Design and Development of Anti-Phishing AG: A Web-Based 3D Serious Game to Improve Phishing Awareness Among Students in Saudi Arabia

Shahad Alzahrani
Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
salzahrani1484@stu.kau.edu.sa (corresponding author)

Sahar Badri
Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
skbadri@kau.edu.sa

Farrukh Nadeem
Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
fabdullatif@kau.edu.sa

Received: 7 February 2026 | Revised: 26 March 2026 | Accepted: 3 April 2026

 DOI: https://doi.org/10.48084/etasr.18035

ABSTRACT

Phishing remains one of the most prevalent social-engineering threats, targeting users' decision-making to obtain sensitive information. To effectively counter such threats, students must be well informed about how phishing attacks work, including the methods and strategies used. However, phishing awareness training is not consistently embedded in school curricula, and when available, it is often delivered through limited, non-interactive sessions. This study presents Anti-Phishing AG, a web-based 3D serious game designed to improve students' ability to recognize and respond to phishing attempts through interactive scenarios and immediate feedback. The game is developed based on a novel assessment and training framework grounded in prior empirical research and aligned with the Saudi National Cybersecurity Authority (NCA) standards and guidance. The study outlines the design of the novel Anti-Phishing AG framework, the development process of the web-based 3D game, and the development and validation of an accompanying survey instrument to measure awareness and learning outcomes. The game is evaluated using a one-group pre-test/post-test design with 702 students from middle and high schools. The findings of this study highlight the value of interactive serious games and tailored educational tools in raising cybersecurity awareness. The study provides a reusable foundation for similar awareness tools. It supports national goals by contributing to cybersecurity education in Saudi society, aligning with one of the key objectives of Vision 2030.

Keywords-phishing awareness; serious game; web-based 3D game; cybersecurity education; assessment framework; Saudi Arabia; Anti-Phishing AG

I. INTRODUCTION

The transition from the physical world to the digital world has brought many benefits, but it has also introduced new risks and challenges. These changes have raised serious concerns about protecting personal and financial information online. Cybercrimes have proliferated rapidly and become a significant global concern [1]. Among these threats, social engineering attacks are particularly concerning because they do not require advanced technical skills, unlike hacking or malware attacks, which are generally beyond the reach of ordinary users. As a result, social engineering techniques are being used to exploit human behavior [2]. Phishing is one of the most common and dangerous forms of social engineering-based cybersecurity threats. It is responsible for 90% of data breaches and

compromises millions of credentials [1]. According to Cisco [2], phishing involves delivering fraudulent messages that appear to originate from trustworthy sources, most commonly through email. The goal of phishing is either to infect the victim's devices with malware or to steal personal information, such as login credentials and credit card numbers. To trick the target into revealing his credentials, attackers send fraudulent messages that appear to come from trusted sources [3]. They use spoofed websites, emails, phone calls, and other forms of communication to deceive the target. These messages are often claimed to be from banks, e-pay systems, and other reputable organizations. The former could be about changing login issues, data loss, or system failure. As a result, victims may unknowingly provide sensitive information such as bank account information, passwords, credit card information, and other financial data [4]. Phishing attacks are among the most significant cybersecurity threats, particularly affecting younger users who may lack sufficient awareness and experience. In Saudi Arabia, where digital transformation is a central component of Vision 2030, enhancing students' ability to recognize and respond to phishing attempts has become important. The present study contributes to this need by introducing a scalable, web-based educational tool that can be implemented in schools to improve phishing awareness.

According to the Anti-Phishing Working Group (APWG), a global organization of counter-cybercrime responders established in 2003, the third quarter of 2022 saw 1,270,883 phishing attacks, the worst quarter for phishing they have ever observed [5]. For instance, Kaspersky Solutions detected and exposed 478,155 phishing attempts targeting businesses in Saudi Arabia during the first half of 2022. A total of 74% targeted online shops, 20% targeted payment systems, such as PayPal and Apple Pay, and 6% targeted domestic banks [4]. These attacks steal people's money and breach their privacy. Despite the growing threat of phishing attacks, many individuals lack the knowledge and experience necessary to protect themselves, particularly against phishing. As a result, strategies for defending against various phishing attack types are needed. Raising awareness of phishing attempts and different types is one of them. There are several ways to increase this type of awareness, with the effectiveness of each approach varying. Research shows that technical controls alone are insufficient to mitigate phishing attacks, highlighting the importance of structured cybersecurity awareness and training programs [6]. In particular, developing cybersecurity awareness models tailored to Saudi students is essential for addressing social engineering threats in a culturally appropriate manner [7]. Students need to understand the strategies and tactics used by attackers to protect themselves. However, not all schools offer cybersecurity awareness programs. Even if they do, it is often limited to a single class or workshop.

According to [8], passive methods such as email and SMS messages are ineffective in raising awareness of cybersecurity and phishing attacks. These traditional methods can be supplemented or replaced by more engaging tools, such as games and videos, to enhance the learning experience. An engaging, game-based approach can be an innovative way to teach students about phishing attacks in a manner that aligns with their age and interests.

