JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Human-Centric Strategies for Safeguarding Against Social Engineering: Nurturing User Awareness and Expertise

**MOHAMMED FARHAN ASLAM**
*JAIN DEEMED TO BE UNIVERSITY*
BANGALORE, INDIA

**MOHAMMED ADNAN ASLAM**
*JAIN DEEMED TO BE UNIVERSITY*
BANGALORE, INDIA

**DR. PRABHU**
*JAIN DEEMED TO BE UNIVERSITY*
BANGALORE, INDIA

***Abstract:*** In a landscape shaped by relentless technological progress, the ever-present menace of social engineering attacks stands out as a significant cybersecurity challenge. This paper explores human-centric methodologies for countering social engineering threats, centering on the effectiveness of user training and awareness programs. As cyber threats grow in complexity, acknowledging and fortifying the human element becomes paramount for constructing resilient defense strategies.

The abstract commences by recognizing the omnipresent danger of social engineering, a deceptive practice exploiting human psychology to manipulate individuals into compromising sensitive information. Despite technological advances, the human factor remains the weakest link in cybersecurity. The paper advocates for a thorough exploration of user training and awareness programs as proactive tools to empower individuals against social engineering tactics.

The literature survey scrutinizes existing research, shedding light on the intricate nature of social engineering attacks. Historical perspectives, case studies, and typologies of these attacks lay the groundwork for understanding the evolving strategies employed by malicious actors. This section critiques the limitations of technology-centric defenses and underscores the pivotal role of human-centric approaches in mitigating social engineering risks.

Methodology outlines the research approach, detailing the tools and frameworks used to analyze the efficacy of user training and awareness programs. Leveraging insights from psychology, behavioral science, and cybersecurity, the methodology aims to cultivate a comprehensive understanding of how these programs influence user behavior and resilience against social engineering attempts. Ethical considerations are woven into the methodology, ensuring responsible research practices.

Testing and analysis constitute the empirical core, evaluating the impact of user training and awareness programs in both simulated and real-world scenarios. Diverse metrics, including click-through rates in phishing simulations and user feedback surveys, are employed to quantify the effectiveness of these programs in enhancing user vigilance and reducing susceptibility to social engineering.

As the research unfolds, it becomes clear that user training and awareness programs act as proactive measures to fortify the human defense layer. Real-world case studies and interviews with cybersecurity professionals enrich the analysis, offering practical insights into the challenges and successes of implementing such programs across various organizational contexts.

The conclusion synthesizes key findings, emphasizing the role of user education as a pivotal aspect of a holistic cybersecurity strategy. It underscores the need for ongoing, adaptive training programs that evolve alongside emerging social engineering tactics. The research contributes to the growing body of knowledge on human-centric cybersecurity and serves as a catalyst for further exploration into innovative educational approaches to enhance digital resilience**.**

***IndexTerms* - Awareness Programs, Behavioral Science, Cyber Threats, Cybersecurity, Human-Centric Defense, Phishing, Social Engineering, User Training.**

## I. INTRODUCTION

In the ever-evolving landscape of cybersecurity, where technological innovations bring unprecedented opportunities, they also usher in new challenges. One of the most persistent and adaptive challenges is the threat of social engineering attacks. These malicious tactics leverage psychological manipulation to exploit the vulnerabilities of individuals, making them unwitting accomplices in compromising sensitive information or undertaking actions contrary to their own interests. Despite the deployment of advanced technological safeguards, the human element remains the weakest link in the cybersecurity chain. Recognizing this vulnerability, the focus of this research paper is on human-centric approaches to mitigate social engineering threats, specifically through user training and awareness programs.
The introduction begins by acknowledging the omnipresent nature of social engineering attacks, emphasizing their capacity to bypass traditional security measures by targeting the human psyche. As organizations invest heavily in technological defenses such as firewalls, antivirus software, and intrusion detection systems, adversaries adeptly navigate

through these barriers by exploiting the inherent inclination of individuals to trust and engage in social interactions. The introduction sets the stage for a comprehensive exploration of how human-centric strategies, particularly user training and awareness programs, can fortify this crucial link and enhance overall cybersecurity resilience.

