International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-3, May 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.3.8
Article ID IRP-1769, Pages 65-74
www.ijircst.org

A Gamified Phishing Awareness Simulator for Senior Citizens

Bhoomi Chavan[1], Harshad Lokhande[2], Kshitij Gedam[3], and *Mrunal Kale[4]

[1, 2, 3, 4] Department of Computer Science and Engineering, MIT Art Design and Technology University, Loni Kalbhor, Pune, India

*Correspondence should be addressed to Mrunal Kale; kalemrunal06@gmail.com

Received: 24 April 2026; Revised: 12 May 2026; Accepted: 26 May 2026

ABSTRACT- This study outlines a gaming-based phishing attack simulator tailored for senior citizens, in view of the fast-growing instances of cybercrimes in which the elderly have problems detecting phishing scams in the form of scamming letters, emails, and phone calls. The proposed solution is a web application that features practical scam stories to test users. Decision-making is a crucial step in the game, and users need to take decisions based on the knowledge acquired. Immediate feedback is provided, accompanied by an explanation about the right course of action to take to avoid phishing attacks. The app will be used to track user progress and improve knowledge. This project seeks to ensure senior citizens are aware of cybersecurity and feel confident using their gadgets without fear of being scammed.

KEYWORDS- Cybersecurity Awareness, Gamification, Senior Citizens, Web Application, Phishing, Cyber threat.

I. INTRODUCTION

The use of digital technology like internet banking, UPI systems, and mobile apps has become integral to our lives. But, along with these developments, the risk of cybercrime such as phishing attacks has also escalated. One group that is particularly susceptible to the risk of digital fraud is senior citizens. Older users have a hard time recognizing fraudulent messages, emails, OTP requests, and fake calls. The lack of knowledge about how to recognize such things and their trusting nature makes them an easy target. Owing to a lack of understanding, people may suffer losses as well as confusion and fear due to these attacks. Although the problem is rising, there has been no effort made to create learning material for older users. Hence, it becomes imperative to design an efficient, easy-to-use, and interactive tool that raises cyber security awareness among seniors.

II. OBJECTIVES

The main purpose of the project is to find a viable solution that would enable elderly people to stay secure against any kind of phishing attacks. It has been designed in such a way as to help enhance cybersecurity knowledge in an effective manner.

Some of the specific purposes of the project are:

- To make the elderly aware of various phishing attacks that exist.
- To assist the users in recognizing fake texts, scam messages, fraudulent links, fake phone calls, and one-time passwords (OTP).
- To make the whole learning process safer and more interactive through the use of gamification methods.
- To build up their confidence when making transactions on digital platforms like online banking and UPI services.
- To minimize the risks of losing money due to such cyberattacks.
- To make cybersecurity knowledge more practical and comprehensible to common people.

III. LITERATURE REVIEW

Advancements in the use of technology have greatly enhanced the ease of interaction in communication, banking, and internet-based transactions. On the other hand, these innovations have been accompanied by an escalation in cyber-attacks, including phishing. This is a form of cyber-crime whereby cybercriminals seek to steal crucial information like passwords, OTPs, and bank account details by disguising themselves as a reputable party. Numerous studies have indicated that phishing has become one of the most prevalent and efficient forms of cyber-attacks because it exploits human errors rather than system flaws. Studies reveal that those individuals with little or no technical expertise are susceptible to becoming victims of these attacks[1],[2] Despite the widespread nature of these threats, research specifically addressing cybersecurity challenges and awareness among the elderly remains limited[3].

This demographic often exhibits unique learning styles and cognitive considerations that necessitate tailored educational approaches for effective cyber threat mitigation [4].

Senior citizens are among the most vulnerable demographics. Literature suggests that older adults have faced difficulties with regards to computer literacy, comprehension of internet applications, and inclination to accept messages from unidentified sources. Some of the methods that have been introduced to combat the problem of phishing awareness is shown in the Table 1.

Table 1: Comparison of Existing Cybersecurity Awareness Approaches

Approach	Method Used	Advantages	Limitations
Education Programs and Workshops [21]	Awareness sessions, seminars, training classes	Improves basic knowledge, easy to organize	Not interactive, users may forget over time, low engagement
Phishing Detection using Email Filters [22]	Automated filtering of suspicious emails using algorithms	Reduces phishing emails automatically, fast detection	May miss advanced scams, does not educate users
Web Browser Security Warning Mechanisms [23]	Displays warnings for unsafe websites or links	Provides real-time alerts, protects users while browsing	Users may ignore warnings, limited to browser usage only
Cyber Security Training Programs [24]	Structured learning modules and courses	Provides detailed knowledge, improves understanding	Often complex, not suitable for senior citizens, less engaging

All the mentioned measures work effectively to some degree; however, they have proven to be ineffective as far as dealing with elderly users because of their complexity and non-interactional approach.

Recently, scientific research pointed out that using a gamified approach could prove highly beneficial for teaching cybersecurity skills. In general, gamification means incorporating challenges, rewards, and feedback into the process of interaction. In addition, according to various studies, people learn faster when actively taking part in situations where decisions need to be made. Nevertheless, the gap related to user-oriented applications, especially designed for older users, still exists[5],[6] (See the table 2).