The use of educational games, simulations, and training tools has been explored to improve phishing awareness. Authors in [9-17] proposed different types of phishing awareness games designed to teach users about phishing techniques and how to identify them. For example, authors in [9, 12] developed phishing awareness games based on the Extended Design, Play, and Experience (EDPE) framework. In [9], the game relied on scripted simulations and quizzes to teach phishing detection. While the game improved users' ability to identify malicious links, particularly among technical students, its design may not be suitable for non-technical users or adaptable to diverse real-world phishing scenarios. In contrast, authors in [12] used a military-style narrative to educate players through missions. The game successfully boosted phishing awareness across all demographics, primarily focusing on URL-based phishing without comparing its impact to traditional methods. Other studies adopted simple and engaging story-based game designs. For example, authors in [10] created a classic game using a fish-and-worm theme to teach users how to identify phishing URLs. It focused on three types of links: subdomain, IP-based, and deceptive. The results indicated that the game was more engaging and effective than traditional learning methods. Similarly, authors in [11] developed the "Sir Firewall" game, which used storytelling to teach phishing detection through email cues. The game increased participants' confidence and knowledge, especially among corporate users, due to its motivational gameplay and immediate feedback. However, not all game-based approaches have demonstrated positive outcomes. Authors in [17] used a bird-and-worm metaphor to teach phishing URLs; however, it failed to achieve any significant awareness. The key issues identified included poor game design, technical limitations, and insufficient instruction before gameplay. Alternative training approaches have been investigated. Authors in [13] compared game-based learning to Context-Based Micro-Training (CBMT) for spotting phishing emails. While both methods were effective, CBMT demonstrated higher accuracy and better behavioral outcomes.

Authors in [15] introduced PhishDefend Quest, a scenario-based game that utilizes social engineering tactics, QR-coded cards, and role-based simulation to teach spear-phishing defense. It offered engaging gameplay and showed strong learning outcomes, especially in URL identification. Also, a game was presented in [14], targeting teenagers in Tanzania. It was found that the culturally tailored mobile game significantly improved both short-term and long-term phishing knowledge compared to traditional methods. Despite these advancements, there are several limitations in existing research. Authors in [9-13, 15, 17] focused mainly on phishing URLs or phishing emails, while other phishing types, such as social engineering, SMS phishing (smishing), or voice phishing (vishing), received less attention. Additionally, most games are developed in English and are not designed for Arabic-speaking users. Except for the game in [12], which was specifically created in Arabic, there are very few Arabic-language educational games addressing phishing awareness. Another limitation is that poorly designed games may fail to improve awareness if they are not accompanied by effective instructional content or engaging gameplay mechanisms [13, 17]. Therefore, the

success of educational cybersecurity games depends heavily on their design quality, cultural relevance, and ability to engage users effectively.

Different evaluation methods have also been used in previous studies. Authors in [9-10, 12] employed a pre- and post-test approach, using a list of URLs to evaluate improvements in phishing detection skills. The game proposed in [10] consisted of four rounds, each focusing on a different type of deceptive URL. In contrast, authors in [14, 26] conducted a survey among 121 teenagers from three types of schools to assess cybersecurity awareness before introducing a mobile game designed to improve phishing detection. Authors in [13] conducted experiments within an email system environment to analyze phishing email detection behavior, while authors in [18] implemented a simulated phishing attack system and embedded training at a large Australian higher education institution. Authors in [19] implemented in-game tests (pre-test and post-test) in a game to analyze its potential influence on students' learning. Additionally, they developed an online survey to gather feedback about the game from students. Authors in [20] evaluated participants using lists of phishing emails before and after training. Authors in [21] discussed the motivation, design, and empirical evaluation of a non-digital game called "PhishI", which aimed to enhance phishing awareness.

Although these studies demonstrate the potential of educational games in improving phishing awareness, there is a lack of Arabic-language phishing awareness games designed specifically for school students. Furthermore, most existing games focus on limited phishing scenarios, particularly phishing URLs or email-based attacks. To address these gaps, the present study introduces the development and evaluation of Anti-Phishing AG, a well-designed educational game for middle and high school students in public and private schools in Saudi Arabia. This game is developed in Arabic. The game's scenarios encompass a range of phishing attack types beyond URL-based phishing. To measure its impact, a survey was conducted with 702 students before and after they played the game. The survey was developed based on the professional framework provided by the Saudi National Cybersecurity Authority (NCA) and previous research. Table I presents a comparison between Anti-Phishing AG and other studies.

TABLE I. COMPARISON OF THE PROPOSED GAME WITH PREVIOUS STUDIES

Study	Arabic language	Cover vishing and smishing attacks	Directed to non-technically educated people	Characters with the student's name and gender
[10]			✓	
[11]			✓	
[12]	✓		✓	
[13]			✓	
[14]		✓	✓	✓
[15]			✓	
[16]		✓		
[17]			✓	✓
Proposed	✓	✓	✓	✓

The key objectives of this study are:

- Designing a reliable survey to measure students' awareness of phishing. The survey is based on earlier studies and the NCA framework. Its effectiveness is tested before and after the game.
- Building a novel, structured framework that guides the development of the Anti-Phishing AG and supports the evaluation of phishing awareness through surveys.
- Implementing a high-quality game (Anti-Phishing AG) using a suitable platform that is convenient for the intended students to improve awareness of phishing attacks.

II. MATERIALS AND METHODS

A. Anti-Phishing AG Framework

Figure 1 outlines a multi-phase approach, which is a novel framework for building and evaluating surveys, as well as developing and accessing Anti-Phishing AG [29]. It is structured into three main phases: Phase 1 (software phishing survey), Phase 2 (game development), and Phase 3 (assessment).

B. Software Phishing Survey

This initial phase focuses on gathering data and designing survey questions to understand software phishing. Data gathering involves collecting relevant information from the NCA standards and frameworks, as well as previous studies. Based on the gathered data, specific survey questions are designed. The latter undergo validation based on previous studies and input from the cybersecurity authority. After validation, the first survey is conducted to gather information from the middle and high school students.

C. Game Development

This phase encompasses the entire development process of the anti-phishing game, divided into the pre-production, production, and post-production stages. Pre-Production includes concept development and analysis, storyboarding, research and development, prototyping, and mapping. The production stage involves 3D modeling, animation, programming, and implementation. The final post-production stage includes testing and launch.