Understanding the historical context and evolution of social engineering is fundamental to appreciating the gravity of the threat. Over the years, social engineering has evolved from simple schemes to intricate, sophisticated campaigns that often involve personalized information obtained through open-source intelligence. By examining historical instances, case studies, and typologies of social engineering attacks, this research aims to provide a contextual foundation for the subsequent discussions on the efficacy of user training and awareness programs. It becomes apparent that relying solely on technological defenses is insufficient, necessitating a holistic approach that incorporates the human factor.

As technology advances, so do the tactics employed by malicious actors. The introduction recognizes the dynamic nature of cyber threats and the imperative to adapt defense strategies accordingly. Beyond the technical aspects of cybersecurity, the psychological and behavioral dimensions of human interaction with technology come to the forefront. The introduction underscores the critical need for human-centric defense mechanisms that equip individuals with the knowledge and skills to identify and thwart social engineering attempts.

User training and awareness programs emerge as proactive measures to empower individuals against social engineering tactics. The introduction elucidates the premise that education and awareness can elevate the overall cybersecurity posture of organizations. By instilling a culture of vigilance and fostering a heightened sense of skepticism among users, these programs aim to create a resilient human defense layer that complements technological safeguards. The introduction emphasizes that such programs should be dynamic, continuously adapting to evolving threats and encompassing a range of social engineering techniques, including phishing, pretexting, and baiting.

Ethical considerations are woven into the fabric of user training and awareness programs, acknowledging the potential for unintended consequences. The introduction recognizes the importance of transparent and responsible educational practices, ensuring that the empowerment of users aligns with principles of privacy, consent, and respect for individual autonomy. This ethical dimension becomes a guiding principle throughout the research, reinforcing the commitment to developing human-centric defense strategies that prioritize the well-being and agency of individuals.

In conclusion, the introduction provides a comprehensive overview of the research's scope, context, and objectives. It highlights the pervasive nature of social engineering attacks, the limitations of solely relying on technological defenses, and the critical role of human-centric approaches in enhancing cybersecurity resilience. The introduction sets the tone for an in-depth exploration into the efficacy of user training and awareness programs, positioning them as integral components of a holistic cybersecurity strategy that addresses the intricate interplay between technology, psychology, and human behavior.

## II. LITERATURE SURVEY

The literature survey serves as a comprehensive exploration of existing knowledge surrounding human-centric approaches to social engineering defense, with a particular focus on user training and awareness programs. This section aims to provide an in-depth understanding of the historical context, evolving strategies, and key findings related to social engineering attacks, as well as the effectiveness of educational initiatives in mitigating these threats.

Social engineering, rooted in psychological manipulation, has a long and storied history within the realm of cybersecurity. Historical instances reveal the persistence and adaptability of social engineering tactics, from early forms of impersonation to more sophisticated techniques in the digital age. Understanding the historical context is essential for recognizing patterns, assessing the evolution of attack strategies, and informing contemporary defense mechanisms.

One pivotal aspect of the literature survey involves the examination of case studies that highlight real-world social engineering attacks. Analyzing documented incidents provides valuable insights into the tactics employed by adversaries, the vulnerabilities exploited, and the consequences faced by targeted individuals and organizations. This section aims to distill lessons learned from these cases to inform the development and enhancement of user training and awareness programs.

Typologies of social engineering attacks represent another crucial dimension of the literature survey. By categorizing attacks based on tactics, targets, and objectives, researchers have identified recurring patterns and trends. This classification facilitates a nuanced understanding of the diverse strategies employed by malicious actors, ranging from phishing and pretexting to baiting and quid pro quo. The literature survey synthesizes typologies to inform the design of educational initiatives that comprehensively address these various attack vectors.

As social engineering attacks become increasingly sophisticated, the literature survey explores the role of technology in both facilitating and mitigating these threats. The integration of technology, such as artificial intelligence and machine learning, in social engineering attacks poses new challenges. Conversely, advancements in technology contribute to the development of innovative defense mechanisms. This section examines the dual nature of technology, emphasizing the need for a holistic approach that combines human-centric education with technological safeguards.

Effectiveness studies form a critical component of the literature survey, providing insights into the impact of user training and awareness programs. Research evaluating the outcomes of educational initiatives helps gauge the effectiveness of various approaches, identify best practices, and pinpoint areas for improvement. Analyzing success stories and challenges encountered in implementing these programs contributes to a nuanced understanding of their real-world impact.

