Online-Journals.org

iJET International Journal of Emerging Technologies in Learning

iJET | eISSN: 1863-0383 | Vol. 21 No. 1 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijet.v21i01.58053

PAPER

Developing a Gamified Cybersecurity Training Program for Remote Work

Fadi Abu-Amara[1] (✉), Ali Khattab[2]

[1]Shenandoah University, Winchester, VA, USA

[2]University of The Potomac, Falls Church, VA, USA

fadi.abuamara@su.edu

ABSTRACT

Remote work has increased since the COVID-19 pandemic. This increase requires stronger protection for the organization's network, devices, and applications. It also requires enhanced security measures to mitigate cyber threats. Regulations and the rise in cyberattacks mandate organizations to train employees on the latest cybersecurity threats and attack techniques. In this work, we develop an interactive web game that raises employee awareness and improves their understanding of the latest cyber threats. The Cyber Battle game consists of three phases, with three scenarios per phase. The password complexity phase educates employees on password complexity, periodic password changes, and secure password storage. The phishing attack phase trains employees on identifying and handling phishing emails. Finally, the remote working phase trains employees on secure personal device usage and document handling when working remotely. To offer an enjoyable and interactive learning experience, we incorporate gamified learning elements into the Cyber Battle game, such as a point system to track progress, progressive levels with gradually increased difficulty, and a leaderboard to encourage healthy competition. We assessed the game's effectiveness using pre- and post-game surveys. The game and survey results show an improvement in employees' cybersecurity awareness. Furthermore, employees provide positive feedback and consider the game a more useful and interactive learning tool than traditional training programs.

KEYWORDS

cybersecurity awareness, gamification, security training, web-based game, employee training

1 INTRODUCTION

The digital age has introduced remarkable technological progress. However, it has also brought a surge in cybersecurity attacks [1]. The evolving cyber threats can significantly disrupt an organization's daily business operations and critical services. Employees are one of the most vulnerable assets within any organization [2]. Due to the insufficient cybersecurity awareness and training among employees about evolving cyber threats, they might accidentally put the company's assets at risk.

Abu-Amara, F., Khattab, A. (2026). Developing a Gamified Cybersecurity Training Program for Remote Work. *International Journal of Emerging Technologies in Learning (iJET)*, 21(1), pp. 22–34. https://doi.org/10.3991/ijet.v21i01.58053

Article submitted 2025-08-04. Revision uploaded 2025-10-16. Final acceptance 2025-12-05.

Cybercriminals target employees using different social engineering attacks to trick them into opening malware-infected email attachments, visiting infected websites, or revealing their login credentials.

Traditional cybersecurity training programs, such as lectures, presentation slides, and video lectures, are becoming inadequate in addressing evolving cyber threats and data breaches [3]. Human mistakes may result in cybersecurity incidents. Therefore, more interactive and engaging training programs are needed [4]. Gamification-based cybersecurity training and awareness programs offer real-world threat scenarios and a safe environment for employees to practice. These programs provide dynamic, enjoyable, safe, and effective training [5]. Furthermore, these programs utilize reward points, game levels, and real-world challenges to enhance user engagement.

This paper introduces a gamified training program designed for employees. The training program includes a pre-game survey, the Cyber Battle game, employee feedback, and a post-game survey. We embedded in the Cyber Battle game different cybersecurity scenarios to encourage hands-on learning. The game includes a point system to track progress, progressive levels with gradually increased difficulty, and a leaderboard to encourage healthy competition. These integrated game features offer an engaging and enjoyable learning experience and improve online practices.

The structure of this paper can be summarized as follows: Section 2 presents the technical background. Section 3 discusses the development of the game and the structure of the cybersecurity training program. Section 4 discusses the experimental results. Finally, Section 5 concludes this paper.

2 BACKGROUND

The reliance on digital platforms to complete daily work tasks has substantially grown, particularly due to the widespread transition to a remote work environment. While this online shift provides flexibility, it increases the attack surface [6]. Companies are investing more in enhancing cybersecurity awareness and knowledge among their employees. This step aims to meet regulatory requirements, improve employees' skills in recognizing and properly responding to cyberattacks, and protect their critical assets. In response to this demand, we propose a gamified cybersecurity training and awareness program as a proactive solution.

2.1 Phishing emails and infected attachments

Phishing emails are considered one of the most common security threats [2]. Social engineering attacks have different types, such as phishing emails, vishing, shoulder surfing, baiting, and tailgating, to name a few. After gathering information about the target, the attacker crafts a highly convincing email. The attacker bypasses most security measures and directly interacts with the victim. Therefore, the attacker has a higher likelihood of success and obtaining sensitive information, such as login credentials, personally identifiable information, or financial data. Employees with inadequate skills in recognizing phishing emails are vulnerable targets.