D. Assessment

The final phase focuses on evaluating the effectiveness of the Anti-Phishing AG. A second survey is conducted after the game deployment to measure how awareness increased afterward. The collected information is then analyzed statistically to measure the awareness gained by users through the game. IBM SPSS Statistics is used for analyzing the results, while the Shapiro-Wilk test is utilized to determine the normality of data distribution [22]. Additional tests are conducted to further understand the results; specifically, the Wilcoxon signed-rank test is used to assess the statistical significance of the improvements in participants' knowledge and behaviors [23]. Correlation analysis is employed to determine the relationship between phishing awareness levels before and after the game and demographic factors. Also, Pearson correlation is deployed to calculate the relationship

between the awareness scores before and after the game. Moreover, the means of the answers to each Likert-scale question are computed before and after the Anti-Phishing AG to assess its efficacy.

The game was designed to teach students how to recognize and respond to phishing attacks. The scenarios of the game build phishing attack awareness in the following phases: (1) Awareness: build phishing awareness among the users, (2) Recognition: users can recognize phishing attacks. (3) Response: developing user behavior to recognize and report threats. (4) Resilience: students learn to deal with threats. This framework provides a reusable blueprint that extends beyond this specific game and can be applied to other cybersecurity education initiatives. This study was carried out in compliance with King Abdulaziz University's ethical guidelines.

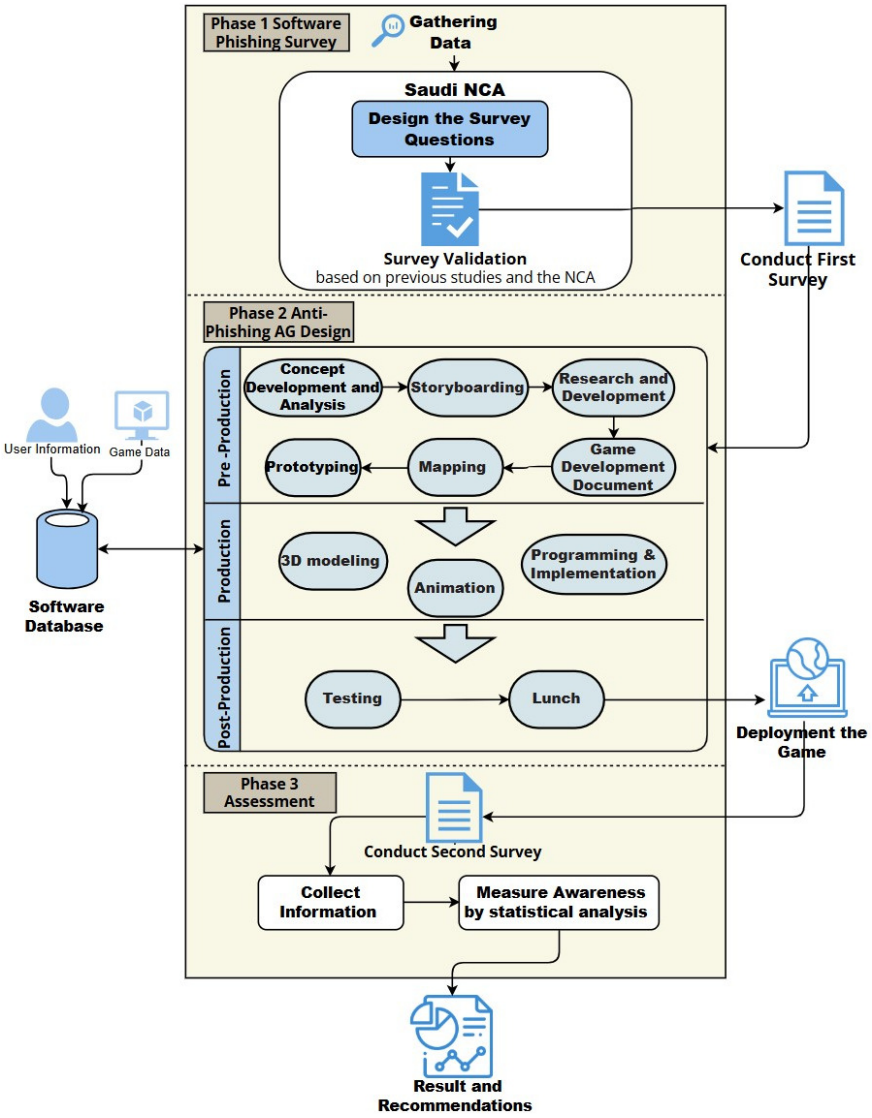

Fig. 1. Anti-Phishing AG framework.

E. Survey Design

A one-group pre-test and post-test study design was employed, with data gathered from the same participants twice. The surveys help understand user behavior and response towards phishing attacks. The sample consists of 13- to 18-year-old Saudi Arabian middle and high school students from both public and private schools. References from earlier research and the principles of phishing attacks, as stated by the NCA [24], served as the basis for the survey questions and their assessment. Participants' demographic information is requested in the pre-test. Pre-game survey includes questions about behavior from earlier research, such as "Do you share your device's secret information (password, username) with friends?" or "Should you download any app or attachment from unknown sources or sent to you by an unknown sender?" [14]. The studies in [6, 12, 18] served as the basis for the development of the survey questions. Since the survey is intended for Arab students, the questions were in Arabic. To determine whether the game was successful in raising participants' awareness of phishing attacks, they retook the survey at the post-test after finishing the game.

