Cybersecurity Awareness in the Digital Age: AwarenessHub's Gamified Solution

1st Muhammad Azhar
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
azharrao26@outlook.com

2nd Ahmad Hamza
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
ahmad9424802@gmail.com

3rd Syed Muhammad Ahsan Bukhari
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
bukhariahsan99@gmail.com

4th khan Bahadar Khan
Department of Information and Communication Engineering
The Islamia University of Bahawalpur
Bahawalpur, Pakistan
khattak@iub.edu.pk

***Abstract*—The increasing sophistication of cyber threats highlights the urgent need for effective cybersecurity awareness. Human error remains a persistent vulnerability, and traditional training methods often lack engagement, resulting in poor knowledge retention and the enduring "intention–behavior gap." This paper reviews existing approaches and emphasizes the benefits of gamification and simulation for improving engagement, learning outcomes, and behavioral change. It introduces *AwarenessHub*, a gamified platform designed for non-technical users that integrates interactive simulations, narrative-driven challenges, and real-time feedback to strengthen practical cyber skills through experiential learning.**

***Index Terms*—cybersecurity awareness, gamification, simulation-based training, human factors, experiential learning, non-technical users**

I. Introduction

The digital landscape faces escalating cyber threats, exemplified by the 2021 Colonial Pipeline ransomware attack, which disrupted operations with the CEO noting compromised defenses [1], [2]. In 2025, incidents like the Qantas breach affecting 6 million customers, the U.S. National Guard network theft by Chinese hackers, and breaches at Meta, Coinbase, AT&T, Google, and Apple highlight this trend. The global cybercrime cost is projected at $10.5 trillion in 2025 [3]. Human factors remain the "weakest link," with 95% of breaches linked to errors like weak passwords or phishing susceptibility [**?**].

Traditional methods—text, presentations, and videos—deliver information but fail to engage learners or foster secure behaviors [4], [5], creating an "intention-behavior gap" where knowledge is not applied [6]. With 95% of cyber incidents tied to human error [7], effective training is urgent. Gamification and simulation offer experiential learning, boosting engagement, retention, and practical skills [8]–[10]. Safe simulations allow failure without risk, enhancing learning [11], as seen in CybAR's improved interaction and skill gains [12].

This paper reviews cybersecurity awareness training literature, focusing on gamified and simulated methods. It analyzes approaches, topics, and outcomes, proposing AwarenessHub—a platform for non-technical users with immersive, story-driven simulations to address educational gaps. Incorporating 2025 insights, it highlights human factors and evolving threats, emphasizing gamified solutions' potential to mitigate risks in a rapidly advancing digital world [13].

II. Training Evolution

Cybersecurity education has evolved from passive instruction to interactive paradigms, reflecting broader trends toward experiential learning. This shift stems from recognizing that mere knowledge dissemination is insufficient for fostering lasting behavioral changes amid dynamic cyber threats.

Early approaches relied on passive delivery methods. Text-based formats, such as manuals and articles, are scalable but suffer from low engagement and retention [14]. Recent studies show users forget approximately 70% of content within 24 hours without interactive elements. Presentation-based techniques, including lectures and webinars, offer dynamism but remain largely passive, with mixed behavioral impacts [15], [16]. In organizational settings, these methods often fail to accommodate diverse learning styles, leading to suboptimal outcomes. Video-based training engages users on specific topics like phishing but lacks interactivity and personalized feedback [17], [18]. Although videos boost knowledge retention by about 20%, the absence of practical application limits behavior change. Information-based delivery, focusing on direct fact provision, overlaps with text methods and hinders deeper cognitive processing [19], [20]. Common in compliance programs, it proves ineffective for long-term skill development. Discussion-based strategies enhance collaborative understanding and improve security attitudes but lack scalability and require skilled facilitation [21], [22]. Overall, these traditional methods prioritize accessibility and cost-effectiveness but fail to provide immersive experiences mirroring real-world cyber challenges.

