Case study

APPLICATION OF SIMULATED PHISHING ATTACKS FOR USER TRAINING

Janeš, H.[1], Bilić, K.[1], Grgić, M.[1]

[1]University of Applied Sciences Velika Gorica, Velika Gorica, Croatia

Abstract: *The aim of this study was to investigate the level of awareness among a focus group regarding phishing threats, utilizing simulated phishing attacks as a training method. Data were gathered by executing a simulated phishing attack on the focus group, followed by an assessment of their proficiency in recognizing such threats. After delivering lectures on security vulnerabilities and phishing attacks, an exit survey was conducted. Participants accessed the survey via a QR code linked to a platform for collecting user feedback. Without their knowledge, the survey included a phishing attempt. This paper presents the outcomes of our research, illustrating the effectiveness of simulated phishing attacks for user training, and identifies the factors that pose significant challenges to users in detecting phishing attacks.*

Keywords: DKU, 2024, phishing, user training

1. INTRODUCTION

In light of the escalating significance of today's digital era and the heightened consciousness surrounding information system security, the prevalence of threats pertaining to information and data theft, as well as phishing attacks, is on the rise. This paper seeks to outline a framework for end-user training utilizing simulated phishing attacks. The introductory segment of this paper furnishes an overview of the threats to information system security and underscores the pivotal role of user education in preventing a majority of malicious attacks. According to data from the National CERT (an entity within the Croatian Academic and Research Network), phishing attacks account for 65.6% of security incidents (based on data from 2023) (Figure 1). Consequently, there exists a pressing imperative for innovative educational methodologies, among which the employment of simulated phishing attacks emerges as a pivotal tool for heightening awareness regarding user and data security.

The second section of the paper outlines the research methodology, beginning with the establishment of research objectives, participant selection, and the creation of simulated phishing attacks, whether announced or unannounced simulations. Through a comprehensive examination of various aspects of conducting simulated attacks, such as scenario development, targeted user selection, and the assessment of training effectiveness, the study explores diverse approaches to evaluating training outcomes, analyzing feedback, and comparing achieved results with intended goals.

By employing both quantitative and qualitative analyses of the gathered data, this study investigates the implications of simulated phishing attacks on user awareness and security.

Particular emphasis is placed on examining the outcomes derived from phishing attack simulations conducted both prior to and subsequent to user training sessions. These findings are anticipated to reveal a clear correlation in users' preparedness to identify and address genuine security incidents. Similar studies on a far larger scale were conducted in a financial institution in Thailand (Chatchalermpun & Daengsi, 2021)

Moreover, the study investigates the impact of several factors on the effectiveness of the training program.

The concluding segment of this paper encapsulates the principal discoveries of the study and clarifies their significance in the realm of mitigating security incidents caused by phishing attacks. It emphasizes the imperative of continually enhancing user education and utilizing innovative educational methods, as demonstrated by simulated phishing attacks. By integrating simulated attacks into educational initiatives and corporate strategies, the potential for creating a more secure online environment and safeguarding users from potential threats becomes feasible. Finally, recommendations for further research efforts and practical applications within the domain of simulated phishing attacks are outlined, with the primary objective of enhancing information system security on a continuous basis. The article *"Phishing Counter Measures and Their Effectiveness – Literature Review"(Purkait, 2012)* provided foundational insights for this research by highlighting the range of anti-phishing strategies and evaluating their efficacy in real-world settings. It inspired the research methodology, particularly in assessing the impact of user awareness and behavioral responses to phishing simulations.