Table 2: Comparison of Existing Methods Used

Research Papers	Method Applied	Disadvantage
Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions [1]	Phishing awareness training	Lack of interactivity
Teaching Johnny not to Fall for Phish [2]	Educational anti-phishing system	Less appealing to senior citizens
A Game Design Framework for Avoiding Phishing Attacks [4]	Game-based learning	Not designed for elderly users
Proposed System – Gamified Phishing Awareness Simulator for Senior Citizens	Web-based gamified phishing awareness simulator	Limited number of participants tested

IV. METHODOLOGY

Project methodology will involve the creation and implementation of a user-friendly, game-based mobile application phishing awareness simulator for elderly individuals. It will be designed with a systematic approach so that the system is both effective and easy to use.

A. Requirement Analysis:

The challenges experienced by senior citizens have been analyzed first. Some of the common challenges experienced by elderly individuals include difficulty in detecting hoax messages, navigating the application interface, and making secure decisions.

These findings led to the determination of the following requirements for the system: Easy-to-navigate interface Hoax message scenarios in real life, Step-by-step instructions, No technical complexities.[7],[8],[9]

B. Creation of Phishing Scenarios

Phishing scenarios were created for each type of commonly used cyber scam, like SMS scams, Email scams, WhatsApp scams, One Time Password (OTP) scams, and Bank scams. These are made to be realistic so that the users will be aware of what scams look like in reality. The phishing exercises that are found in the mobile based application can be controlled using a central database in order to facilitate different phishing scams in front of the users. These exercises have been designed using simple language, graphics, and the correct form of messages appropriate for older individuals. It should be noted that the mobile application enables the user to practice safely without any cybersecurity threats.

C. Gamification Implementation

In order to make the learning process interactive and engaging, gamification methods such as reward systems based on scores, several levels of difficulty, immediate feedback, and performance tracking will be used in the proposed system. This method will help learners increase their knowledge about phishing while being highly engaged and motivated. These gamification elements are implemented within the design of the interface of the mobile-based application. The system tracks the scores, levels, and progression of the users through the backend database of the system, which enables constant tracking of the performances. This application ensures that the system is easily accessible without complicated installation procedures, which makes the system more convenient for the elderly people.

D. System Design

This system is designed to be a mobile based application through which the user gets a dynamic experience while learning about phishing scams. The system has been made senior-friendly in terms of its interface by using large buttons, easy language, and visuals so that it can be used easily by senior users.

The idea of using a scenario-based learning method was used in which scenarios of phishing attacks like SMS scams, email scams, WhatsApp scams, and OTP scams were presented to the users. The users had to analyze those scenarios and make decisions accordingly. Through realistic simulations, the users would learn how phishing scams are executed in the real world. Scores, levels, and feedback

mechanisms were used to keep the user motivated through the process of learning.

See the Figure 1, it shows the workflow diagram of our system.