These conventional methods deliver foundational knowledge but struggle to drive behavioral change due to inherent limitations. A key issue is low engagement, as passive formats fail to sustain interest, resulting in superficial learning [8], [23]. Without enjoyment or competition, as in gamified approaches, motivation declines rapidly. Insufficient behavioral change persists, with knowledge gains rarely translating into consistent actions [24], [25]. The intention-behavior gap widens without practice or reinforcement opportunities. Hands-on experience is notably absent, impeding practical skill development [26], [27]. Simulations, however, enable real-time decision-making in controlled settings, bridging this gap effectively. Generic content, ignoring user diversity in proficiency and preferences, further limits impact [28]. Modern personalized platforms demonstrate how tailored content improves relevance and efficacy. Limited feedback mechanisms allow misconceptions to persist without correction [29]. Research shows timely feedback, as in interactive games, can increase retention by up to 50%. A trade-off emerges: scalable online passive methods contrast with resource-intensive in-person interactive sessions, which yield better attitudes [21], [23]. Using linear regression on data breach incidents reported in the United States of America from 2009 to 2017, the study validates human factors as a weak-point in information security [30].

TABLE I
TRAINING METHODOLOGIES.

Training delivery method	Number of mentions	Percentage of total mentions (N=122)
Game-based	37	30.3%
Presentation-based	19	15.6%
Info-based	16	13.1%
Simulation-based	15	12.3%
Text-based	13	10.7%
Video-based	13	10.7%
Discussion-based	6	4.9%
Punishment-based	1	0.8%
Hypermedia	1	0.8%
Multimedia	1	0.8%
Total	**122**	**100.0%**

The pie chart in Fig. 1 illustrates this distribution, highlighting gamification's prominence in recent literature as a response to the shortcomings of earlier methods.

III. Research Insights

Analysis reveals patterns in topics, outcomes, and method efficacy, providing a foundation for optimizing cybersecurity training.

Phishing dominates the literature's topics, reflecting its prevalence as a cyber threat. Phishing is the most common techniques used by the threat actors at 35% [31], [32]. However, comprehensive resilience requires training beyond phishing detection. For instance, Wen et al. (2017) demonstrate reduced susceptibility through interactive games [33]. Outcomes include behavior changes, knowledge gains, attitude shifts, perception changes, and behavioral intentions [34]–[42]. Gamified training often measures enjoyment, recognizing its role in sustaining learning and engagement [43].

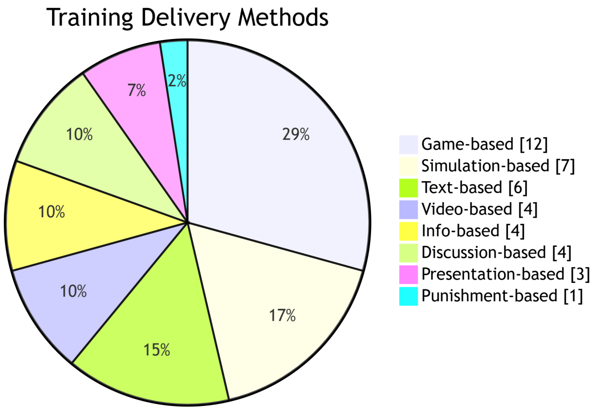

Fig. 1. Training delivery methods distribution.

Gamified and simulated training outperforms traditional methods in behavior, retention, and enjoyment [9], [12], [44]–[46]. Adinolf et al. (2019) highlight enhanced critical thinking and decision-making via agent-based virtual reality [47], [48]. Other topics include password safety, malware recognition, workplace protocols, and ransomware defense [45], [49], [50]. Some studies cover general awareness, focusing on broad foundational concepts [42]. Recent MIT Sloan report from September 2025 noted that 80% of ransomware attacks now use artificial intelligence. , underscore emerging threats [51].

Experiential learning in cybersecurity aligns with educational advancements, fostering practical skills in rapidly changing fields [27], [52], [53]. Personalized approaches, as noted by Li and Wong (2019), enhance effectiveness by tailoring content, informing platforms like AwarenessHub [54], [55].