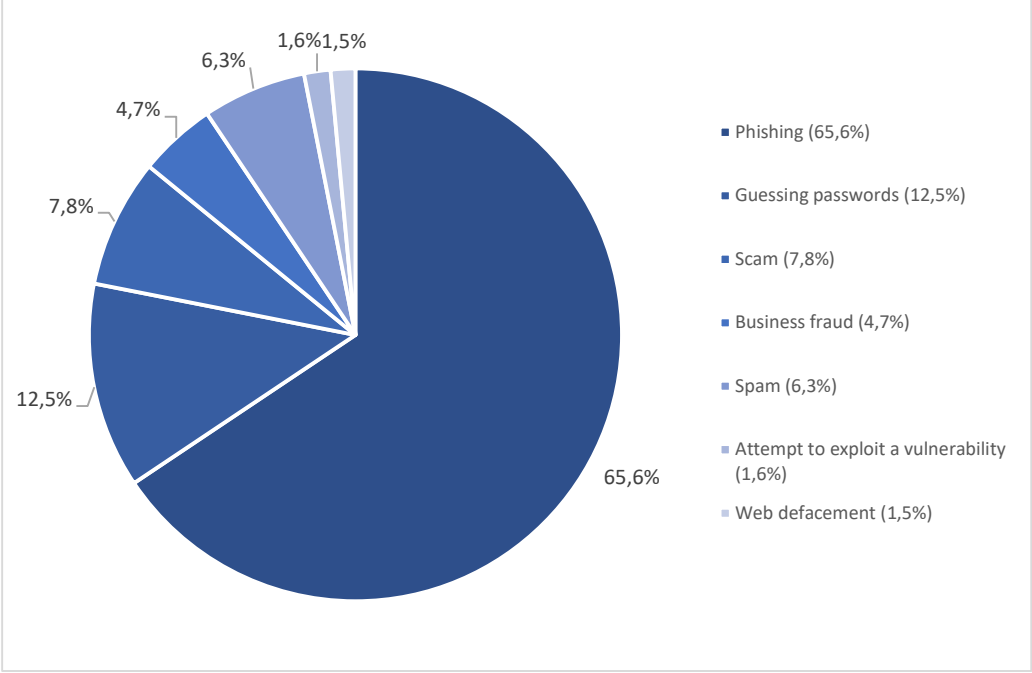

Figure 1: National CERT – security incidents in December 2023 (Nacionalni CERT (2024, April))

2. THREATS TO INFORMATION SYSTEM SECURITY

In the contemporary digital landscape, the security of information systems holds paramount importance. As organizations and individuals increasingly depend on digital platforms for the storage, processing, and transmission of data, the threats to these systems have proliferated in both variety and sophistication. Cybersecurity threats present substantial risks, including data breaches, financial losses, reputational damage, and operational disruptions. The evolution of cyber threats necessitates a multi-faceted approach to security, incorporating technological defenses, policy frameworks, and continuous user awareness programs. Emerging threats such as ransomware, phishing, and advanced persistent threats require sophisticated countermeasures and proactive strategies. Moreover, the integration of artificial intelligence and machine learning in both attack and defense mechanisms adds complexity to the cybersecurity landscape. Consequently, understanding the human factor, particularly user behavior and awareness, becomes crucial. By enhancing user education and promoting best practices, organizations can significantly reduce vulnerabilities and bolster their overall cybersecurity posture. Numerous researchers have utilized simulated phishing exercises to assess participants' awareness and their responses to security threats ((Jakobsson & Ratkiewicz, 2006, Steyn et al., 2007). These studies leverage realistic phishing scenarios to evaluate not only the detection capabilities of participants but also the effectiveness of their countermeasures, providing insight into the practical application of security awareness in mitigating phishing threats. Phishing attacks rely heavily on human error. Comprehensive phishing awareness training programs can equip users with the knowledge to identify and avoid phishing attempts. Training should cover recognizing suspicious emails, verifying the legitimacy of requests, and reporting potential phishing incidents. Simulated phishing exercises can also be an effective tool. By periodically sending simulated phishing emails, organizations can assess the effectiveness of their training programs and identify users who may need additional training. Some other training programs may include password management education, recognizing social engineering attacks, incident reporting and response to name a few. For example, educating users about safe browsing practices is essential in preventing malware infections. Users should be trained to recognize and avoid malicious websites, understand the risks of downloading files from untrusted sources, and use secure browsers with up-to-date security features. Training should also cover the importance of verifying website URLs before entering sensitive information and using encrypted connections (HTTPS) whenever possible. Social engineering attacks exploit human psychology to manipulate individuals into divulging confidential information. Training programs should educate users about common social engineering tactics, such as pretexting, baiting, and tailgating. By understanding how social engineers operate, users can be more vigilant and skeptical of unsolicited requests for information or access. Role-playing scenarios can be an effective training method, allowing users to practice responding to potential social engineering attempts. This all leads to incident reporting and response. Prompt reporting of security incidents is crucial in minimizing damage. Users should be trained to recognize signs of a security breach, such as unusual system behavior or unauthorized access attempts, and know the proper channels for reporting these incidents.