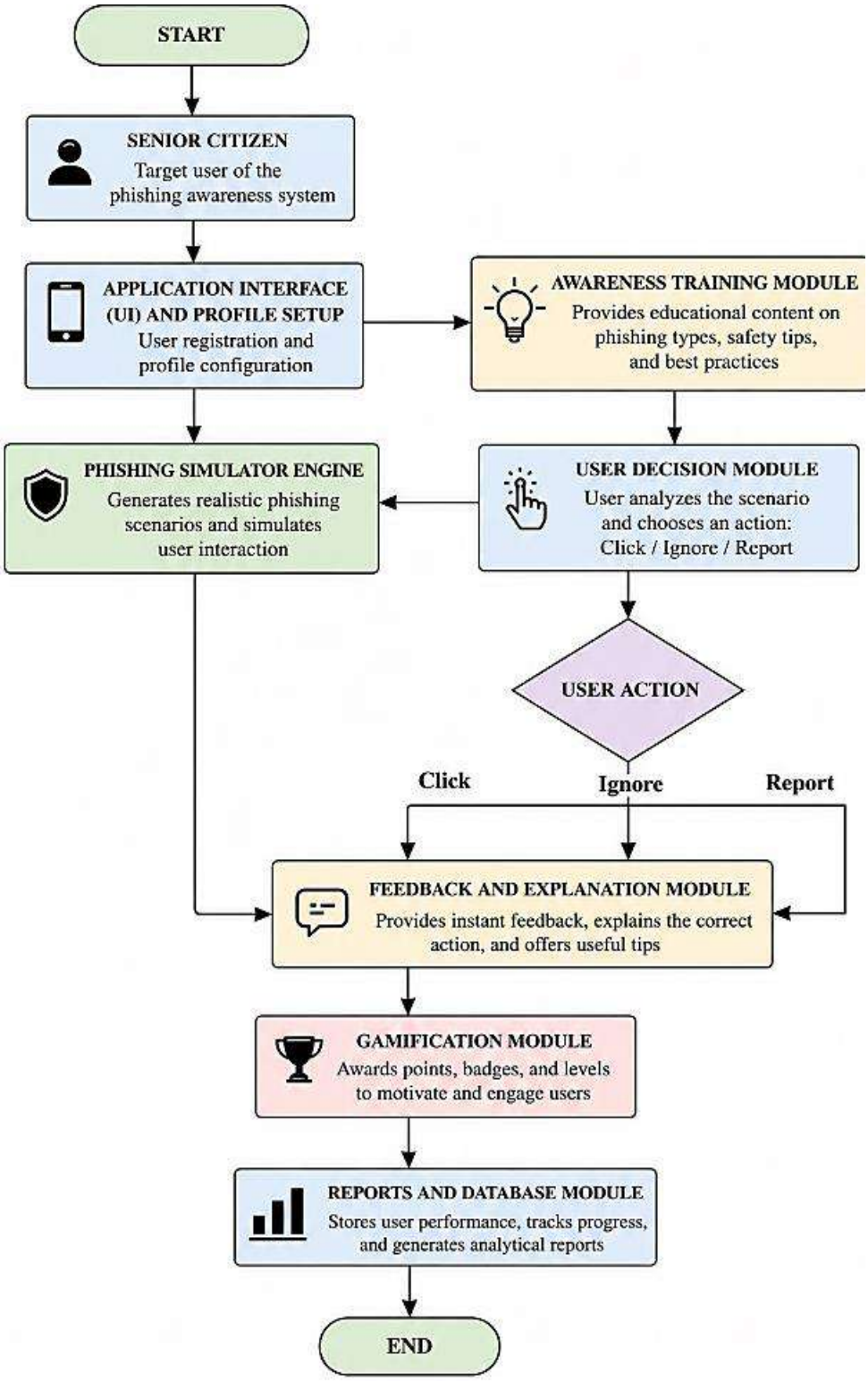

Figure 1: Flow chart of our system

A. Feedback and Learning System

- After each user response, the system offers:
- Why the situation is safe or dangerous Information on safety precautions and signs of danger. How to respond appropriately in reality.
- Such a learning opportunity ensures that users can learn from their mistakes in a safe setting.

B. Testing and Verification

- The software undergoes testing to verify its:
- Ease of use by elderly individuals Functionality in all scenarios Readability and navigability Accuracy of feedback and response generation

- The user's interaction with the program is monitored to determine if the program successfully raises awarenes and enhances decision-making skills.

V. SYSTEM ARCHITECTURE

The architectural design of the proposed system tries to build an easily navigable environment for elderly people. The modular architecture in this case ensures that the components serve different purposes in a way that makes the operation of the application seamless. Once the input is made into the system, the application layer will process the input by obtaining appropriate information from the database and evaluating the input made by the user. On the basis of the result of this evaluation, instantaneous feedback will be given to the user with appropriate scores.
Moreover, the architecture is flexible and scalable in a sense that it can incorporate additional scenarios in the future, uch as support for multilingual and voice assistance. Security issues are also considered in the sense that there will be no collection of personal information from the user. The logic layer serves as the kernel of the entire application, taking care of user input processing, decision-making, gameplay management, and providing corresponding responses to them. The data layer involves a well-designed scenario database comprising several phishing attack types, including fake SMS, emails, WhatsApp messages, and OTP fraud attacks[10],[11],[12]. See the below Figure 2.

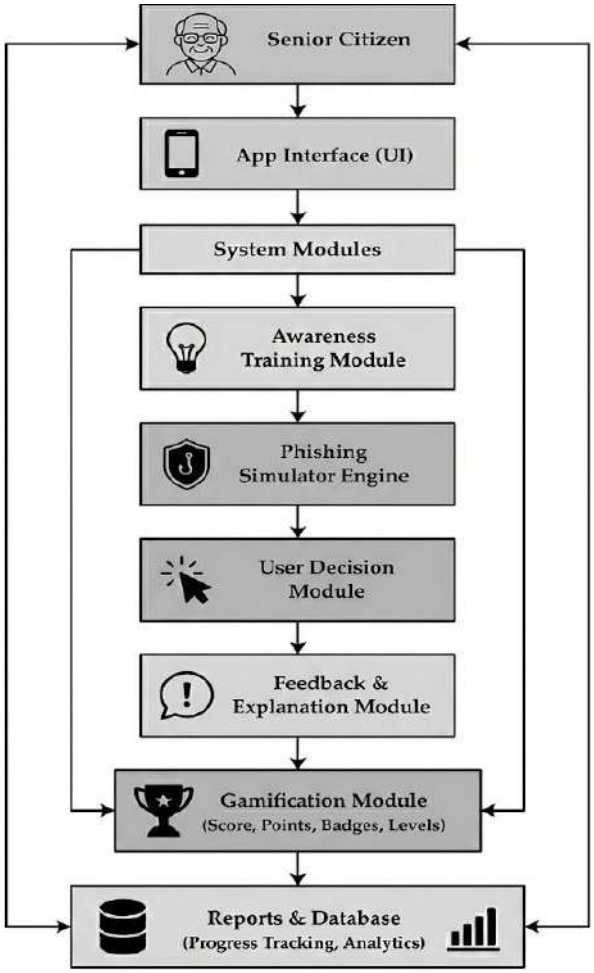

Figure 2: System Architecture

- User Interface (UI) Layer: This forms the front end of the application where the user interface occurs. The UI layer is developed specifically for senior citizens, and it includes: Larger buttons Simpler language Intuitive navigation Content that relies on visuals. The user interface layer shows phishing examples through SMS, emails, or phone calls and enables users to choose their actions.
- Application Logic Layer: This represents the main processing engine of the software. Its responsibilities include Showing scenarios to the user Obtaining user feedback (safe / scam classification) Analyzing user inputs Determining the flow of the game (level, score, etc.) It makes sure that the program works efficiently and appropriately reacts to user actions.
- Scenarios Database: This module contains all the information related to phishing scenarios in the software, such as: Phishing text SMS messages Phishing emails Scam phone calls WhatsApp scams. The Scenario Database is an essential feature in the system responsible for storing all phishing content utilized by the application. The database contains various scenarios created according to real-life phishing tactics employed by criminals.