Nowadays, attackers utilize artificial intelligence (AI) large language models to generate targeted phishing emails. These emails trick employees into opening malicious attachments or visiting infected websites. A single employee mistake can result in installing malware on their machine. The installed malware then infects

other devices in the same network, opens a backdoor for the attacker to exfiltrate data, or installs other malware. The impact of phishing emails includes financial loss, data breaches, and reputational damage. Therefore, enhancing employees' skills in identifying and responding to phishing attacks is crucial for protecting critical assets, daily business operations, and mitigating the likelihood and impact of these attacks.

2.2 Gamification

Gamification is an effective strategy in cybersecurity awareness and training programs [1, 3]. This concept is used to expand user engagement and enhance learning outcomes. Gamification includes using gamified learning elements in training programs to increase interactivity and motivation among employees. Thus, gamification training programs are expected to enhance learners' engagement and enjoyment while ensuring better retention of knowledge and sustained behavior change.

In this paper, we propose a Cyber Battle training program that utilizes gamified components to provide an immersive and engaging cybersecurity awareness and training experience. This training program includes a point system to track employees' progress, embedded real-world threat scenarios, and a leaderboard for healthy competition among employees. Additionally, the game utilizes tasks to enhance employees' engagement, learning experience, and knowledge retention.

2.3 Related work

One of the main reasons cyberattacks and data breaches are increasing at an alarming rate is that conventional cybersecurity training methods, such as presentations, lectures, and video lectures, are not effective against sophisticated social engineering attacks [1, 2]. Security breaches that result from human mistakes are increasing, and there is an increased need for better cybersecurity education practices. Gamification is a recent trend in the context of cybersecurity training where elements of game-playing are used to enhance user engagement and learning.

In this section, the use of gamification in spreading cybersecurity awareness and educating employees is explored. A study integrated a structured training program with pre- and post-training phishing simulations. Employees participated in surveys and an interactive game with embedded realistic threat scenarios. This systematically designed game with different levels enhanced employees' skills in password strength, social engineering tactics, malware dissemination, and phishing identification [1]. In another work, a gamified training platform was developed. It integrated training videos, challenges, and feedback. 1,178 employees received training on recognizing and responding to phishing attacks. However, it lacked detailed behavioral insights [7].

In [8], an interactive web-based platform that utilized gamification to spread cybersecurity awareness for university students was developed. The platform integrated quizzes, storytelling, and gamification. Another study developed a serious game that integrated the traditional South African Morabaraba board game into a cybersecurity awareness program [9]. Players took the role of either defenders or attackers. They also inserted tokens to increase cybersecurity awareness. A recognized limitation was the requirement of broader testing across various demographics to measure the game's success.

The PeriHack is a serious board and card game developed to simulate attacker and defender dynamics in cybersecurity scenarios [10]. The game players explore vulnerabilities in a network, perform attacks, and allocate suitable defenses within a certain budget. However, it lacked empirical studies on measuring how well the game works in schools. Another work developed a video game to spread cybersecurity awareness about network security. The application integrated puzzles and targeted university students [11].

Another study created a quiz-based gamified intervention program. The quiz indicated an immediate need to improve knowledge in network security and social engineering. However, no actual game was developed and implemented [12]. Another study developed a mobile application with gamified elements to promote cybersecurity awareness among university students [13]. However, the mobile app should be validated in a more diverse population. In another work, a self-paced course that integrated game elements, such as points, badges, and levels, was developed. The course improved cybersecurity awareness and increased their learning motivation [14]. In a multi-study of long-term skills and knowledge retention, gamified cybersecurity training and awareness programs were analyzed [15]. Results of these training programs show significant improvement in the participants' skill in recognizing and responding to phishing attacks.

Another study created a gamified training platform for 43 undergraduate students. The platform integrated quizzes, real-life scenarios, and badges [16]. A mini video game was developed to teach young adults about privacy and security risks. However, the game lacked long-term knowledge and behavior retention tracking [17]. Another research work developed a quiz-based gamified platform for university students. However, it lacked metrics to track long-term knowledge and behavior changes [18].

In conclusion, the related work we surveyed in this section highlights the potential for using gamification in improving cybersecurity knowledge and spreading awareness of the latest cyber threats. Gamified-based training programs offer more engaging and interactive learning than conventional training programs. Such programs should increase user engagement, knowledge retention, and encourage online behavior change. However, there is a need for a long-term evaluation of these training programs, using a large sample, targeting employees of different roles, and applying them to organizations from different sectors. These limitations indicate a need for continued innovation and research in this field. Therefore, we developed the Cyber-Battle training program.

3 GAMIFIED TRAINING PROGRAM

This project aims to develop a web-based game that educates employees and raises their awareness of different cyber threats in a fun and interactive way. The Cyber Battle game includes three phases, with three threat scenarios for each phase as follows:

- **Password Phase:** This phase spreads awareness about password complexity, password change cycles, and secure password storage.
- **Phishing Attack Phase:** This phase teaches employees smart practices against phishing emails, infected attachments, and automatic antivirus update cycles.

- **Remote-Working Phase:** This phase spreads awareness of the threats presented by employee personal devices and the disposal and transmission of confidential documents.