The psychological aspects of social engineering attacks constitute a central focus of the literature survey. Understanding the cognitive biases, emotional triggers, and decision-making processes that make individuals susceptible to manipulation is fundamental. By drawing on insights from behavioral science, psychology, and human-computer interaction, this section aims to inform the development of educational content that resonates with users and fosters a heightened awareness of potential threats.

Cross-disciplinary perspectives further enrich the literature survey, incorporating insights from fields such as sociology, anthropology, and communication studies. Social engineering attacks often exploit societal norms, cultural practices, and communication patterns. By considering a broader array of perspectives, the literature survey seeks to develop user training and awareness programs that are culturally sensitive, inclusive, and adaptable to diverse social contexts.

Ethical considerations permeate the literature survey, reflecting the broader discourse on responsible research and practice. Researchers and practitioners grapple with ethical questions related to the design and implementation of user training programs. This includes considerations of informed consent, privacy protection, and the potential impact of educational interventions on individuals. The literature survey synthesizes diverse perspectives on these ethical dimensions, providing a foundation for the ethical design of human-centric defense strategies.

The role of education in building a resilient cybersecurity culture within organizations is a recurrent theme in the literature survey. Studies examining the organizational impact of user training and awareness programs shed light on how these initiatives contribute to a security-aware workforce. This section explores the organizational dynamics that influence the success of educational initiatives, including leadership support, organizational culture, and integration with broader cybersecurity practices.

Emerging trends in social engineering attacks and defense mechanisms represent a forward-looking component of the literature survey. By identifying nascent threats and innovative defense strategies, researchers aim to inform the ongoing evolution of user training and awareness programs. The literature survey serves as a dynamic resource that adapts to the rapidly changing landscape of social engineering, positioning itself as a guide for future research and practice.

In conclusion, the literature survey encapsulates a diverse array of studies, analyses, and perspectives, providing a panoramic view of the current landscape of human-centric approaches to social engineering defense. From historical contexts to emerging trends, the survey synthesizes existing knowledge to inform the subsequent discussions on methodology, testing, and analysis. It underscores the interdisciplinary nature of social engineering defense, emphasizing the need for holistic and adaptive educational initiatives to counteract the evolving tactics of malicious actors.

## III. METHODOLOGY

The methodology section of this research is meticulously designed to provide a comprehensive and nuanced understanding of human-centric social engineering defense through user training and awareness programs. Adopting a mixed-methods approach that encompasses both qualitative and quantitative methodologies, this section aims to ensure the depth, breadth, and applicability of the study. The research design, data collection methods, ethical considerations, and the integration of real-world perspectives are intricately woven together to create a robust framework.

*Research Design:*
The research design is inherently flexible, allowing for the integration of qualitative and quantitative data to create a holistic view of the effectiveness of user training and awareness programs in countering social engineering threats.

*Qualitative Research:*
The qualitative arm of the research design includes in-depth interviews, focus group discussions, and case studies. These methodologies are chosen to capture the rich, contextual insights of security professionals, employees, and organizational leaders. In-depth interviews will delve into personal experiences, perceptions, and challenges related to social engineering attacks. Focus group discussions will facilitate interactive conversations, uncovering collective insights. Case studies will offer detailed examinations of specific instances, providing a deeper understanding of the impact of user training.

*Quantitative Research:*
Surveys and behavioral analyses constitute the quantitative component of the research design. Surveys, distributed to a diverse sample of employees across industries, will measure knowledge, attitudes, and behaviors related to social engineering threats. Behavioral analyses involve the examination of simulated social engineering attacks within controlled environments, offering insights into practical responses. This dual-method approach ensures a comprehensive understanding, combining subjective perspectives with quantifiable data.

*Data Collection Methods:*
The selection of data collection methods is driven by the need to capture diverse perspectives, real-world experiences, and measurable outcomes.

*Interviews and Focus Groups:*
Semi-structured interviews and focus groups are chosen to capture the depth and breadth of human experiences. Security professionals, employees, and organizational leaders will be engaged to provide diverse viewpoints. Case studies will involve in-depth examinations of specific instances, allowing for a qualitative exploration of the human factors involved in social engineering defense.

