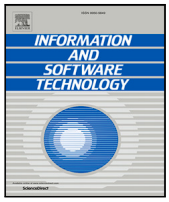
Information and Software Technology 170 (2024) 107426

Contents lists available at ScienceDirect

Information and Software Technology

journal homepage: www.elsevier.com/locate/infsof



Can serious gaming tactics bolster spear-phishing and phishing resilience? : Securing the human hacking in Information Security

Affan Yasin [a], Rubia Fatima [b], Zheng JiangBin [a], Wasif Afzal [c,*], Shahid Raza [c,d]

[a] School of Software, Northwestern Polytechnical University, Xian, 710072, Shaanxi, China
[b] Department of Computer Science, Emerson University, Multan, Pakistan
[c] School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden
[d] RISE Research Institutes of Sweden, Sweden

ARTICLE INFO

Keywords:
Human factor in security
Phishing attack
Scam
Education
Serious game
Information security

ABSTRACT

Context: In the digital age, there is a notable increase in fraudulent activities perpetrated by social engineers who exploit individuals' limited knowledge of digital devices. These actors strategically manipulate human psychology, targeting IT devices to gain unauthorized access to sensitive data.
Objectives: Our study is centered around two distinct objectives to be accomplished through the utilization of a serious game: (i) The primary objective entails delivering training and educational content to participants with a focus on phishing attacks; (ii) The secondary objective aims to heighten participants' awareness regarding the perils associated with divulging excessive information online.
Methodology: To address these objectives, we have employed the following techniques and methods: (i) A comprehensive literature review was conducted to establish foundational knowledge in areas such as social engineering, game design, learning principles, human interaction, and game-based learning; (ii) We meticulously aligned the game design with the philosophical concept of social engineering attacks; (iii) We devised and crafted an advanced hybrid version of the game, incorporating the use of QR codes to generate game card data; (iv) We conducted an empirical evaluation encompassing surveys, observations, discussions, and URL assessments to assess the effectiveness of the proposed hybrid game version.
Results: Quantitative data and qualitative observations suggest the "PhishDefend Quest" game successfully improved players' comprehension of phishing threats and how to detect them through an interactive learning experience. The results highlight the potential of serious games to educate people about social engineering risks.
Conclusion: Through the evaluation, we can readily arrive at the following conclusions: (i) Game-based learning proves to be a viable approach for educating participants about phishing awareness and the associated risks tied to the unnecessary disclosure of sensitive information online; (ii) Furthermore, game-based learning serves as an effective means of disseminating awareness among participants and players concerning prevalent phishing attacks.

1. Introduction

It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it[1]

[Stephane Nappo]

Relevance of Modern Digital Security: The increasing prevalence of smartphones and smart devices has elevated the importance of information security in the digital realm. The widespread adoption of these devices, coupled with insufficient education and awareness regarding associated risks, has created an opportunity for social engineers to exploit them. Consequently, individuals and companies alike have suffered significant material and reputational losses, emphasizing the critical need for robust global security measures. From the perspective of a hacker, it becomes apparent that, within a company, employees, as

* Corresponding author.
E-mail addresses: affan.yasin@outlook.com (A. Yasin), rubiafatima91@hotmail.com (R. Fatima), zhengjb@nwpu.edu.cn (Z. JiangBin), wasif.afzal@mdu.se (W. Afzal), shahid.raza@ri.se (S. Raza).

[1] https://www.goodreads.com/quotes/tag/cyber-security

https://doi.org/10.1016/j.infsof.2024.107426
Received 8 November 2023; Received in revised form 11 January 2024; Accepted 15 February 2024
Available online 23 February 2024
0950-5849/© 2024 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

a human factor, represent the weakest link susceptible to information theft through phishing attacks [1].

The imperative for information security extends to digitalized cities, where various systems, ranging from traffic signals and healthcare facilities to surveillance cameras and airport operations, are interconnected through the Internet, forming the Internet of Things (IoT) [2]. This interconnectedness exposes such cities and globally networked systems to vulnerabilities exploited by social engineers [3]. For organizations, it is crucial to develop methods and techniques to strengthen application security and ensure information integrity. Disseminating knowledge about potential vulnerabilities and fostering awareness to counteract these challenges is paramount. Notably, research underscores that humans are the most susceptible element in such scenarios [4,5], easily targeted in contexts such as hospital IT systems, smart vehicles, and smartphones [2,3].

In a hypothetical scenario, envision a situation where a hacker gains unauthorized access to an airport security system through password prediction or social engineering tactics. The potential consequences are alarming; the intruder could compromise the system, manipulate flight schedules, alter air routes, and make demands in exchange for control. The aftermath involves not only financial and reputational losses but also raises concerns about security, reliability, and credibility. The intangible losses may require considerable time to recover. While technology has undoubtedly streamlined various tasks, enabling seamless financial transactions and remote management with a single click, it has simultaneously provided a fertile ground for attackers and hackers.

In this complex landscape, the human element emerges as the most vulnerable aspect of information security, underscoring the critical need to educate and train individuals on the intricacies of spear-phishing and phishing attacks.

Understanding Social Engineering and Phishing Attacks: The term Social engineering has been introduced and defined by researchers as the "art of influencing individuals to disclose sensitive information, is known as a social engineering attack" [6,7]. In the realm of information security, social engineering pertains to incidents wherein an information system is infiltrated through the application of social tactics [8]. Among the most prevalent methods is the employment of phishing attacks to extract required data and information. The field of information technology is grappling with Phishing [9] as one of the most potent threats, capable of dissuading individuals from its utilization. Phishing manifests as a deceitful endeavor, enabling an attacker to obtain sensitive user identity information, including passwords, security codes, and transaction details. This malicious activity involves the assailant dispatching fraudulent emails, messages, and websites to individuals identified as potential targets. These attacks align with deception theory, wherein a sender deliberately transmits a message to induce false beliefs or conclusions in the recipient [10,11]. False or spoofed emails and websites are frequently employed by social engineers and attackers to deceive and breach valuable information [12,13]. The process of a phishing attack is illustrated in Fig. 1.

Awareness strategies in Countering Social Engineering Attacks: Upon closer examination of various approaches to mitigate social engineering attacks, it is evident that researchers and practitioners employ diverse strategies. These strategies include conducting seminars and workshops for knowledge dissemination [14], providing education through simulated environments [15], utilizing traditional teaching methods [16], employing gaming methods (such as tabletop and software games) [17], leveraging the expertise of white hat hackers, and incorporating virtual cyber ranges via live streams [18]. Each method has its merits and limitations, and there is no one-size-fits-all solution. The selection of a strategy should be based on the specific context, situation, and target audience, emphasizing the importance of "Situational Awareness".

Empowering Learning Through Game-Based Approaches: Games present an effective avenue for educating and training individuals about phishing, leveraging relatable scenarios from everyday life to facilitate a learning experience. Through gameplay, participants engage with the rules of the environment, gaining insights into the dos and don'ts of the context. Game design elements further empower players to assume significant roles and make bold decisions without the weight of real-life consequences [19]. The concept of Serious Games has emerged as a promising strategy for engaging learners and conveying information in an innovative and straightforward manner [20]. The efficacy of game-based learning spans various domains and educational levels, encompassing subjects such as mathematics [21], programming [22], collaborative airport management [23], and cyber security awareness [24,25]. Noteworthy research by Qian et al. and Chang et al. [26,27] underscores the positive impact of game-based learning on learning outcomes across diverse fields, highlighting its encouraging effects on participants' educational achievements .

Game-based Education Counters Phishing attacks: Countless endeavors by researchers are underway to mitigate the financial and reputational repercussions inflicted by phishing attacks. Numerous studies underscore that digital games serve as a readily accessible and effective avenue for training individuals on the intricacies of phishing emails (attacks) [28,29]. Recent instances of phishing endeavors[2] vividly underscore the urgent necessity for public awareness, given the pervasive presence of over five billion individuals equipped with laptops, tablets, and 4G/5G-enabled smartphones. A foremost priority resides in enlightening the masses about phishing [30,31]. Researchers have orchestrated training sessions employing diverse educational materials, including lectures, videos, and games. Notably, post-training assessments revealed that participants engaged in gaming were adept at differentiating fraudulent websites [32]. Similarly, Junger et al. [33] have concurred, highlighting humans' heightened susceptibility to phishing attacks, often arising from inadequate training and education about such schemes. Thus, it becomes imperative to instill in individuals the necessary education and training to bolster their resilience against phishing and spam emails. This imperative education serves to fortify the human element, often the weakest link in the chain of a system [34]. An imperative mandate thus emerges: to equip individuals with the knowledge and skills required to thwart the potentially devastating consequences of phishing attacks, safeguarding invaluable personal and corporate information. The idea to design a game to combat phishing attacks has been derived from the latest portal[3] and from research studies [25,35].

Research Contribution(s): The following are the contributions of the research study:

1. Design, and development of web-based version (Hybrid version) of the role-based game (PhishI).
2. Enhanced understanding of Social Engineering and Phishing attacks.
3. Utilizing and embedding the knowledge & findings from the previous research to design, develop the game.
4. Detection and Prevention Techniques embedded in the game design and process.
5. Strengthening the design principles through the integration of instructional strategies, Social Engineering Ontology and other relevant learning techniques.
6. The game will augment participants' comprehension of how online information sharing can be exploited by malicious actors, enabling them to formulate phishing attacks.

[2] https://www.hackmageddon.com/category/security/cyber-attacks-timeline/

[3] http://www.gamification.co/2016/03/02/teaching-kids-cybersecurity-game-based-training/

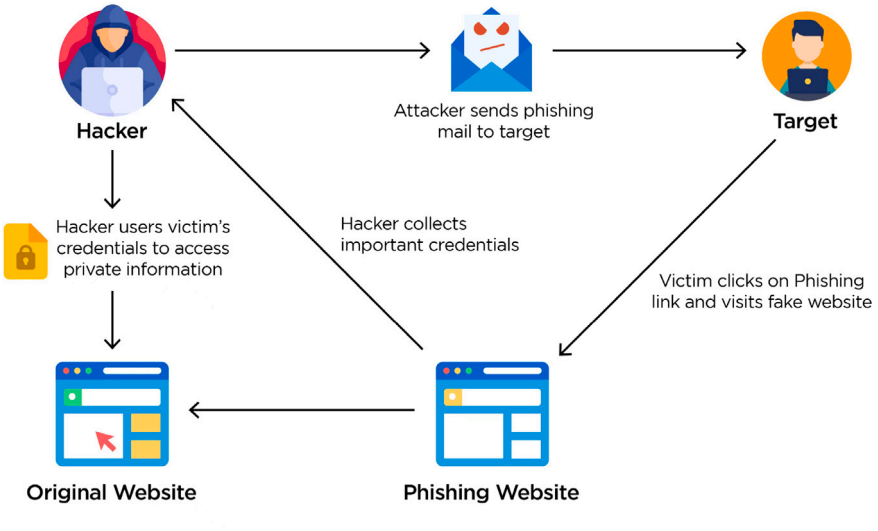


Fig. 1. Illustrates the general process of a phishing attack, wherein a hacker initiates the scheme by sending a deceptive email. The victim, upon clicking, unwittingly shares sensitive information on a fraudulent website. Subsequently, the hacker obtains the acquired information to gain unauthorized access to the legitimate website.