Several employees will be chosen to take a pre-game survey, which measures their cybersecurity awareness level. The employees will then play the game. Then, the same employees will be asked to fill out a post-game survey to assess their cybersecurity awareness level. The Cyber Battle game uses multiple game mechanics: a point system to track progress (in this game, it is called "security level"), leveling to progress players to the next phase, a leaderboard to motivate players, challenges and quests to keep the players engaged, onboarding to ensure usability and ease of play, and engagement loops to structure activities.

The Cyber Battle game is a web-based game that educates employees about several types of cyberattacks. The game presents different cybersecurity concepts in simple language so employees of different cybersecurity knowledge levels can learn. Furthermore, the Cyber Battle game is designed to be engaging, which motivates players to complete all game levels enjoyably. Finally, the game content includes real-world threat scenarios, images, challenges, motivations, and levels. Once the player finishes the game, they receive a certificate of completion and appreciation.

Figure 1 shows a flowchart of the proposed Cyber Battle cybersecurity training and awareness program. The program starts with a pre-game survey to establish a baseline of the participants' cybersecurity knowledge. The game starts by authenticating the player's identity. Once the player authenticates successfully, they progress through the three phases: password phase, phishing attack phase, and remote-working phase. The player is offered an optional one-minute break between phases. Each phase contains threat scenarios and other gamified components to improve the player's experience during gameplay. Participants receive in-game feedback after every phase, allowing instant reinforcement of the best security practices to handle each scenario. The game's iterative progression facilitates continuous improvements and constructive insights. Once players complete the game, they fill out a post-game survey to assess their improvement level, and then they receive a completion certificate.

The password awareness phase of the Cyber Battle game is illustrated in Figure 2. The phase starts with a text box prompting players to create a password. It provides feedback to the player, and based on the complexity of the created password, it increases or lowers their security level. In the second scenario, the player encounters a notification of a password change; they have to decide to immediately change their password, set a reminder to change it later, or choose not to change their password. Every choice impacts the player's security level. Finally, the third scenario prompts players to choose their usual practice of saving their passwords, which includes using password management software, a web browser, a plain text file, or sticky notes. If the player chooses an insecure storage option, it reduces their security level. Next, the player receives constructive feedback about their choices throughout this phase, which guides them toward more secure password practices. This phase ends with a summary of the player's performance and their achieved security level and score.

