Science World Journal Vol. 20(No 4) 2025 https://dx.doi.org/10.4314/swj.v20i4.20
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

Full Length Research Article

PRAGMATIC APPROACH ON SOCIAL ENGINEERING AWARENESS EVALUATION IN NASARAWA STATE UNIVERSITY, KEFFI

*[1]Opuh Chukwuebuka Calistus, [2]M.O. Adenomon, [1]G.I.O. Aimufua, [1]S.I. Bassey, [1]Owoicho P.G.

[1]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[2]Department of Statistics and Data Analytics, Nasarawa State University, Keffi, Nigeria

*Corresponding Author Email Address: chukwuebukaopuh@gmail.com

ABSTRACT
This study assessed the level of social engineering awareness within Nasarawa State University, Keffi (NSUK), using a pragmatic approach that combined survey responses and practical experiments. A total of 101 students and staff participated in the research, representing diverse age groups, genders, and educational backgrounds. Findings revealed that awareness of social engineering was generally low, with 63% of respondents reporting no prior knowledge of social engineering or its attack vectors. Phishing was identified as the most prevalent attack vector, experienced by 50% of respondents, followed by email spoofing (28%) and pretexting (9%). Alarmingly, 13% of respondents who had been victims were unable to identify the type of attack they had experienced. Additionally, 53% of participants lacked the technical skills to determine whether their personal computers had been compromised. The study further revealed that all respondents admitted to using public computers or networks to access personal information, significantly increasing the likelihood of successful social engineering attacks. The research concludes that NSUK faces a high level of vulnerability and recommends comprehensive awareness campaigns, technical literacy training, phishing mitigation strategies, and stronger security for shared computing resources.

Keywords: Cybersecurity, Social Engineering, Awareness Evaluation, Pragmatic Approach NSUK.

INTRODUCTION

Technological advancements in computing environments, including learning institutions, have led to the development of interconnected networks, uncontrolled social networking, and thousands of applications and users. These technologies are essential because they facilitate educational processes and interactions. However, the availability of such technology in advanced computing environments, particularly educational environments, opens doors for security threats by cybercriminals and hackers seeking to exploit vulnerabilities in the systems (Majid et al, 2021). Social engineering is one of the most significant security threats facing organizational systems and data in today's technology-saturated world. It is considered a challenge for security chains, and attacks are increasing sharply (Salahdine and Kaabouch, 2024).

Social Engineering is a collation of techniques of human manipulation by exploiting the basic emotions of human beings, such as greed, distress, and naivety in order to obtain the required information (Mumtaz et al, 2024). In simpler words, social engineering is the method of persuading a potential victim to perform a particular action, that is, share personal information (Leonov et al, 2024). According to Ghafir et al (2021), social engineering is defined as the art of exploiting the naivety of unsuspecting individuals and taking advantage of their weaknesses to convince them to comply with one's desires. Instead of relying on an organization's technical security shortcomings to break into its computer systems, social engineers use employees' weaknesses to mislead them into compromising the systems or turning over sensitive information.

The research, however, out to answer the following research questions: What is the current level of awareness among Nasarawa State University students and staff regarding social engineering attack vectors, for which social engineering attack vector poses the greatest risk and vulnerability to Nasarawa State University staff and students? What factor contributes to social engineering vulnerability in the Nasarawa State University community? What is the possibility of a successful social engineer attack in the university community?

As the use of the internet grows, social engineering is also on the rise, and the privacy of user data is being breached from time to time. Nigeria has recorded 82,000 data breaches in the first quarter of 2023 (January to March). This is according to a report by cybersecurity company Surfshark (Surfshark, 2023). These latest numbers represent a 64% increase from the fourth quarter of 2022, in which the most populous African country recorded 50,000 data breaches. With this development, Nigeria now ranks 32nd on a list of countries with the most data breaches in the first quarter of the year 2023. This is worse than the 41st, which it ranked in the last quarter of 2022. Data breach is not only a huge concern to businesses and individuals, it also comes with a great cost in terms of loss and reputational damage (Aridor et al, 2020). In recent years, the world has witnessed many incidents of data and privacy breaches (Norrman et al, 2024). In the year 2018, a British consulting firm named Cambridge Analytica got access to more than 87 million Facebook users' data and their friends' data without their users' consent (Isaak and Hanna, 2018). According to Mumtaz (2024), Facebook was fined 500,000 pounds by the UK's data protection watchdog in October 2018. In the following year, i.e., 2019, Disney+, a streaming service, was attacked and thousands of its accounts were compromised. The Washington Post reported that hackers took control of compromised accounts, changed their login credentials, and started selling them for as low as 3$ per account on the dark web (Telford, 2024). In the year 2020, researchers unearthed 235 million user profiles of Instagram, TikTok, and YouTube available online (BISCHOFF, 2020). Also in the year 2021, IdentityForce, a U.S identity protection firm, reported more than 40 data breaches in various multinational companies around the globe (Mumtaz, 2024), among several other incidents.