Incident response training should also cover the steps users need to take in the event of a suspected breach, such as disconnecting from the network, preserving evidence, and notifying the IT department immediately.

Cyber threats are constantly evolving, making continuous security education essential. Organizations should establish ongoing training programs that keep users informed about the latest threats, security trends, and best practices. Regularly updating training materials and conducting refresher courses can help reinforce good security habits and ensure that users remain vigilant against emerging threats. Organizations should also encourage a culture of security awareness (Puhakainen & Siponen, 2010), where users feel empowered to stay informed and proactive in protecting information systems.

3. PROBLEM ANALYSIS AND RESEARCH METHODS

Phishing constitutes a sophisticated form of social engineering, involving deceitful practices where perpetrators present themselves falsely and use seemingly authentic requests to coerce potential victims into taking actions that serve the attackers' interests. This type of criminal activity employs a variety of manipulative techniques aimed at extracting sensitive information from users, such as usernames, passwords, and credit card details, ultimately for financial exploitation. Phishing schemes are most commonly executed through electronic mail, wherein unsuspecting recipients are prompted to click on hyperlinks that lead them to malicious websites. These websites are designed to mimic the appearance of legitimate entities like banks, electronic payment systems, and other similar organizations, thereby deceiving users into believing they are interacting with a trusted source.

In addition to email, other digital communication platforms are frequently utilized for phishing attempts. These include online forums, instant messaging services, and social networking sites. Social networks are particularly hazardous in this context because they harbor extensive personal information that can be exploited for identity theft. Furthermore, messages originating from compromised accounts of friends or acquaintances carry a veneer of credibility, making it more likely for victims to trust and respond to them. This diverse approach to phishing underscores the need for heightened awareness and robust security measures to protect against these pervasive and evolving threats.

This study employs both quantitative and qualitative analysis to examine the impact of simulated phishing attacks on user awareness and security. During a lecture on safe internet usage a discussion among users was facilitated. The purpose of which was to explore the understanding of phishing attacks, how users can recognize phishing attacks and their general awareness of cybersecurity threats. Additionally, surveys were administered before and after the lecture. These surveys had multiple benefits. At first, they facilitated discussions among users to identify common themes and misconceptions about phishing, this also helped in tailoring educational content to address specific gaps in users' knowledge. The survey which was administered after the lecture was used to gather feedback on lecture whether it was effective or ineffective, providing valuable insights for improvements. As a part of the lecture content analysis of phishing emails has also been conducted with the aim to identify common

tactics and themes used by attackers. Also, personal stories from individuals who have encountered phishing attempts made the educational content more relatable and memorable.
A simulated phishing attack was conducted on a sample of 152 users. The objective of this research is to demonstrate a direct correlation between user preparedness and their ability to recognize and mitigate real security incidents. To facilitate the study, a "fake" login page for platform for collecting user feedback was created.

4. ACTIVITY PLAN AND REQUIRED RESOURCES

The testing and simulated attack were conducted under controlled conditions to ensure user safety, with two distinct focus groups selected. The first group (advanced users) consisted of individuals who rated their prior knowledge of information security as high based on an initial survey, while the second group (basic users) rated their prior knowledge as satisfactory.
During a lecture on safe internet usage and associated threats, a survey was conducted. Participants accessed the survey via a QR code provided during the lecture presentation. The task required participants to scan the QR code and attempt to log in to the web resource. At this point, a simulated phishing attack was executed, and the study monitored whether the users would recognize the phishing attack.

