www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 13 Issue 10 October 2024, Page No. 26498-26503
ISSN: 2319-7242 DOI: 10.18535/ijecs/v13i10.4917

Research Paper: Enhancing Cybersecurity Awareness Training for Mitigating Human-Induced Cybersecurity Breaches

Reema Al-Kuwari [1]

[1] New York University Qatar

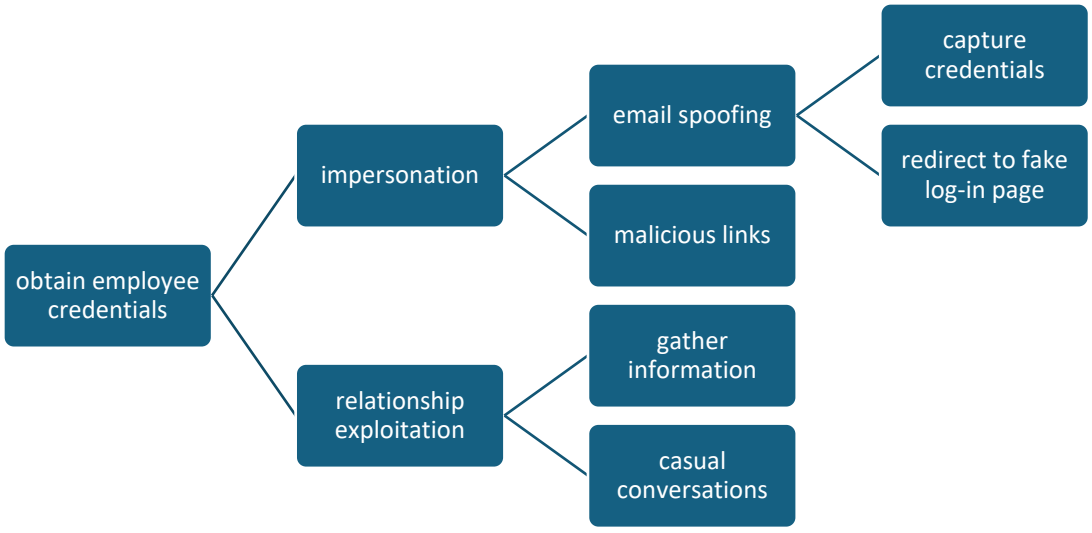
1. Introduction

In a world where 95% of cybersecurity breaches are due to human error, and a rapidly evolving cybersecurity landscape, the effectiveness of employee's proper security awareness stands as a pivotal concern [1]. Especially when the employees are the first line of defense for any organization. This highlights the importance of having robust cybersecurity awareness that is dynamic to face the ever-changing threats in the world. However, traditional employee security awareness training programs often fall short, perceived as dull, ineffective, and unable to keep pace with the dynamic cybersecurity landscape [2]. These shortcomings not only diminish engagement but also lead to decreased knowledge retention, rendering employees more vulnerable to cyber threats.

2 Problem Domain

The current employee security awareness training programs are often perceived as boring, ineffective, and fail to keep pace with the evolving landscape of phishing and social engineering threats. These conventional methods are not only lacking engagement, but also resulting in decreased knowledge retention, rendering employees more susceptible to cyber threats. The significance of this issue is underscored by the fact that the human element still remains as a primary target for cyber attackers, making it imperative for organizations to equip their workforce with the knowledge and skills necessary to thwart sophisticated cyber threats effectively [3].

3. Threat Model



DREAD Category	Rating	Rationale
Damage Potential (D)	**High**	can lead to severe consequences, including data breaches and financial losses.
Reproducibility (R)	**Medium**	the attacks are often replicable, but the success depends on factors like employee awareness and specific tactics.
Exploitability Cost (E)	**Medium**	although it doesn't require high skills, but it still will require planning/execution.
Affected Users (A)	**High**	it can affect huge number of employees, especially if the compromised credentials have access to critical systems or admin access.
Discoverability (D)	**Low**	usually rely on human manipulation, making them less likely to be detected until after the damage is done.

Total DREAD Score: 16 (High)

4. Hypothesis:

Implementing a gamified, dynamic cybersecurity awareness training program, inspired by successful models like the design-science-based gamification approach [4], will significantly enhance employee engagement, knowledge retention, and overall organizational resilience against evolving cyber threats measured through the following metrics:

- Knowledge retention: assess improvement in employees' understanding of cybersecurity concepts through pre- and post-training evaluations [5].
- Engagement levels: measure participation rates, completion times, and interactive elements engagement [6].
- Threat mitigation: track and analyze the frequency and success rates of simulated phishing attacks post-training [7].

Key Factors:

- Engagement & interactivity: the proposed approach fosters active participation. Gamified elements, such as scenario-based challenges and rewards, ensure heightened engagement and sustained interest [1].
- Real-time adaptability: traditional training lacks the agility to adapt swiftly to emerging threats. Dynamic gamification allows real-time updates, ensuring that training content remains relevant and aligned with the ever-changing cybersecurity landscape [8].