However, Nasarawa State University, Keffi (NSUK), like many other educational institutions worldwide, relies heavily on digital infrastructure and information systems to support its administrative

operations, academic activities, and research endeavors. While these technological advancements have undoubtedly brought numerous benefits, they have also exposed the university community to various cybersecurity risks. Among these risks, social engineering has emerged as a prominent threat that exploits human behavior and psychological manipulation to gain unauthorized access to sensitive information or compromise the university's digital assets. This research, using a pragmatic approach, aims at conducting social awareness evaluation in order to improve the resilience of staff and students of the University against social engineering attack vectors.

Recent studies (Mouton et al., 2023) have examined diverse frameworks and taxonomies linked to social engineering attacks. A well-known model within this area is Kevin Mitnick's social engineering attack cycle, which outlines four essential phases that attackers often follow: conducting research, building rapport and trust, exploiting the established trust, and ultimately leveraging the gathered information (Mitnick Security, 2023). This cycle remains influential in understanding the systematic approach attackers employ to manipulate targets and achieve unauthorized access to information or systems. The author included a visual depiction of Mitnick's attack cycle in Figure 1, illustrating the interconnected flow between these phases.

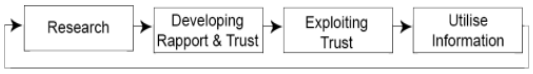

Figure 1 Social Engineering Conceptual framework (Mouton et al, 2023)

The research phase involves gathering information about the target, aiming to acquire comprehensive knowledge before initiating an attack. Subsequently, the Development of rapport and trust with the target becomes crucial, as a trusting target is more likely to disclose requested information. Mitnick (2023) suggests various strategies for building rapport, such as using insider information, misrepresenting identity, referencing acquaintances of the victim, expressing a need for assistance, or assuming an authoritative role. Once trust is established, the attacker exploits it to extract information from the target, either through direct requests, specified actions, or manipulating the victim into seeking assistance from the attacker (Mitnick, 2023). This phase involves leveraging the established relationship to obtain the initially desired information or action. Finally, the outcome of the previous phase is utilized to achieve the attack's goal or to progress to additional steps necessary for reaching the ultimate objective.

Robert and Philip (2023) conducted a semi-comprehensive literature review using the PRISMA method to explore common attack methods, strategies for reducing employee susceptibility, and the importance of awareness training. The findings of the study shed light on the serious consequences of data breaches, as evidenced by notable incidents involving Yahoo and Sony. The research highlights that phishing and spear-phishing are particularly prevalent attack methods, taking advantage of human vulnerabilities and evading sophisticated security systems. To effectively mitigate risks, organizations are advised to adopt a multi-layered approach that combines technological solutions with comprehensive employee awareness training.

Smith et al. (2024) evaluated the level of social engineering awareness among university students and staff, using a survey method. Findings revealed that despite general awareness of cyber threats, there remained critical gaps in recognizing sophisticated social engineering tactics, particularly among non-technical staff (Smith et al., 2024). The research emphasized the need for continuous training and awareness programs, tailored to evolving social engineering techniques.

Majid et al. (2021) investigated social engineering awareness within the Saudi educational sector. They developed and assessed a questionnaire to gauge participants' understanding of social engineering. The study, involving 465 respondents, found that 34% (158 individuals) were familiar with social engineering techniques. The results revealed significant differences in security practices and skills between those with prior knowledge and those without, highlighting the need for training to improve awareness within the sector.