Research Questions: Below mentioned are the research questions we investigate within this study:

- **RQ1:** In what manner can insights from various fields be combined to create an effective game-oriented approach for addressing social engineering, with a specific focus on enhancing awareness about phishing?
  - **RQ1.1:** How can the design and development of a compelling and informative game for raising awareness about phishing incorporate elements such as social engineering concepts, tactics of persuasion, crafting engaging narratives, leveraging data from social media, various attack strategies, and the methodology of character personas?
- **RQ2:** To what extent does the suggested game-centered/game based awareness strategy for promoting phishing awareness prove its effectiveness when subjected to empirical assessments?

Research Methodology: To fulfill the objectives of our research endeavor, the research paper is structured into seven sections. Section 2 expounds upon the meticulous design rationale underpinning our devised game. To begin, we explore Bloom's Taxonomy to enhance comprehension and provide a lucid overview. Given the interdisciplinary nature of the proposed solution, we amalgamate knowledge from diverse fields, ensuring equilibrium within the game-based resolution. The social engineering ontology serves as the foundational blueprint for the game design, alongside an exposition of the incorporation of gamification elements and core driving factors. We meticulously integrate insights from security requirements engineering into the game, aligning our approach with the findings present in the literature. In Section 3, a comprehensive exposition of game assets, procedures, and regulations is presented. Commencing with the game's narrative, we subsequently delve into the mechanics of game cards and the game's attack process. Additionally, a website (Hybrid Version) of the game has been developed, representing a progressive step in game design and phishing education. Moving forward to Section 4, a thorough account of the empirical evaluation unfolds. Diverse methods are employed to gauge participants' learning outcomes, including observations, surveys, analysis of drafted phishing emails, review session discussions, and Pre-Post URL surveys. Section 5 provides an overview of the literature review pertaining to the relevant subject matter. Finally, Section 6 engages in a detailed discussion and concluding remarks, encapsulating the essence of the paper's findings.

2. Game design rationale

2.1. Utilizing learning taxonomy

We have integrated Bloom's taxonomy of the cognitive domain into our game PhishI, as referenced in the study [36]. Referencing Fig. 2, this taxonomy has been segmented into five distinct tiers of anti-phishing learning. Furthermore, these five tiers have been subdivided into various components. The initial tier denotes Objectives, the subsequent tier encompasses Application Domains, the third tier emphasizes Learning Processes, the fourth tier encapsulates Knowledge Integration and Gamification, and finally, the fifth tier signifies Assessment

The application of Bloom's taxonomy, encompassing various levels of cognitive engagement, to elucidate the integration of our phishing awareness objective. The arrangement of goals and their corresponding facets is illustrated in Fig. 2. Upon reviewing the figure, the left-hand side delineates the dimensions, while the center elaborates on distinct approaches. For instance, within the "Learning" dimension, the content focuses on the array of knowledge participants will acquire through the game.

2.2. Embedding knowledge of MITRE ATT&CK in game design

To leverage insights from prior literature, we have incorporated the cyber taxonomy outlined in the referenced study [37]. This taxonomy delineates various stages of cyber attacks and their contexts. Table 1 provides a detailed breakdown of how we integrated these phases into our game design and processes.

2.3. Integration of knowledge from diverse disciplines

To formulate the serious game, an amalgamation of insights from diverse research domains has been orchestrated. Commencing with the realm of Information Security, discernment pertaining to phishing

Fig. 2. Depicting the adaptation of Bloom's Taxonomy for embedding knowledge and understanding. The five phases discussed include Goal, Application Areas, Learning, Embedding Knowledge in games, and Evaluation.

Table 1
Embedding knowledge of *MITRE ATT&CK* in Game Design for better cybersecurity education and awareness.

Sr. No	Cyber taxonomy phases	Where we embedded in game design and process
1	Assessment and impact testing	This aspect is incorporated into the evaluation stage of the game process, wherein we evaluated the understanding of social engineering and phishing scenarios.
2	Training scenarios	The educational/training element is integrated into the attack scenarios. Participants utilized the provided data to create phishing attack scenarios.
3	Training methods	Game-based learning methods are employed to educate and train the participants.
4	Orchestration	The participants orchestrate the attack using the organizational map, employee information from social media, persuasive methods, and rules card.
5	Infrastructure	The infrastructure is depicted in the game design aspect, where the organizational map is presented for better understanding and targeting.

attacks, encompassing scenarios, templates, and corresponding countermeasures, has been acquired. The architectural underpinning for shaping the fundamental blueprint and progression of the game has been gleaned from the domain of game design. Correspondingly, principles rooted in the field of Human–Computer Interaction (HCI), namely the cultivation of Personas and the strategic infusion of gamification, have been harnessed. A comprehensive delineation of the specific subjects and subtopics harnessed from these multifarious fields is visually explicated in Fig. 3 for reference.

2.4. Utilizing social engineering ontology as the foundation for design

An ontology can be characterized as a compilation of concepts and classifications that delineate a subject, elucidating its characteristics and interconnections. In our research, we have utilized the foundational design of the game from the ontology of Social Engineering developed by Mouton et al. [6]. All the attributes within the ontology correspond to elements integrated into the game. *An enhancement in the ontology* includes the incorporation of the *Information gathering platform* attribute within the game context (depicted in Fig. 4). Elaborated descriptions of each attribute are presented below.

- **Attack:** An incident involving a phishing scheme or a social engineering maneuver designed to deceive unsuspecting targets. Illustrative examples encompass counterfeit invoice scams and deceptive CEO impersonation emails, among others.
- **Attacker:** The individual or entity responsible for executing the phishing attack, typically cybercriminals who aim to achieve financial gains or access to confidential credentials. However, perpetrators may also include insiders or nation-state groups.
- **Target:** The entity or organization that the social engineering attack aims to manipulate or exploit.
- **Compliance Principle:** Psychological triggers that attackers manipulate to secure compliance from their targets, including elements such as reciprocity, scarcity, authority, and social proof.
- **Technique/Tactics:** Precise methodologies employed within the context of the attack, such as pretexting, baiting, or reverse social engineering etc. These tactics are derived from established social engineering frameworks.
- **Goal/Objective:** The intended outcome sought by the attacker through the execution of the attack, which may encompass objectives like the theft of credentials, dissemination of malware, financial exploitation, or data exfiltration.
- **Medium:** The means through which the attack is carried out, including channels like email, phone calls, SMS messages, and others.

Fig. 3. Depicts the incorporation of knowledge from diverse research disciplines/areas into the design, development, and evaluation phases of the game.

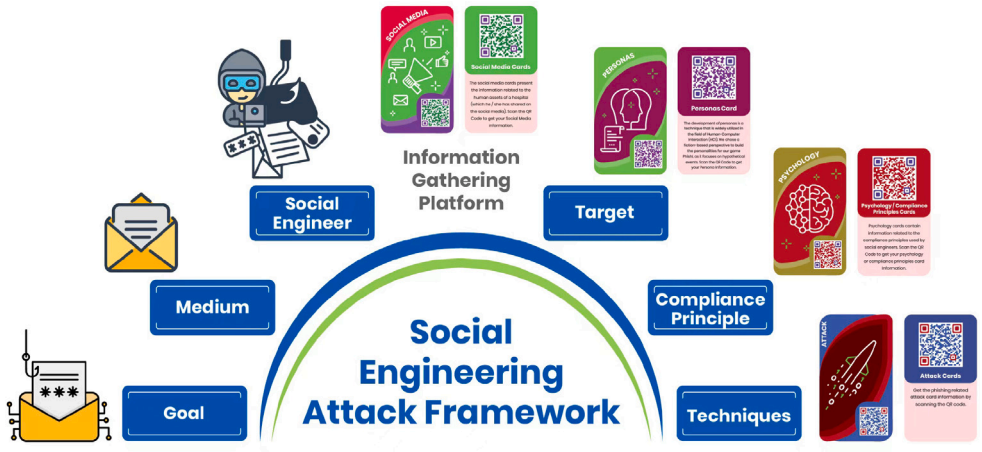


Fig. 4. Security requirements ontology as the basis of Knowledge model.
Source: Adapted from Mouton et al. [6] Ontology.

- **Social Engineer:** A skilled hacker adept at employing techniques to manipulate individuals into disclosing information or performing actions that serve the attacker's interests.
- **Information Gathering Platform/Sources:** Resources leveraged by attackers to acquire background information about their targets before launching attacks. These resources encompass platforms such as social media, databases, and sources on the dark web.

2.5. Augmenting contextual comprehension via a class diagram

A class diagram, an integral component of the Unified Modeling Language (UML), constitutes a structural diagram employed within the realm of software engineering. Its purpose is to visually represent the classes, attributes, operations (or methods), and interconnections among objects within a system, offering insights into the system's underlying structure. This diagram serves both as a means of in-depth modeling, facilitating the translation of models into actual computer

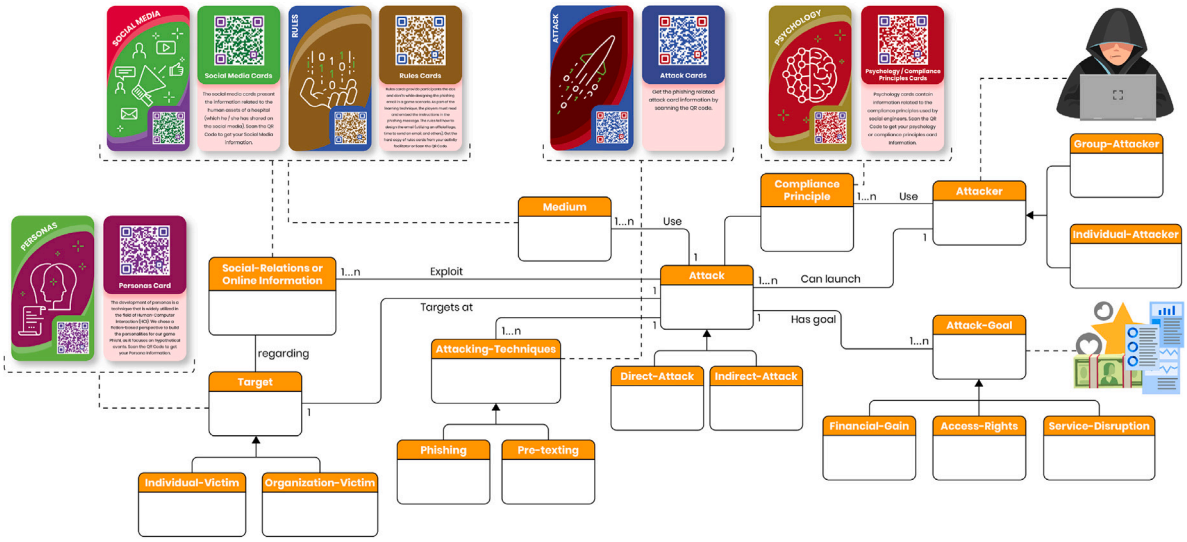


Fig. 5. Leveraging game attributes derived from Social Engineering Ontology and augmenting interconnections through a class diagram to enhance comprehension of the contextual relationships.

Table 2
Gamification core drives.