IV. Gamification Benefits and Examples

Gamification uses game elements like points, badges, and narratives to enhance motivation and engagement in learning. Baxter et al. (2016) applied basic gamification to IT compliance training, showing significant improvements in compliance behaviors in lab and field tests [56]. This demonstrates how competitive and rewarding elements can turn mundane training into an interactive experience, encouraging participation. Similarly, Chen et al. (2020) created a self-efficacy game to raise hacking awareness, boosting users' confidence in addressing cybersecurity issues [38], [57]. These examples highlight gamification's ability to impart knowledge and build psychological resilience against cyber threats.

Simulation-based methods offer hands-on training by replicating real-world scenarios in controlled settings. Beuran et al. (2018) developed the CyTrONE framework, enabling risk-free practice against complex attacks [27]. Studies show simulations improve retention by up to 40% compared to passive methods, narrowing the intention-behavior gap. For critical infrastructure, Cook et al. (2017) used experiential learning to enhance situational awareness in industrial control systems, fostering proactive security behaviors [26]. In 2025, trends indicate gamification mitigates 74% of insider threats, which are increasing in evolving digital landscapes [58]. Overall, these benefits underscore gamification's role in making training effective, enjoyable, and relevant to daily cyber challenges.

V. Proposed AwarenessHub

AwarenessHub overcomes traditional training limitations by using gamification tailored for non-technical users, ensuring accessibility and relevance in building cybersecurity skills.

Its design principles emphasize experiential learning through interactive simulations mimicking real cyber threats. Gamified progression systems, including points and badges, motivate users to advance through levels, while narrative-driven scenarios foster immersion and emotional investment. Immediate feedback reinforces correct behaviors and corrects errors in real-time, based on educational theories [29]. Simplified, adaptive content adjusts to user proficiency, incorporating real-world relevance to make abstract concepts tangible [59]. Behavioral nudges guide users toward secure habits, bridging knowledge gaps [60]. Together, these principles create a user-friendly platform prioritizing practical skill development over rote memorization.

Key modules feature simplified challenges to build foundational skills progressively. Cryptography Unveiled introduces encoding and decoding techniques, like substitution ciphers, to demystify encryption. XOR Cipher Quest explores XOR operations for data obfuscation, offering hands-on binary manipulation practice. Missing Treasure Map and Substitution Cipher Mystery enhance analytical thinking through pattern recognition in historical contexts. Hash Hunt covers hash functions and password strength, teaching secure authentication. Cloud Security Journey and Reconnaissance/Trail of Troubles simulate log analysis to detect unauthorized access, fostering investigative skills. Network Security Basics, including Stay Aware Using Nmap and SQL Injection Safari, address common exploits via vulnerability scanning and injection puzzles. A Phishing Defense Simulator provides interactive email scenarios to identify social engineering, targeting the 90% of incidents tied to human error. The Ransomware Response Challenge offers decision-making trees for incident handling, reflecting 2025 ransomware trends. These modules ensure comprehensive, engaging coverage in a story-based format.

VI. Architecture & Flow

AwarenessHub employs a modular web architecture based on COFELET [61], enabling flexible and scalable deployment.

The architecture includes several core components. The gaming context comprises the user interface, virtual cyberspace environments, and feedback systems that provide immersive experiences. The task engine validates user actions and manages challenge progression, ensuring accurate assessments. Learner profiles track individual progress, enabling personalization and adaptive learning paths. These elements collaborate to form a cohesive platform supporting diverse user needs.

The user flow starts with an onboarding assessment to determine initial proficiency. A personalized learning path is then created based on the user's skills and goals. Users engage with modules via interactive challenges and narratives, receiving immediate feedback and rewards to reinforce positive outcomes. Reinforcement occurs through periodic reviews, quizzes, and behavioral nudges [60]. This structure fosters continuous improvement and long-term retention.