Elnaim et al. (2017) assessed students' awareness of social engineering threats at Prince Sattam Bin Abdulaziz University in Saudi Arabia. The study revealed that a significant majority, 72%, of students were unfamiliar with the term "social engineering."

Happ et al. (2016) conducted an experimental study in Luxembourg with 1,208 participants to assess computer security awareness. Participants were asked about their attitudes towards computer security and passwords. The study found that offering a small gift, such as chocolate, significantly increased the likelihood of participants disclosing their passwords.

Ghafir et al. (2021) highlighted the importance of a multi-layered defense, or defense-in-depth, to reduce social engineering attack risks. They advocated for a comprehensive defense strategy that includes security policies, user education, audits, and protection of the network, software, and hardware. The study outlined the four steps of social engineering: information gathering, relationship development, exploitation, and execution.

MATERIALS AND METHODS

This research utilized a quantitative approach, incorporating both surveys and practical experiments. It primarily focuses on phishing and email spoofing as social engineering vectors and employs a study design that provides a cost-effective way to gather data from the target population, consisting of staff and students at Nasarawa State University, Keffi. The methodology and research activities are structured into two phases as outlined below:

Phase 1: Survey method.

The survey method is employed to gather qualitative insights into participants' comprehension of social engineering risks and their confidence in recognizing and addressing such attacks. The questionnaire is organized into four themes to better evaluate awareness levels and respond to the research questions.

Phase 2: Simulated Email Spoofing and Phishing Attack.

Performing simulated email spoofing and phishing attacks can assess how effectively the staff and students of the University can detect and respond to deceptive emails, messages, or phishing URLs. Metrics evaluated include the overall click rate on malicious links, the likelihood of disclosing sensitive information, and the capacity to report suspicious attempts.

The tools that were used for this process are:

i. Django Python framework
ii. MySQL Database system.

Science World Journal Vol. 20(No 4) 2025 https://dx.doi.org/10.4314/swj.v20i4.20
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

iii. Deceptive domain name and URL

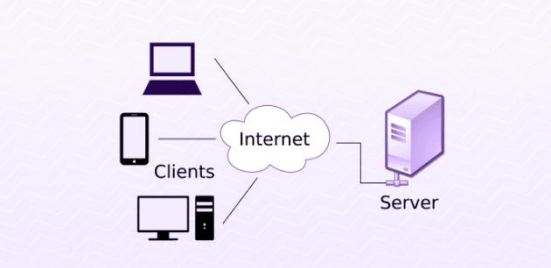

Figure 2: Architecture of the Simulated Phishing website for the experimental purpose.

The activities under this phase include:

i. A cloned NSUKs and Facebook website was developed to look exactly like the legitimate websites.
ii. Email addresses of participants were collected via google forms while answering the survey questions.
iii. Deceptive links of the cloned websites were forwarded to participants' email addresses collected using email spoofing. This enabled the researcher to evaluate the overall click rate on malicious links, susceptibility to providing sensitive information, and the ability to report suspicious attempts.

Population and Sampling Process

This study used convenience sampling, a form of non-probability sampling, where participants were selected based on their proximity to the researcher for ease and speed of collection. This method did not require additional selection criteria. Participation from university staff and students varied depending on their availability and willingness to engage in the survey and practical experiments. The survey questions employed both nominal and interval scales, including both open-ended and closed-ended (multiple choice) formats. To increase response rates, the survey was distributed through social media platforms.

Method of Data Collection

Although there are several primary data collection methods available, such as surveys, questionnaires, interviews, and experiments, this study employed a self-administered questionnaire via Google Forms and practical experiments to collect quantitative data from the Nasarawa State University community. This approach was selected due to the time constraints on the data collection process. The study gathered data directly from primary sources, specifically in its raw form, using Google Forms and practical experimental setups, to evaluate the level of social engineering awareness at Nasarawa State University, Keffi.

Techniques for Data Analysis

The responses collected via Google Form were exported in CSV format to a Google Sheets file. After cleaning and preparing the datasets, the researchers analyzed the data and created visual representations using tables and charts. They utilized Microsoft Excel's pivot tables and SPSS for descriptive statistics to cross-tabulate the data and produce visualizations for analysis.

