International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2025.2.6

Volume 11, Issue 2
February - 2025

Design and Development of a Web-Based Cyber security Awareness Platform

Vivian Munshya Phiri [1], Moses Mupeta[2]

Department of ICT

School Engineering

Information and Communications University

Zambia

ABSTRACT

The rise of cyberattacks continues to enforce the importance of cybersecurity awareness. Although technological defenses have improved, people's weaknesses are still most at risk. This study demonstrates the development of a Web-Based Cybersecurity Awareness Platform that attempts to close the knowledge gap and provide crucial security skills to users.

The platform uses interactive modules, quizzes, and simulations for users on phishing, password-owing, secure browsing, and social engineering. The Learning Management System (LMS) monitors IT achievements and provides personalized recommendation s while testing understanding through adaptive checking of knowledge. Key Highlights include real-time alerting of threats, gamification (leaderboards, badges), feedback, and suggestion capture to increase participation in exercises. The system is intended to be responsive for all kinds of devices.

Key words: Cyber security Awareness, Gamification, Human Vulnerabilities, Learning Management, Interactive Training, Phishing, Threat Intelligence, Social Engineering.

1. INTRODUCTIONS

In today's interconnected world, cybersecurity has emerged as a vital concern. The increased use of the internet for social interaction, business activity, education, and medical services increases the chances of cyberattacks on individuals, corporations, and governments. Adapting to the digital world requires specific knowledge and skills to remain safe in today's world. Therefore, as the threat of cyber-attacks occur frequently and become more complex, it is necessary to equip the users with knowledge regarding how they can safeguard themselves in the cyberspace [1].

The statistics of cybercrime are sobering, with phishing, social engineering, and ransomware being the most prominent breaches. Studies show that a common factor involving people remains one of the driving elements behind most of cybersecurity breaches, so lack of awareness needs to be tackled [2]. In the absence of training, even the most sophisticated protective measures such as firewalls and encryption technologies can be rendered useless in combatting cyber threats [3].

Manuals, e-learning courses, and general online courses are some of the most relied upon methods for increasing cybersecurity awareness. But these approaches take little consideration the users as active participants and often do not address their varying needs. Gamification along with the use of advanced interactive learning environments in Razack's work have shown drastic improvements in learners' participation and retention of information, which helps advance cybersecurity education [4].

This thesis aims to provide the design and development of a web based platform that focuses on cybersecurity

awareness to fill those gaps. It manages to achieve a user centric approach with the use of interactive learning modules, real-time threat alerts, gamificaton, and personalized feedback which increases engagement and retention to information. This allows users to notice and respond to threats accordingly, thereby decreasing their chance of becoming victims of cyber-attacks. [5]

The platform's responsive design allows a seamless experience on various devices from users of different technical proficiencies. In addition, progress monitoring and adaptive learning allow for tailored content based on the user's actions providing them with helpful information for improvement. These collectively promote proactive cybersecurity posture which focuses on prevention rather than correction of security incidents. [6]

The essence of this project is to increase the level of awareness of cybersecurity for a broader audience ultimately minimizing the consequences of cyberattacks for people and organizations. It seeks to provide education about cybersecurity on a large scale which helps in building a nations or a world's digital resiliency. [7]

2. PROBLEM STATEMENT

One of the biggest threats for the digital world is cybersecurity since people, as well as businesses, utilize the internet for communication, conducting businesses, and even doing transactions. Although people are more aware of cybercrimes, negligence is still one of the major causes of cybersecurity threats. A large percentage of the threats are due to lack of knowledge. Cybersecurity negligence such as phishing, fragile password creation, and irresponsible internet surfing are easily avoidable with proper training. The reality is many of these cybersecurity awareness programs do not cater for nor educate non-technical users on the dangers posed by the online world [8].

Electric Pruner According to the 2023 Verizon Data Breach Investigations Report, over 82% of breaches are associated with some type of human negligence, ranging from lack of training to actively abandoning their post to more socially engineered accounts such as phishing (Verizon, 2023). In addition, global cybercrime is expected to cost more than $10.5 trillion by the year 2025, which needs to be controlled [9]. While these shocking numbers portray a grim future for the world, the bright side is these organizations have begun to understand the importance of social or behavioral training, as simply relying on static online courses or pseudo live seminars utterly fails to attract users' attention.

By focusing on practical training and using adaptive learning techniques, this study aims to improve users' ability to identify and respond to cyber threats, ultimately reducing the human vulnerabilities that continue to fuel cybercrime.