Implementation of AwarenessHub leverages web technologies for broad device accessibility. Embedded security measures simulate threats safely, avoiding real risks. Evaluation will use metrics like engagement rates, pre- and post-training tests, and behavioral surveys to assess impact. Scalability relies on cloud-based hosting, supporting growing user bases while maintaining performance.

VII. Discussion

Gamification's potential in cybersecurity training is evident from the literature, yet several challenges persist that must be addressed for widespread adoption. Ensuring inclusivity for diverse user groups, including those with varying technological literacy or disabilities, requires careful design to avoid alienating segments of the audience. Measuring long-term impact beyond short-term studies is another hurdle, as many evaluations focus on immediate outcomes rather than sustained behavioral changes over months or years [50], [62]. Content must also be regularly updated to reflect evolving threats, such as AI-driven attacks and deepfakes, which are becoming more sophisticated. AwarenessHub's modular structure facilitates these updates through user feedback loops and agile development, allowing for rapid incorporation of new scenarios based on emerging risks.

In comparative analysis, AwarenessHub stands out from existing platforms like CybAR [12] or PHISHY [35] by emphasizing non-technical narratives and broad module coverage, integrated with 2025 threat landscapes including deepfake detection. This focus on storytelling makes complex topics approachable, potentially increasing adoption among everyday users who may find technical jargon intimidating. Future work could integrate AI for dynamic scenario generation, tailoring challenges in real-time to user performance. Empirical testing in diverse groups, such as small and medium-sized businesses where 49% lack adequate training [63], would validate its effectiveness. Exploring virtual reality extensions could further enhance immersion, while longitudinal studies over 6-12 months would provide insights into lasting behavior change, contributing to the field's understanding of gamified training's real-world value.

VIII. Evaluation

A small-scale pilot study was conducted to provide preliminary evidence of the effectiveness of *AwarenessHub*. Twelve participants (eight undergraduate students and four