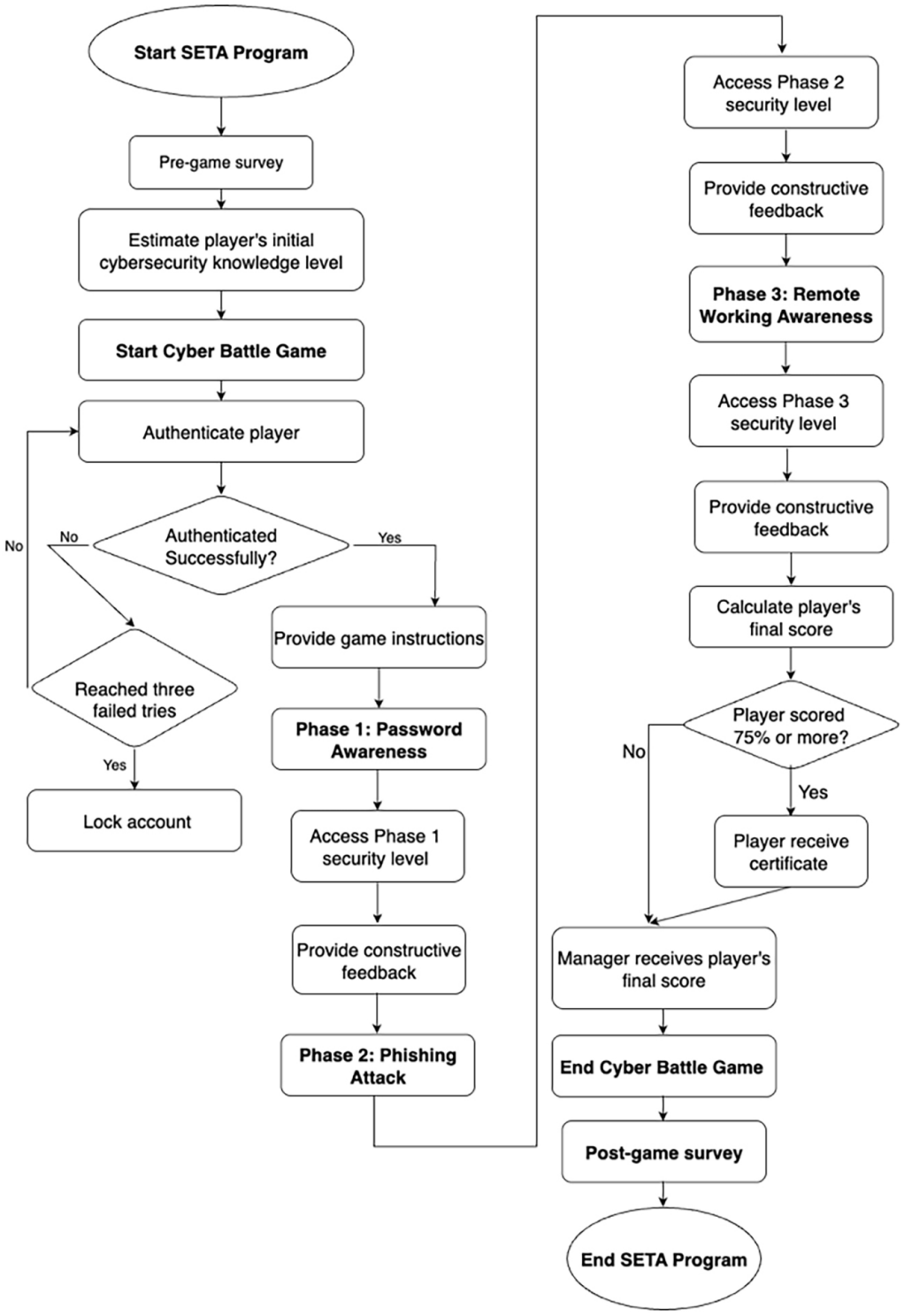

Fig. 1. Gamified cybersecurity training program

The phishing attack phase is illustrated in Figure 3. This phase trains players to identify email phishing attempts. The phase starts with displaying a deceptive email. The player is faced with three options: (1) contact the company to verify the e-mail, (2) ignore the e-mail, or (3) interact with the email's embedded link or attachment. After this, the player is introduced to the second scenario that uses different

techniques, such as an urgent request for personal information or a message regarding a fake account problem. Similarly, the player has to choose to validate, ignore, or interact with the content of the email. The third scenario of this phase incorporates social engineering elements to increase email credibility. After each scenario, the player's security level is reactively updated according to the choices they made and the associated consequences of their actions. After each scenario, the player receives constructive feedback on the correct response they should make, along with the associated risks of their incorrect responses. The second phase ends with an overall performance summary of the player and the total points the player earned.