1) Survey Design

The survey was designed by analyzing related works to determine which phishing attack types were covered and whether they included questionnaires. Most previous studies are based on phishing emails, followed by phishing URLs, whereas a few studies cover vishing and smishing-type attacks. The designed survey emphasizes URL phishing, email phishing, vishing, and smishing. It consisted of two parts: the first part included demographic-related questions such as gender, educational level, and school type. The second part focused on user behavior and awareness questions. These questions were further divided into five parts: Phishing via links (URLs), (2) Email phishing, (3) Call phishing (Vishing), (4) SMS Phishing (Smishing), and (5) Fraud detection and information sharing. The Likert scale was employed to collect the responses. Authors in [9-10, 12] covered URL structure and teaching and testing participants' ability to recognize fraudulent URLs by explaining the different parts of the URL. The present study also covered this type of phishing by including questions about URLs and explaining the URL structure in the game to the participants. Public awareness campaigns [24, 25] have been employed to raise awareness about fraud and phishing. The "Be careful" campaign from Saudi banks and the other awareness campaigns from the NCA have demonstrated their effectiveness. The "Be careful" campaign website features a section called "Challenge your awareness," which includes a list of questions designed to measure public awareness. Similarly, authors in [8, 25] covered different aspects of cybersecurity, including internet usage, security software and tools, phishing awareness, browser security, cybersecurity knowledge, and social network platforms.

2) Survey Validation

To validate the survey, an analysis of related works in accordance with the NCA standards and framework was conducted, as presented in Table II. Different NCA guidelines, including Essential Cybersecurity Controls, the Saudi Cybersecurity Higher Education Framework (SCyber-Edu), Data Cybersecurity Controls, and Guide to Cybersecurity Practices for Employees in the Work Environment, were used for the survey validation.

F. Game Development

Game development begins by reviewing previous anti-phishing games and studies to identify their limitations and attempt to address them. Then, a concept is developed, and the story is written. After that, the game is designed, animated, and programmed. Finally, test and launch are conducted. The game design incorporates various game elements, including points, time, and other essential aspects. The awards and scores that students collect through the game are tangible, serving as an incentive for them to complete the game. For example, students may be rewarded with bonuses in some courses, receive a reward to purchase items from the school canteen with a specific amount, or have it counted as volunteer hours in school.

1) Concept and Storyline

The story of the game centers on a hero in a fantasy world free of phishing and fraud. By educating people on how to identify fraudulent texts, this hero aims to protect individuals in the real world from fraud and phishing. The game begins in a peaceful world, free from phishing, fraud, or infiltration attempts. In this ideal scenario, the user embarks on a journey to help real-world people avoid falling victim to scams. Through five gates in the ideal world, the player enters the real world. At each gate, the player encounters someone willing to assist in determining whether the websites or messages they receive are legitimate or false. Every gate the player enters earns points, with the player attempting to accumulate as many points as possible.

After finishing the five levels, the player is prompted to decide whether to continue to the golden level and increase their score total. Those whose awareness level is struggling throughout the first five phases have the chance to raise their awareness/knowledge and improve their points during the golden level. In the game, there is a main character, the hero (male or female), who can assist people in the real world, and Non-Player Characters (NPCs) that represent individuals in the real world who require assistance. Each of the five stages covers a distinct phishing attack. Level 1 covers phishing by SMS (smshing), Level 2 covers phishing via phone (vishing), Level 3 covers phishing via email, Level 4 covers phishing via URL, and Level 5 covers fraud detection and information sharing. The players are asked if they would like to advance to the golden level and increase their score after completing the five levels and determining their level of awareness. If the player properly answers the first question at the golden level, they receive five points, and the level ends. If not, the player proceeds to finish the remaining questions at the level and receives between 0 and 6 points from the golden level.

About 20 min are required to complete the pre-test and post-test, as well as to play the game. There are five stages with twelve questions, and each level requires 30 s to complete. Additionally, it takes about 9 min to complete the pre-test and post-test. Game scenarios and player feedback are based on Saudi bank campaigns [25] and NCA awareness materials [24]. Each scenario has a different set of options for points to be earned. Depending on how this behavior impacts exposure to phishing, there are responses with three, two, one, and zero points. After completing each level, the player receives feedback messages, which are the same for all players, regardless of the level or score. Feedback comments about the types of phishing that are discussed at each level are included. The feedback messages are based on the findings reported in [12, 18].

2) Game Mechanics

There are five levels in the game, and each level lasts 1-2 min. The player must deal with several fraud scenarios that are presented at each level. To move the character in the world, the player utilizes the WASD or arrow keys, while the spacebar is used for jumping. Players receive 0 to 6 points for each correct response. Each level focuses on one particular type of phishing attack. The level cannot be repeated by the player. At the end of every level, the game provides feedback messages, as shown in Figure 2.

TABLE II. VALIDATION OF THE ANTI-PHISHING AG FRAMEWORK

File	Controls		[11]	[9]	[12]	[10]	[14]	[13]	[18]	[19]	[20]	[21]	[27]
Essential Cybersecurity Controls	Cybersecurity awareness and training program	Secure handling of email services, especially phishing emails	✓				✓	✓	✓	✓	✓	✓	
		Secure internet browsing				✓	✓				✓		
		Secure use of social media					✓					✓	
	Data and information protection	Data and information privacy					✓			✓		✓	✓
SCyber-Edu	Cybersecurity foundations	Social engineering and the role of the human elements in cybersecurity	✓		✓	✓	✓		✓			✓	
	Cyber threats	Models and types of cyber threats	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
		Attack techniques: viruses, ransomware, and social engineering	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Awareness and understanding	Risk perception and communication	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Cyber hygiene	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Cybersecurity education		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Cyber vulnerabilities and threat awareness	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Cyber crime	Cyber crime types: intrusions, ransomware, espionage, fraud, extortion, data leakage, data destruction, data falsification		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Cyber stalking and predators	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Identity theft	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Privacy	Personally identifiable information					✓						
		Practices related to preserving privacy (determining the purpose for storing or sharing data, integrity, confidentiality, accountability, and auditing)	✓				✓						
		Risks and types of attacks on privacy	✓	✓	✓	✓	✓						
Data Cybersecurity Controls	Cybersecurity governance	Risks of sharing documents and information through unsecured communication channels	✓				✓	✓					
	Cybersecurity defense	Data and information protection	✓	✓	✓	✓	✓	✓		✓	✓	✓	