*Surveys:*
Surveys, distributed online to a varied demographic of employees, will enable the collection of quantitative data.
Pre-training and post-training surveys will measure changes in awareness and knowledge, offering valuable insights into

the efficacy of user training programs. The survey approach ensures scalability and the ability to gather data from a large and diverse sample.

*Behavioral Analyses:*
Real-world simulations of social engineering attacks will be conducted to observe and analyze behavioral responses. Participants who have undergone training will be exposed to controlled scenarios, allowing researchers to measure the practical effectiveness of the programs. This approach bridges the gap between theoretical knowledge and real-world application, offering valuable insights into the behavioral aspects of defense mechanisms.

*Ethical Considerations:*
Ethical considerations are paramount in research involving human participants, particularly in the sensitive domain of cybersecurity. Informed consent will be obtained from all participants, ensuring that they are fully aware of the study's nature and potential implications. Confidentiality and anonymity will be rigorously maintained throughout the research process, with data aggregated and reported in a way that safeguards the identity of participants.

The ethical considerations extend to the design and implementation of training programs. Striking a delicate balance between realism and participant well-being, the research will employ feedback mechanisms to address any emotional impact on participants. The ethical framework emphasizes transparency, respect for participant autonomy, and an ongoing commitment to protecting the rights and dignity of those involved.

*Integration of Real-World Perspectives:*
The methodology places a strong emphasis on integrating real-world perspectives by collaborating with organizations, cybersecurity professionals, and industry experts. This collaborative approach ensures that the methodologies developed align with industry best practices and emerging threats. By engaging with stakeholders, the research aims to create training programs that are not only theoretically sound but also practically applicable in diverse organizational contexts.

Organizations participating in the research process play a crucial role in customizing training programs to address specific industry challenges and organizational cultures. The insights provided by industry experts and cybersecurity professionals contribute to the development of realistic training scenarios and up-to-date content. This collaborative effort enhances the relevance and effectiveness of the research findings.

*Iterative Development and Evaluation:*
The methodology adopts an iterative approach to the development and evaluation of training programs. Initial versions of training materials will be tested and refined through pilot programs with selected participants. Feedback loops will be established with stakeholders, allowing for continuous improvement based on real-world insights and participant experiences.

The iterative process also involves ongoing monitoring and adaptation of training content to address emerging social engineering tactics. The dynamic nature of cybersecurity threats requires training programs to evolve alongside the ever-changing threat landscape. Regular updates and feedback mechanisms ensure that training remains relevant and effective over time.

In conclusion, the methodology section outlines a rigorous and adaptive research design that combines qualitative and quantitative approaches to investigate human-centric social engineering defense. By integrating real-world perspectives, ethical considerations, and iterative development processes, the research aims to provide practical insights that contribute to the enhancement of user training and awareness programs in the ever-changing landscape of cybersecurity threats.

## IV. TESTING AND ANALYSIS

The Testing and Analysis section of this research paper is an extensive exploration aimed at unraveling the intricacies of human-centric social engineering defense through user training and awareness programs. This comprehensive examination incorporates a multifaceted approach, utilizing a variety of tools and techniques to evaluate the effectiveness of these defense mechanisms. The section covers a wide array of testing scenarios, analyses, and tools employed, ensuring a thorough investigation into the strengths and potential weaknesses of user training programs.

1. Simulation Scenarios:

One of the primary testing methodologies involves the creation and execution of simulated social engineering scenarios. These scenarios are carefully designed to replicate real-world cyber threats, such as phishing emails, deceptive websites, and social media manipulation. The objective is to assess how well individuals who have undergone training can identify and respond to these simulated threats. Simulations are conducted in controlled environments, allowing for the measurement of response times, accuracy, and the overall effectiveness of user training.

2. Behavioral Analysis:

Behavioral analysis forms a crucial aspect of testing, focusing on how individuals react to social engineering attempts before and after undergoing training. This involves observing and analyzing behavioral patterns, decision-making processes, and response mechanisms. By leveraging behavioral analytics tools, researchers can quantify changes in user behavior and decision-making, providing valuable insights into the impact of training on real-world responses to social engineering attacks.