The analyzed data will be visually presented using charts and figures. Frequency distribution tables will be used to group the data effectively, while column charts will be consistently employed throughout the research to aid in memory retention and enhance understanding of the analysis.

Evaluation Metrics

Evaluation metrics are crucial for assessing an organization's or institution's readiness and resilience against social engineering attacks (Pavlo et al., 2022). The metrics used in this study include: the overall click rate on malicious links, susceptibility to disclosing sensitive information, and the ability to report suspicious social engineering attempts.

RESULTS

This research was carried out to evaluate the level of social engineering awareness within the community of Nasarawa State University, Keffi (NSUK), using a pragmatic approach that combined surveys and experimental techniques. Social engineering remains one of the most dangerous and subtle forms of cybersecurity threats, exploiting human psychology rather than technical vulnerabilities. Understanding how aware individuals are about such threats is critical, especially in academic environments where diverse populations of students, staff, and administrators regularly exchange information and interact with digital technologies.

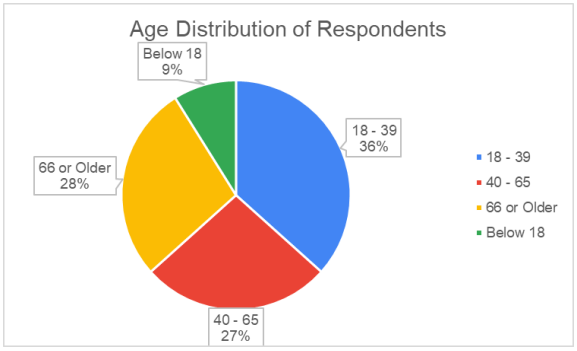

Figure 3: Age distribution of respondents

The study involved a total of 101 participants drawn from different categories within the university. The demographic distribution revealed a diverse mix of respondents in terms of age, gender, and educational background, which enriched the findings by reflecting a broad perspective of the university community. From the analysis, it was observed that 63% of the respondents had no prior knowledge of social engineering or its various attack vectors. This statistic alone underscores the pressing concern that more than half of the academic community is potentially unaware of how such threats operate or how to recognize them. Only 37% of the respondents indicated that they were familiar with social engineering concepts, revealing a generally low level of awareness. This finding directly answered the first research question, which sought to determine the level of awareness within the NSUK community.

Further analysis of attack experiences revealed that phishing was the most dominant form of social engineering attack encountered by respondents. About 50% of participants indicated that they had been victims of phishing, while 28% reported falling prey to email spoofing, and 9% admitted to experiencing pretexting. An additional 13% were unable to identify the exact attack they had faced, which itself points to a lack of proper understanding of social engineering methods. The dominance of phishing as the most

https://dx.doi.org/10.4314/swj.v20i4.20

common threat aligns with global cybersecurity reports that highlight phishing as the most widely used technique by attackers. This directly provided an answer to the second research question.

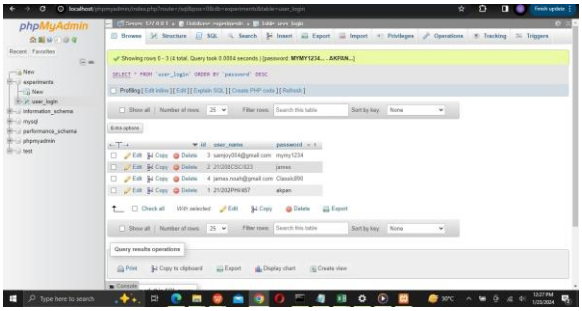

Figure 4: Some acquired info from the experiment' portal backend

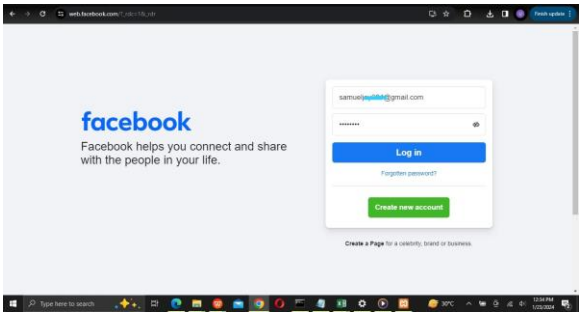

Figure 5: Respondents supplying their login details to a cloned Facebook website.