Various types of phishing incidents are included in the database, including false SMS messages, fake emails, WhatsApp scams, and OTP-based fraud phone calls. Each

scenario in the database comprises a message, a set of user choices (which could be safe or scam), and an explanation of the message. Once the user selects an option, the database will provide relevant feedback immediately. Scenarios within the database are classified into varying degrees of difficulty. They start with the simplest form, which may seem obvious to users, and increase in difficulty level towards the most realistic phishing attacks. The database can accommodate other phishing scenarios in the future without any modifications to ensure the database is current with changing cyber threats.

- Feedback and Progress Monitoring Module: This module serves to: Provide immediate feedback upon completion of the step. Explain whether the scenario is safe or not Show safety pointers and warning symbols. Monitor user performance (score, level, progress). The general flow of the system may be summarized as follows: User opens the app. Phishing scenario is shown User makes a choice (safe or scam). System analyzes the answer. Feedback and explanation are provided. Score and progress are updated. Next scenario is shown. Such an architectural design makes sure that the system will be simple, scalable, and efficient, and at the same time will make learning enjoyable and appropriate for elderly people.

VI. RESULTS

The designed phishing simulation game tool was assessed for its usability, efficiency, and engagement level, especially with senior users. The assessment looked into how effectively the mobile-based application enhances phishing skills, decision-making, and confidence levels using gamified approaches.

A. Operational Outcome

The designed simulation app has successfully replicated various forms of phishing attacks including SMS frauds, phishing emails, WhatsApp scam messages, and deceptive phone calls. With the simulation software, users are able to assess various phishing scam scenarios and make their decision based on whether they find the situation secure or not. Instantaneous feedback is available immediately after every decision made by the user with proper explanations of all possible warning signs that the phishing message might include. User scores have been kept in order to measure user performance levels.

In conclusion, the Gamified Phishing Awareness Simulator for Senior Citizens has proven to be effective in improving cybersecurity awareness among elderly people. At first, most users were unable to identify phishing attacks especially when the messages contained urgent requests for OTP, fraudulent messages from banks, suspicious links to financial transaction pages, or emotionally driven scam messages. With time, users are becoming adept at spotting warning signs such as urgent messages, grammar mistakes, suspicious links, unknown senders, and demands for confidential information.

Gamification elements, such as scoring mechanisms, levels, feedback notifications, and progress, boosted engagement levels and motivated users to continue with their learning process. The elderly were able to gain confidence in using digital tools for activities like online banking, UPI payments, WhatsApp communication, and mobile apps. Moreover, the program provided a secure space where people can make mistakes while learning without exposing themselves to any cybersecurity threats. In conclusion, the mobile application designed proved to be effective based on its operational performance due to its interactive learning approach, practical phishing simulation, and good usability design.

B. User Knowledge and Understanding

It was found that users can: Be better aware of phishing emails through repeated usage Recognize warning signs like urgent emails, unrecognized links, and OTP requests Perform actions correctly during doubtful circumstances. Scenario-based learning allowed users to learn practically rather than just theoretically.

C. User Experience (Elderly Focus)

Upon conducting testing and observing users: An easy-to-use interface made the app convenient for elderly users to navigate large buttons and instructions made using the app less confusing Users felt comfortable in learning from safe environment Immediate feedback assisted in minimizing fears and boosting confidence. Gamification was well received by users. Engagement via Gamification. Gamification techniques like scoring, levels, and tracking helped increase: Engagement of the users Motivation to keep learning Retention of the concepts of cybersecurity. There was higher engagement than the usual approaches used[13],[14],[15].

This project shows how a simple, engaging, and gamified approach is sufficient for teaching cybersecurity to seniors. From the findings, the recommended system appears to be an appropriate strategy in minimizing phishing threats amongst older adults through awareness and interactive learning techniques. This is consistent with studies that indicate the use of gamification, like that used in this simulation, always leads to improvement in terms of retaining information and behavior change during cybersecurity training [16]. It is also consistent with previous studies on the effectiveness of serious gaming on improving the ability of users to recognize phishing scams compared to conventional means of education [17], [18].

Demographics of Participants: The experiment-based assessment was performed on 20 participants who are senior citizens within the age group of 55 to 70 years. The participants consist of both male and female individuals with basic technical skills to operate smartphones and use the Internet. Most of the participants have prior information about using services like UPI, WhatsApp, online banking, etc.; however, they lack information on phishing, scams, and cybersecurity.

D. Experimental Evaluation

An experiment was carried out on the use of the proposed system by conducting a simple usability test on thirty seniors ranging in the age bracket from 55 to 70 years old. These individuals had prior knowledge about smartphone usage but lacked adequate knowledge concerning cybersecurity. Participants were asked to conduct a phishing awareness pre-test before interacting with the gamified phishing awareness application. A post-test followed after participants engaged with the application and conducted phishing scenarios. Improvement was noted in terms of phishing awareness and scams identification capabilities. This is given in Table 3 and also in Figure 3.