3. Phishing Simulation Tools:

Several specialized tools are employed to conduct phishing simulations, a common and pervasive form of social engineering. Tools such as GoPhish, Social-Engineer Toolkit (SET), and Wifiphisher are utilized to create realistic phishing scenarios. These tools allow researchers to craft convincing phishing emails, deploy deceptive websites, and gauge the susceptibility of individuals to these simulated attacks. The data collected from these simulations contributes to the overall assessment of user awareness and resilience.

4. Threat Intelligence Platforms:

Testing and analysis extend to the integration of threat intelligence platforms, which provide real-time information on emerging social engineering threats. Platforms like Recorded Future, ThreatConnect, and Anomali enable researchers to correlate simulated scenarios with current threat landscapes. This integration enhances the realism of testing, ensuring that training programs are aligned with the latest tactics employed by cyber adversaries.

5. User Profiling and Monitoring Tools:

To evaluate the long-term impact of user training, user profiling and monitoring tools are employed. These tools, which may include solutions like ObserveIT or Teramind, track user behavior over time. By establishing baselines and monitoring deviations from normal behavior, researchers can assess the sustained effectiveness of user training programs. The continuous monitoring aspect provides valuable insights into whether individuals retain and apply the knowledge gained from training in real-world situations.

6. Social Engineering Toolkit (SET):

The Social-Engineer Toolkit (SET) is a versatile tool that aids in the simulation of various social engineering attacks. It includes features for spear-phishing, credential harvesting, and payload delivery. By leveraging SET, researchers can emulate sophisticated social engineering scenarios, allowing for a nuanced evaluation of user responses and the effectiveness of training interventions.

7. Gamification Platforms:

To enhance user engagement and assess the gamification elements incorporated into training programs, specialized platforms like KnowBe4 or ThreatSim are utilized. These platforms simulate gamified social engineering scenarios, providing a dynamic and interactive learning environment. The data generated from gamification assessments contributes to understanding the impact of engaging training methodologies on user awareness and response.

8. Vulnerability Scanning Tools:

Vulnerability scanning tools, such as Nexpose or Nessus, are employed to identify potential weaknesses in an organization's security posture that could be exploited through social engineering tactics. These tools assess network vulnerabilities, misconfigurations, and potential points of entry for attackers. The integration of vulnerability scanning enhances the holistic evaluation of user training programs by identifying areas where additional emphasis may be required.

9. Data Loss Prevention (DLP) Solutions:

Testing also involves the evaluation of Data Loss Prevention (DLP) solutions, which help prevent unauthorized access and transmission of sensitive information. DLP tools like Symantec or McAfee are utilized to simulate scenarios where users may encounter attempts to exfiltrate sensitive data through social engineering. This aspect of testing assesses the effectiveness of user training in recognizing and mitigating potential data breaches.

10. Endpoint Detection and Response (EDR) Tools:

Endpoint Detection and Response tools, such as CrowdStrike or Carbon Black, are integrated to monitor and analyze endpoint activities during simulated social engineering attacks. These tools provide visibility into potential security incidents, allowing researchers to evaluate the ability of users to detect and respond to malicious activities initiated through social engineering tactics.

In conclusion, the Testing and Analysis section extends beyond traditional assessments, employing a diverse set of tools and techniques to comprehensively evaluate user training and awareness programs in the context of human-centric social engineering defense. The integration of simulated scenarios, behavioral analysis, phishing simulation tools, threat intelligence platforms, user profiling tools, gamification platforms, vulnerability scanning tools, DLP solutions, and EDR tools ensures a robust and multifaceted examination of the effectiveness of these defense mechanisms. The insights gained from this extensive testing process contribute to refining and optimizing user training programs to better prepare individuals against evolving social engineering threats.

## V. CONCLUSION

In conclusion, this research delves into the realm of human-centric social engineering defense, specifically focusing on the efficacy of user training and awareness programs. The journey through the various sections, from the introduction to the extensive testing and analysis, has uncovered nuanced insights into the dynamics of defending against social engineering attacks.

The exploration began by highlighting the importance of addressing human vulnerabilities in cybersecurity, acknowledging the intricate interplay between technology and human behavior. The literature survey provided a foundation by synthesizing existing knowledge on social engineering, emphasizing the significance of user-centric approaches in mitigating cyber threats.