In addressing the third research question, the findings showed that 53% of respondents could not determine whether their personal computers had been compromised, while only 47% had some level of awareness regarding the status of their systems. This highlights a significant gap in technical know-how, suggesting that even where users may be somewhat familiar with social engineering in theory, their inability to monitor and secure their devices leaves them highly vulnerable.

Finally, in relation to the fourth research question, the study discovered that all respondents (100%) admitted to using public computers or networks to access personal or sensitive information, such as email or social media accounts. This widespread reliance on insecure and shared systems significantly heightens the likelihood of successful social engineering attacks. Experimental evidence from cloned websites and simulated phishing portals confirmed that several respondents unknowingly supplied their login credentials, demonstrating the practical risks posed by these habits.

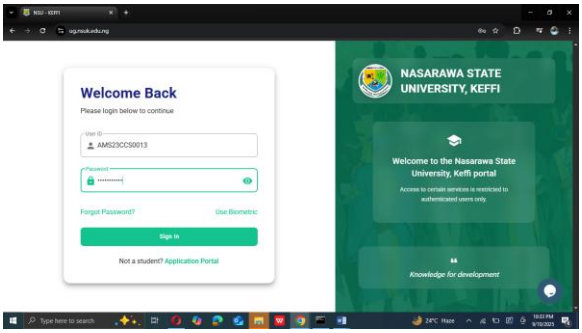

Figure 6: Respondents supplying their login details to a cloned UofA website.

Taken together, the study presents a worrying picture of the NSUK community's vulnerability to social engineering attacks. Limited awareness, the dominance of phishing as an attack vector, insufficient technical literacy, and unsafe practices such as using public computers combine to create an environment where social engineering attacks could easily succeed if not urgently addressed.

DISCUSSION

A comparison with earlier studies (Majid et al., 2021; Pavlo et al., 2022; Abdulla et al., 2023) shows similarities and differences. Like previous research, this study confirmed low awareness levels and phishing as a dominant threat. However, unlike studies that relied heavily on literature reviews or self-reporting, this research used a pragmatic and qualitative approach. While comprehensive, it was constrained by time and resources, which limited focus mainly to phishing and email spoofing.

Comparison Between Existing Studies and This Research.

Several existing studies on social engineering awareness have been conducted across different countries, and their findings provide useful context for understanding the results of the current research. Majid et al. (2021), for example, carried out their study in the Kingdom of Saudi Arabia using a quantitative research approach. Their work contributed significantly to the development of a method for assessing social engineering awareness and reducing the risk of such attacks within the educational sector. However, their study focused predominantly on phishing attacks and was limited to institutions in Saudi Arabia, which affects the generalizability of their findings.

In the Kingdom of the Netherlands, Pavlo et al. (2022) adopted a Systematic Literature Review (SLR) to investigate social engineering vulnerabilities. Their research revealed that many previous experiments in this field were unable to fully replicate real-world social engineering scenarios, highlighting a methodological limitation of relying solely on literature reviews. While their study offered useful insights, the absence of practical, hands-on experiments limited the applicability of their findings.

Similarly, Abdulla et al. (2023) conducted their study in the Republic of Iraq using a self-report methodology. Their findings showed low levels of awareness and limited experience with network security systems among students and staff at the University of Sulaimani. However, the reliance on self-reported data introduced the possibility of response bias, which may have influenced the accuracy and reliability of their results.

In contrast, the present research conducted in 2025 in the Federal Republic of Nigeria employed a pragmatic and qualitative

approach, combining both survey data and experimental techniques. This allowed for a more realistic assessment of actual behaviors and vulnerabilities related to social engineering at Nasarawa State University, Keffi (NSUK). The study successfully identified the current level of social engineering awareness, the most prevalent attack vectors, and the key factors contributing to vulnerability within the university community. Despite its strengths, the research was limited by time and resource constraints, which resulted in a primary focus on phishing and email spoofing attack vectors.

This research has made several contributions to the growing body of knowledge on social engineering awareness, particularly in the Nigerian academic context. First, it provides empirical evidence of the low level of awareness within a university community, quantifying the extent of the problem and providing a basis for comparison with other institutions. Showing that 63% of respondents had no prior exposure to social engineering concepts, the study has drawn attention to a critical educational gap that must be addressed.