Table 3: Experimental evaluation of user performance in pre-test and post-test

Evaluation Metric	Pre-Test	Post-Test
Awareness Score	42%	84%
Scam Identification	38%	81%
User Confidence	45%	86%
User Engagement	52%	90%

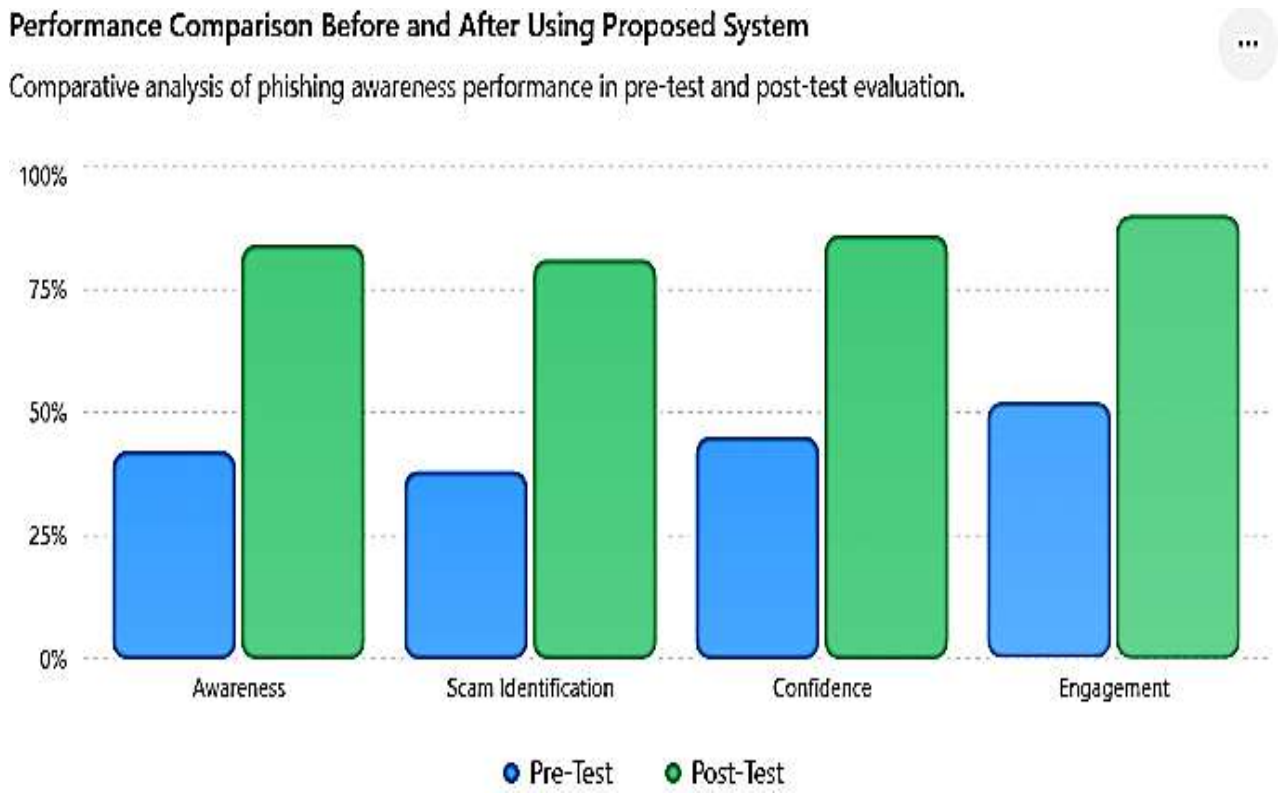

Figure 3: Comparison of performance of users before and after utilizing the proposed system

In the above Figure 3, it illustrates the effectiveness of the proposed phishing awareness system by comparing user performance in pre-test and post-test evaluations. The graph shows significant improvement across all measured parameters, including awareness, scam identification, confidence, and engagement after using the system. Post-test scores are considerably higher than pre-test scores, indicating that the proposed system successfully enhanced users' ability to recognize phishing attempts, improved their confidence in identifying scams, and increased overall engagement in cyber security awareness activities. . In Figure 3, the user interface of the phishing awareness simulator is presented, which provides information on the dashboard through which phishing scenarios can be accessed by users to monitor their learning status.
Graphical representations of the final outputs have been shows in Figure 4, and Figure 5.