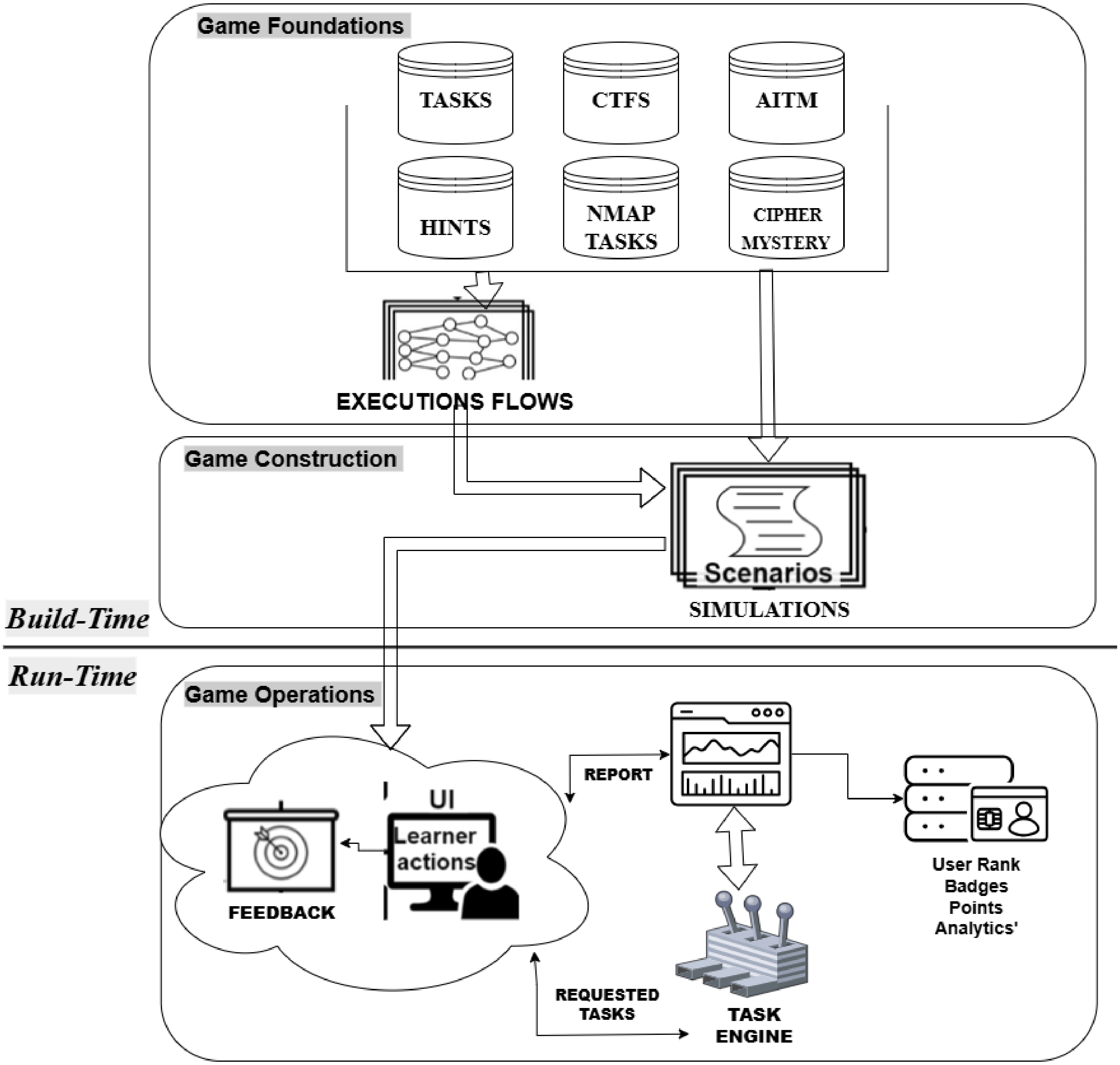

Fig. 2. The COFELET design framework Architecture for AwarenessHub.

staff members) with non-technical backgrounds completed the evaluation in three phases: (1) a pre-test consisting of 10 cybersecurity awareness questions, (2) interaction with two modules (phishing detection and social engineering), and (3) a post-test and usability survey.

The mean pre-test score was 56.7%, which increased to 81.3% in the post-test. A paired t-test confirmed that the improvement was statistically significant ($p < 0.01$). Usability feedback was positive, with a median System Usability Scale (SUS) score of 78, corresponding to "good" usability. Participants particularly highlighted the engaging nature of the gamified challenges and the usefulness of real-time feedback.

These findings are consistent with prior work. [64] et al. Demonstrated that interactive awareness methods significantly improved knowledge, attitude, and behavior. Similarly, [65] and Love showed that gamified designs improved phishing threat avoidance behavior.

Although limited in scale, these results suggest that *AwarenessHub* can improve both knowledge retention and user engagement. A larger-scale evaluation will be required to validate these initial results across diverse user groups.

IX. Conclusion

Traditional training inadequacies necessitate innovative approaches. Gamification bridges engagement and behavior gaps. AwarenessHub empowers non-technical users, fostering cyber resilience through experiential, enjoyable learning. By addressing human factors head-on, this platform represents a step forward in mitigating the escalating costs and impacts of cyber threats in the digital age.

References

[1] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A review of colonial pipeline ransomware attack," in *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 2023, pp. 8–15.

[2] J. W. Goodell and S. Corbet, "Commodity market exposure to energy-firm distress: Evidence from the colonial pipeline ransomware attack," *Finance Research Letters*, vol. 51, p. 103329, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1544612322005086

[3] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technol. Innov. Manag. Rev.*, vol. 4, pp. 13–21, 2014.

[4] A. Alruwaili, "A review of the impact of training on cybersecurity awareness," *Int. J. Adv. Res. Comput. Sci.*, vol. 10, no. 5, p. 5, 2019.

[5] C. McCoy and R. T. Fowler, "'you are the key to security': establishing a successful security awareness program," *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services*, pp. 346–349, 2004.