The player can choose between two gender options, male and female, as depicted in Figure 3, and customize the character by entering their name. Each of the five gates has a different scenario. Since each response has points ranging from three to zero, the player assists by selecting the most appropriate response to prevent fraud. In each scenario, the player has 30 s to respond to the question. The main objective of the game is to earn as many points as possible from each level. After finishing every level, the collected points are shown, and depending on their response at each level, players are notified of their awareness level.

3) Technology

The game is a 3D game designed and developed using Unreal Engine 5. Unreal Engine is a widely used and highly effective game engine for developing various types of video games [28]. Unreal Engine is also used for real-time 3D visualization, virtual production, and simulation across various industries requiring high-fidelity graphics. The game was developed to run on the web, making it more accessible from anywhere on any device.

Fig. 2. Anti-phishing AG feedback page.

Fig. 3. Gender selection option.

4) Scenarios

There are five levels in the game, each with different scenarios corresponding to five different phishing attacks.

a) Level I: Smishing

The objective of this level is to make the player aware of SMS phishing (smishing). The story begins at this level when the NPC asks the hero for assistance in confirming the legitimacy of a text message he received informing him about a shipment delivery issue. As illustrated in Figure 4, the player (the hero) needs to decide the appropriate answer to handle this case and determine whether it is fraudulent. The response determines how many points the player receives. The NPC then receives a follow-up message from his friend, requesting the code that was sent to his phone to complete the event booking procedure. The player has to select the best response after verifying it.

a) Level II: Vishing

This level aims to inform the player of the dangers of call phishing, also known as vishing, and how it occurs. The player sees the NPC making a phone call at the beginning of the scenario and asks her what she is doing. The NPC states that because her exam is coming up, she is speaking with a Qiyas employee to give him her details and the OTP so that he can update her information on the website. The player instructed the NPC to verify if she was speaking to a Qiyas-affiliated employee. After that, the player has to select the most appropriate option to handle this circumstance. The NPC then receives another call from an unidentified number, claiming to be an employee working for a web-development platform that the NPC had just signed up to complete a course assignment. The employee then provides NCP with instructions on how to use the platform. Now, the player must assist the NPC in responding to this call by making the right decision, as displayed in Figure 5.

Fig. 4. Level I: smishing scenario example.

Fig. 5. Level II: vishing scenario example.

b) Level III: Email Phishing

In this level, the player learns about email phishing and its methods. The scenario begins when the NPC receives an email offering a discount on a game he has wanted to buy for a long time. The email requests his personal information, credit card number, and OTP before the discount time ends. The player says, 'Let's check the email first.' Then, the player must decide and choose the best answer to deal with this situation. After that, the NPC received another email stating that his account had been hacked, with his personal information and photos compromised. The hackers then demand money from NPC. The player, as portrayed in Figure 6, interprets the message as threatening and attempts to assist the NPC by selecting the most suitable response to address this situation. The third question is a picture of an email page containing an attachment of a mathematics course review. The player must decide what to do with this email.

a) Level IV: URL Phishing

The objective of this level is to teach the player about URL phishing and how to protect themselves from it. The scenario begins when the NPC wants to shop online and searches for the website, checking if it is the correct one. Then, the player helps her learn how to verify the website by choosing the best answer, as shown in Figure 7. After that, the NPC says she

wants to buy an electronic game and asks which website to purchase from. The player helps her by choosing from which website to buy, either trusted sites or sites that provide games at the lowest price.

Fig. 6. Level III: email phishing scenario example.

Fig. 7. Level IV: URL phishing scenario example.

b) Level V: Fraud Detection and Information Sharing

This level explains to the player the risks of fraud detection and information sharing and how to safeguard against them. The scenario begins when the NPC inquires about learning more about phishing attacks, and the player explains some hypotheses to him. The first hypothesis is "You have free time, and you want to try a video game, but you do not know how to buy and download it. What will you do?" Figure 8 shows the second hypothesis: "You had a scientific discussion with an unknown person on the X app, and he became one of your followers. He continued talking to you until he asked about your age and guessed your interests. How do you respond to him?", and the third hypothesis is "In this era, it has become easy to be exposed to fraud. For example, if you received a message during this period regarding a foundation course for the aptitude test, and after checking, it turns out to be a fraudulent message. Why is that?" Then the player must answer these hypotheses. After that, the level ends, and the feedback page appears.

a) Level VI: Golden Level

This level is not mandatory; the player can enter after finishing the first five levels to improve their score. The scenario of the golden level consists of a series of questions, such as "You played an online game with someone, and he wanted to get to know you more, so what do you do?" The player must answer by choosing one of the answers and then continue to the next question, which is "Your anonymous friend contacted you via WhatsApp and suggested participating in an electronic games competition as a team and/.He asked you for the verification code sent to you so that he could complete the registration, so what do you do?". This scenario is illustrated in Figure 9. The third question is "Let's assume that your anonymous friend was able to access your WhatsApp account due to the verification code you provided him, and he started impersonating you and requesting money from your contacts on WhatsApp, what would you do?". The last question is "Your anonymous friend offered to recover your account for a fee and stop defrauding your contacts, what do you do?". If the player answers the first question correctly, he earns five points, and the level ends; however, if the player makes a mistake, he has to complete all the questions.