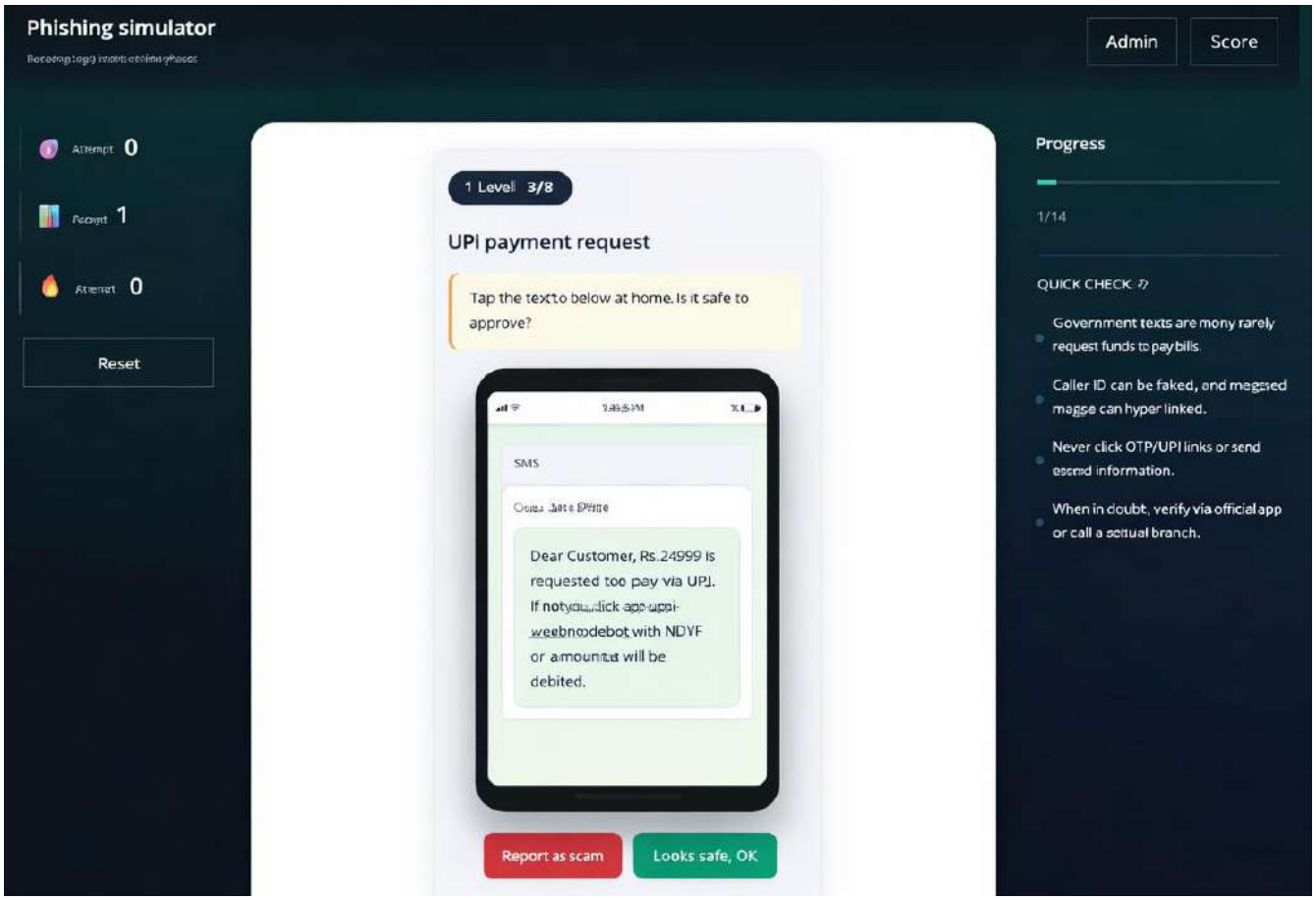

Figure 4: Login and phishing simulation dashboard of the proposed system

In the above Figure 4, it depicts the phishing detection model in an interactive manner where the user comes across some suspicious messages from which the user has to judge if they are legitimate or phishing messages.