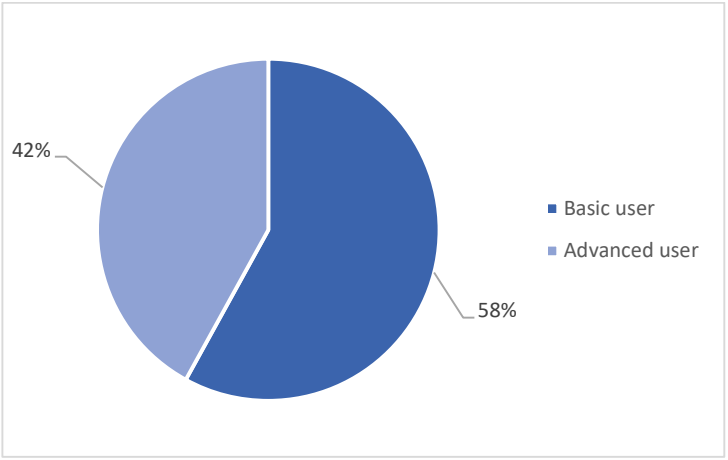

Figure 2: User Entrance Survey

As illustrated in Figure 2, the distribution of users into two distinct categories - advanced users and basic users - reveals significant insights into the composition of our study population. The first group, identified as advanced users, constituted 42% of the total survey respondents (64 individuals). On the other hand, the remaining 58% of the respondents, equating to 88 individuals, were categorized as basic users. The distinction between these groups is critical for analyzing the impact of phishing awareness and response rates, as the level of user expertise can significantly influence the outcomes of educational interventions and susceptibility to phishing attacks.

5. IMPLEMENTATION OF SIMULATED ATTACK

Simulated phishing attacks, which are targeted attempts to assess users' vulnerability to social engineering strategies, inherently raise significant legal and ethical concerns. Legally, conducting such simulations without explicit consent may violate privacy laws and cybercrime statutes, as they involve deceptive practices to acquire potentially sensitive information from users. Ethically, the implementation of deceptive tactics, even within a controlled experimental framework, poses questions regarding respect for user autonomy and the potential psychological impact on individuals subjected to these simulated attacks. The ethical implications of deception in research are well-documented, emphasizing the need for informed consent and the minimization of harm to participants (Babbie, 2013; Resnik, 2018). Consequently, it is essential to meticulously address these legal and ethical considerations, ensuring that any such testing is carried out with the informed consent of participants or with appropriate organizational authorization, thereby upholding both legal compliance and ethical standards (Sieber, 1992). During implementation of simulated phishing attack conducted in this study, no personal data was recorded, stored, or distributed and consent from organizational authority was given.

As part of the lecture, participants were presented with various examples of phishing attacks to illustrate common tactics used by cybercriminals. Following this educational segment, a survey was conducted to assess the participants' ability to distinguish between authentic and fraudulent Internet resources. The findings from this survey are depicted in Figure 3. The data analysis revealed that participants' recognition of genuine Internet resources largely conformed to anticipated patterns.

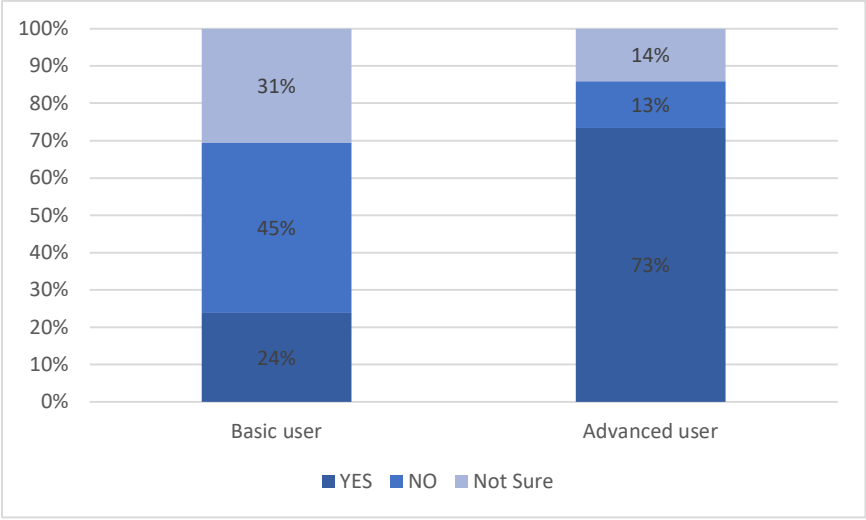

Figure 3: Phishing attack recognition survey

Participants were able to identify several subtle indicators of phishing, such as grammatical errors, variations in social network names, incorrect web addresses, and inaccurately designed logos. These results align with previous research, which has shown that users often rely on surface-level cues to judge the authenticity of online content (Alsharnouby et al., 2015). For