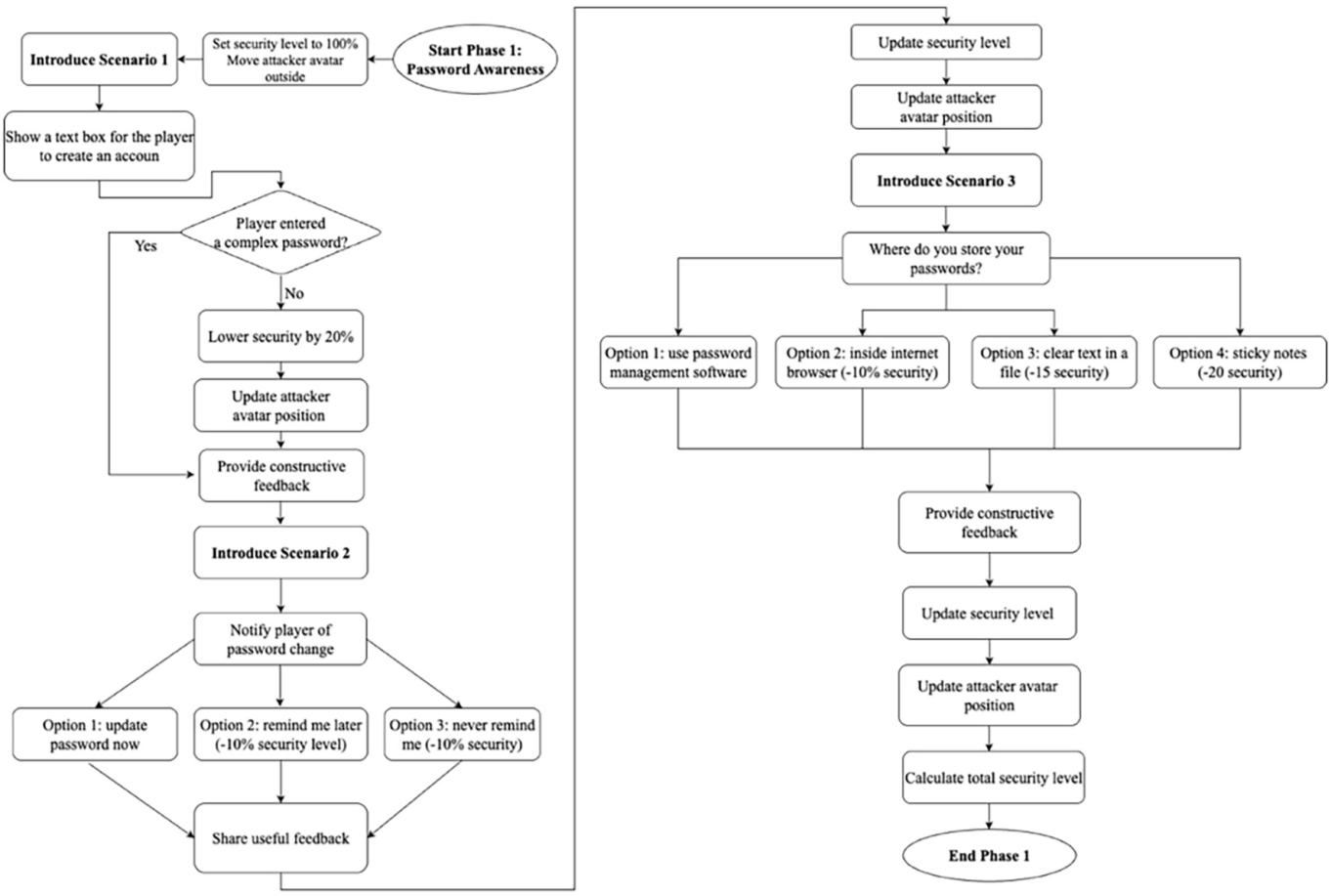

Fig. 2. Flowchart of the password awareness phase

Figure 4 illustrates the remote working phase of the Cyber Battle game. This phase focuses on cybersecurity best practices and secure practices that employees should follow during their remote work. The first scenario of this phase begins with the player opening their work laptops to find an urgent task email. However, their laptop is not working properly to be able to finish the urgent task. The player has three options: visiting the company's technical support to fix their work laptop, contacting the technical support to find a solution, or using their personal device to finish the urgent task. Choosing to use a personal device results in a reduction in the player's security level due to the potential security risks. For the second scenario, the player is asked about their usual practice during a break. The options include locking their laptop or leaving it unlocked. An unlocked laptop causes a decrease in the security level as it presents a vulnerability. Finally, the third scenario presents a

common paper disposal procedure in the remote work setting. The player is asked for their usual paper disposal practice. The options include shredding the paper or simply throwing it away without shredding. The latter option is vulnerable to dumpster diving threats. During this phase, players earn feedback on their selection, which educates them on secure remote working practices. At the end of this phase, the game summarizes the player's performance.