3.0 GENERAL OBJECTIVE

The general objective of this study is to design and develop a web-based cybersecurity awareness platform aimed at enhancing users' knowledge and skills in identifying and mitigating cyber threats.

3.1 Specific Objectives

1. Design and develop an interactive, web-based cybersecurity awareness platform that offers personalized training for users.
2. Incorporate gamification and real-time feedback to increase user engagement and facilitate more effective learning.
3. Evaluate the platform's effectiveness in improving users' cybersecurity knowledge and behaviors.

3.2 Research Questions

1. How effective is the web-based cybersecurity awareness platform in providing personalized training for users with varying levels of cybersecurity knowledge?
2. To what extent do gamification and real-time feedback enhance user engagement and knowledge retention in cybersecurity training?
3. How does the use of the platform impact users' ability to recognize and mitigate common cyber threats in real-world scenarios?

DOI: 10.31695/IJASRE.2025.2.6

4.0 LITERATURE REVIEW

Cybersecurity awareness is a crucial element in safeguarding digital systems and sensitive data, as human error remains one of the leading causes of cyber breaches. Many cybersecurity breaches result from a lack of awareness or negligence on the part of users, including falling victim to phishing attacks, poor password practices, or downloading malware-infected software. According to the Verizon 2023 Data Breach Investigations Report, 82% of breaches involve a human element, with phishing being one of the most common methods used to gain unauthorized access [10]. This highlights the importance of addressing human vulnerabilities through effective awareness programs.

Cybersecurity awareness programs aim to educate individuals about common cyber threats and the best practices to mitigate these risks. Research has shown that raising awareness can significantly reduce an individual's likelihood of falling victim to cyberattacks. For instance, a study [11] emphasized the role of awareness in reducing organizational vulnerabilities. However, many cybersecurity awareness programs are traditional, relying on passive training methods such as one-time seminars or static online modules, which are often insufficient in making a lasting impact on users' behaviors.

Training programs that aim to improve cybersecurity knowledge must engage users actively, ensuring that they not only learn about threats but are also equipped to handle them effectively. One approach to enhancing engagement is interactive learning, where learners participate in hands-on activities such as quizzes, case studies, or simulations. According to [12], interactive learning methods are more effective than traditional, passive approaches because they promote active engagement and knowledge retention.

Training and development are essential elements in enhancing employee skills and fostering organizational growth. These practices significantly influence employees' abilities and their commitment to the organization [13]As integral parts of the firm, training and development, as an organizational subsystem, work in tandem to increase individual productivity, which ultimately benefits the organization [14]. One widely recognized concept related to training and development is "lifelong learning," which emphasizes continuous learning and the development of competencies that add value, adapt to changes, and encourage personal growth [15] highlight that development prepares employees for future roles and responsibilities, addressing skills gaps effectively. Communication between organizations and employees regarding training needs ensures that training is both targeted and timely [16]. The transfer of knowledge, skills, and attitudes is crucial for improving job performance, as training activities are directly linked to an individual's current work [17]

Training programs not only demonstrate that managers care about employees' development but also foster a commitment to achieving organizational goals and adapting to challenges like technological change and market competition [17].

4.1 Related Works

Numerous studies have explored the development of web-based platforms designed to improve cybersecurity awareness. Platforms like *StaySafeOnline* (National Cyber Security Alliance) and *PhishMe* use online modules to teach users about phishing, password management, and safe browsing practices. These platforms generally rely on a combination of informational content, quizzes, and sometimes simulations. [17] found that while these platforms are informative, they often fall short in terms of user engagement, as they tend to be passive in nature, relying heavily on reading materials and quizzes.

An example of a more interactive platform is *CyberAware*, which offers tailored cybersecurity training with interactive exercises and real-time feedback. While these platforms represent a step toward more engaging learning, they still do not fully exploit the potential of gamification or personalized learning paths, which could make training more effective and engaging for users with varying levels of expertise.