Core drives	Description	Intrinsic/Extrinsic	Where in the Game?
Development & Accomplishment	Individuals possess a yearning for personal growth and the achievement of aspirations in life.	Extrinsic	The game encompasses a structured process that begins with the selection of target assets and progresses through the development of the phishing email. This journey spans from raw information acquisition to the creation of the phishing email.
Empowerment of creativity & feedback	The introduction of creativity and feedback as integral components of the activity can enhance participant motivation.	Intrinsic	Participants employ their creativity and expertise to craft phishing emails. The diversity of attack scenarios varies based on participants' experiences, knowledge, and the cards drawn during the game.

code, and as a tool for overarching conceptual modeling of the application's structural framework. The class diagram associated with the devised game, intended to provide a fundamental comprehension of attributes and their interrelations, is depicted in Fig. 5.

2.6. Embedding gamification core drives

Gamification refers to the incorporation of game elements, such as points, badges, and leader-boards, into non-gaming contexts. Its primary aim is to leverage the same levels of engagement and motivation commonly observed in the realm of gaming. This concept finds extensive application in domains beyond gaming, particularly in marketing, where companies deploy gamification to captivate customers and consequently boost their financial gains [38,39].

Within this context, the Gamification model – specifically the Octalysis framework proposed by Yu-Kai Chou[4] – serves as both a behavioral and motivational framework. Through thorough examination, we have embedded two of its motivational drivers into our game design. For a comprehensive understanding, refer to Table 2.

2.7. Embedding game elements

The following are the gaming elements integrated into our phishing game.

- **Points:** In order to determine the game's victor, a point system must be established, and the same principle applies to our conceived and proposed game. The composed email undergoes assessment based on this point system to ascertain the game's ultimate winner [40].
- **Achievement:** Within the game's framework, players strive to attain success by crafting a phishing email that is both precise and well-calibrated. This accomplishment allows participants to acquire the highest possible points during the evaluation phase, culminating in their victory in the game [40].
- **Challenge** [41]: In order for the game to be captivating and enjoyable, the inclusion of a game conflict is essential. This conflict is addressed by the active participation of the game's contestants. Within our game, this essential element is intricately woven into the process of adeptly harnessing information to compose phishing emails. Additionally, the crafted phishing emails undergo a subsequent evaluation and deliberation, leading to the allocation of points that ultimately determine the victor of the game session.
- **Collaboration/Collaborative Learning:** The phenomenon of peer learning seems to be an intrinsic facet of youth culture, occasionally manifesting even within solitary gaming sessions or individual projects [42]. With the intention of surmounting collective hurdles and cultivating the amalgamation of students' informal and formal learning experiences, we have orchestrated the game to be conducted in group settings. This strategic arrangement facilitates the participants in exchanging their knowledge and viewpoints. Additionally, the incorporation of deliberative dialogues and feedback sessions within the gaming process aims to augment collaborative dynamics and enhance the dissemination

[4] https://www.udemy.com/course/gamification-behavioral-design-the-octalysis-framework/

Table 3
Alignment of game process with Security Requirements Engineering (SRE) process.
Source: Adapted from [25].

SRE Process	Boström [43]	Haley[44]	Presence in designed Game (PhishDefend quest)
Definition of concepts	x	x	Game rules and manual
Business objectives	x	✓	Game objective
Misuse/Threats modeling	✓	✓	Social media cards
Assets identification	✓	✓	Personas cards
Coding standards	✓	x	x
Categorize and prioritize	✓	x	Victim selection & draft phishing attack
Inspection and validation	x	✓	Inter teams discussion
Process planning	x	x	Design Rationale of Protection

of expertise related to the conception and feasibility of diverse attack scenarios.

2.8. Aligning with the security requirements engineering process

In order to formulate the game procedure and harmonize it with the imperatives of Security Requirements Engineering and the Social Engineering attack process, we systematically examined diverse security methodologies documented in the literature. A comprehensive correspondence between these methodologies and our game was established, and this alignment is outlined in detail in Table 3. In Table 3, the symbol '✓' denotes the inclusion of a particular phase within the game, while 'X' signifies its absence.

3. Game assets, process and rules

3.1. Game map and story

The illustration of the hospital system's layout and geographical representation can be observed in Fig. 6. The characters devised for the purpose of the gaming simulation are visually identifiable within the geographical layout. Each member of the hospital staff possesses an Information Technology gadget, such as a smartphone, laptop, desktop, smartwatch, among others, which facilitates their internet connectivity. The personnel of the hospital access the online sphere through virtual means, symbolized by the entity denoted as "Social Media" in the context.

Game Story: King Edward Medical University seeks your expertise to hack their advanced security system. Use gathered data from an employee's social media to craft a convincing phishing email for employees knowledge evaluation.

3.2. Game cards

The game cards are devised with a provision for a QR code, enabling participants to scan and access the most up-to-date data and information pertinent to the game. These cards are visually illustrated in Fig. 7.

- **Attack Card:** We delimited the scope of our design to specifically address attacks related to phishing, given that the game places notable emphasis on fostering awareness of and comprehension about phishing.
- **Rules Card:** In the context of the gaming environment, participants receive guidance on the actions to take and avoid through instructional cards as they construct phishing emails. Players must absorb and incorporate these instructions into their phishing communications, constituting a fundamental component of the learning journey. These guidelines delineate the structure of the email, encompassing elements such as the integration of an official logo and the timing of email dispatch, among other factors. Thoroughly scrutinizing the rules cards is of paramount importance for gamers, as it guarantees adherence to the indispensable procedures essential for crafting phishing emails. Rules cards are shown in Fig. A.16 (Appendix).
- **Personas Card:** Implemented within our game, as elucidated in the work by Nielsen [45], is the incorporation of the personas technique, strategically designed to enhance players' grasp of the fundamental principles of phishing. The creation of personas stands as a widely embraced approach within the domain of research in human–computer interaction (HCI). In the context of our game titled "PhishDefend Quest", which revolves around hypothetical scenarios, we have embraced a narrative-oriented approach in shaping characters. Within the framework of our game, we have meticulously crafted a fictitious hospital setting, replete with characters embodying medical professionals, nurses, laboratory technicians, and IT experts.
- **Psychology Card:** The psychological strategies harnessed by social engineers are expounded upon in the psychology cards, which delve into the realm of compliance concepts. These cards were meticulously devised with the aim of familiarizing individuals with a spectrum of psychological tactics that social engineers employ in orchestrating their attacks.
- **Social Media Card:** The data pertaining to the hospital's human resources is portrayed by means of employing social media cards. These cards, featured within the game, seamlessly incorporate simulated data sourced from diverse social media platforms including but not limited to Facebook, Twitter, and analogous platforms.

The format of the cards is visually represented in Fig. 7.

3.3. Game attack process

Phishing, a form of social engineering, employs email as a communication medium to target individuals with the objective of obtaining unauthorized access, data, information, passwords, or other valuable assets. Prior research illustrates that such attacks unfold across distinct phases [40]. These sequential stages are replicated within the game framework, as elucidated below and visually depicted in Fig. 8.

- **PHASE 1 — Selection of Targets/Victim Selection:** In this stage, participants are tasked with choosing a target individual from the game map.
- **PHASE 2 — Information Gathering/Data Collection:** During this stage, participants are obligated to acquire information pertaining to the designated target by employing social media and Persona cards.
- **PHASE 3 — Drafting Email:** During this stage, participants are tasked with composing a phishing email by utilizing insights from knowledge, persona card, psychology cards, and rules cards. The amalgamation of information from these cards, along with the construction of a narrative, contributes to the creation of a more authentic-looking phishing email. This enhanced realism facilitates a higher likelihood of successfully deceiving the target entity.
- **PHASE 4 — Send/Email Dissemination:** In this game phase, participants are required to exchange the drafted phishing emails for the purpose of review and subsequent discussion.

Fig. 6. Illustration of a game security setting featuring a hospital, where various personnel operate. Personas mimic the profiles of employees/stakeholders, and social media cards display information related to these stakeholders for a comprehensive understanding of the environment.

Fig. 7. Various card types crafted for the game, featuring embedded QR codes for a hybrid version capable of generating random data each time participants scan them.

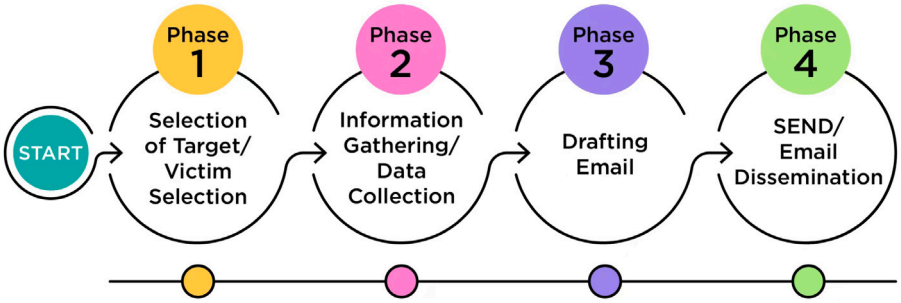
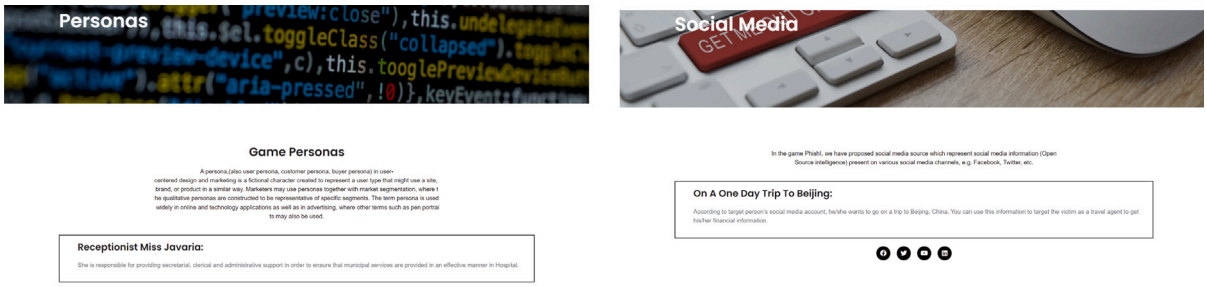


Fig. 8. Phishing Attack process extracted from the past research literature and govt data of SE attacks were further used as the game process. The same four steps were mapped for better relatedness and understanding of the participants.



(a) Persona Card - Generating Dynamic Card Data (b) Social Media Card - Generating Dynamic Card Data

Fig. 9. Illustrates the web pages of Persona and Social Media. Upon refreshing these pages, it displays random data, providing variability for multiple players to access diverse information. This variability aids in evaluating various scenarios, considering different data for Personas, Social Media, and Persuasive Methods.

Win or Lose assessment: The assessment framework comprises three distinct domains: email composition (2 points), conceptualization of idea/scenario (2 points), and effective incorporation of accessible information into the construction of the phishing email (2 points). The victorious team is determined based on the cumulative point tally. The final deliberation phase of the game, termed the discussion session, will culminate in the selection of the winning team.

3.4. Website design — A hybrid version

In previous instances, we have undertaken the design and development of role-based games aimed at imparting knowledge to participants regarding phishing attacks, social engineering exploits, perils linked with excessive online divulgence of personal information, and the enhancement of software design rationales.

In the earlier iteration, players were required to employ various cards placed on the map (including Personas cards, Social Media cards, Persuasion cards, etc.) to acquire pertinent data and progress within the game. Building upon this, our subsequent endeavor involves the transformation of this role-based game into a hybrid version. To achieve this, a comprehensive website was constructed that houses the requisite data for the aforementioned cards. Each card on the map is affixed with a QR code that, upon scanning, directs participants to the pertinent webpage. This webpage then provides the specific data associated with the corresponding card type. For instance, scanning the QR code on a Personas card redirects the participant to the Personas web-page, revealing the relevant data (as depicted in Fig. 9).