Fig. 8. Level V: fraud detection and information sharing scenario example.

Fig. 9. Level VI: golden level scenario example.

III. RESULTS AND DISCUSSION

The study provides important insights for improving cybersecurity education in Saudi Arabia. The study utilizes a serious game (Anti-Phishing AG) to enhance middle and high school students' understanding of phishing, emphasizing the importance of engaging and interactive learning strategies in cybersecurity education. The results indicate that incorporating game-based elements into teaching strategies significantly increases student engagement. Traditional methods of teaching cybersecurity struggle to attract younger audiences. However, when interactive scenarios, challenges, and feedback systems are included, students are better equipped to recognize phishing attacks and respond appropriately.

The study focuses on the demographics most vulnerable to phishing attempts; middle and high school students were selected, ensuring a diverse range of educational levels. The

findings show no discernible differences in improvement by gender, level of education, or school type, suggesting that the Anti-phishing AG was generally effective across all demographic groups. These results demonstrate the inclusivity of the intervention and its effectiveness as a teaching tool for all students. Participants who were more cautious before the Anti Phishing AG tended to stay cautious after it. However, the moderate association reduced the direct effect of pre-game awareness on post-game outcomes. This suggests that playing this game had a clear impact on improving awareness among participants with lower initial scores.

Most questions showed notable improvements in mean comparisons between before and after the Anti-Phishing AG, suggesting behavioral changes and increased knowledge of phishing attempts. Statistical analysis confirmed significant increases in phishing knowledge, with most questions showing p-values below the 0.05 significance level. As depicted in Figure 10, one of the most significant areas for improvement was awareness about phishing via links (URLs). The correct response to phishing links increased from 48.9% before playing Anti-Phishing AG to 55% after playing Anti-Phishing AG.

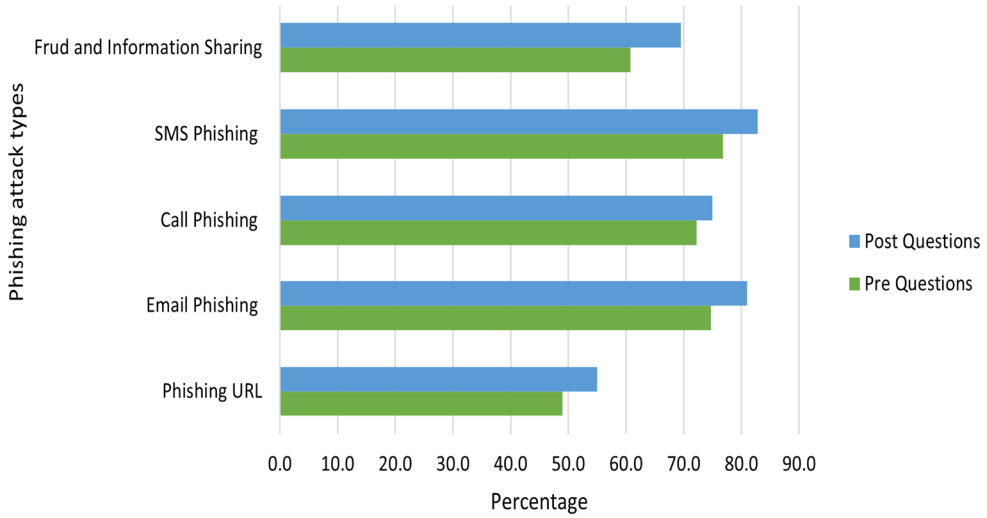

Fig. 10. Correct answers before and after playing Anti-phishing AG.

Regarding the verification of website URLs and the identification of phishing links, participants' behavior changed significantly by 13%, from 57.5% before playing the Anti-Phishing AG to 70.8% after playing the Anti-Phishing AG. These results demonstrate that the Anti-Phishing AG was particularly effective in educating users on how to identify phishing attempts that utilize deceptive URLs, which are among the most common methods employed by cybercriminals. Fraud detection and information sharing also reported a significant improvement; participants were more cautious when publishing personal information online and demonstrated a greater understanding of key concepts, such as social engineering. As shown in Figure 10, the rate of accurate responses to questions on fraud detection and information exchange increased from 60.8% before the Anti-Phishing AG to 69.5% afterward. This implies that the Anti-Phishing AG successfully educated students on how cybercriminals utilize psychological manipulation and private information.

Additionally, participants' self-assurance and understanding of the risks associated with phishing increased. Due to the Anti-Phishing AG, significant progress was made in addressing SMS phishing behaviors. Figure 10 shows that the percentage of right responses was 76.8% before the AG and 82.8% following it. Participants become careful when replying to texts and clicking on unknown links. Participants' ability to recognize and avoid phishing efforts that included messages about package deliveries significantly increased. This shift implies that participants are less likely to trust SMS messages that exploit common delivery circumstances, a tactic typically used by attackers. In case of unsolicited links in SMS messages, participants' behavior showed considerable improvement. This outcome demonstrates the effectiveness of the Anti-Phishing AG's ability to increase participants' awareness when visiting links in SMS, which is a primary method by which phishing attacks begin.

The Anti-Phishing AG was particularly successful in changing smishing-related behaviors and increasing awareness of phishing threats. Participants become more cautious and suspicious when they get text messages that contain links or make fraudulent claims, which are typical in phishing attacks targeting mobile users. The significant behavioral changes observed in this group demonstrate the effectiveness of the Anti-Phishing AG in reducing vulnerability to SMS phishing attempts. As demonstrated in Figure 10, email phishing exhibited a significant change. Before Anti-Phishing AG, 74.7% of respondents correctly identified email phishing, which increased to 81% after using it.

