technology-society. *Science and Technology Education and the Quality of Life, 2.*

Salahdine, F., & Kaabouch, N., (2019). Social engineering attacks: A survey. *Future internet, 11*(4), 89.

SCRIBD. (2011, Jun 9). The official social engineering framework- computer based social engineering tools-social engineering toolkit. Retrieved from http://www.socialengineer.org

Segovia, F., Torres, L., Rosillo, M., Tapia, E., Albarado, F., & D. Saltos, D. (2017). Social engineering as an attack vector forransomware. In *Proceedings of the Conference on Electrical Engineering and Information CommunicationTechnology*,1-6. Pucon, Chile.

Trusted Sec. (2013). Social-engineer toolkit. Retrieved from: https://www.trustedsec.com/downloads/socialengineer-toolkit/, last accessed 03/12/2013.

Wyld, D. C., & Nagamali, D. (2021). Computer science and information technology. *2nd International Conference on Soft Computing, Artifical Intelligence and Machine Learning (SAIM 2011)* (p.146). Toronto, Canada.

Xiangyu, L., Qiuyang, I., & Chandel, S. (2017). Social engineering and insider threats. In *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, 25-34. Nanjing, China.

Author Information

Trust Tshepo Mapoka
University of Botswana
Botswana, South Africa
Contact e-mail:mapokat@ub.ac.bw

Keneilwe Zuva
University of Botswana
Botswana, South Africa

Gaedupe Kukumara
University of Botswana
Botswana, South Africa

Tebogo Seipone
University of Botswana
Botswana, South Africa

Tranos Zuva
Vaal University of Technology
Vanderbijlpark, South Africa

To cite this article:

Mapoka, T.T., Zuva K., Kukumara G.K., Seipone T., & Zuva, T. (2023). Exploring social engineering attacks using spear phishing in a university. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 24*, 21-28.