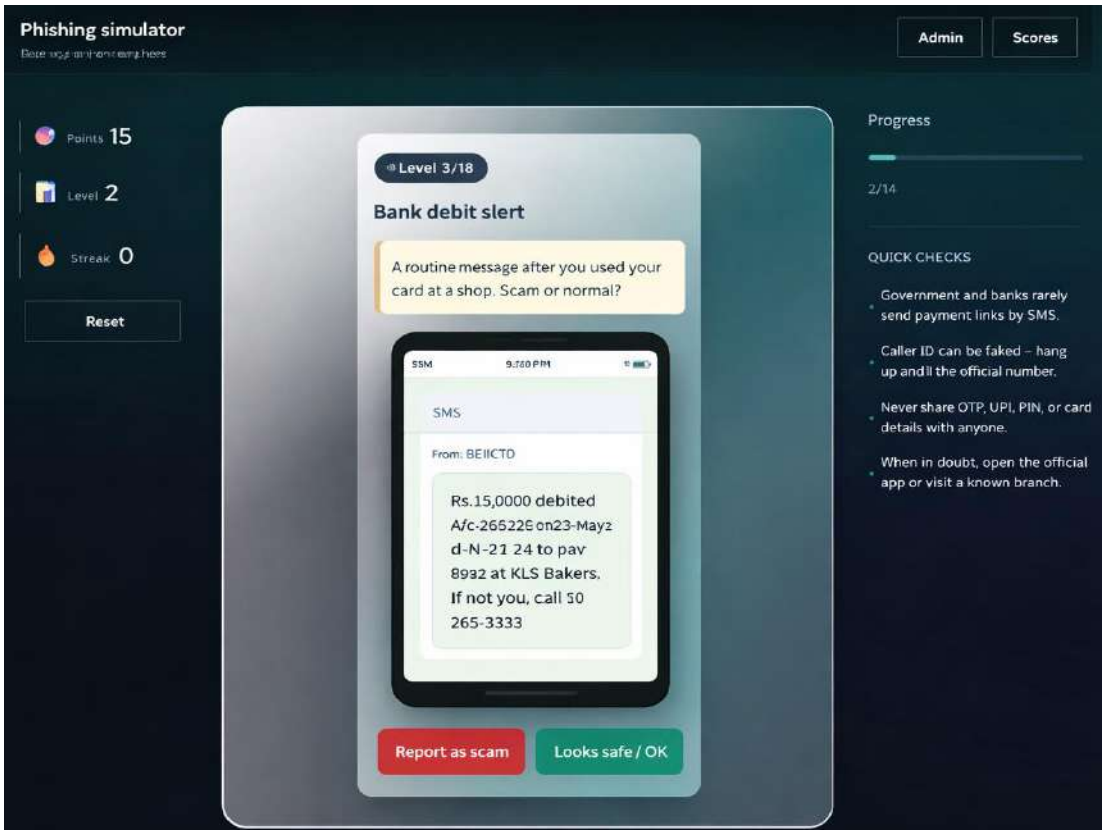

Figure 5: Phishing detection interface

In Figure 5, it shows the feedback generation part of the system, where feedbacks are given to the user after his/her decision.

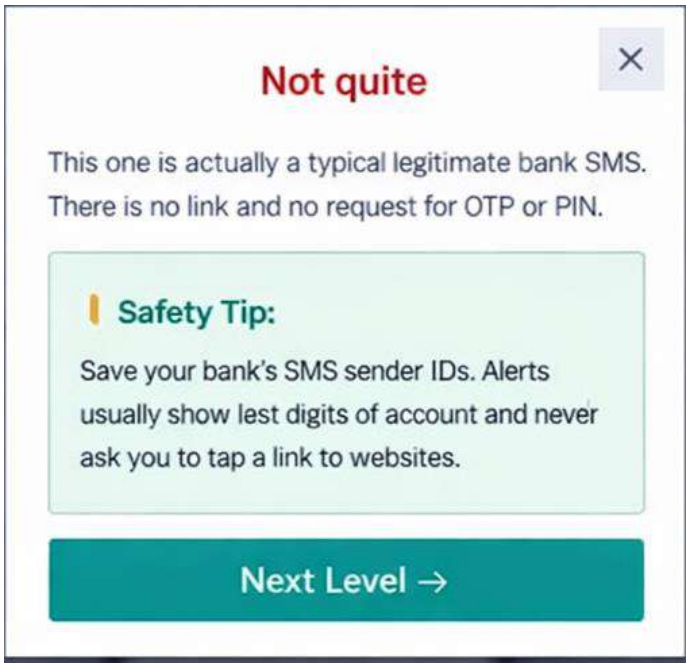

Figure 6: Feedback and warning notification generated after user response

In above Figure 6 shows the system immediately reacts to the user's action in the phishing scenario, issuing a warning notification and explanatory feedback. In this case, the system informs the user that the message is a legitimate SMS from a bank and states that there are no malicious elements such as phishing links or OTP requests. Also, a security tip is provided to guide users on how to spot genuine bank messages. This feedback module helps users understand, boosts cybersecurity awareness, and provides interactive learning with guided explanations.

VII. DISCUSSION

In below Table 4 reveals that traditional methods like awareness programs, detection systems, and structured training modules often suffer from drawbacks such as passive learning, low engagement, and dependence on automated systems. However, the system proposed in this paper offers an interactive and practical learning environment based on the real-life phishing scenarios, decision-making activities, immediate feedback, and gamification elements. The comparison indicated that the proposed system is more engaging, user-friendly, and effective for senior citizens in improving cybersecurity awareness and independent scam identification skills.

Table 4: Comparison of Existing Phishing Awareness Approaches and Proposed System

Approach	How it Works	Limitation	Your System Improvement
Awareness Programs	Users are taught through sessions or reading material	Passive learning, easy to forget	Provides hands-on learning through real-life scenarios
Detection Systems (Email/Browser)	Automatically detect and warn about phishing	Users depend on system, no skill development	Trains users to identify scams independently
Training Modules	Structured cybersecurity courses	Complex and not engaging for seniors	Simple interface with easy language and visuals
Our Gamified Simulator	Interactive scenarios with decision-making and feedback	—	Practical, engaging, and confidence-building learning for senior citizens

(Source: Compiled by the authors)

VIII. CONCLUSION

This paper presents a gamified phishing awareness simulator for senior citizens. Due to the high prevalence of cyber-fraud with increasing numbers of digital platforms such as online banking services and various mobile apps, older adults who have poor technical knowledge have become increasingly exposed to the risk of being targeted. The suggested approach to dealing with this problem involves creating an interactive and easily accessible tool. It will allow users to learn about cybersecurity using realistic scam examples. From the experimental analysis, it can be clearly seen that the system is capable of improving phishing awareness, scam detection skills, and the level of user confidence while working on digital platforms. Further improvements can be made to the system by incorporating support in multiple languages, voice guidance, and phishing prevention tools. Thus, by using educational aspects in conjunction with gamification, one can achieve simplicity, efficiency, and applicability of learning process in the app. As it follows from the results obtained during testing the program, this approach can help significantly raise cybersecurity awareness among older adult users as well as improve their decision-making and confidence. Overall, this project has not only academic importance but also a considerable social value because it targets the vulnerable social group[19],[20].