DOI: 10.31695/IJASRE.2025.2.6

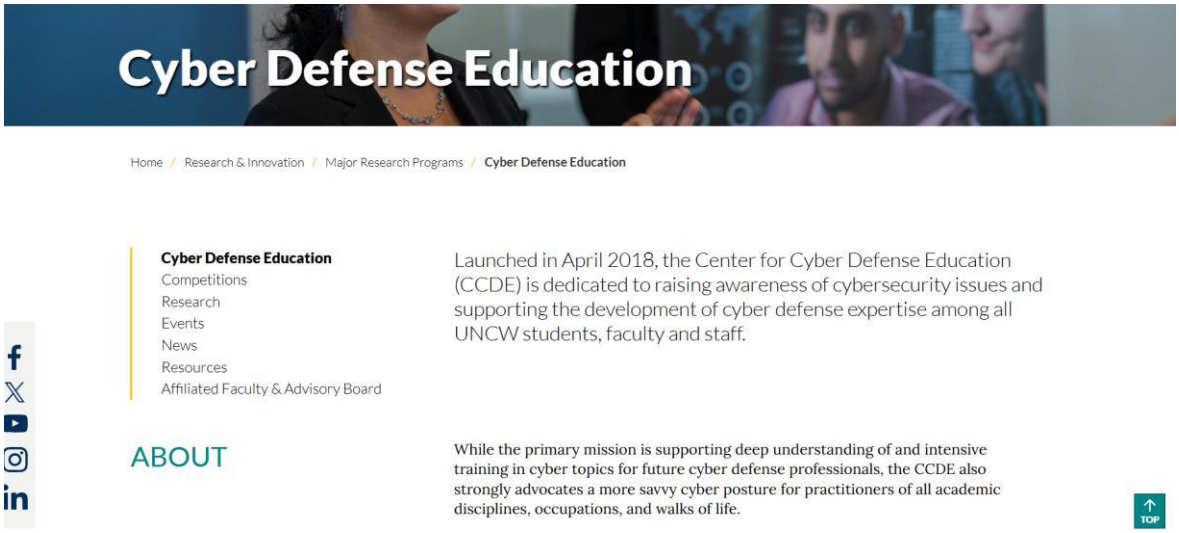

Figure 1: Gamification Platform

Source: Author (2025)

5.0 METHODOLOGY

5.1 Research Design

The research adopts a mixed-methods approach, combining both qualitative and quantitative research techniques. This design was chosen to capture a comprehensive understanding of the effectiveness of the web-based cybersecurity training platform and to ensure that both user experiences and measurable outcomes are considered. The study is primarily descriptive and exploratory in nature, as it seeks to explore existing gaps in cybersecurity awareness training and assess the impact of the proposed platform.

5.2 Baseline Study

Before the implementation of the web-based cybersecurity awareness platform, a baseline study was conducted to assess the current level of cybersecurity knowledge among the target audience. This baseline study serves as the foundation for evaluating the effectiveness of the platform in enhancing users' cybersecurity awareness and behavior. It also provides insight into the strengths and weaknesses of existing awareness programs, allowing for targeted improvements in the platform design.

5.2.1 Data Collection

Data collection for the baseline study was carried out using a combination of surveys, interviews, and observations. The following methods were employed:

- **Surveys**: A structured survey was distributed to a sample of users to gather quantitative data on their current knowledge of cybersecurity. The survey contained questions related to common cyber threats (such as phishing, malware, and password security), as well as their familiarity with cybersecurity best practices. The responses were analyzed to identify areas of weakness in user knowledge.

5.2.2 Research Approach

The system will be developed using the Waterfall Model, which is a traditional and widely used software development methodology characterized by a linear-sequential life cycle. This model is often regarded as one of the first formalized approaches in software engineering, providing a simple, structured, and easy-to-understand framework for developing software. The Waterfall Model is especially useful when the project requirements are clearly defined and stable, making it well-suited for our web-based cybersecurity awareness platform, where the objectives and features are clearly outlined from the start.