instance, Jakobsson and Myers (2007) emphasize that grammatical errors and discrepancies in domain names are commonly exploited by phishers to deceive users. However, the study also underscores a crucial gap in the ability to detect more sophisticated phishing attempts. Research by Sheng et al. (2010) indicates that while basic training can improve users' ability to identify simple phishing attacks, more advanced training is necessary to equip users with the skills to recognize complex phishing schemes that do not exhibit obvious signs of deception. The results suggest that further education and training are necessary to enhance the participants' phishing detection capabilities. This is particularly important given the increasing sophistication of phishing tactics, which now often include highly realistic fake websites and personalized spear-phishing attacks (Kumaraguru et al., 2010). Therefore, incorporating more comprehensive and continuous cybersecurity education, which includes exposure to advanced phishing tactics and the development of critical thinking skills, is essential for reducing susceptibility to these threats.

Overall, the ability to discern minor discrepancies in Internet resources is a positive outcome, yet it also highlights the need for ongoing training to keep pace with the evolving nature of phishing attacks. Ensuring that users are well-equipped to identify both basic and sophisticated phishing attempts is critical for enhancing overall cybersecurity resilience (Hong, 2012).

At the conclusion of the lectures addressing security vulnerabilities and phishing attacks, an exit survey was conducted. Participants were instructed to access the survey by scanning a QR code, which embedded a link to an online platform designed for collecting user feedback. This method of distribution was chosen for its convenience and efficiency, allowing participants to navigate quickly and easily to the survey using their mobile devices. The QR code facilitated seamless access to the survey platform, ensuring a higher response rate and minimizing the potential for errors that can occur when manually entering URLs. This also meant that fake URL used in phishing attack was for the most part hidden from participants. The link provided through the QR code did not lead to the familiar platform but rather to a "fake" page. Users were prompted on this page to log in with their private credentials.

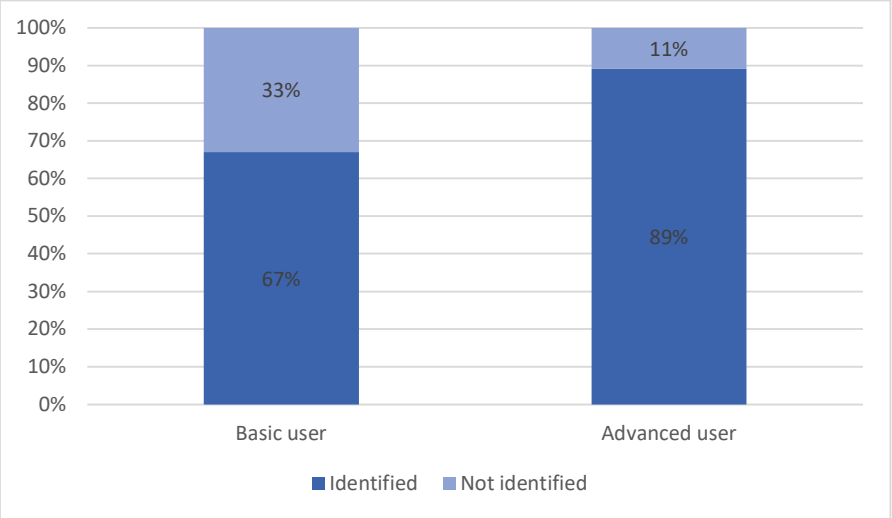

Figure 4:Exit Survey - Phishing Attack

Following the simulated phishing attack, a comprehensive presentation of the results was conducted. This presentation included a detailed analysis of the participants' responses, highlighting the key findings and metrics from the simulation. The analysis was further enriched by comparing these results with data obtained from a previous survey focused on participants' ability to recognize phishing attacks.

In the simulated phishing attack, 67% of the basic users were able to correctly identify the phishing attempt, while 33% failed to do so. This indicates a significant vulnerability within the basic user group, suggesting a need for enhanced training and awareness programs tailored to their specific needs and levels of understanding. In contrast, the advanced users demonstrated a higher level of proficiency, with 89% successfully identifying the phishing attack and only 11% failing to recognize it. This disparity underscores the importance of user expertise in cybersecurity resilience.