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proc. SIGCHI Conf. Human Factors in Computing Systems (CHI)*, 2010, pp. 373–382. Available from: https://doi.org/10.1145/1753326.1753383

[2] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 1–31, 2010. Available from: https://doi.org/10.1145/1754393.1754396

[3] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work? A literature review of empirical studies," in *Proc. 47th Hawaii International Conference on System Sciences (HICSS)*, 2014, pp. 3025–3034. Available from: https://aaltodoc.aalto.fi/items/3cd38178-dacf-47ed-b719-8caba5c1f5f9

[4] 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, 2013. Available from: https://doi.org/10.1016/j.chb.2012.12.018

[5] H. N. Lokhande and S. D. Markande, "Adaptive streetlight controlling for smart cities," *International Journal of Applied Engineering Research*, vol. 13, no. 10, pp. 7719–7723, 2018. Available from: https://tinyurl.com/mtx4wefh

[6] M. D. Grilli, N. P. M. Kaufman, A. Gluck, D. H. Nguyen, A. M. Greenberg, and P. A. Reuter-Lorenz, "Is this phishing? Older age is associated with greater difficulty discriminating between genuine and phishing emails," *NPJ Digital Medicine*, vol. 3, no. 1, 2020. Available from: https://doi.org/10.1093/geronb/gbaa228

[7] D. James, L. A. Boyle, and D. A. Bennett, "Correlates of susceptibility to scams in older adults without dementia," *Journal of Elder Abuse & Neglect*, vol. 26, no. 2, pp. 107–122, 2014. Available from: https://doi.org/10.1080/08946566.2013.821809

[8] Pelicano'll, M. D. Grilli, N. P. M. Kaufman, and P. A. Reuter-Lorenz, "Phishing vulnerability compounded by older age, APOE4, and lower cognition," *PNAS Nexus*, vol. 3, no. 2, 2024. Available from: https://doi.org/10.1093/pnasnexus/pgae296

[9] M. Button, C. Lewis, and J. Tapley, "Preventing fraud victimisation against older adults: A typology of tools and strategies," *Crime Science*, vol. 13, no. 1, 2024. Available from: https://doi.org/10.1016/j.ijlcj.2024.100672

[10] S. Rathi, S. Pande, and H. Lokhande, "Smart Garbage Collection System," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 5, 2017. Available from: https://www.ijraset.com/fileserve.php?FID=7151

[11] University College London (UCL), "Older adults as victims of online financial crime," *UCL Policy Briefing*, Dec. 2021. Available from: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003165828-15/futures-gloria-laycock

[12] Safer Internet India, "Understanding senior citizens' experience with online fraud: A survey-based assessment," 2025. Available from: https://doi.org/10.1108/JAP-11-2025-0041

[13] H. Chen, J. Smith, and L. Wang, "Examining older adults' vulnerability to online health scams: A Routine Activity Theory approach," *Frontiers in Public Health*, 2025. Available from: https://doi.org/10.3389/fpubh.2025.1585851

[14] Y. Shang, "The psychology of the internet fraud victimization of older adults," *Frontiers in Psychology*, vol. 13, 2022. Available from: https://doi.org/10.3389/fpsyg.2022.912242

[15] Burton, "Exploring how, why and in what contexts older adults are at risk of cybercrime victimization," *Computers & Security*, 2022. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0531556521004605

[16] V. Kara Giannopoulos, "Cybercrime awareness and victimization in older individuals," *Computers in Human Behavior Reports*, 2021.

[17] Pacheco, "Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors," *arXiv Preprint*, 2024. Available from: https://arxiv.org/abs/2403.09208

[18] K. L. Tan et al., "Cybercrime vulnerability among older adults in Malaysia," *Arhiv za Tehničke Nauke*, 2025. Available from: https://arhivzatehnickenauke.com/article/634

[19] L. R. Shapiro, "Cyber-enabled imposter scams against older adults in the United States," *Security Journal*, 2025. Available from: https://doi.org/10.1057/s41284-025-00483-3

[20] H. N. Lokhande and S. R. Ganorkar, "Optimizing Real-Time Object Detection on Edge Devices: A Transfer Learning Approach," *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, vol. 12, no. 21s, pp. 3896–3903, 2024. . Available from: https://tinyurl.com/9pv47d8e

[21] I. C. Li, Y. C. Chen, L. L. Hsu, C. H. Lin, and N. J. Chrisman, "The effects of an educational training workshop for community leaders on self-efficacy of program planning skills and partnerships," IEEE Journal of Advanced Nursing, vol. 68, no. 3, pp. 600–613, Mar. 2012, doi: 10.1111/j.1365-2648.2011.05755.x. . Available from: https://doi.org/10.1111/j.1365-2648.2011.05767.x

[22] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 4, pp. 2070–2090, 2013, Available from: https://doi.org/10.1109/SURV.2013.030713.00020

[23] Venn, “Browser Security in 2025: Threats, Defenses, and 5 Security Solutions,” *Venn Learn Center*.. Available from: https://www.venn.com/learn/browser-security/

[24] S. Nasir, “Exploring the effectiveness of cybersecurity training programs: Factors, best practices, and future directions,” in *Proceedings of the Cyber Secure Nigeria Conference*, vol. 1, Jul. 2023, pp. 9–22.. Available from: https://www.cybersecurenigeria.org/proceedings