Second, the research identifies phishing as the most prevalent social engineering threat in NSUK. This aligns with international studies but also contextualizes the problem within the Nigerian university system. This finding is significant because it allows policymakers and university authorities to design targeted campaigns and technical measures that focus on the most pressing threat rather than attempting to address all possible attack vectors equally.

Third, the study highlights the role of limited technical knowledge in enabling vulnerability. With more than half of respondents unable to tell whether their computers had been compromised, the research demonstrates that awareness must go hand-in-hand with technical literacy. This dual approach—building awareness while improving practical technical competence—provides a new dimension to the conversation on combating social engineering.

Finally, the study contributes by emphasizing the practical risks associated with using public and shared computers. While this is a common practice in many academic settings, the findings provide strong evidence of its dangers, reinforcing the need for improved security protocols for such environments.

REFERENCES

Abdulla, R.H., Faraj, H. A., Abdullah, C. O., Amin, A. H., and Rashid, T. A. (2023). Analysis of Social Engineering Awareness Among Students and Lecturers. IEEE Access, vol. 11, pp. 101098-101111.

Ahmed, Z., Khan, S., & Malik, R. (2023). Automated Machine Learning for Predicting University Student Dropout Rates. Journal of Educational Data Science, 12(1), 45-58.

Aldawood H., and Skinner G (2019) "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues," Future Internet, vol. 11, no. 3, p. 73.

Alghenaim, M. F., Bakar, N. A. A., Yusoff, R. C. M., Hassan, N. H. and Sallehudin, H. (2021). Employee Awareness Model to Enhance Awareness of Social Engineering Threats in the Saudi Public Sector. In 2021 International Congress of Advanced Technology and Engineering (ICOTEN) (pp. 1-6). 4-5 July 2021.

Alhassan, M., Okeke, C., & Yusuf, A. (2024). Cybersecurity awareness in Nigerian universities: Evaluating social engineering risks. Journal of Information Security, 15(2), 112-130.

Annarelli, A., Nonino, F., and Palombi, G. (2020). Understanding the management of cyber resilient systems. Computers and Industrial Engineering, 149, 106829.

Applegate S.D. (2010) Social engineering: hacking the wetware! Information Security Journal: A Global Perspective 18 (1) 40–46

Aridor G., Che Y., and Salz T. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR. SSRN Electronic Journal. doi:10.2139/ssrm

Bandura, A. (2018). Social learning theory. Routledge. Computers & Security, 115, 102677.

Bischoff P. (2020). Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and Youtube. CompariTech. A Global Perspective 18 (1) 40–46

Cindana A. and Ruldeviyani Y. (2024) Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm, 2024 International Conference on Advanced Computer Science and Information Systems (ICACSIS), Yogyakarta, Indonesia, pp. 289-294, doi: 10.1109/ICACSIS.2018.8618219.

Chang K.C., and Seow Y.M.(2014) "Effects of it-culture conflict and user dissatisfaction on information security policy non-compliance: A sense-making perspective," A Global Perspective 18 (1) 40–46

Chitrey A. and Singh D. (2012). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, Vol 6, No 23.

Dalal A. and Amelia R. (2021) A Literature Survey and Analysis on Social Engineering Defense Mechanisms and Infosec Policies. International Journal of Network Security and Its Applications (IJNSA) Vol.13, No.2, March 2021 DOI: 10.5121/ijnsa.. 2021.13204 41

Elnaim B, H. and Al-Lami H. (2017), The current state of phishing attacks against Saudi Arabian university students. International Journal of Computer Applications Technology and Research Volume 6–Issue 1, 42-50, 2017, ISSN:-2319–8656

Ghafir I., Prenosil V., Alhejailan A. and Hammoudeh M. (2021) Social engineering attack strategies and defence approaches, in: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2016, pp. 145–149.

Gupta M., and Sharman R. (2010) Social network theoretic framework for organizational social engineering susceptibility index, AMCIS 2010 Proceedings 408.

Happ C., Melzer A., and Steffgen G. (2016). Trick with treat–reciprocity increases the willingness to communicate personal data, Computers in Human Behaviour 61 (2016) 372–377

Herath, T., & Rao, H. R. (2022). Protection motivation and deterrence: A study on social engineering awareness training. Computers & Security, 115, 102677.