[6] A. Bhattacherjee and C. Sanford, "The intention–behaviour gap in technology usage: the moderating role of attitude strength," *Behav. Inf. Technol.*, vol. 28, no. 4, pp. 389–401, 2009.

[7] M. Ishaq, K. Kifayat, and M. Zafar, "A survey on human factors in cyberspace: A new dimension of privacy threats," in *2023 International Conference on Communication, Computing and Digital Systems (C-CODE)*. IEEE, 2023, pp. 1–6.

[8] F. F. G. Alotaibi, "Evaluation and enhancement of public cyber security awareness," Ph.D. dissertation, University of Plymouth, United Kingdom, 2019.

[9] C. B. Mayhorn and P. G. Nyeste, "Training users to counteract phishing," Ph.D. dissertation, North Carolina State University, 2011.

[10] A. Sykosch, C. Doll, M. Wübbeling, and M. Meier, "Generalizing the phishing principle: Analyzing user behavior in response to controlled stimuli for it security awareness assessment," *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020.

[11] E. Loffler, B. Schneider, P. M. Asprion, and T. Zanwar, "Cysecescape 2.0-a virtual escape room to raise cybersecurity awareness," *Int. J. Serious Games*, vol. 8, no. 1, p. 1, 2021.

[12] H. Alqahtani and M. Kavakli-Thorne, "Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)," *Information*, vol. 11, no. 2, p. 2, 2020.

[13] L. Leung, B. Duhoux, A. Legay, and S. Kieffer, "Integrating gamification, recommender system, and chatbot in cybersecurity training: A user-centered approach for enhanced engagement and motivation," in *International Conference on Human-Computer Interaction*. Springer, 2025, pp. 245–264.

[14] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, p. 3, 2014.

[15] J. Lamour, "Impact of user awareness and training of infosec practitioners on data security," *Dissertation Abstracts International Section A: Humanities and Social Sciences*, vol. 68, no. 12-A, 2008.

[16] P. Kim, "Measuring the effectiveness of information security training: a comparative analysis of computer -based training and instructor -based training," *ProQuest Dissertations and Theses*, 2010.

[17] R. Röpke, "Extending game-based anti-phishing education using personalization: design and implementation of a framework for personalized learning game content in anti-phishing learning games," Ph.D. dissertation, Dissertation, RWTH Aachen University, 2023, 2023.

[18] O. Khairallah and M. Abu-Naseer, "The effectiveness of gamification teaching method in raising awareness on email phishing: Controlled experiment," 2024.

[19] S. L. Hepp, R. C. Tarraf, A. Birney, and M. A. Arain, "Evaluation of the awareness and effectiveness of it security programs in a large publicly funded health care system," *Health Inf. Manag. J.*, vol. 47, no. 3, p. 3, 2018.

[20] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. J. M. Cano, "An effective cybersecurity training model to support an organizational awareness program: the cybersecurity awareness training model (catram). a case study in canada," *J. Cases Inf. Technol.*, vol. 21, no. 3, p. 3, 2019.

[21] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study," *Comput. Secur.*, vol. 29, no. 4, p. 4, 2010.

[22] P. P. Puhakainen, "A design theory for information security awareness," Ph.D. dissertation, Oulun Yliopisto, Finland, 2006.

[23] P. P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," *MIS Quart.*, vol. 34, no. 4, p. 4, 2010.

[24] A. Ertan, G. Crossland, C. Heath, D. Denny, and R. B. Jensen, "Cyber security behaviour in organisations," *CoRR*, vol. abs/2004.11768, 2020.

[25] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from 'shadow security': why understanding non-compliance provides the basis for effective security," *Workshop On Usable Security*, 2014.

[26] A. Cook, R. G. Smith, L. Maglaras, and H. Janicke, "Scips: using experiential learning to raise cyber situational awareness in industrial control system," *International J. Cyber Warfare Terror.*, vol. 7, no. 2, p. 2, 2017.

[27] R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: cytrone," *Comput. Secur.*, vol. 78, pp. 43–59, 2018.