DOI: 10.31695/IJASRE.2025.2.6

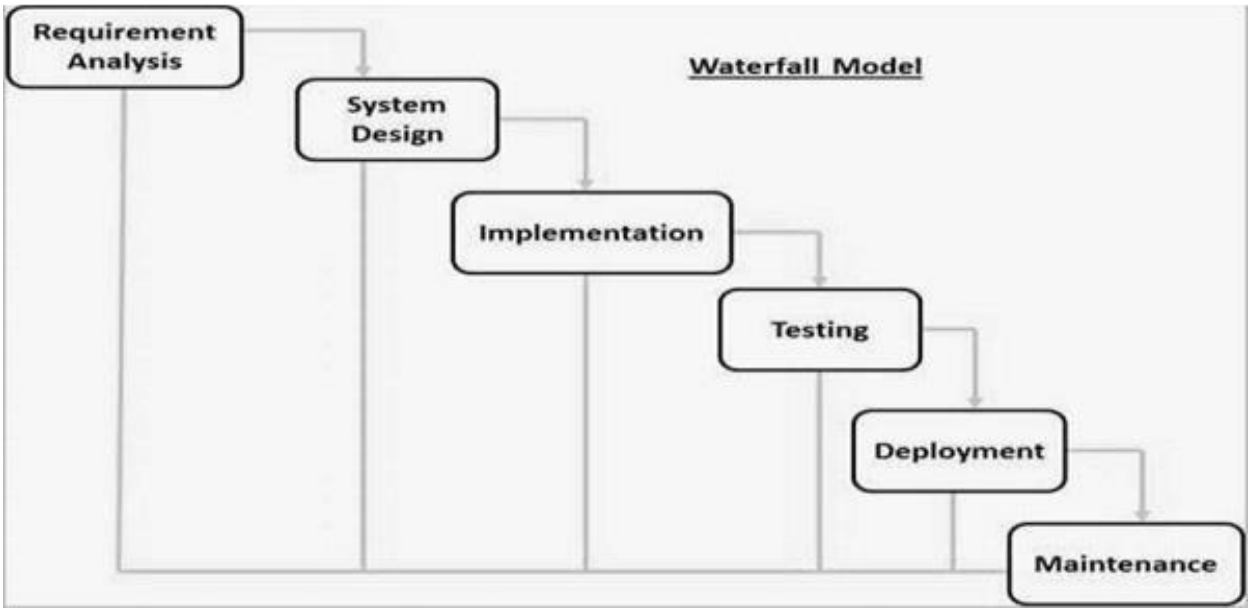

Figure 2: Waterfall model

5.3 Development of the Application

The Development of the Application phase marks the actual creation of the Web-Based Cybersecurity Awareness Platform based on the design and system specifications outlined in the previous stages. This phase involves translating the system design into functional code, where the platform's features and functionalities are implemented as per the agreed requirements. The development process is divided into different tasks, which are organized according to the various modules or components of the system, including user authentication, content delivery, quizzes, real-time feedback, and security mechanisms.