The comparative analysis between the simulation results and the survey data provided valuable insights. The survey, which assessed theoretical knowledge of phishing attacks, showed a similar trend, although with slight variations. By comparing these sets of data, we can better understand the correlation between theoretical knowledge and practical application. The findings suggest that while advanced users possess both the theoretical understanding and practical skills to identify phishing attacks, basic users may benefit from more targeted and practical training approaches.

This analysis not only highlights the current effectiveness of existing training programs but also identifies specific areas for improvement. The significant difference in recognition rates between basic and advanced users points to the necessity of differentiated training strategies that cater to varying levels of user proficiency. Ultimately, this comprehensive approach to evaluating and comparing user responses will serve as a critical foundation for the development of more effective educational initiatives. By systematically analyzing the differences in how basic and advanced users respond to simulated phishing attacks, as well as their performance in theoretical assessments, we can identify specific knowledge gaps and areas of vulnerability. This detailed understanding allows for the design of targeted training programs that address the unique needs of different user groups, ensuring that educational content is both relevant and impactful.

6. CONCLUSIONS

The threats to information system security are diverse and constantly evolving, posing significant risks to individuals and organizations. While technical defenses are crucial, the human factor remains a critical vulnerability. Comprehensive user education programs play a pivotal role in preventing most malicious attacks by equipping users with the knowledge and skills to recognize and respond to threats. By addressing common threats such as phishing, malware, ransomware, insider threats, DDoS attacks, zero-day exploits, SQL injection, Man-In-The-Middle attacks, and weak passwords, organizations can significantly enhance their security posture. Effective user education programs should cover a wide range of topics, including phishing awareness, safe browsing practices, password management, social engineering, incident reporting, security updates, use of security tools, mobile device security,

data protection, and continuous learning. Real-world examples illustrate the devastating consequences of inadequate security training. Implementing best practices for user education, including assessing training needs, developing comprehensive materials, leveraging simulated attacks, encouraging continuous learning, monitoring effectiveness, promoting a security-first culture, and collaborating with IT and security teams, can help organizations build a resilient defense against cyber threats. Ultimately, the success of cybersecurity efforts depends on the collective vigilance and proactive engagement of all users. By fostering a culture of security awareness and continuous education, organizations can better protect their information systems and maintain the trust of their stakeholders.

REFERENCES

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future internet 12*(10), 168. https://doi.org/10.3390/fi12100168

Alsharnouby, M., Alaca, F. & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Andric, J., Oreski, D., & Kisasondi, T. (2016, May 1). Analysis of phishing attacks against students. https://doi.org/10.1109/mipro.2016.7522363

Babbie, E. (2013). *The Practice of Social Research* (13th ed.). Wadsworth, Cengage Learning.

CERT.hr. (2024, April). Statistika računalno-sigurnosnih incidenata - CERT.hr. CERT.hr -. https://www.cert.hr/statistika/

Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. *IOP Conference Series Materials Science and Engineering*, *1088*(1), 012015. https://doi.org/10.1088/1757-899x/1088/1/012015

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, *106*, 1-20. https://doi.org/10.1016/j.eswa.2018.03.050

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.

Jakobsson, M., & Ratkiewicz, J. (2006). Designing ethical phishing experiments. *ROT13*. https://doi.org/10.1145/1135777.1135853

Jakobsson, M. & Myers, S. (2007). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1–31. https://doi.org/10.1145/1754393.1754396

Puhakainen, N., & Siponen, N. (2010). Improving Employees' compliance through Information Systems Security Training: An Action Research study. *MIS Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security*, *20*(5), 382–420. https://doi.org/10.1108/09685221211286548

Resnik, D. B. (2018). *The Ethics of Research with Human Subjects: Protecting People, Advancing Science, Promoting Trust*. Springer.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. and Downs, J. (2010) Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373-382. https://doi.org/10.1145/1753326.1753383

Sieber, J. E. (1992). Planning ethically responsible research: A guide for students and internal review boards. Sage Publications, Inc.

Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity Theft — Empirical evidence from a Phishing Exercise. In *IFIP International Federation for Information Processing/IFIP* (pp. 193–203). https://doi.org/10.1007/978-0-387-72367-9_17

What is Spear-phishing? Defining and Differentiating Spear-phishing from Phishing. (2023, February). Digital Guardian. https://www.digitalguardian.com/blog/what-spear-phishing-defining-and-differentiating-spear-phishing-phishing