Notably, a key implementation aspect pertains to the dynamic nature of the data. Upon every visit or page refresh, the data changes, leading to the generation of varied scenarios for participants. This dynamic nature not only imbues the experience with dynamic values but also offers the potential for the emergence of diverse participant-generated scenarios. The web page's functionality and the ever-changing data are showcased in the video accessible via the provided link. Representative visuals from the website are depicted in Figs. A.17 and A.18 (Appendix). The comprehensive video showcasing the design of the website is available for viewing through the Mendeley link.[5]

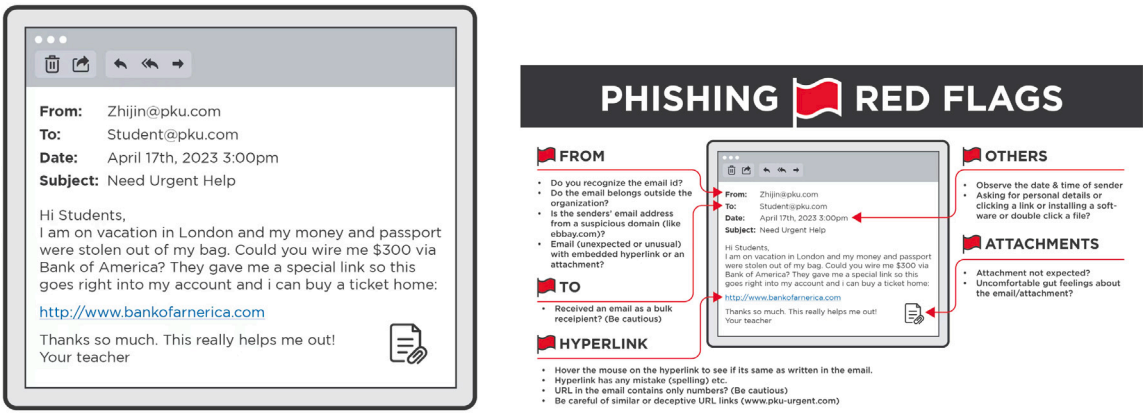
4. Empirical evaluation of an activity

4.1. Pilot session — Interactive dialogue on the phished email: Ice-breaking exercise

During the pilot session, participants were presented with a scenario in which they were informed that their ongoing course or subject (selecting any course from the previous semester) had concluded. Subsequently, they received an email during the night purportedly from their teacher or mentor, bearing a name and email address that appeared authentic. This email conveyed a sense of urgency, mentioning an accident or issue that required immediate assistance. The requested assistance typically involved actions like downloading a file, printing it, and sending it to a designated recipient, with the implication that this would facilitate the installation of an infected file or access to sensitive account information.

In Fig. 10(a), the provided sheet was handed to the participants to evaluate what anomalies they could identify in the scenario. Following a 5–10 min period for examination, a discussion session ensued, during which red flags were elucidated and explained (as depicted in Fig. 10(b)). This pilot session was instrumental in establishing foundational knowledge and context for the participants in preparation for the subsequent gaming session.

[5] Rubia Fatima, Affan Yasin (2023), "Hybrid Version of the Game - Website", Mendeley Data, V1, doi:10.17632/ktxwhcfkt2.1.



(a) Phished Email (b) Indicators of Suspicion in the Template Email Formulation

Fig. 10. Phished email card displayed on the left side, utilized in the Pilot session as an ice-breaking activity and for basic knowledge gathering. The accompanying figure on the right side illustrates various ways to identify a phished email.

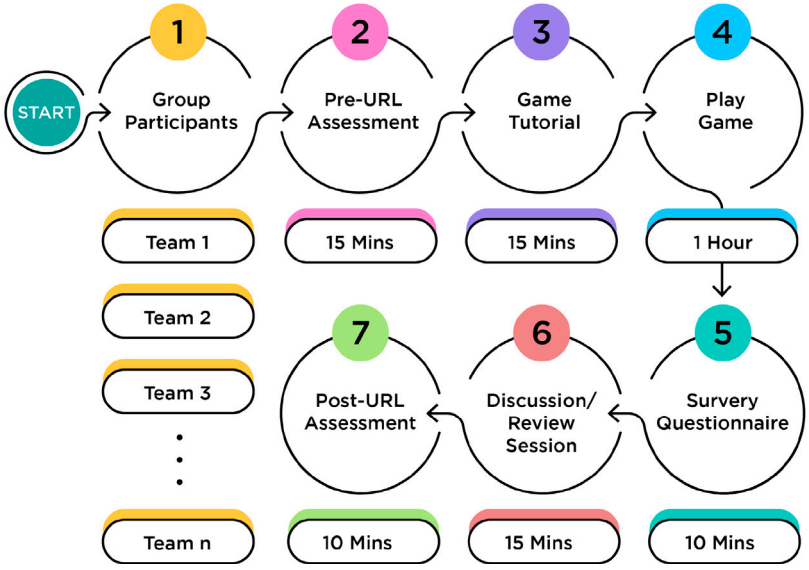


Fig. 11. Detailed illustration of the empirical evaluation process, delineating the flow and temporal allocation from group formation to post-URL assessment.

4.2. Full-scale game session

Fig. 11 illustrates the intricacies of our empirical assessment. Initially, during the primary phase, randomized groups were constituted. Subsequently, a preliminary URL assessment was executed to gauge the initial proficiency of the participants. In the subsequent phase, a comprehensive game tutorial was administered, wherein the game mechanics were expounded to the participants in greater detail. Following this, a game session, also referred to as a play session, was carried out. In this session, participants adhered to a prescribed process and fabricated a simulated phishing email, drawing upon the hypothetical scenarios and information provided by the game. Subsequent to the game session, a deliberative session ensued, involving interactive discussions and feedback. The primary objectives were to disseminate knowledge about phishing emails and to deliberate upon the feasibility of such attacks. Additionally, this session facilitated the allocation of points to the teams, thereby enabling the identification of a victor. Lastly, post-game URL sessions were conducted to assess the acquired knowledge. Moreover, a comparative analysis between the pre-game and post-game URL assessments was undertaken to evaluate the extent of learning achieved. Fig. 12 additionally demonstrates the dispersion of distinct teams among various rooms.

4.2.1. What and where to teach?

Within Table 4, a comprehensive breakdown is presented, elucidating the vital educational elements seamlessly incorporated across various stages of the devised and suggested game.

4.2.2. Template case study & scenarios of phishing developed by participants

Template Case Study — Game Example: A specific occurrence of the game is presented in Table 5 for reference. We are confident that this case instance will provide a clearer comprehension of the procedural aspects of the activity.

Deciphering of phished scenarios: Furthermore, the decoded fraudulent or phished email, which was crafted by participants during the gaming session, is displayed below. The process of decoding is intended to assist the reader in identifying specific components, showcasing how this exercise of creating a phished email could contribute to identifying potential phishing attacks in the future.

- **Scenario 1:**
  - **Human Asset/Target Person/Employee:** Wei Kiu

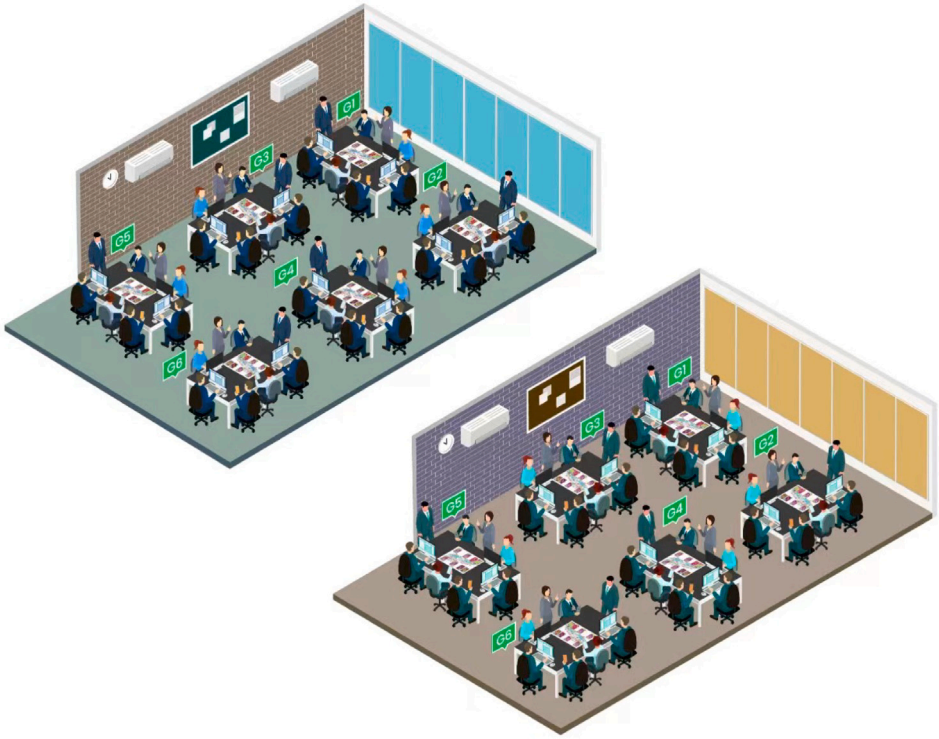


Fig. 12. Visualization of the class setting depicting the arrangement and placement of different participants.

Table 4
What and where to teach in PhishDefend quest.

What to teach	Where to teach
Excessive disclosure of personal information (online) can be damaging (Information disclosure).	**PHASE 2:** Information gathering
Detection of Fraudulent/Phishing emails Recognition of counterfeit URLs and subdomains	**PHASE 3:** Drafting email (hypothetical scenario making) **PHASE 3:** Drafting phishing email (using hypothetical scenario making) **PHASE 4:** Employing phishing message design cards
Recognition of comparable and misleading domains	**PHASE 3:** Drafting phishing email (using hypothetical scenario making) **PHASE 4:** Employing phishing message design cards
Emails — Need and Greed/Curiosity/Authority (Psychology)	**PHASE 3:** Drafting phishing email (using hypothetical scenario making) **PHASE 4:** Employing phishing message design cards
Identify psychology targeting in	**PHASE 3:** Drafting phishing email using hypothetical Scenario making **PHASE 4:** Employing phishing message design cards

- **Social Media Card/Information:** Interested in Business Administrated degree. Need for information about specialization courses or thesis topic.
- **Psychology Card/Persuasion Model:** Need & Greed Curiosity.
- **Phishing Email/Spear-Phishing:** Dear Kin, I am writing to you about the Business Administration course of Cornell University. It will be open for application this week. Please check the detail information attached in this email. Moreover, our school provides scholarship for outstanding students. You can apply for it by clicking this link: http://scholarship.business.123.com. Attention, the deadline for application is April 20, 2023.
  Prof Yu Liu,
  Business Administration Representative
  Cornell University

• **Scenario 2:**

- **Human Asset/Target Person/Employee:** Zhang Wei
- **Social Media Card/Information:** Interested in Business Administrated degree. Need for information about specialization courses or thesis topic
- **Psychology Card/Persuasion Model:** Curiosity, Need and Greed, Obey the authority
- **Phishing Email/Spear-Phishing:** Dear Mr. Zhang, You have won an all paid trip to Germany. The trip has been sponsored by the CEO. To claim your free trip, fill the application attached and return it to the HR as soon as possible.
  Miss Iris
  Human Resource

• **Scenario 3:**

- **Human Asset/Target Person/Employee:** Miss Lin
- **Social Media Card/Information:** Looking for someone in my circle who has knowledge and experience regarding scholarship
- **Psychology Card/Persuasion Model:** Trust, Need and Greed

Table 5
Describes a specific scenario wherein a participant obtained randomly generated values for personas, social media, and persuasive (card) elements from the website. It illustrates how the player utilized this information to formulate the attack scenario — A Game Instance. (The data extracted from the game cards is represented by the olive color.)