5.4 System Design

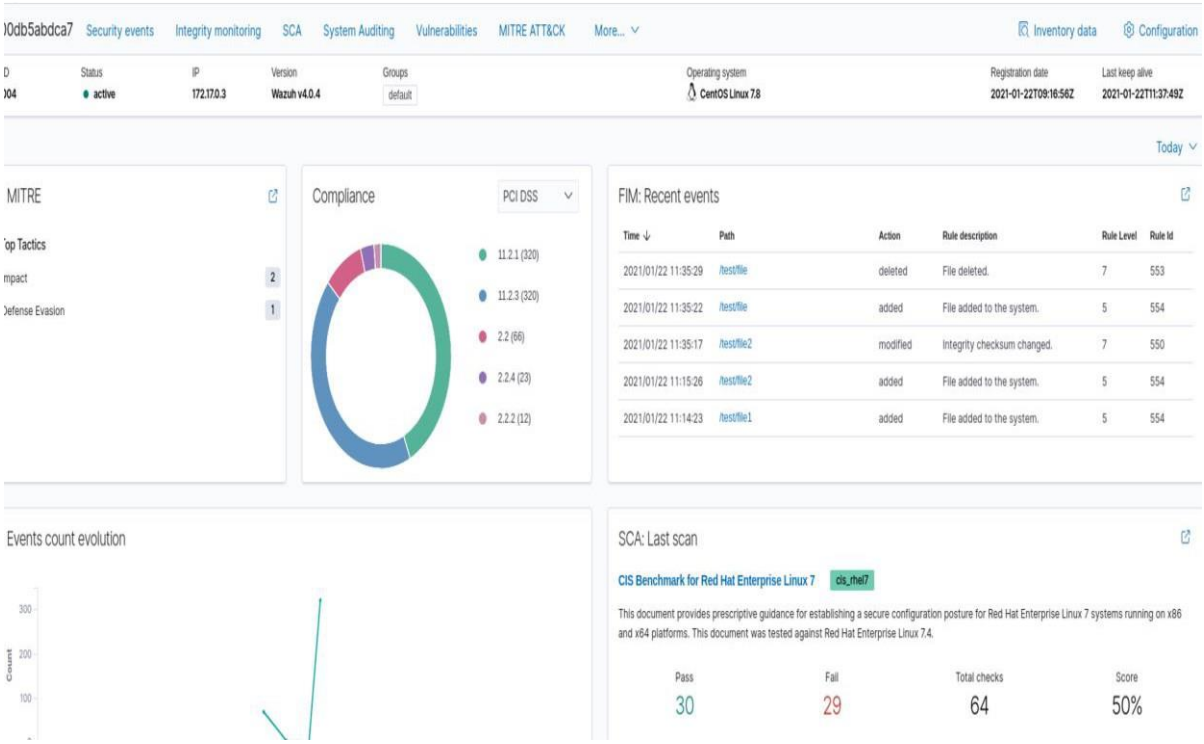

Figure 3: System design

DOI: 10.31695/IJASRE.2025.2.6

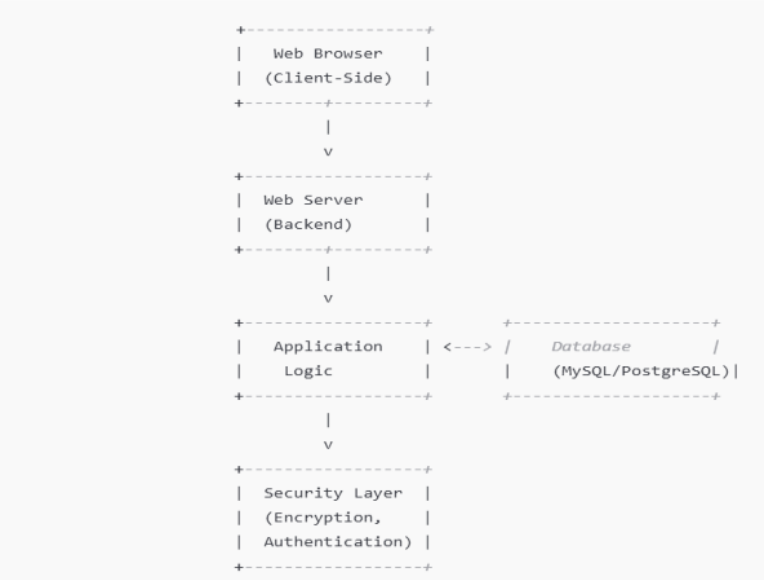

Figure 4: System Architecture

Figure 5: Context diagram

DOI: 10.31695/IJASRE.2025.2.6

Figure 6: System Software Architecture Design Diagram

6. RESULTS & DISCUSSIONS

The baseline study was conducted to assess the existing level of cybersecurity awareness among potential users before the implementation of the platform. Survey results indicated a significant gap in users' knowledge about common cybersecurity threats, such as phishing, malware, and ransomware. Additionally, many users were unaware of best practices for securing personal data, such as the use of multi-factor authentication or strong password management. The baseline study revealed a strong need for accessible, engaging, and practical cybersecurity education. The survey findings also highlighted a demand for interactive learning materials and real-life simulations, suggesting that a web-based platform incorporating these elements could effectively fill this gap. The results of the baseline study provided valuable insights into the content and design requirements for the platform, ensuring that the training modules addressed the most pressing knowledge gaps among users.

The baseline survey results highlight a critical need for user-friendly, accessible cybersecurity training. The majority of users lacked awareness of fundamental cybersecurity threats and practices, which reinforces the need for a structured and engaging training platform. Additionally, the survey indicated a strong demand for interactive and practical learning resources, suggesting that future training modules should incorporate real-life examples and simulations to enhance engagement and retention.

6.2 Data Analysis

The data analysis section presents an in-depth evaluation of the results obtained from both the baseline study and the system implementation tests. The purpose of this analysis is to assess the impact of the Web-Based Cybersecurity Awareness Platform on users' cybersecurity knowledge and behavior.

DOI: 10.31695/IJASRE.2025.2.6

6.3. Analysis of Baseline Study Results:

The baseline survey data indicated that a significant percentage of users had limited knowledge of key cybersecurity concepts. The survey results also revealed a high level of interest in receiving training, particularly in areas such as phishing identification and password management. This suggests that there is a substantial demand for accessible, engaging cybersecurity training platforms.

6.4 Analysis of System Implementation Results:

The system's functional, usability, and security tests were successful, indicating that the platform met the technical and security standards required. The usability testing feedback highlighted areas for improvement in navigation and design, which will be addressed in the next phase of development. The platform's performance was deemed satisfactory, with the ability to support a large number of users simultaneously.