Anti-Phishing AG has multiple features, including the availability in the Arabic language, a rarity among games of this type. Additionally, Anti-Phishing AG covers a broader range of phishing attack types than previous studies, encompassing SMS phishing, call phishing, URL phishing, and email phishing. Moreover, Anti-Phishing AG provides

characters for both males and females, allowing participants to name their characters.

Previous research had several limitations, including a lack of cultural relevance and language barriers. Anti-Phishing Phil [10], for instance, was primarily in English, which made it harder for non-native English speakers to understand, particularly younger Arabic-speaking students. To address this, Anti-Phishing AG has been developed entirely in Arabic, utilizing scenarios, examples, and communication methods that are appropriate to the region, thereby significantly increasing realism and player engagement. Furthermore, unlike studies that focus mainly on URL-based phishing [9, 10, 12], the proposed game addresses a wider range of phishing techniques, including smishing and vishing, which are increasingly common in mobile-based environments.

Another limitation of similar games includes the limited representativeness of the sample. It was more challenging to generalize the results of [15-17] since they mostly used smaller or more homogeneous groups, frequently college students. In contrast, the present study engaged 702 teenagers from middle and high schools, selected through random sampling from diverse backgrounds, who attend both public and private schools. Additionally, earlier games, such as in [15], focused primarily on scenario-driven interactions, failing to adequately address real-world issues, such as call phishing, SMS, and authentic website verifications. The proposed game offers a more thorough strategy that integrates multiple phishing techniques, safeguarding players against real-world phishing attacks.

The study encountered numerous difficulties during game launch and data collection. For the game to function on all school devices, it had to be uploaded to a server with an unstable internet connection. Other significant issues include the lack of computer facilities with old and outdated computers. Due to these limitations, only a small number of players could participate at a time, and the game required a considerable amount of time to complete. Additionally, the implementation faced difficulties due to the final exam schedule.

After implementation and result analysis, several adjustments were made to the Anti-Phishing AG framework. In the first phase, the Software Phishing Survey phase, the survey is designed and validated, resulting in a completed survey. These survey questions are included in the game development phase. The current version of the game stores user information and survey answers. Following the first survey, the game is played, and the second survey is conducted afterward. In the third phase, the Assessment phase, survey data are collected from the database for analysis.

Overall, the results suggest a statistically significant improvement in students' awareness of phishing attacks. The study also provides a robust foundation for future phishing education campaigns, emphasizing the importance of interactive and targeted teaching strategies. Additionally, the game raises awareness of cybersecurity in Saudi society, which is one of the Kingdom's top priorities under Vision 2030.

IV. CONCLUSION

This study presented Anti-Phishing AG, a serious game developed to improve phishing awareness among Saudi Arabian middle and high school students. The game is based on guidelines provided by the Saudi National Cybersecurity Authority (NCA) standards and frameworks. The study proposes a novel framework encompassing survey design and validation, game design, and the development process. The study offers several significant new insights for enhancing cybersecurity education in Saudi Arabia.

The selection of middle and high school students ensures participation from a diverse range of educational levels while focusing on groups most susceptible to phishing attempts. The study demonstrates the effectiveness of the intervention as a teaching method. Anti-Phishing AG and other game-based learning programs are essential for helping students better understand the dangers of phishing. This interactive method improves students' memory retention and provides them with the skills necessary to recognize and respond to phishing attempts. Traditional approaches to cybersecurity education, such as lectures and textbook-based training, often struggle to motivate younger students. Anti-Phishing AG not only serves as an effective educational tool but also provides a practical framework that can be adapted to raise awareness of cybersecurity threats for other target groups, such as corporate employees or trainees.

Future studies should include additional survey questions for every scenario and randomize their appearance for each participant. Generative AI models can also be used to create scenarios and questions tailored to each participating category. Future studies should broaden the target audience to include other groups, such as employees, for training purposes. Furthermore, a dashboard displaying players' educational level, school attendance, and the rankings of the highest-scoring players can be included to encourage competition among players.

DECLARATION OF COMPETING INTERESTS

The authors declare no competing interests.

ACKNOWLEDGMENT

This study was funded by KAU Endowment (WAQF) at King Abdulaziz University, Jeddah, Saudi Arabia. The authors would like to acknowledge WAQF and the Deanship of Scientific Research (DSR) for their technical and financial support.

DATA AVAILABILITY

The code supporting the findings is publicly available at [29].

REFERENCES

[1] S. Das, C. Nippert-Eng, and L. J. Camp, "Evaluating User Susceptibility to Phishing Attacks," *Information & Computer Security*, vol. 30, no. 1, pp. 1–18, Jan. 2022, https://doi.org/10.1108/ICS-12-2020-0204.

[2] "What Is Phishing?," *Cisco*, 2025. https://www.cisco.com/site/us/en/learn/topics/security/what-is-phishing.html.

[3] M. F. Ansari, P. K. Sharma, and B. Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *International Journal of Smart Sensor and Adhoc Network.*, pp. 61–72, Mar. 2022, https://doi.org/10.47893/IJSSAN.2022.1221.

[4] "Financial Cyberthreats Targeting Businesses in Saudi Arabia Drop by 24% in Q2 of 2022," *Kaspersky*, Oct. 2022. https://me-en.kaspersky.com/about/press-releases/financial-cyberthreats-targeting-businesses-in-saudi-arabia-drop-by-24-in-q2-of-2022.

[5] "Phishing Activity Trends Reports: 1Q-2025," *Anti-Phishing Working Group*, Mar. 2025. https://apwg.org/trendsreports.