Sr. No	Attribute/Dimensions	Game instance
1.	Persona Detail (Persona CARDS) Developed by Team A	Mr. Jue, an intern, is currently serving as a Network Administrator at the hospital.
2.	Social media information (Social media CARDS)	In-need of Post-doctoral opportunity
3.	Vulnerability of human asset	Looking for post-doctoral opportunity
4.	Psychology to target (Psychology CARDS)	Need for greed
i.	Drafted/Crafted Phishing email	Regarding the social media post, there are available opportunities for postdoctoral positions at our university. We kindly request you to share your CV as an initial step in the process.
ii.	Score given by reviewers	5 out of 6 (Total points)
iii.	Reply by Team No # A	Include the name of the university, along with an authentic email address and cell number, to add a touch of realism and authenticity.
iv.	Suggestion given by experts/ mentors	1. The composed phishing email demonstrates a harmonious composition. 2. The attacker possesses the ability to utilize diverse channels for disseminating the deceptive message
v.	Reply by Team No # A	Agree/OK

  - **Phishing Email/Spear-Phishing:** Hi Wei Zhang, I am San Zhang, an undergraduate student at MIT. I saw your post and i just want to share that i also applied for the scholarship last year. The scholarship is 10000$ per year. I think my experience and scholarship information can help you. Here is my contact (sanzhang@mit.com). Feel free to contact me.
    Best Wishes,
    SanZhang

- **Scenario 4:**
  - **Human Asset/Target Person/Employee:** Miss Jane
  - **Social Media Card/Information:** Interested in Medical Specialization. Need for information about specialization courses or thesis topic
  - **Psychology Card/Persuasion Model:** Need & Greed, Curiosity
  - **Phishing Email/Spear-Phishing:** Dear Jane, I am writing to you about the Medical specialization course of Harvard University. It will be open for application this week. Please check the detail information attached in this email. Moreover, our school provides scholarship for outstanding students. You can apply for it by clicking this link: http://scholarship.business.123.com. Attention, the deadline for application is April 20, 2023.
    Prof Yu Liu,
    Medical Degree Coordinator
    Harvard University

- **Scenario 5:**
  - **Human Asset/Target Person/Employee:** Miss Yanan
  - **Social Media Card/Information:** Wish/Like to go on holiday to Germany.
  - **Psychology Card/Persuasion Model:** Curiosity, Need and Greed, Obey the authority
  - **Phishing Email/Spear-Phishing:** Dear Miss. Yanan, You have won an all paid trip to Europe. The trip has been sponsored by the Medical hospital. To claim your free trip, fill the application attached and return it to the HR as soon as possible.
    Miss Leotong
    Human Resource

- **Scenario 6:**
  - **Human Asset/Target Person/Employee:** Miss Jai Yidi
  - **Social Media Card/Information:** Looking for someone in my circle who has knowledge and experience regarding scholarship
  - **Psychology Card/Persuasion Model:** Trust, Need and Greed
  - **Phishing Email/Spear-Phishing:** I am San Zhang, an undergraduate student at MIT. I saw your post and i just want to share that i also applied for the scholarship last year. The scholarship is 10000$ per year. I think my experience and scholarship information can help you. Here is my contact (sanzhang@mit.com). Feel free to contact me.
    Best Wishes,
    SanZhang

4.2.3. *Eliciting security requirements utilizing threat modeling technique*

Threat modeling is the methodical analysis of a system's business and technical aspects. It identifies potential threats and outlines steps to counter them. A threat refers to unauthorized access to an organization's sensitive data, applications, or network. The goal of threat modeling is to comprehend an organization's assets, predict threats, and plan how to mitigate them [46].

Within our gaming approach, the phished emails that have been created and developed are subsequently treated as potential risks to the organization. To effectively address and diminish these risks, the devised attack scenarios can serve the purpose of instructing the organization's personnel and staff. A subset of the threats and scenarios formulated within the gaming context are employed to identify training subjects or areas that aid in countering phishing and social engineering attacks. The process can be seen in Fig. 13.

4.2.4. *Pre-post URL survey*

In the development of the pre- and post-URL surveys, our focus has been directed towards a range of classifications pertaining to phishing URLs. The encompassed categories are indicated as follows — (In this context, 'TP' represents Type):

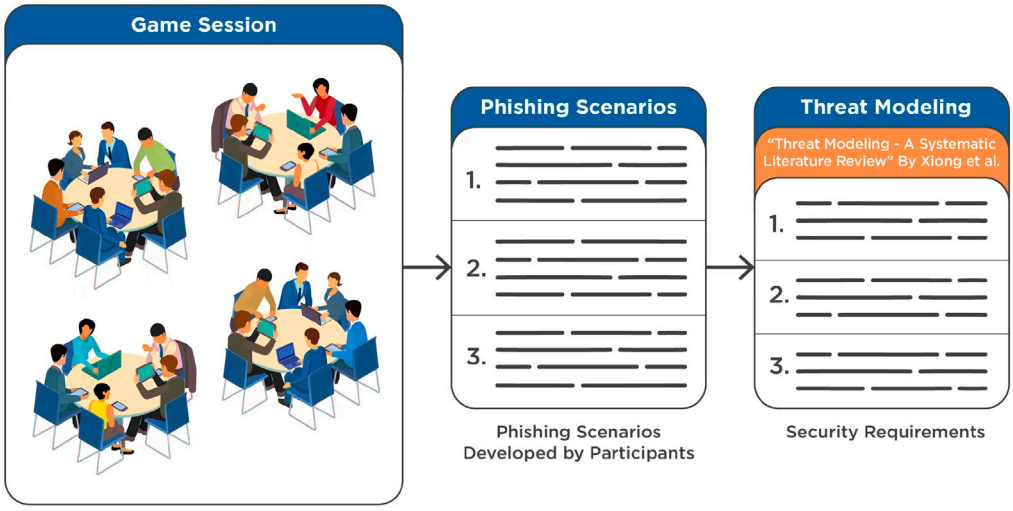


Fig. 13. Illustration detailing how the generated phishing attack scenarios from the game session were subsequently utilized in eliciting security requirements through the application of the Threat Modeling technique [46].

Table 6
Pre-Game participants identification of URL.

Phished URL type	URL	Phished URL	Not sure	Legitimate URL	Correct answer	Correct percentage
TP1, TP4, TP6	www.f4ceb00k.com	78	3	16	Phished URL	80.4%
TP2		30	4	63	Phished URL	30.9%
TP3	https://secure-paypal-login.com	27	1	69	Phished URL	27.8%
TP5	http://bit.ly/amazon-deals	48	0	49	Phished URL	49.4%
TP1, TP4, TP6	www.appl3-support.com	28	0	69	Phished URL	28.8%
TP7	http://123.45.67.89/microsoft-login	43	2	52	Phished URL	44.3%
–	https://www.researchgate.net	10	19	68	Legitimate URL	70.1%
TP3	www.micr0soft-support.info	40	5	52	Phished URL	41.2%
TP1, TP2, TP3	www.twittter-security.org	65	2	30	Phished URL	67.0%

- **TP1**: Conventional Phishing URL (through altered spelling), for instance, bankofamerika.com.
- **TP2**: Subdomain Manipulated Phishing URL (via sub-domain alteration), such as secure-bankofamerica-login.com.
- **TP3**:HTTPS-based Phishing URLs, exemplified by secure-paypal-login.com.
- **TP4**: Redirect Phishing URL, illustrated by verified-link.com.
- **TP5**: Phishing URL Concealed via URL Shortening Service, demonstrated by bit.ly/avftgg.
- **TP6**: Misleading Phishing URL (employing deceptive methods to alter the URL), such as www.g00gle.com.
- **TP7**: Numeric String Phishing URL, represented by http://144.77.66.1/ebay/.

To evaluate the participants' comprehension, surveys were conducted before and after exposure to URLs. Within these surveys, participants were provided with a series of URLs and were required to ascertain the legitimacy of each URL, distinguishing between legitimate sources and phishing attempts through analysis. The findings of the initial survey are outlined in Table 6, whereas the subsequent survey outcomes are outlined in Table 7. The ultimate column in both tables highlights the proportion of accurate responses. The conspicuous upward trend in these percentages underscores the enhancement in participants' learning over the course of the session.

In comparison to the other URL within the pre-survey, the heightened accuracy in identifying the first URL (www.f4cebook.com) may potentially be attributed to its resemblance to a renowned web address, specifically "www.facebook.com". Any deviation from this established similarity can be readily discerned and emphasized. This occurrence could potentially contribute to the elevated accuracy observed among participants in correctly identifying the first URL during the pre-survey assessment.

Upon the completion of the post-URL survey, a dedicated discussion session ensued to deliberate upon the legitimacy of URLs featured in both the pre- and post-surveys. This facilitated a comprehensive exploration of whether the URLs had been subjected to phishing and the underlying rationale. By utilizing both surveys as reference points, participants gained a more extensive comprehension of the subject matter.

A thorough examination of the two tables (Tables 6 and 7) reveals that participants have acquired a heightened proficiency in URL identification. However, the level of awareness remains approximately at 85 percent. While this signifies progress in knowledge and understanding, there remains room for further enhancement through continued education. To this end, the implementation of hybrid methodologies, which amalgamate diverse techniques, can be advantageous. The realm of phishing education encompasses multifaceted aspects including URL scrutiny, sub-domain comprehension, and in-depth analysis of emails for signs of phishing.

Regarding URL awareness, it is evident that a few more sessions are necessary to refine participants' learning concerning the identification of phished URLs.

4.2.5. *Observations & feedback*

- Within the session, an observation emerged that the participants expressed a requirement for an increased number of examples during the preliminary phase to enhance their understanding. This inclination arose from inquiries directed towards the organizer during the gaming session, specifically concerning the

Table 7
Post-Game participants identification of URL.

Phished URL category	URL	Phished URL	Not sure	Legitimate URL	Correct answer	Correct percentage
TP1, TP6	www.netfllx.com	89	3	5	Phished URL	91%
TP2, TP3		72	4	21	Phished URL	74%
TP2, TP3	https://google-security-update.com	78	2	17	Phished URL	80%
TP4	www.linkedinsupport-redirect.com	71	4	13	Phished URL	73.1%
TP2, TP6	http://tinyurl.com/microsoft-security	84	2	11	Phished URL	86%
TP6	www.appl3-support-alerts.com	86	2	9	Phished URL	88%
TP7	http://555.666.777/paypal-login	92	4	1	Phished URL	94.8%
–	www.pinterest.com	4	2	91	Legitimate URL	93%
–	www.twitch.tv	8	3	86	Legitimate URL	88%

application of "persuasion techniques" data in the composition of phishing emails.

