K. Abhiraj Mohan, 2025, 13:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Cybercecurity Awareness Platform Using Gamafication

K. Abhiraj Mohan, Professor Dr. S. Prasanna
Department of Computer Science, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, India

Abstract- Cybersecurity threats continue to rise, posing significant risks to organizations by exploiting human vulnerabilities, particularly among employees. Traditional security awareness programs, relying on slideshows, classroom training, and videos, often fail to sufficiently engage or educate users. This research introduces a gamified cybersecurity awareness program known as the Zero-Day Awareness Program (ZDAP), designed to enhance employees' knowledge and response to cyber threats through interactive learning. This study reinforces the importance of experiential learning in cybersecurity education and encourages organizations to adopt gamified methods for security training.

Keywords- Cybersecurity Awareness, Gamification, Phishing Simulation, Chatbot Assistance, Interactive Training.

I. INTRODUCTION

The quick pace at which cyber infrastructures evolve has caused organizations to encounter increased cybersecurity attacks, potentially leading to breaches of data, financial loss, loss of reputation, and litigation. Employees have traditionally been found to be the weakest link in an organization's security infrastructure due to the insufficient awareness or lack of understanding regarding cybersecurity threats. Cyber attackers capitalize on this aspect of humans using methods such as phishing, social engineering, and malware spreading. Although organizations implement technical and administrative security measures in place, these programs rely largely on user activities to succeed.

Hence, employing security education, training, and awareness (SETA) programs is important for enhancing employee watchfulness.

Traditional methods that SETA uses, such as PowerPoint presentation, video, classroom discussion, and policy document, generally do not involve users in an effective way or support knowledge recall.

With ever-more-complex cyberattacks, there is a compelling need for new, interactive, and user-centric training methods.

Our Website Design

To address these constraints, this research suggests a gamification-based cybersecurity training approach known as the Zero-Day Awareness Program (ZDAP). The program

Includes phishing simulations, surveys, and a five-stage interactive video game that simulates real-world cybersecurity situations. Every stage deals with specific threat vectors like poor passwords, phishing emails, malware programs, and social engineering techniques.

II. LITERATURE SURVEY

The continuous rise in cyber threats has prompted organizations to adopt more extensive security awareness programs. Conventional methods, such as seminars, videos, and policy manuals, have been found to be ineffective due to their passive learning methods and limited participation. In response to this gap, researchers have been looking for gamification, artificial intelligence, and chatbot-mediated learning as new strategies for enhancing cybersecurity awareness and behavior change.

Giboney et al. (2023) emphasized the use of conversational agents in scalable Security Education, Training, and Awareness (SETA) programs, with higher rates of engagement and learning outcomes through interactive elements [1]. Dash et al. (2022) created an AI-based training platform that showed high threat detection among employees compared to static training documents [2]. Likewise, Fung et al. (2022) designed a chatbot with Dialogflow to answer cybersecurity questions, thus allowing users to learn through natural language interfaces [3]. Gamified learning has also been found to be a robust mechanism for incorporating real-world scenarios into security training programs. Jin et al. (2018) and Hart et al. (2020) designed game-based modules for

K-12 students and employees, respectively, with a remarkable increase in phishing and social engineering tactic understanding [4][5]. Abu-Amara et al. (2021) created a SETA-themed game that simulates password strength and physical security challenges, thus providing a foundation for more engaging awareness materials [6]. Recent studies have also looked into hybrid models combining gamification and live phishing simulation. Sophos (2020) illustrated simulation tools for real-time vulnerability testing, while Gundu (2023) utilized ChatGPT to nudge secure conduct among employees through reminders and nudges [7][8]. Yasin et al. (2018) also presented a cybersecurity education card game (SREG), which deals with asset identification and human behavior with threats incorporated [9].

Alotaibi et al. (2017) also demonstrated that gamified mobile apps can raise awareness more effectively than conventional classroom settings [10].

III. MODULE-WISE DESCRIPTION

The proposed Zero-Day Awareness Program (ZDAP) is developed using modular units that work collaboratively to deliver effective cybersecurity training through gamification. Each module contributes to different phases of the awareness lifecycle, including threat assessment, knowledge evaluation, interactive simulation, user support, and performance feedback. The major modules are listed below:

1. Phishing Simulation Module

The Phishing Simulation Module is essential when evaluating employees' susceptibility to social engineering attacks by using controlled and ethical phishing simulations. The module utilizes two simulations, one pre-game and the other post-game, to critically evaluate the increase in awareness and responses to phishing attacks. The initial phishing message is tailored with common attack indicators like deceptive sender names, suspicious links, and convincing words in an effort to gauge the number of users clicking on the malicious link.