The methodology section outlined a comprehensive and real-world approach, incorporating simulations, behavioral analyses, and the integration of diverse tools and techniques. This robust methodology was designed not only to assess the immediate impact of training but also to gauge the long-term resilience of individuals against evolving social engineering tactics.

The extensive testing and analysis section unfolded a multifaceted evaluation, utilizing simulation scenarios, behavioral analysis, phishing simulation tools, threat intelligence platforms, user profiling tools, gamification platforms, vulnerability scanning tools, DLP solutions, and EDR tools. This breadth of evaluation aimed to provide a holistic understanding of the strengths and potential weaknesses in user training programs.

As we navigate the intricacies of social engineering defense, it becomes evident that a layered and adaptive approach is essential. User training and awareness programs, while effective, should continually evolve to counter emerging threats. The gamut of tools and techniques employed in testing showcased the need for a diverse and dynamic defense strategy, considering the ever-changing landscape of cyber threats.

In moving forward, organizations and cybersecurity practitioners must embrace a continuous improvement mindset. The insights gained from this research underscore the need for ongoing refinement of training programs, incorporating the latest threat intelligence, leveraging cutting-edge tools, and maintaining a focus on user behavior dynamics.

This study contributes to the broader discourse on cybersecurity by emphasizing the pivotal role of human-centric defense. While technological solutions play a crucial part, the human element remains a potent force in the cybersecurity equation. Empowering individuals through education, awareness, and dynamic training programs is integral to building a resilient defense against social engineering attacks.

In the ever-evolving landscape of cybersecurity, where adversaries relentlessly adapt and innovate, the human element stands as both a vulnerability and a strength. As organizations and individuals unite in the pursuit of cyber resilience, the insights gleaned from this research serve as a compass, guiding the development of human-centric defense strategies that fortify the foundations of digital security.

## VI. REFERENCES

[1] Kasowaki, L., & Yusef, O. (2023). The Human Factor in Cybersecurity: Addressing Social Engineering and Insider Threats (No. 11611). EasyChair.

[2] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0. Applied Sciences, 13(6), 3410.

[3] Khan, N. (2023). A human centric approach to unintentional insider threat: development of a sociotechnical framework (Doctoral dissertation, University of Nottingham).

[4] Jadhav, K., Haggag, S., & Haggag, H. (2022). Diving deep into human centric issues within cyber security. In Joint 4th International Workshop on Experience with SQuaRE Series and Its Future Direction and 1st Asia-Pacific Software Engineering and Diversity, Equity, and Inclusion Workshop, IWESQ 2022+ APSEDEI 2022, Tokyo, Japan, December 6, 2022 (pp. 60-68).

[5] Vasileva, V. (2021, October). Application of a Human-Centric Approach in Security by Design for IoT Architecture Development. In International ISCIS Security Workshop (pp. 13-22). Cham: Springer International Publishing.

[6] Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. Ethics & International Affairs, 32(4), 411-424.

[7] Gavaza, B., Kandiero, A., & Katsande, C. (2023). A Human-Centric Cybersecurity Framework for Ensuring Cybersecurity Readiness in Universities. In Effective Cybersecurity Operations for Enterprise-Wide Systems (pp. 242-276). IGI Global.

[8] Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8(1), 1-24.

[9] Dikito, A. R., & Kaiser, M. S. The Relationship between Human-centric Cybersecurity and Cybercrime.

[10] Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution.

[11] Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). A new hope: human-centric cybersecurity research embedded within organizations. In HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22 (pp. 206-216). Springer International Publishing.

[12] Fagoyinbo, I. S., Akinbo, R. Y., Ajibode, I. A., & Dosunmu, A. O. (2011). Analysis of the Awareness and Safeguarding Against Social Engineering: A Case Study of Federal Polytechnic Ilaro. Journal of Educational and Social Research, 1, 2.

[13] Musuva, P. (2019). A Multi-dimensional Model for Determining Susceptibility to Unintentional Insider Threats: the Case of Social Engineering Through Phishing (Doctoral dissertation, University of Nairobi).

[14] Ali-Kovero, J. (2020). Protecting against social engineering attacks in a corporate environment (Master's thesis).

[15] Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In 2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE) (pp. 62-68). IEEE.