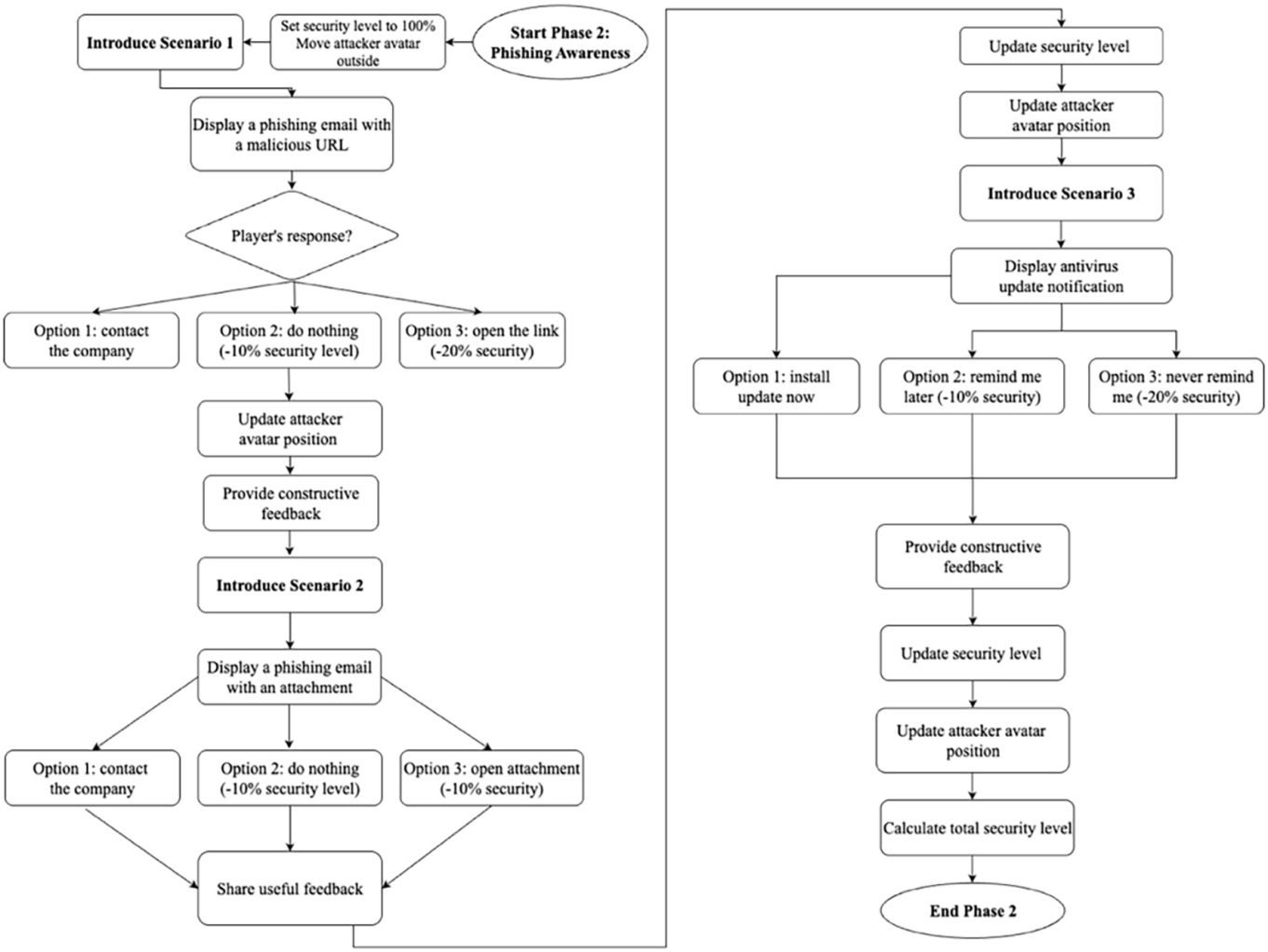

Fig. 3. Flowchart of the phishing attack phase

4 EXPERIMENTAL RESULTS

The proposed awareness and training program consists of four main components: (1) a pre-game survey, (2) a Cyber Battle game, (3) a post-game survey, and (4) employee feedback. The game is created to raise employees' awareness and educate them on the latest cyber threats. To assess the employees' knowledge of cybersecurity threats and best practices, a pre-game survey is used. After the employees finish the game, a post-game survey is used to estimate the improvement level in their knowledge of cybersecurity threats and attack techniques.

The Cyber Battle game is developed by integrating HTML, Cascading Style Sheets (CSS), and the Python programming language. On the front end, the game uses HTML

for page layout, CSS for formatting the pages and improving their visual appearance, and JavaScript to improve the players' experience through offering dynamic features. For the back end, the server-side logic is implemented using Python to manage game data and process user choices. In summary, integrating these tools should make the game interactive and offer an enjoyable player experience. Figure 5 shows the game homepage.