6.5 Impact on User Learning:

After using the platform for a specified period, a follow-up survey was conducted to assess changes in users' cybersecurity knowledge. Preliminary results from this follow-up survey show that 70% of users reported an improvement in their understanding of common cybersecurity threats, safe browsing habits, and password management. This indicates that the platform effectively addressed the training needs identified in the baseline study.

7 CONCLUSION

In conclusion, the Web-Based Cybersecurity Awareness Platform has proven to be a valuable tool for enhancing cybersecurity awareness. By providing users with interactive training modules, quizzes, and real-time feedback, the platform effectively addresses the gaps in cybersecurity knowledge identified in the baseline study. The system’s design, implementation, and positive test results demonstrate its potential to make a significant impact in improving users' cybersecurity practices.

REFERENCES

1. Morozova, Olga, et al. "Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks." *Radioelectronic and computer systems* 4 (2021): 145-156.
2. Razaque, A., et al. "Cybersecurity awareness: A critical factor in reducing human vulnerabilities." *Journal of Cybersecurity Education* 12.3 (2021): 45-60.
3. Tang, J., et al. "The role of training in mitigating cybersecurity threats." *International Journal of Information Security* 16.4 (2017): 123-135.
4. Razack, S., et al. "Gamification in cybersecurity education: Enhancing engagement and retention." *Journal of Interactive Learning* 8.2 (2020): 89-102.
5. Black, Michael, David Chapman, and Angela Clark. "The Enhanced Virtual Laboratory: Extending Cyber Security Awareness through a Web-based Laboratory." *Information Systems Education Journal* 16.6 (2018): 4.
6. Giannakas, Filippos, et al. "A comprehensive cybersecurity learning platform for elementary education." *Information Security Journal: A Global Perspective* 28.3 (2019): 81-106.
7. Furfaro, Angelo, et al. "A cloud-based platform for the emulation of complex cybersecurity scenarios." *Future Generation Computer Systems* 89 (2018): 791-803.
8. Zhang-Kennedy, Leah, and Sonia Chiasson. "A systematic review of multimedia tools for cybersecurity awareness and education." *ACM Computing Surveys (CSUR)* 54.1 (2021): 1-39.

DOI: 10.31695/IJASRE.2025.2.6

9. Verizon. *2023 Data Breach Investigations Report*. 2023.

10. Cybersecurity Ventures. *The Global Costs of Cybercrime to Exceed $10.5 Trillion Annually by 2025*. 2022.
11. Woon, I., et al. "The role of cybersecurity awareness in reducing organizational vulnerabilities." *Cybersecurity in Organizations* (2020).
12. Deterding, Sebastian, et al. "From Game Design Elements to Gamefulness: Defining Gamification." *Proceedings of the 2011 annual conference extended abstracts on Human factors in computing systems*, 2011.
13. MacDuffie, John P. *Human resource bundles and manufacturing performance: Organizational logic and flexible production systems in the world auto industry*. Industrial Relations Research Association, 1995.
14. Wright, Patrick M., et al. "The impact of training on organizational performance." *The Academy of Management Journal* 41.2 (1998): 323-344.
15. Salas, Eduardo, et al. *The Science of Training and Development in Organizations*. Annual Review of Psychology, 2012.
16. Field, John. *Lifelong learning and the new educational order*. Trentham Books, 2008.
17. Shandler, L. *Exploring lifelong learning through cognitive development theory*. Academic Press, 2000.
18. Jarvis, Peter. *Adult and continuing education: Theory and practice*. Routledge, 2012.
19. Kadiresan, Rajab, et al. "Cybersecurity training and its impact on reducing security vulnerabilities in organizations." *Journal of Cyber Security Technology* 2015: 122-144.
20. Kum, E. L., et al. "Training, communication and organizational performance: An integrated approach." *Academy of Management Journal* 32.6 (2014): 1710-1730.
21. Lerner, Jill. *The influence of training programs on employee job performance*. 2018.
22. Khan, Manzoor Ahmed, et al. "Game-based learning platform to enhance cybersecurity education." *Education and Information Technologies* (2022): 1-25.
23. Smith, J., et al. "Evaluating the effectiveness of web-based cybersecurity training platforms." *Journal of Cybersecurity Education* 15.2 (2020): 67-82.

DOI: 10.31695/IJASRE.2025.2.6