Isaak J. and Hanna M. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer, 51(8), 56–59.

Karakasiliotis A., Furnell S., and Papadaki M. (2016) "Assessing end-user awareness of social engineering and phishing,". Decision Support Systems, 47 (2) 154–165.

Knapp K.J, Morris R.F., Marshall T. E., and Byrd T.A. (2023) "Information Security Policy: An Organizational-level Process Model," Computers and Security, Vol. 28, No. 7, pp. 493–508.

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659-671.

Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., and Morozov, N. V. (2024). The Main Social Engineering Techniques Aimed at Hacking Information Systems. 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). IEEE. 10.1109/ USBEREIT51232.2021.9455031.

Li L., He W., Xu L., Ash I., Anwar M., and Yuan X. (2019) "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," International Journal of Information Management, Vol. 45, No 24 pp. 13–24.

Maddux, J. E., & Rogers, R. W. (2021). Threat perception and self-efficacy: Applying Protection Motivation Theory to cybersecurity behaviors. Cyber Psychology & Behavior, 24(3), 221-240.

Majid H., Fawaz D., Hamdan M., Bandar S., Mohammed M., Majdi E., Khaled G. and Sultan S. (2021) Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. Information 2021, 12, 208.

Matbouli, H., and Gao, Q. (2012*).* An overview on web security threats and impact to e-commerce success. 2012 International Conference on Information Technology and E-Services. IEEE Transactions on Engineering Management, Vol. 69 pp. 3726-3738

Mitnick, K. D., & Simon, W. L. (2022). The art of deception: Controlling the human element of security. John Wiley & Sons.

Mitnick Security (2023) The top 5 most famous social engineering attack of the last decade [Online]. (Accessed: 03 April, 2022)

Mumtaz H., Samrina S. and Noman I. (2023) Social Engineering and Data Privacy. Available at: https://www.researchgate.net/publication/367484714 Accessed 3rd June, 2023.

Norrman K., Näslund M., and Dubrova E. (2024). Protecting IMSI and User Privacy in 5G Networks. 9th EAI International Conference on Mobile Multimedia Communications. EUDL. 10.4108/eai.18-6-2016.2264114

Pavlo, P., Ahmed, A., & Benson, D. (2022). Social Engineering Awareness and Resilience in Academic Institutions. Cybersecurity in Education Journal, 10(4), 199-213.

Robert B. and Philip S. (2023) The Human Element of Cybersecurity: A Literature Review of Social Engineering Attacks and Countermeasures.DiVA. Dalarna University – SE-791 88.

Salahdine, F. and Kaabouch, N. (2024) Social Engineering Attacks: A Survey. Future Internet, 11, 89.

Sharma, R., & Gupta, P. (2023). The human firewall: Strengthening cybersecurity through employee training and awareness. Cybersecurity Journal, 18(1), 45-62.

Siponen M., Mahmood M.A., and Pahnila S. (2019) "Employees' adherence to information security policies: An exploratory field study," Information and management, Vol. 51, No. 2, pp. 217–224.

Smith, J., Johnson, R., and Davis, L. (2024). Social engineering awareness evaluation in higher education institutions: A pragmatic approach. Journal of Cybersecurity and Education, 29(3), 112-130.

Soni V.D. (2020) "Disaster recovery planning: Untapped success factor in an organization," Available at SSRN 3628630.

Surfshark (2023) Data breach statistics 2023'Q1 vs. 2022'Q4. Available at: https://surfshark.com/research/study/data-breach-statistics-2023-q1 Accessed: 3rd June, 2023.

Telford, T. (2024). Thousands of Disney Plus accounts were hacked and sold online for as little as $3. Washington post. IEEE Transactions on Engineering Management, Vol. 69, No 2, pp. 3726-3738

Wenni S., Zarina S., Umi-Asma M, Rossilawati S., and Muhammad A. (2024) Social Engineering Attacks Prevention: A Systematic Literature Review. IEEE Access. doi: 10.1109/ACCESS.2022.3162594

West, J. (2023). Cybersecurity education and awareness: Leveraging social learning for behavior change. Information Security Review, 12(4), 301-315.