[6] A. Darem, "Anti-Phishing Awareness Delivery Methods," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7944–7949, Dec. 2021, https://doi.org/10.48084/etasr.4600.

[7] G. Alotibi, "A Cybersecurity Awareness Model for the Protection of Saudi Students from Social Media Attacks," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13787–13795, Apr. 2024, https://doi.org/10.48084/etasr.7123.

[8] T. Alharbi and A. Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data and Cognitive Computing*, vol. 5, no. 2, May 2021, Art. no. 23, https://doi.org/10.3390/bdcc5020023.

[9] D. A. S. Wibawa, H. Setiawan, and Girinoto, "Anti-Phishing Game Framework Based on Extended Design Play Experience (DPE) Framework as an Educational Media," in *2022 7th International Workshop on Big Data and Information Security*, Depok, Indonesia, Oct. 2022, pp. 107–112, https://doi.org/10.1109/IWBIS56557.2022.9924935.

[10] S. Sheng *et al.*, "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, Pittsburgh, PA, USA, Jul. 2007, pp. 88–99, https://doi.org/10.1145/1280680.1280692.

[11] L. Kassner and A. Schönbohm, "A Serious Game to Improve Phishing Awareness," in *Games and Learning Alliance*, vol. 13647, K. Kiili, K. Antti, F. De Rosa, M. Dindar, M. Kickmeier-Rust, and F. Bellotti, Eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 109–117.

[12] A. Baiomy, M. Mostafa, and A. Youssif, "Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks," *Indian Journal of Science and Technology*, vol. 12, no. 44, pp. 01–10, Nov. 2019, https://doi.org/10.17485/ijst/2019/v12i44/147850.

[13] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," *Future Internet*, vol. 14, no. 4, Mar. 2022, Art. no. 104, https://doi.org/10.3390/fi14040104.

[14] R. C. T. Panga, J. Marwa, and J. D. Ndibwile, "A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 466–489, Jun. 2022, https://doi.org/10.3390/jcp2030024.

[15] A. Yasin, R. Fatima, Z. JiangBin, W. Afzal, and S. Raza, "Can Serious Gaming Tactics Bolster Spear-Phishing and Phishing Resilience?: Securing the human hacking in Information Security," *Information and Software Technology*, vol. 170, Jun. 2024, Art. no. 107426, https://doi.org/10.1016/j.infsof.2024.107426.

[16] A. Rahartomo, A. T. A. Ghaleb, and M. Ghafari, "Phishing Awareness via Game-Based Learning," in *37th International Conference on Software Engineering Education and Training*, Ottawa, ON, Canada, Apr. 2025, pp. 287–291, https://doi.org/10.1109/CSEET66350.2025.00036.

[17] A. Yasin, R. Fatima, L. Wen, Z. JiangBin, and M. Niazi, "What Goes Wrong During Phishing Education? A Probe into a Game-Based Assessment with Unfavourable Results," *Entertainment Computing*, vol. 52, Jan. 2025, Art. no. 100815, https://doi.org/10.1016/j.entcom.2024.100815.

[18] W. Yeoh, H. Huang, W.-S. Lee, F. Al Jafari, and R. Mansson, "Simulated Phishing Attack and Embedded Training Campaign," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 802–821, Jul. 2022, https://doi.org/10.1080/08874417.2021.1919941.

[19] P. Weanquoi, J. Johnson, and J. Zhang, "Using a Game to Improve Phishing Awareness," *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, no. 2, Dec. 2018, https://doi.org/10.62915/2472-2707.1040.

[20] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What Hack: Engaging Anti-Phishing Training Through a Role-Playing Phishing Simulation Game," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, Glasgow, Scotland, UK, May 2019, pp. 1–12, https://doi.org/10.1145/3290605.3300338.

[21] R. Fatima, A. Yasin, L. Liu, and J. Wang, "How Persuasive is a Phishing Email? A Phishing Game for Phishing Awareness," *Journal of Computer Security*, vol. 27, no. 6, pp. 581–612, Oct. 2019, https://doi.org/10.3233/JCS-181253.

[22] S. Yang and G. Berdine, "Normality Tests," *The Southwest Respiratory and Critical Care Chronicles*, vol. 9, no. 37, pp. 87–90, Jan. 2021, https://doi.org/10.12746/swrccc.v9i37.805.

[23] "Wilcoxon Signed-Rank Test using SPSS Statistics," *Laerd Statistics*, 2025. https://statistics.laerd.com/spss-tutorials/wilcoxon-signed-rank-test-using-spss-statistics.php.

[24] "Regulations Documents," *National Cybersecurity Authority*, 2025. https://nca.gov.sa/en/regulatory-documents/.

[25] "Saudi Banks-Be Careful," *Saudibanks*, Jan. 2025. https://saudibanks.com.sa/en/becareful.

[26] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A Survey on Internet Usage and Cybersecurity Awareness in Students," in *14th Annual Conference on Privacy, Security and Trust*, Auckland, New Zealand, Dec. 2016, pp. 223–228, https://doi.org/10.1109/PST.2016.7906931.

[27] E. J. Williams and A. N. Joinson, "Developing a Measure of Information Seeking About Phishing," *Journal of Cybersecurity*, vol. 6, no. 1, Jan. 2020, Art. no. tyaa001, https://doi.org/10.1093/cybsec/tyaa001.

[28] "What Is Unreal Engine?," *Bairesdev*, Oct. 2022. https://www.bairesdev.com/blog/what-is-unreal-engine/.

[29] S. Alzahrani, "Anti Phishing AG Public." GitHub, Mar. 2025, [Online]. Available: https://github.com/salzahrani-coder/AntiPhishing_AG.