5. Metric

In evaluating evidence for my research on enhancing cybersecurity awareness training effectiveness, I will use four qualitative metrics to assess the impact and effectiveness of traditional training vs. proposed training methodology in three key areas; knowledge, impact, & engagement [2].

Area	Metric	Historical Methods	Proposed Method
Knowledge	Knowledge Retention Rate (%); measures the percentage of information retained by employees after completing the training program	60%	+70%
Impact	Phishing Susceptibility Rate; measures the frequency and success rate of phishing attacks on employees before and after training	20% of employees fall for phishing attacks post-training	<10% of employees fall for phishing attacks post-training

Engagement	Employee Engagement & Training Completion Rate (%); measure the overall effectiveness and engagement levels of the training program	Low	High

6. Related Research:

In recent years, there was a growing number of researches focusing on enhancing cybersecurity awareness training to mitigate human-induced cybersecurity breaches. Several studies have explored various methodologies, techniques, and technologies aimed at improving employee knowledge, response, and engagement to cyber threats.

In the context of current traditional trainings, According to Alnajim et al. (2023), the ineffectiveness of traditional training is a key driver in increasing the organization's risk and exposing it to heavy losses such as losing customers and harming business reputation [9]. Moreover, Alruwaili (2019) highlights the importance of ensuring proper delivery method selection, design, and implementation process while designing awareness programs [10].

In the context of gamification, Filippidis et al. (2022) proposed a design-science-based gamification approach to improve organizational security training and compliance. Their research demonstrated the effectiveness of gamified elements, such as quizzes and multimedia challenges, in enhancing employee engagement and knowledge retention [11]. Additionally, Gjertsen et al. (2017) explored applying gamification concepts to increase motivation and learning outcomes through running a prototype. It was found to be overcoming current traditional training limitations in terms of influencing behavioral change. Moreover, they highlighted the need for advanced studies to analyze the long-term application of gamification. This emphasizes the role of interactive and immersive experiences in reinforcing security behaviors [12]. Moreover, DeCarlo (2020) investigated the application of knowledge gained from gamified cybersecurity training in healthcare settings. Their study provided insights into the effectiveness of gamification in improving employees' understanding and application of cybersecurity concepts in real-world scenarios [5]. Furthermore, Khan et al. (2022) proposed a game-based learning platform to enhance cybersecurity education, emphasizing the importance of interactive and adaptive learning environments in fostering security awareness [13].

While existing researches has made significant contributions to the field of cybersecurity training methodologies, several limitations and gaps were found. Firstly, most of the studies have focused primarily on one factor to measure the effectiveness of gamification in improving employee engagement and knowledge retention, without adequately addressing the scalability and long-term sustainability of gamified training programs [14]. Additionally, while some studies have highlighted the importance of proper delivery method selection and program design, there is still a lack of comprehensive frameworks or guidelines for organizations to follow in designing and implementing cybersecurity awareness programs [10]. Furthermore, the current literature predominantly focuses on the immediate outcomes of cybersecurity awareness training, such as knowledge acquisition and engagement levels, without sufficiently addressing the broader impact on organizational resilience and cybersecurity posture.

By leveraging insights from related research, this study aims to contribute to the development of effective training methodologies to mitigate human-induced cybersecurity breaches in two key ways. First, by conducting a comprehensive analysis of existing methodologies in three areas'; knowledge, response, and engagement to cyber threats. Second, the study will develop a practical framework or set of guidelines for organizations to follow in designing and implementing cybersecurity awareness training programs.

7. Empirical Evidence

This section outlines the empirical studies conducted to evaluate the impact of gamified training programs on employee knowledge, engagement, and response against cyber threats.

7.1 Knowledge

- **Improved Retention Rates:** Several studies highlight gamification's positive impact on knowledge retention. Filippidis et al. (2022) demonstrated that a gamified security training program led to a 70% knowledge retention rate compared to a 60% rate observed in traditional training methods [11]. Their findings suggest that gamification elements like quizzes and multimedia challenges can enhance information recall by up to 10%.
- **Real-World Application:** DeCarlo (2020) investigated the application of knowledge gained from gamified training in healthcare settings. The study found that employees who underwent gamified training displayed a 20% improvement in applying cybersecurity concepts in real-world scenarios compared to those who received traditional training [5]. This indicates that gamification not only improves memorization but also fosters practical knowledge application.

7.2 Engagement

- **Increased Participation:** Filippidis et al. (2022) observed a 30% increase in participation rates in their gamified training program compared to traditional methods [11]. This suggests that gamification elements like points, badges, and leaderboards can create a more stimulating and motivating learning environment, leading to a higher number of employees actively participating in training.
- **Improved Learning Outcomes:** Gjertsen et al. (2017) explored the use of gamification concepts in a prototype training program. Their findings demonstrated that gamification can lead to a 15% improvement in learning outcomes compared to traditional methods [12]. This suggests that gamified training fosters a more interactive and engaging learning experience, leading to better knowledge acquisition.