- The preliminary activity or session serves to furnish participants with an initial comprehension of the task at hand, along with insights into the analysis of phishing emails to fortify defenses against phishing attacks.
- The declaration made within the classroom, apprising participants of their role as attackers, engenders a sense of contentment among them and augments their engagement with the provided instructions and guidelines.

4.2.6. Survey questionnaire design and results

The survey research model was adapted from the study Huigang Liang et al. [47]. In this sub-section, our primary objective was to empirically examine the proposed theoretical relationships through a rigorous statistical analysis. To achieve this, we employed well-established analytical tools, namely SPSS and Smart-PLS, to scrutinize our research framework. This comprehensive examination encompassed several distinct stages of analysis. Initially, a descriptive analysis was undertaken to provide an overview of the demographical questions and the research variables by assessing their descriptive statistics. Subsequently, a correlation analysis was performed to gauge the interrelationships between the various constructs under investigation. Following this, regression analyses were conducted utilizing ANOVA to probe the hypothesized relationships in depth.

Out of the total 112 participants who took part in the game sessions for the evaluation, it is important to note that 7 participants had to leave early due to scheduling conflicts with other classes and were consequently unable to complete the survey. Additionally, 8 participants completed the survey with consistently extreme positive or extreme negative responses. To ensure the integrity and impartiality of the data, each of the comments and issues mentioned in the survey that indicated a negative experience was meticulously reviewed individually. However, upon examining the comment and suggestion section of the survey, it was determined that no comments or feedback were provided.

In light of these considerations and after careful deliberation, it was decided to exclude the data from these 15 participants from the analysis. Therefore, the analysis was conducted using data from 97 participants to maintain the quality and reliability of the research findings.

Demographical Profile and Descriptive Statistics: Initially, an assessment of the demographic profile was conducted to examine the frequency distribution of various demographic variables. The outcomes, as presented in Table 8, encompassed an evaluation of demographic attributes such as age, gender, year of study, and educational background. In terms of age, it was observed that approximately 11% of respondents were aged 20 or below, while roughly 58% fell within the age bracket of 21 to 25. Approximately 27% of the survey participants were aged between 26 and 29, with around 4% aged 30 or above. This analysis reveals that the predominant age group among respondents was between 21 and 25. In respect to gender distribution, about 75% of the respondents identified as male, while approximately 25% identified as female, indicating a clear majority of male participants. Regarding educational attainment, approximately 65% of the respondents held undergraduate degrees, whereas about 25% possessed postgraduate qualifications, thus highlighting the prevalence of undergraduate respondents. Lastly, with regard to the "years of study" variable within their respective degree programs, it was observed that around 13% of respondents had studied for less than one year, approximately 12% were in their second year of study, and roughly 50% were in the third year of their degree program. Additionally, approximately 25% of the participants were in their fourth year or beyond. This analysis underscores that the majority of respondents were in the third year of their academic programs.

Table 8
Demographical profile.

		Frequency	Percent	Cumulative percent
Age	20 and below	11	11.3	11.3
	21–25	56	57.7	69.1
	26–29	26	26.8	95.9
	30 and above	4	4.1	100.0
	Total	97	100	
Gender	Male	73	75.3	75.3
	Female	24	24.7	100.0
	Total	97	100.0	
Year of study	<= First year	13	13.4	13.4
	Second year	12	12.4	25.8
	Third year	48	49.5	75.3
	>= Fourth year	24	24.7	100.0
	Total	97	100.0	
Education	Undergraduate	63	64.9	64.9
	Postgraduate	34	35.1	100.0
	Total	97	100.0	

Following the examination of the demographic profile, a thorough analysis of descriptive statistics was carried out (as presented in Table 9). In this analysis, key descriptive measures including the mean, standard deviation, skewness, and kurtosis were computed for both the demographic data and the research constructs under investigation.

The descriptive statistics provided insights into the characteristics of the research constructs. Specifically, the mean values for year of education (2.86), program (1.35), perceived severity (3.30), perceived susceptibility (2.28), perceived threat (3.31), avoidance motivation (3.78), self-efficacy (1.88), avoidance behavior (2.51), safeguard cost (3.50), and safeguard effectiveness (2.42) were carefully examined. Additionally, the standard deviation values for these constructs were determined: year of education (0.95), program (0.48), perceived severity (0.94), perceived susceptibility (0.91), perceived threat (1.18), avoidance motivation (1.09), self-efficacy (0.62), avoidance behavior (1.11), safeguard cost (1.32), and safeguard effectiveness (0.84).

Furthermore, skewness and kurtosis, which are indicators of the distribution's shape, were assessed for all the constructs. It is noteworthy that the values for skewness and kurtosis for all the constructs fell within the range of +2 to −2. This observation suggests that the data pertaining to the study constructs adhere to the normality assumption, indicating that the data distribution is reasonably close to a normal distribution.

Table 9
Demographical profile.

Constructs	Mean	Std. Deviation	Skewness		Kurtosis	
			Statistic	Std. Error	Statistic	Std. Error
Year of Education	2.86	0.95	−0.68	0.24	−0.31	0.49
Program	1.35	0.48	0.64	0.24	−1.63	0.49
Perceived Severity	3.30	0.94	−0.81	0.24	0.20	0.49
Perceived Susceptibility	2.28	0.91	0.58	0.24	−0.47	0.49
Perceived Threat	3.31	1.18	−0.81	0.24	−0.62	0.49
Avoidance Motivation	3.78	1.09	−1.00	0.24	0.46	0.49
Self-Efficacy	1.88	0.62	0.22	0.24	−0.98	0.49
Avoidance Behavior	2.51	1.11	0.57	0.24	−0.55	0.49
Safeguard Cost	3.50	1.32	−0.65	0.24	−0.79	0.49
Safeguard Effectiveness	2.42	0.84	0.33	0.24	−0.36	0.49

Table 10
Correlation between study constructs.

Sr.	Constructs	1	2	3	4	5	6	7	8	9	10	11	12
1	Age	1											
2	Gender	0.079	1										
3	Year of Education	-.230*	0.164	1									
4	Programme	−0.156	-.271**	0.090	1								
5	Avoidance Behavior	−0.116	−0.134	0.116	0.104	1							
6	Avoidance Motivation	−0.004	−0.025	.363**	0.067	.435**	1						
7	Perceived Severity	.215*	.208*	.404**	−0.052	0.044	.574**	1					
8	Perceived Susceptibility	−0.029	−0.023	0.112	0.037	.344**	.497**	0.034	1				
9	Perceived Threat	0.114	0.071	.388**	0.055	.221*	.774**	.809**	.274**	1			
10	Safeguard Cost	−0.048	−0.147	.258*	0.130	.428**	.875**	.488**	.240*	.738**	1		
11	Safeguard Effectiveness	−0.147	−0.006	.248*	−0.042	.315**	.666**	.303**	.735**	.470**	.451**	1	
12	Self-Efficacy	−0.023	−0.094	0.153	−0.016	.473**	.621**	0.074	.575**	.253*	.507**	.701**	1

* p <= 0.05: Correlation is significant at the 0.05 level (2-tailed).
** p <= 0.01: Correlation is significant at the 0.01 level (2-tailed).

Correlation Analysis: In the course of the correlation analysis, the relationships between various study constructs were scrutinized, and the findings are presented in Table 10. The results highlight the following associations:

- *Age* exhibited no significant correlation with Gender, Year of Education, Programme, Avoidance Behavior, Avoidance Motivation, Perceived Susceptibility, Perceived Threat, Safeguard Cost, Safeguard Effectiveness, and Self-Efficacy. However, a significant positive correlation was identified between Age and Perceived Severity (β = 0.21, p <= 0.05).
- *Gender* displayed no significant correlation with Year of Education, Avoidance Behavior, Avoidance Motivation, Perceived Susceptibility, Perceived Threat, Safeguard Cost, Safeguard Effectiveness, and Self-Efficacy. Nevertheless, noteworthy associations were observed between Gender and Programme (β = 0.27, p <= 0.01), as well as between Gender and Perceived Severity (β = 0.21, p <= 0.05).
- *Year of Education*:
  - Insignificant relationships with Programme, Avoidance Behavior, Perceived Susceptibility, and Self-Efficacy.
  - Significant positive correlations with Perceived Severity (β = 0.40, p <= 0.05), Avoidance Motivation (β = 0.36, p < 0.01), Perceived Threat (β = 0.39, p <= 0.01), Safeguard Cost (β = 0.26, p <= 0.05), and Safeguard Effectiveness (β = 0.25, p <= 0.05).
- *Programme*: Insignificant relationships with all other study constructs.
- *Avoidance Behavior*: Positively correlated with Avoidance Motivation (β = 0.435, p <= 0.01), Perceived Susceptibility (β = 0.344, p <= 0.01), Perceived Threat (β = 0.221, p <= 0.05), Safeguard Cost (β = 0.428, p <= 0.01), Safeguard Effectiveness (β = 0.315, p <= 0.01), and Self-Efficacy (β = 0.473, p <= 0.01). No significant relationship was found with Perceived Severity.
- *Avoidance Motivation*: Positively correlated with Perceived Severity (β = 0.574, p <= 0.01), Perceived Susceptibility (β = 0.497, p <= 0.01), Perceived Threat (β = 0.774, p <= 0.01), Safeguard Cost (β = 0.875, p <= 0.01), Safeguard Effectiveness (β = 0.666, p <= 0.01), and Self-Efficacy (β = 0.621, p <= 0.01). Except for Perceived Susceptibility and Self-Efficacy, all other constructs positively correlated with Perceived Severity (β = 0.809, p <= 0.01), Safeguard Cost (β = 0.488, p <= 0.01), Safeguard Effectiveness (β = 0.303, p <= 0.01), and Self-Efficacy (β = 0.074, p <= 0.01).
- *Perceived Susceptibility*: Positively correlated with Perceived Threat (β = 0.274, p <= 0.01), Safeguard Cost (β = 0.240, p <= 0.05), Safeguard Effectiveness (β = 0.735, p <= 0.01), and Self-Efficacy (β = 0.575, p <= 0.01).
- *Perceived Threat*: Positively correlated with Safeguard Cost (β = 0.738, p <= 0.01), Safeguard Effectiveness (β = 0.470, p <= 0.01), and Self-Efficacy (β = 0.253, p <= 0.01).
- *Safeguard Cost*: Positively correlated with Safeguard Effectiveness (β = 0.451, p <= 0.01) and Self-Efficacy (β = 0.507, p <= 0.01).
- *Safeguard Effectiveness*: Positively correlated with Self-Efficacy (β = 0.701, p <= 0.01).

These findings shed light on the nature and strength of relationships among the variables studied, highlighting the specific connections that warrant further attention and analysis.

Regression Analysis: To ascertain the influence of independent variables on the dependent variable, a comprehensive regression analysis was conducted, and the results are presented in Tables B.12 through B.23. Notably, all the regressed predictors demonstrated a significant relationship with their respective dependent variables. Furthermore, the significance of the F values for all the regression paths indicates that the findings align with and support the hypothesized relationships, validating the hypotheses posited in this study.

- **Path 1**: The interaction between Perceived Susceptibility and Perceived Severity on Perceived Threat was examined as part

Table 11
Controlling variables for internal validity.