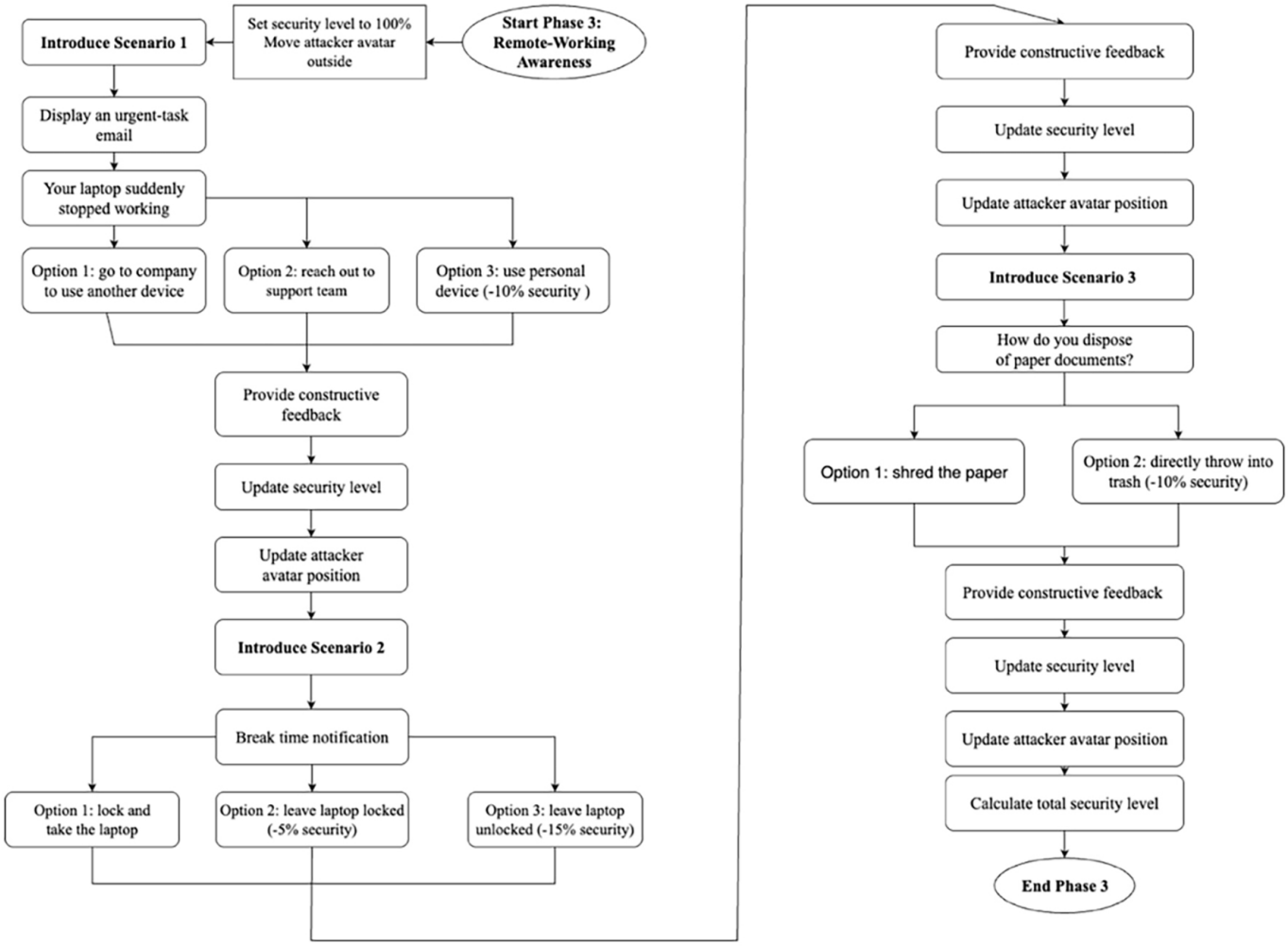

Fig. 4. Flowchart of the remote working phase

We sent the pre-game survey to 40 employees. The survey includes 15 questions that test employees' cybersecurity awareness of password management, phishing emails, and software updates. The survey also captures employees' daily cybersecurity practices during remote working and their satisfaction with annual cybersecurity awareness programs. On the other hand, the post-game survey consists of 15 questions that evaluate employees' knowledge of best cybersecurity practices during remote work, password management practices, and handling phishing emails. After the employees finished the Cyber Battle game, they were asked to complete the post-game survey.

When we compared the pre-game survey results with the post-game survey results, there was a noticeable increase in the cybersecurity awareness of employees. The survey results indicate average pre-game results of 50.8% and average post-game

results of 76.7%. This data indicates that employees' cybersecurity awareness level increased by 75.6% after finishing our proposed awareness program. Such an outcome reflects a better retention of knowledge about cybersecurity best practices and understanding of the latest techniques used by hackers.

Fig. 5. Game homepage

Another method used to measure the cyber battle awareness program's effectiveness is employee feedback. All 40 employees provided positive feedback about their awareness experience. The Cyber Battle game helped employees strengthen their knowledge about password best practices, recognize and report phishing emails, and adopt remote working best cybersecurity practices. In addition, employees indicated that the game was entertaining and engaging, and they felt that this new approach made learning more enjoyable compared to traditional methods. Furthermore, employees liked the gamified aspects, including the point system, leveling, and leaderboard, which offered competition and drove motivation. The game scenarios include real-world examples that employees face in their day-to-day operations. These embedded scenarios aim to improve employees' understanding and recognition of cybersecurity threats and hacker techniques. Besides, employees liked the reinforcement of best cybersecurity practices and the game's immediate feedback after incorrect responses. In contrast, employees find traditional approaches to security awareness and training, such as video lectures, lectures, or online articles, boring and challenging to remember. On the other hand, some employees requested adding more levels that target other social engineering attacks.

We integrated features in the Cyber Battle game that contributed to the success of the awareness and training program, such as a point system, level-up points for progressive increase of difficulty, and a leaderboard for encouraging competitiveness among the players. Additionally, to provide an interactive learning experience to players, we included challenges and quests in all game phases. Finally, the game provides clear instructions and a guided experience in each scenario of the three phases.

In conclusion, the obtained experimental results and positive employee feedback indicate that our cybersecurity awareness and training program is successful and has achieved its mission. The game's design and interactive elements raised employees' cybersecurity knowledge.

5 CONCLUSION AND FUTURE WORK

We proposed a cybersecurity awareness and training program to address the critical need of employees. The Cyber Battle game educates employees on how to recognize and respond to different real-world cyber threats. The game addressed important issues such as secure password creation, change, and storage practices. It also taught employees how to recognize and respond to phishing email attacks. Finally, the game educated employees on secure remote working practices. The game integrates interactive scenarios, challenges, quests, and a rewarding system. In addition, the pre- and post-game surveys were used to assess the impact of the training program on employees' daily cybersecurity practices. The experimental results and employees' feedback indicate that gamified training is engaging and more effective than traditional training methods.

Future research will explore the long-term retention of gained cybersecurity knowledge and enhance cybersecurity daily practices in the face of emerging cyber threats and evolving cyberattack techniques. We plan to integrate more scenarios that cover ransomware, social engineering, deepfakes, and insider threats. Finally, AI will be integrated to ensure a personalized training experience.

6 ACKNOWLEDGMENTS

The authors thank the anonymous reviewers for their valuable feedback.

7 STATEMENTS AND DECLARATIONS

No funding was received to assist with the preparation of this manuscript.

8 CONFLICT OF INTEREST

The authors declare no conflict of interest regarding the publication of this paper.

9 REFERENCES

[1] F. Abu-Amara *et al.*, "Spreading cybersecurity awareness via gamification: Zero-day game," *Int. J. Inf. Technol.*, vol. 16, pp. 2945–2953, 2024. https://doi.org/10.1007/s41870-024-01810-4

[2] L. Hadlington, *Cyberpsychology: The Science of Online Behavior*, 1st ed. London, UK: Kogan Page, 2022.

[3] A. Gwenhure and F. S. Rahayu, "Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review," *Int. J. Serious Games*, vol. 11, no. 1, pp. 83–99, 2024. https://doi.org/10.17083/ijsg.v11i1.719

[4] S. Furnell, *Computer Insecurity: Risking the System*, 2005th ed. London: Springer, 2005. https://doi.org/10.1007/1-84628-270-5

[5] F. Abu-Amara *et al.*, "Cyber shield security awareness program," in *Proc. 8th Int. Conf. Comput. Sustain. Glob. Dev.*, New Delhi, India, 2021, pp. 422–425.