[28] T. Mashiane, Z. Dlamini, and T. Mahlangu, "A rollout strategy for cybersecurity awareness campaigns," *Proceedings of the 14th International Conference on Cyber Warfare and Security (ICCWS 2019), Stellenbosch, South Africa*, pp. 243–250, 2019.

[29] R. E. Dihoff, G. M. Brosvic, M. L. Epstein, and M. J. Cook, "Provision of feedback during preparation for academic testing: learning is enhanced by immediate but not delayed feedback," *Psychol. Rec.*, vol. 54, no. 2, pp. 207–231, 2004.

[30] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's internet of things," *Heliyon*, vol. 7, no. 3, 2021.

[31] F. P. E. Putra, U. Ubaidi, A. Zulfikri, G. Arifin, and R. Ilhamsyah, "Analysis of phishing attack trends, impacts and prevention methods: Literature study," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 413–421, 2024.

[32] M. Hijji and G. Alam, "A multivocal literature review on growing social engineering based cyber-attacks/threats during the covid-19 pandemic: challenges and prospective solutions," *Ieee Access*, vol. 9, pp. 7152–7169, 2021.

[33] Z. A. Wen, Y. Li, R. Wade, J. Huang, and A. Wang, "What.hack: learn phishing email defence the fun way," in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 2017, pp. 234–237.

[34] A. Baillon, J. de Bruin, A. Emirmahmutoglu, E. van de Veer, and B. van Dijk, "Informing, simulating experience, or both: a field experiment on phishing risks," *PLoS One*, vol. 14, no. 12, p. 12, 2019.

[35] G. CJ, S. Pandit, S. Vaddepalli, H. Tupsamudre, V. Banahatti, and S. Lodha, "PHISHY - a serious game to train enterprise users on phishing awareness," in *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 2018, pp. 169–181.

[36] D. Kletenik, A. Butbul, D. Chan, D. Kwok, and M. LaSpina, "Cyber secured: a serious game for cybersecurity novices," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2020, p. 1307.

[37] S. Abraham, "Exploring the effectiveness of information security training and persuasive messages," Ph.D. dissertation, State University of New York at Albany, 2012.

[38] T. Chen, M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer, "Hacked time: design and evaluation of a self-efficacy based cybersecurity game," *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, pp. 1737–1749, 2020.

[39] S. Abraham and I. Chengalur-Smith, "Evaluating the effectiveness of learner controlled information security training," *Comput. Secur.*, vol. 87, 2019.

[40] S. T. Hammond, "Threat and coping appraisals on information security awareness training effectiveness: a quasi-experimental study," Ph.D. dissertation, Capella University, 2019.

[41] R. Anzaldua Jr, “Does information security training change hispanic students’ attitudes toward the perception of risk in the management of data security,” Ph.D. dissertation, Northcentral University, 2016.

[42] A. Alzahrani and C. Johnson, “Autonomy motivators, serious games, and intention toward isp compliance,” *Int. J. Serious Games*, vol. 6, no. 4, p. 4, 2019.

[43] J. Jayalath and V. Esichaikul, “Gamification to enhance motivation and engagement in blended elearning for technical and vocational education and training,” *Technology, Knowledge and Learning*, vol. 27, no. 1, pp. 91–118, 2022.

[44] R. W. Helms, R. Barneveld, and F. Dalpiaz, “A method for the design of gamified trainings,” 2015.

[45] M. Dixon, N. A. G. Arachchilage, and J. Nicholson, “Engaging users with educational games: the case of phishing,” in *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–6.

[46] K. F. Tschakert and S. Ngamsuriyaroj, “Effectiveness of and user preferences for security awareness training methodologies,” *Heliyon*, vol. 5, no. 6, p. 6, 2019.

[47] S. Adinolf, P. Wyeth, R. Brown, and R. Altizer, “Towards designing agent based virtual reality applications for cybersecurity training,” in *Proceedings of the 31st Australian Conference on Human-Computer-Interaction*, 2019, pp. 452–456.