Control factor	Explanation
Class instructor	The presence of both the class instructor and the activity facilitator was ensured within the class to provide assistance and guidance to students whenever required.
Class time	The class schedule was segmented into various segments, as elaborated upon in the evaluation segment.
Learning context	The educational content of the game was available in English language.
Class setting	The students in the class were randomly distributed into various groups.
Teaching method	PowerPoint slides were employed to elucidate the game process and regulations to the students
Gender, age, academic qualification	The participants' educational level, age, and gender were established and remained constant from the commencement of the activity.

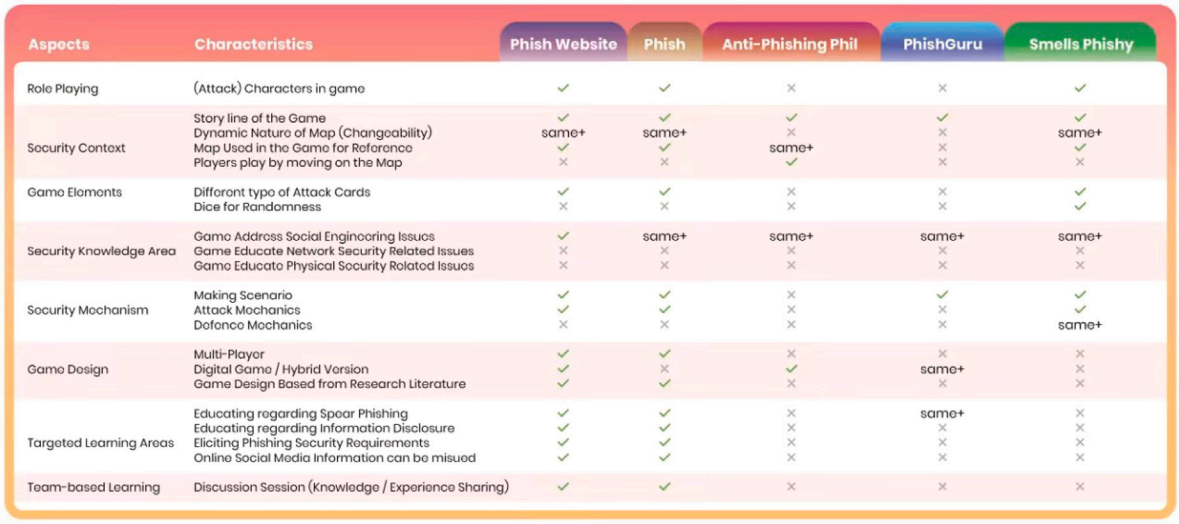


Fig. 14. Detailed comparison of the designed game presented in the first column with other similar phishing awareness games in subsequent columns.

of the regression analysis, and the specific details can be found in Tables B.12, B.13, and B.14 (Appendix). These tables likely provide insights into how these variables interact to influence Perceived Threat, shedding light on the nuanced relationship between these constructs.

- **Path 2**, which involves the interaction of Perceived Susceptibility and Perceived Severity on Perceived Threat, was analyzed and the specific details can be found in Tables B.15, B.16, and B.17 (Appendix). These tables are likely to provide a deeper understanding of how this interaction affects Perceived Threat, offering insights into the complex relationship between these variables and their combined impact on perceptions of threat.
- **Path 3**, which explores the antecedents of Avoidance Motivation, has been analyzed and the specific details can be found in Tables B.18, B.19, and B.20 (Appendix). These tables likely provide information about the factors that contribute to and influence Avoidance Motivation, helping to elucidate the underlying determinants of this important construct in your study.
- **Path 4**, which investigates the relationship between Avoidance Motivation and Avoidance Behavior, has been thoroughly examined, and the specific details can be found in Tables B.21, B.22, and B.23 (Appendix). These tables likely provide insights into how Avoidance Motivation influences and correlates with Avoidance Behavior, shedding light on the behavioral implications of motivational factors in your study.

Summary: In this sub-section, the utilization of SPSS and PLS-SEM methodologies was chosen to explore the hypothesized direct and interaction paths due to their capability to effectively analyze complex multivariate research frameworks. The results of the analysis reaffirmed the significance of all the direct and interaction hypotheses, thus validating the proposed relationships and contributing to a more comprehensive understanding of the research constructs.

4.3. Validity threats & limitations

Every research endeavor encounters potential threats to its validity, prompting researchers to employ diverse strategies for mitigation [48]. As a collective, we diligently worked to identify and alleviate these threats. Selected strategies are elaborated upon herein to provide readers with a comprehensive comprehension:

- ***Conclusion validity*** pertains to the dependability of research findings [49,50], ensuring the safeguarding of study conclusions. Anonymous survey data was collected from players and processed using a tool. Researchers engaged in collaborative analysis of tabulated and graphical data for potential insights, thereby mitigating conclusion validity concerns. Additionally, external researchers reviewed the outcomes for feedback, aiming to diminish any conclusion-related biases. Furthermore, the current empirical evaluation involved a limited number of participants, introducing a potential conclusion validity concern. This concern will be addressed in future assessments by expanding participant involvement.
- ***External Validity:*** Providing a comprehensive account of the controlled activity context within the study is crucial, as it enables meaningful comparisons between cases. Each individual case study holds considerable value, contributing to a profound comprehension of the subject [50]. While our empirical assessment of this serious game transpired in a diverse class setting, the pursuit of external validity verification remains a prospective endeavor for future investigations.
- ***Theoretical Validity:*** Behavior can be influenced by prior experiences [50]. Certain students might have encountered specific security attacks before, potentially influencing their engagement with the game. This could result in an enhanced learning curve

Fig. 15. In-depth comparison between the designed game, featured in the first column, and other cyber security games presented in the subsequent columns.

evident in subsequent surveys. To mitigate this potential bias, Pre and Post URL surveys were implemented to gauge learning behavior objectively.

- ***Internal Validity:*** Internal validity pertains to potential researcher bias and data interpretation [49,50]. In order to mitigate internal validity concerns within the controlled activity, researchers engaged in comprehensive discourse and experience-sharing regarding the empirical evaluation's conception and implementation. Following in-depth deliberation, refined procedures underwent testing with a limited student cohort for validation and refinement, subsequently undergoing review by external researchers for additional insights. Table 11 explains the variables for Internal validity.

Table B.12
Regression model analysis.

R	R square	Adjusted R square	Std. Error of the estimate
.845	.715	.709	.54275

a. Predictors: (Constant), Perceived Susceptibility, Perceived Severity.

Table B.13
ANOVA.

Model	Sum of squares	df	Mean square	F	Sig.
Regression	69.334	2	34.667	117.684	.000b
Residual	27.690	94	.295		
Total	97.025	96			

a. Dependent Variable: Perceived Threat,
b. Predictors: (Constant), Perceived Susceptibility, Perceived Severity.

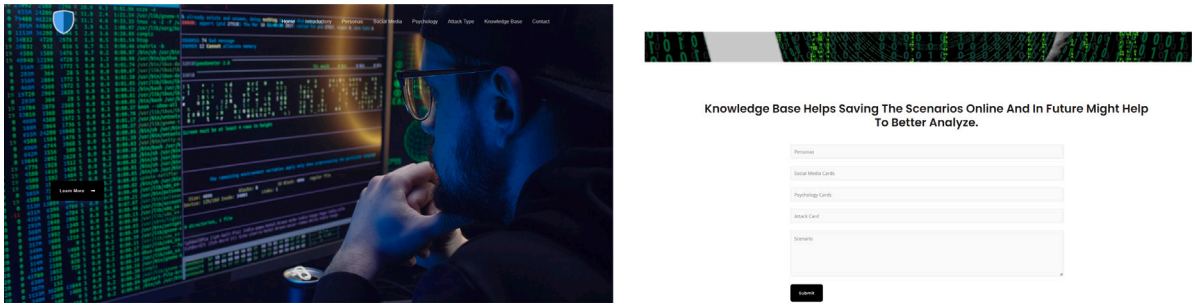
5. Literature review

Various literary references were scrutinized to extract pertinent studies. Moreover, to investigate preprints, the methodology outlined in the referenced study [51] was employed. Multiple research investigations have underscored the prevalent use of social engineering through phishing techniques and have proposed approaches for addressing these challenges through game-based learning models. This underscores the imperative for users, be they employees within an organization, students in an educational institution, or general users, to acquire knowledge about phishing attacks. In this regard, Kirlappos et al. [52] explicitly argued that in today's highly digitalized era the chances of an online user coming across a cyberattack is quite significant due to the fact that fake websites are even appearing on renowned search engine platforms such as Google and Yahoo. Several latest and previous studies have been conducted related to the implementation of game-based learning in the models and frameworks for the control of various cybercrimes and SE attacks. Researchers have supported the claim that the game-based approach is effective in increasing users' understanding of SE attacks, such as phishing attacks. Arachchilage et al. [53] reported that game-based learning changes the state of the user in such a way that they are moved into an environment where their learning becomes mentally better.

Arachchilage et al. [54] executed a survey-based study to construct a game-based framework that aimed to increase motivation among computer users to adopt avoidance behavior to tackle phishing attacks. Their framework was built using the Technology Threat Avoidance Theory (TTAT). They used 150 computer users as the target population to gather feedback. Their finding showed that there is an urgent need to address several human behavioral factors, including perceived threat, self-efficacy, safeguard effectiveness, etc. They concluded that such a game-based framework could not only prevent phishing attacks but also other malicious information system security threats. In a similar study, Arachchilage et al. [55] developed a mobile game-based prototype to increase motivation for avoidance behavior of phishing attacks among computer users. To this end, they employed a game design framework along with game elements and conducted the post- and pre-test assessments to evaluate the effectiveness of the game design framework. They found that post-test assessment depicted significant effectiveness of the game design framework in increasing motivation among participants for awareness regarding phishing attacks.

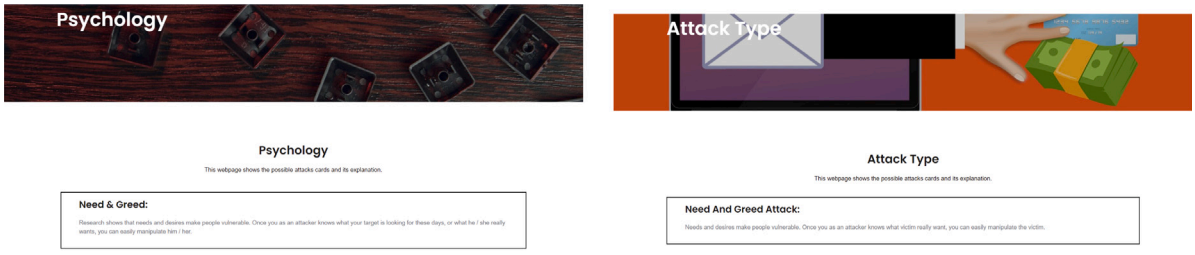
Xenos [56] conducted a study in which they develop an online 3D environment for learning about phishing attacks based upon a game-based approach. In this environment, phishing attacks and many other social engineering attacks were simulated. They reported that this 3D environment enabled learners to develop awareness regarding such attacks through real-time experience. In their study, Baral et al. [57] asserted the need for the adoption of game-based learning as SE attacks such as phishing attacks include human interaction as being the weakest link. Moreover, it has been found that gathering social engineering security requirements through traditional methods has become ineffective. Beckers et al. [58] argued that serious games can be a helpful tool to elicit social engineering security requirements. The authors further argued that games take into consideration the participants from an individual context and give special attention to the aspect of the human aspect. Thus, training humans for cybersecurity via gamed based approach is effective.