[6] L. Hadlington, *Brain, Behaviour and the Digital World*, 1st ed. UK: Nottingham Trent University, 2017.

[7] P. Bitrián *et al.*, "Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours," *J. Bus. Res.*, vol. 179, p. 114685, 2024. https://doi.org/10.1016/j.jbusres.2024.114685

[8] A. K. A. Razack and M. F. M. Saad, "Enhancing cybersecurity awareness through gamification: Design an interactive cybersecurity learning platform for multimedia university students," *J. Inform. Web Eng.*, vol. 3, no. 3, pp. 21–40, 2024. https://doi.org/10.33093/jiwe.2024.3.3.2

[9] M. Nkongolo, "CyberMoraba: A game-based approach enhancing cybersecurity awareness," in *Proc. 19th Int. Conf. Cyber Warfare and Security*, South Africa, 2024. https://doi.org/10.34190/iccws.19.1.1957

[10] R. D. Arushi, "PeriHack: Designing a serious game for cybersecurity awareness," in *2022 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE),* Hung Hom, Hong Kong, 2022, pp. 630–634. https://doi.org/10.1109/TALE54877.2022.00108

[11] K. Hilliard *et al.*, "Using gamification to enhance mastery of network security concepts," *J. Cybersecur. Educ. Res. Pract.*, vol. 2024, no. 1, 2024. https://doi.org/10.62915/2472-2707.1187

[12] F. Fatokun *et al.*, "Cybersecurity knowledge deterioration and the role of gamification intervention," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 43, no. 1, pp. 66–94, 2025. https://doi.org/10.37934/araset.43.1.6694

[13] F. Alotaibi and M. Papadaki, "Enhancing cyber security awareness with mobile games," in *12th International Conference for Internet Technology and Secured Transactions*, 2017, pp. 129–134. https://doi.org/10.23919/ICITST.2017.8356361

[14] T. M. Tran *et al.*, "Gamification-based cybersecurity awareness course for self-regulated learning," *Int. J. Inf. Educ. Technol.*, vol. 13, no. 4, pp. 724–730, 2023. https://doi.org/10.18178/ijiet.2023.13.4.1859

[15] J. B. Kim *et al.*, "The impact of gamification on cybersecurity learning: multi-study analysis," *Comm. Assoc. Info. Sys.*, vol. 56, pp. 57–96, 2025. https://doi.org/10.17705/1CAIS.05603

[16] O. J. Mason *et al.*, "Preparing UK students for the workplace: The acceptability of a gamified cybersecurity training," *J. Cybersecur. Educ. Res. Pract.*, vol. 2024, no. 1, pp. 1–7, 2024. https://doi.org/10.32727/8.2023.35

[17] G. Tempestini *et al.*, "Improving the cybersecurity awareness of young adults through a game-based informal learning strategy," *Information*, vol. 15, no. 10, p. 607, 2024. https://doi.org/10.3390/info15100607

[18] A.A.J. Maluda *et al.*, "Evaluating the effectiveness of gamification to increase cybersecurity awareness among students," *Int. J. Data Sci. Adv. Anal.*, vol. 4, no. 2, pp. 154–158, 2023. https://doi.org/10.69511/ijdsaa.v4i0.157

10 AUTHORS

Fadi Abu-Amara is an Associate Professor in the Division of Applied Technology at Shenandoah University, Winchester, VA, USA. He joined Shenandoah in 2022 after

previously serving as an Assistant Professor in both Jordan and the United Arab Emirates. Dr. Abu-Amara brings over 24 years of experience spanning teaching, research, industry, and academic leadership. He has received outstanding performance awards, letters of appreciation from institutional leadership, and consistently high evaluations from students. His teaching portfolio includes courses in cybersecurity, computer science, and computer engineering. His research interests focus on cryptography, gamification for cybersecurity awareness, blockchain-based solutions for electricity and water management, and the use of robotics to support academic development in children with autism (E-mail: fadi.abuamara@su.edu).

Ali Khattab is a doctoral researcher in Computer Science with a focus on Cybersecurity at the Department of Computer Science, University of the Potomac, Virginia campus, Falls Church, VA, USA. He holds a Bachelor of Science in Civil Engineering and an MBA with a focus in Project Management, providing him with a diverse academic foundation that bridges engineering, business, and technology. Drawing on professional experience in sectors such as engineering and logistics, Khattab brings a systems-level perspective to his research. His work focuses on developing cybersecurity strategies to protect smart buildings and critical infrastructure from emerging threats, cyberattacks, and intrusions. By combining his expertise in physical infrastructure and digital security, Khattab aims to bridge the gap between the built environment and cybersecurity. His long-term goal is to contribute to the design of safer, smarter, and more resilient systems in an increasingly connected world (E-mail: ali.khattab@student.potomac.edu).