This module not only raises awareness but also provides experiential, real-time learning experiences that often outperform traditional training techniques. The use of simulated phishing attacks in combination with interactive learning

enables users to better understand the true consequences of clicking on unsafe links and helps to develop practices for recognizing, reporting, and avoiding potential future attacks.

Fig- Phishing Simulation Module

2. Awareness Survey Module

The Awareness Survey Module is used to quantify employees' pre-program cybersecurity awareness and assess the effect of the Zero-Day Awareness Program (ZDAP) after deployment. The module uses systematic pre-game and post-game surveys comprising 15 random questions in all cyber hygiene domains, such as password behavior, handling data, responding to incidents, phishing awareness, and system security behavior.

Prior to initiating the interactive game, a pre-game survey is administered to all players with the objective of assessing their current level of knowledge and typical behavioral responses. The survey serves as a diagnostic instrument that detects areas of knowledge deficit and assists in the design of follow-up reinforcement, if necessary.

The questions are framed to mirror actual security problems and not theoretical optimum procedures, requesting players to check what they "usually do" in a specified situation. This approach yields a more accurate representation of their behaviors.

After the game is finished, the same users are asked to fill out the post-game survey. This process helps to evaluate the retention of concepts, improve decision-making skills, and behavioral changes induced by training. Comparative analysis of pre- and post-survey data helps the researchers and administrators measure the effectiveness of the gamification-based training process.

Additionally, anonymity and confidentiality of the responses are strictly maintained to enable honest participation. The module is scalable and can be integrated with third-party tools or survey websites for better data visualization and reporting. Overall, this module is the core component of the program's assessment plan and provides critical metrics for validating the effectiveness of cybersecurity awareness programs.

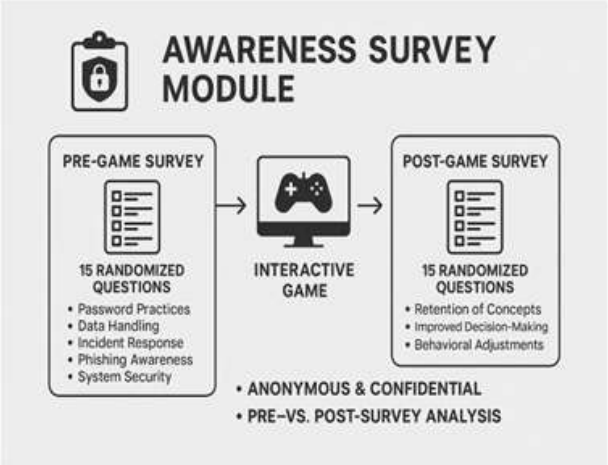

Fig- Awareness Survey Module

3. Interactive Game Module

The Interactive Game Module is the core component of the system, offering an engaging, gamified experience for cybersecurity training. It consists of five different levels, each of which is a defined cybersecurity threat scenario. The scenarios include common issues like poor password practices, phishing, software misuse, and social engineering techniques. Players' choices and actions throughout each level directly affect the game's direction and outcome. As an example, if a player misses a phishing email or chooses a poor password, they can face penalties in the form of data breaches or new accounts.

Fig- Interactive Game Module

The module's design is such that it enables users to confront real-world cybersecurity challenges in a secure and controlled environment, thereby facilitating a more efficient and long-lasting learning process. The game's interactive nature further serves to enhance decision-making capabilities, with players compelled to think critically about their cybersecurity methods. Moreover, the game has various levels of difficulty, making it possible for new as well as experienced users to gain from the learning process. With the progress of the user from one level to the next, they acquire access to new scenarios that increasingly become more complex, reflecting the dynamic nature of cybersecurity threats. This transition not only increases participation but also promotes ongoing improvement in cybersecurity awareness.

4. Chatbot Support Module

The Chatbot Support Module is an integrated feature designed to assist players during gameplay. It serves as a helpful companion by providing explanations of technical terms, offering hints, and answering queries that arise throughout the game. Cybersecurity concepts can be intimidating for beginners, so the chatbot is programmed to break down complex ideas into simple, understandable language. Players can ask questions like, "What is phishing?" or "Why is password complexity important?" and receive clear, concise answers to help them progress through the game.

In addition to aiding with technical terms, the chatbot ensures that players remain engaged and don't feel stuck at any point. If a player is unsure of how to proceed with a particular level, the chatbot can provide gentle hints or guide them through a series of actions that lead to the correct solution. This feature is particularly valuable for users with minimal technical backgrounds, as it lowers the barriers to understanding cybersecurity concepts. The chatbot operates in real time, making it a seamless addition to the gaming experience. By offering personalized support, it ensures that every player, regardless of experience level, can follow along and gain a thorough understanding of cybersecurity best practices.