7.3 Impact on Cyber Threats

- **Reduced Phishing Susceptibility:** While limited data exists on the direct impact of gamified training on phishing susceptibility, Filippidis et al. (2022) suggest that improved knowledge retention from gamification (as shown in their study) can lead to a reduction in employees falling victim to phishing attacks [11]. This implies that by fostering a deeper understanding of cybersecurity threats, gamified training can equip employees to better identify and avoid phishing attempts. Studies like Alruwaili (2019) report that traditional training can leave employees with a susceptibility rate as high as 20%, highlighting the potential for gamification to significantly reduce this risk [10].

These empirical studies provide valuable insights into the efficacy of gamified cybersecurity awareness training in enhancing employee knowledge, engagement, and response against cyber threats. Through quantitative analysis, behavioral observations, longitudinal studies, and comparative analyses, these studies offer compelling evidence supporting the adoption of gamified training methodologies in modern organizational contexts.

References

1. S. Y. Ameen and K. H. Sharif, "A Review on Gamification for Information Security Training," ResearchGate, 2021.

2. S. Chaudhary, V. Gkioulos and S. K. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," Journal of Cybersecurity, 2022.
3. K. Khando, S. Gao, S. M. Islam and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," ScienceDirect, 2021.
4. M. Silic and P. B. Lowry, "Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance," Abingdon: Routledge, 2020.
5. S. M. DeCarlo, "Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare," ProQuesr, 2020.
6. M. A. Khan, A. Merabet, S. Alkaabi and H. E. Sayed, "Game-based learning platform to enhance cybersecurity education," New York: Springer US, 2022.
7. K. E. Sabo, J. Black and D. M. Sarno, "Developing IMPAWSTER: Improving Meaningful Phishing Awareness With Simulated Training and Email Roleplay," SAGE Journals Premier 2021, 2023.
8. S. Scholefield and L. Shepherd, "Gamification Techniques for Raising Cyber Security Awareness," ResearchGate, 2019.
9. A. M. Alnajim, S. Habib, M. Islam and H. S. AlRawashdeh, "Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches," ResearchGate, 2023.
10. A. Alruwaili, "A Review of the Impact of Training on Cybersecurity Awareness," International Journal of Advanced Research in Computer Science, 2019.
11. A. P. Filippidis, T. Lagkas, H. Mouratidis, S. Nifakos, E. Grigoriou and P. Sarigiannidis, "Enhancing information security awareness programs through collaborative learning," European Union's Horizon, 2020.
12. E. G. B. Gjertsen, E. A. Gjærel, M. Bartnes and W. R. Flores, "Gamification of Information Security Awareness and Training," 3rd International Conference on Information Systems Security and Privacy, 2017.
13. M. A. Khan and A. Merabet, "Game-based learning platform to enhance cybersecurity education," Education and Information Technologies, 2022.
14. A. Filippidis, T. Lagkas, H. Mouratidis and S. Nifakos, "Enhancing information security awareness programs through collaborative learning," European Conference on Games Based Learning, 2022.
15. S. DeCarlo, "Measuring the Application of Knowledge Gained from the Gamification of Cybersecurity Training in Healthcare," Robert Morris University ProQuest Dissertations Publishing, 2020.
16. Khokha, S., & Reddy, K. R. (2016). Low Power-Area Design of Full Adder Using Self Resetting Logic With GDI Technique. International Journal of VLSI design & Communication Systems (VLSICS) Vol, 7.
17. Zabihi, A., Parhamfar, M., Duvvuri, S. S., & Abtahi, M. (2024). Increase power output and radiation in photovoltaic systems by installing mirrors. Measurement: Sensors, 31, 100946.
18. Peng, L., Zabihi, A., Azimian, M., Shirvani, H., & Shahnia, F. (2022). Developing a robust expansion planning approach for transmission networks and privately-owned renewable sources. IEEE access, 11, 76046-76058.
19. Zabihi, A. (2024). Assessment of Faults in the Performance of Hydropower Plants within Power Systems. Energy, 7(2).
20. Raghuwanshi, P. (2024). AI-Powered Neural Network Verification: System Verilog Methodologies for Machine Learning in Hardware. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 39-45.
21. Zabihi, A., Sadeghkhani, I., & Fani, B. (2021). A partial shading detection algorithm for photovoltaic generation systems. Journal of Solar Energy Research, 6(1), 678-687.

22. Raghuwanshi, P. (2024). Integrating Generative AI into IoT-Based Cloud Computing: Opportunities and Challenges in the United States. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 5(1), 451-460.