[48] N. Glaser, Z. Parishani, A. C. Joshi, and P. Calyam, “Leveraging virtual reality for neurodivergent representation in cybersecurity education: An emerging technology report,” *Technology, Knowledge and Learning*, pp. 1–14, 2025.

[49] M. Curry, B. Marshall, J. Correia, and R. E. Crossler, “Infosec process action model (ipam): targeting insiders’ weak password behavior,” *J. Inf. Syst.*, vol. 33, no. 3, p. 3, 2019.

[50] N. Chowdhury and V. Gkioulos, “Cyber security training for critical infrastructure protection: a literature review,” *Comput. Sci. Rev.*, vol. 40, 2021.

[51] M. Siegel, S. Zeijlemaker, V. Baxi, and S. Raajah, “Cybersecurity at mit sloan,” 2025.

[52] B. Bertone, P. Wagner, and J. Pauli, “Experiential learning: Innovative approaches to post-secondary cybersecurity education,” *Journal of Cybersecurity Education, Research and Practice*, vol. 2025, no. 1, p. 15, 2025.

[53] D. Moloja, “Fortifying the future: Innovative approaches to cybersecurity education and training in the digital age,” in *International Conference on Information Technology-New Generations*. Springer, 2025, pp. 117–128.

[54] K. C. Li and B. T.-M. Wong, “Features and trends of personalised learning: A review of journal publications from 2001 to 2018,” *Personalized Learning*, pp. 4–17, 2023.

[55] ——, “How learning has been personalised: a review of literature from 2009 to 2018,” *Blended Learning: Educational Innovation For Personalized Learning*, pp. 72–81, 2019.

[56] R. J. E. W. Baxter, D. K. Holderness Jr, and D. A. Wood, “Applying basic gamification techniques to it compliance training: evidence from the lab and field,” *J. Inf. Syst.*, vol. 30, no. 3, p. 3, 2016.

[57] H. Chen, Y. Zhang, S. Zhang, and T. Lyu, “Exploring the role of gamified information security education systems on information security awareness and protection behavioral intention,” *Education and Information Technologies*, vol. 28, no. 12, pp. 15 915–15 948, 2023.

[58] A. Shahzadi, K. Ishaq, N. A. Nawaz, F. Rosdi, and F. A. Khan, “Unveiling personalized and gamification-based cybersecurity risks within financial institutions,” *PeerJ Computer Science*, vol. 11, p. e2598, Feb. 2025.

[59] V. Prain, P. Cox, C. Deed, J. Dorman, D. Edwards, C. Farrelly, M. Keeffe, V. Lovejoy, L. Mow, P. Sellings, B. Waldrip, and Z. Yager, “Personalised learning: lessons to be learnt,” *Br. Educ. Res. J.*, vol. 39, no. 4, pp. 654–676, 2013.

[60] R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Yale University Press, 2008.

[61] M. N. Katsantonis, A. Manikas, I. Mavridis, and D. Gritzalis, “Cyber range design framework for cyber security education and training,” *International Journal of Information Security*, vol. 22, no. 4, p. 1005–1027, Mar. 2023. [Online]. Available: http://dx.doi.org/10.1007/s10207-023-00680-4

[62] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, “Experiencing cybersecurity one game at a time: a systematic review of cybersecurity digital games,” *Simul Gaming*, vol. 51, no. 5, p. 5, 2020.

[63] M. Azhar, A. Abiodun, I. Oyinlola, N. Mensah, and P. Kamau, “Cybersecurity awareness among radiography teachers in africa and its potential impact in the digital age of medicine,” *BMC Medical Education*, vol. 25, no. 1, p. 6, 2025. [Online]. Available: https://doi.org/10.1186/s12909-025-07755-x

[64] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, “Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior,” *IEEE Access*, vol. 10, pp. 132 987–132 999, Dec. 2022.

[65] N. A. G. Arachchilage and S. Love, “A game design framework for avoiding phishing attacks,” *Computers in Human Behavior*, vol. 29, no. 3, pp. 706–714, May 2013.