Fig- Chatbot Support Module

5. Performance Evaluation and Feedback Module

The Performance Evaluation & Feedback Module should provide players with a comprehensive report of their knowledge of cybersecurity as well as decision-making skills. After completing the entire five levels of the game, this module calculates a score based on players' decisions and performance throughout the game. The score obtained depicts the player's ability to identify cybersecurity threats, make secure choices, and solve various problems.

The measurement of performance is a double-edged sword, serving to motivate individuals as

well as provide a learning opportunity. It motivates the participants to look at their own performances, thereby cultivating a growth mindset. By providing individualized feedback, the module enables the users to monitor their progress and identify some cybersecurity practices that require special attention. In general, it adds value to the educational content of the game, with participants leaving with a greater understanding of how to defend themselves against cyberattacks in real life.

Fig- Performance Evaluation & Feedback Module

IV. GAME MECHANISMS AND RESILIENCE IN CYBERSECURITY AWARENESS TRAINING THROUGH GAMIFICATION

In the construction of cybersecurity awareness training games, caution needs to be exercised to maintain the integrity and effectiveness of the training experience through the strength of game mechanisms. Methods that utilize gamification, like the Zero-Day Game, depend on the integrity of the system architecture and its ability to process various user inputs and actions that simulate real-world cybersecurity situations. Fault tolerance in the game is the system's capability to recover from unexpected user behavior, mistakes, or malicious attacks during game play, presenting a seamless user experience despite potential issues.

The Zero-Day Game works through a sophisticated network of interactions where players get engaged in decision-making that replicates actual cybersecurity threats. As the situations evolve, the resilience of the system is challenged in terms of the game's ability to respond to emergent player behavior and adapt to a variety of decisions, including failures like weak password protocols or susceptibility to phishing attacks. The dynamic nature of the game necessarily demands continuous adaptation to be able to offer meaningful challenges without overwhelming the player.

Additionally, a network's resilience to errors is vital to seamless content delivery in training. This is particularly significant in multiplayer environments where trainees perform real-time communications, simulating cyber defense strategy and coordinated response. When technical errors or disconnections occur, the system can either temporarily stop the game or alter scenarios to minimize its impact on training, thus allowing users to continue with effective learning.

V. CONCLUSION

The gamification of cybersecurity awareness training, such as in the Zero-Day Game, is an important step in educating individuals regarding important cyber threats and best practices for their mitigation. By presenting interactive simulations of actual problems, players are nudged to make well-informed decisions, thus gaining a clearer understanding of cybersecurity concepts in an actual and interactive setting. The tiered design of the game, from poor passwords to phishing, vulnerable software, and social engineering, provides for thorough consideration of cybersecurity matters, with users gaining practical experience in a safe environment.

In conclusion, the Zero-Day Game illustrates the gamified learning capability to enhance cybersecurity awareness. Through simplifying intricate concepts and gamifying them, it not only teaches users but also enables them to embrace improved cybersecurity habits. As cyberattacks

become more sophisticated and evolve with time, such creative training mechanisms will be imperative to prepare individuals with the know-how and skillset to protect themselves and their organizations from ever- evolving attacks. The game provides a scalable and flexible mechanism that can be applied across different industries to increase overall cybersecurity awareness and resilience.

REFERENCES

1. Giboney, J. S., et al. (2023). Know your enemy: conversational agents for security, education, training, and awareness at scale. Computers & Security, 129(C), 103207.
2. Dash, B., et al. (2022). An effective cybersecurity awareness training model: first defense of an organizational security strategy. International Research Journal of Engineering and Technology (IRJET), 9(4), 1–6.
3. Fung, Y. C., et al. (2022). A chatbot for promoting cybersecurity awareness. Cyber Security, 370, 379–387.
4. Jin, G., et al. (2018). Game-based cybersecurity training for high school students. Proceedings of the 49th ACM Technical Symposium on Computer Science Education, 68–73.
5. Hart, S., et al. (2020). Riskio: a serious game for cybersecurity awareness and education. Computers & Security, 95, 1–18.
6. Abu-Amara, F., et al. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. International Journal of Information Technology. https://doi.org/10.1007/s41870-021- 00760-5
7. Sophos (2020). Sophos Central Training Platform. Retrieved from https://www.sophos.com/en-us.aspx
8. Gundu, T. (2023). Chatbots: a framework for improving information security behaviours using ChatGPT. IFIP Advances in Information and Communication Technology, 674, 418–431.
9. Yasin, A., et al. (2018). Design and preliminary evaluation of a cybersecurity requirements education game (SREG). Information and Software Technology, 95, 179–200.
10. Alotaibi, F., et al. (2017). Enhancing cybersecurity awareness with mobile games. Proceedings of the 12th International Conference on Internet Technology and Secured Transactions (ICITST), 129–134.