Fig. A.16. Displays recommendations for participants to enhance the deceptive nature of phishing email (Design Cards/Rule Card).



(a) Homepage of the Game Website (b) Compiling Attack Scenarios in Knowledge Base

Fig. A.17. Website developed for the game.



(a) Psychology Card - Generating Dynamic Card Data (b) Attack Card - Generating Dynamic Card Data

Fig. A.18. Creating dynamic card data on page refresh.

Table B.14
Coefficients.

Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	2.348E−5	.055		.000	1.000
Perceived Severity	.800	.055	.800	14.514	.000
Perceived Susceptibility	.247	.055	.246	4.471	.000

a. Dependent Variable: Perceived Threat.

Table B.15
Model summary.

R	R square	Adjusted R square	Std. Error of the estimate
.895a	.802	.795	.45468

a. Predictors: (Constant), Safeguard Effectiveness x Perceived Threat, Safeguard Effectiveness, Perceived Threat.

Table B.16
ANOVA.

Model	Sum of squares	df	Mean square	F	Sig.
Regression	77.773	3	25.924	125.401	.000 b
Residual	19.226	93	.207		
Total	96.999	96			

a. Dependent Variable: Avoidance Motivation
b. Predictors: (Constant), Safeguard Effectiveness x Perceived Threat, Safeguard Effectiveness, Perceived Threat.

In another recent study, Baral et al. [57] conducted empirical research to propose a game-based approach to enhance users' motivation to behavior in order to avoid phishing attacks. Their model aimed at enhancing users' self-efficacy to tackle cybersecurity issues. They employed social cognitive theory to explore knowledge attributes required for threat avoidance behavior. Then, these identified attributes were incorporated into a game-based prototype developed by the authors. They concluded that their integrated gaming design would be quite helpful in creating users' self-efficacy against the menaces of social engineering attacks. Baslyman et al. [59] also proposed a board game named "Smells Phishy?" in order to increase awareness regarding the common SE attacks including phishing attacks. They developed the board game and executed their experiment using 121 respondents. They found that including the board game in the learning model increased participants' motivation to increase awareness about phishing attacks and the ways to tackle these scams. They concluded that these games should be frequently used as they increase users' interest in learning.

Khan et al. [60] conducted a study in which they developed a game-based platform that aims to increase students' and users' learning regarding cyberattacks such as phishing attacks. It was adapted from an ARCS motivational model. The design of the model entailed a virtual lab where the students can practice their learning and skills. It includes tools such as fun puzzles and educational games to enhance students' knowledge of cybersecurity issues. In a relevant study, Hendrix et al. [61] conducted an exploratory study with an aim to evaluate whether a game-based approach can be an effective strategy or tool to increase awareness and security against certain cybercrimes, such as phishing attacks through email, false web pages, etc. To this end, they employed an integrated approach by using a literature review in combination with a general web search. They found that games were an effective source of controlling phishing attacks. However, they also reported that there was an explicit lack of game-based learning initiatives from stakeholders, i.e., government, organizations, etc.

Cone et al. [62] performed a study to assess the efficacy of the game-based approach in enhancing basic information awareness regarding phishing and other cybercrimes that involve human factors. To this end, they employed a video game "CyberCIEGE" to incite interest in cybersecurity among users. They found that this game can be significantly utilized in developing basic awareness among computer and internet users about the threats of cybercrimes. In the following year, Fung et al. [63] conducted another study to inspect the influence of the simulation-based CyberCIEGE game on the awareness of information security among students in Thailand. The authors concluded that in the next phases of these projects, such games will impart positive impacts on students' learning regarding information security and its related threats.

In a previous study, Sheng et al. [64] evaluated the effectiveness of a game, namely "Anti-Phishing Phil" in developing the behavior of avoiding phishing attacks among computer users. The participants of the research study were allowed to perform game-related activities to detect scams and fraudulent web activities. They found that playing games increased participants' ability to detect any fraudulent activity on the internet in comparison to those who did not play games (the false positive rare was shrank to 14% from 30%). They concluded that a game-based approach can be an invaluable tool in creating awareness among computer users regarding the threats of phishing and other social engineering attacks.

In their study, Silic et al. [65] termed online self-disclosure (OSD) as a threat to cybersecurity and a common attack of social engineering. They conducted a survey-based study to evaluate the role of gamification in creating awareness among susceptible individuals by using a design science research approach. They employed two artifacts: text and visual. They aimed to explore the association between technology artifacts and human experience. They found that text-based artifacts performed better at providing instrumental results. They concluded that their gamified design science research approach was quite effective in devising strategies for regulating employees' information and ensuring its security. In another recent study, Wen et al. [66] introduced the game "What. Hack" which is a valuable tool to learn basic awareness about phishing attacks. The authors argued that not phishing attack learning, but this game would also provide an opportunity to perform actual simulation of phishing attacks by using role-playing games approach. They concluded that their game-based model was much more effective than traditional and other standard methods of controlling social engineering attack control.

In their empirical research work, Tseng et al. [67] developed a game to increase the learning about phishing attacks on online content websites among the end-users. They aimed to explore the stereotype attributes of the techniques used in these attacks by proposing a phishing attack frame hierarchy. Using their model, they enhanced the game contents of web pages affected by phishing attacks. In order to assess the efficiency and effectiveness of their model framework, they developed an anti-phishing game. They found that most lecturers had increased understanding of the phishing attack and were satisfied with this game-based approach. Moreover, Roepke et al. [68] conducted a review using a systematic literature review approach and the product search approach to examine the effectiveness of serious games for end users. Their hypotheses testing revealed that there are several games available without prior understanding and skills for users the protection against cyberattacks.

Weanquoi et al. [69] constructed a 2D game "Bird's Life" to evaluate the improvement in cybersecurity using the game-based learning approach among students. To this end, the executed pre-test, post-test as well as online administered survey and employed in the evaluation procedure. Their findings revealed that students enjoyed these games and it enhanced their interest in learning about cybersecurity.

Table B.17
Coefficients.

Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	.180	.054		3.321	.001
Safeguard Effectiveness	.360	.052	.360	6.858	.000
Perceived Threat	.272	.073	.273	3.744	.000
Safeguard Effectiveness_x_Perceived Threat	−.383	.061	−.443	−6.313	.000

a. Dependent Variable: Avoidance Motivation.

Table B.18
Model summary.

R	R square	Adjusted R square	Std. Error of the estimate
.939a	.881	.876	.35348

a. Predictors: (Constant), Self-Efficacy, Perceived Threat, Safeguard Effectiveness, Safeguard Cost.

Table B.19
ANOVA.

Model		Sum of squares	df	Mean square	F	Sig.
1	Regression	85.504	4	21.376	171.078	.000b
	Residual	11.495	92	.125		
	Total	96.999	96			

a. Dependent Variable: Avoidance Motivation.
b. Predictors: (Constant), Self-Efficacy, Perceived Threat, Safeguard Effectiveness, Safeguard Cost.

Table B.20
Coefficients.

Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	−4.255E−5	.036		−.001	.999
Safeguard Cost	.513	.063	.513	8.149	.000
Safeguard Effectiveness	.208	.057	.208	3.623	.000
Perceived Threat	.260	.061	.260	4.250	.000
Self-Efficacy	.149	.059	.149	2.512	.014

a. Dependent Variable: Avoidance Motivation.

Table B.21
Model summary.

R	R square	Adjusted R square	Std. Error of the estimate
.435a	.189	.180	.90998

a. Predictors: (Constant), Avoidance Motivation.

Table B.22
ANOVA.

Model	Sum of squares	**df**	Mean square	F	Sig.
Regression	18.319	1	18.319	22.123	.000b
Residual	78.666	95	.828		
Total	96.985	96			

a. Dependent Variable: Avoidance Behavior
b. Predictors: (Constant), Avoidance Motivation.

They concluded that such games could be quite crucial in spreading awareness regarding cybersecurity issues and improved versions of these games should be introduced in future research works. Giannakas et al. [70] discussed the development of an app that was based upon the game-based approach. The app aimed to educate users about cyberattacks, especially phishing attacks. They argued that this game is quite convenient for learning about phishing attacks as it can be used outside the classrooms as well.

Van Steen et al. [71] placed special focus on the behavioral aspect of humans in terms of computer and internet phishing and cyberattacks. They reiterated the need for immediate training against cybercrimes. To this end, they introduced a cybersecurity serious game to protect users from cyberattacks through cybersecurity training. In order to evaluate the efficiency and effectiveness of this game, developed compared it with another game that was not based upon cybersecurity. From a theoretical point of view, they employed the theory of planned behavior in their model. Their findings exhibited that cybersecurity games showed higher scores than non-cyber security games in terms of perceived behavioral control against cyberattacks.

Raman et al. [72] also conducted empirical research to ascertain the impact of the game-based approach on the learning of students of cybersecurity. To this end, they divided students into two groups: one who played the game (EG1) and the other without playing the game (EG2). Their results showed that the second group (EG2) depicted a better understanding of the cyberattacks. They concluded with the need to employ such game-based techniques in cybersecurity courses.

- The detailed comparison of the proposed game (Phish-W website) with other similar phishing games can be seen in Fig. 14.
- The detailed comparison of the proposed game (Phish-W website) with other social engineering games can be seen in Fig. 15.

6. Conclusion

Spear-phishing and phishing attacks stand as prevalent and significant global threats to internet security. These malicious tactics involve the use of deceptive or forged emails to gain unauthorized access to users' sensitive information, encompassing crucial data like system passwords, transactions, and online banking credentials. Consequently, the imperative for companies to fortify their vital information and data against such assaults has become paramount. Notably, a recurring pattern in these attacks is the attribution of responsibility to humans, highlighting the human factor's role in such breaches. The nature of how sensitive data becomes compromised, whether accidentally or deliberately, results in potential damage to both reputation and financial standing. Phishers employ fabricated messages and emails to manipulate users into divulging sensitive data. Emerging research forecasts an escalation in both the frequency and potency of phishing attacks, underscoring the need for robust efforts to disseminate awareness and provide effective training to counter these threats [30,73,31]. Studies also indicate that heightened security awareness significantly bolsters users' capability to detect fraudulent schemes [74].

This research encompasses the development and empirical evaluation of a serious game aimed at enhancing users' awareness and understanding of phishing and spear-phishing threats. The analysis of participant learning outcomes and survey feedback reveals the effectiveness of this game-based intervention in improving skills related to identifying phishing attacks and fostering cautious behaviors concerning the sharing of sensitive information online.

The inclusion of QR codes in the hybrid version of the game introduces an interactive and captivating approach for users to acquire knowledge about prevalent phishing techniques and associated risks. Quantitative measures of learning improvement, combined with favorable qualitative feedback, substantiate the use of serious games as a

Table B.23
Coefficients.

Model	Unstandardized coefficients		Standardized coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	4.572E−5	.092		.000	1.000
Avoidance Motivation	.435	.092	.435	4.703	.000

a. Dependent Variable: Avoidance Behavior.

promising avenue for security awareness training, with a particular focus on countering social engineering threats.

Nevertheless, being an initial study, it is essential to acknowledge certain limitations, such as the sample size and the absence of longitudinal data to assess knowledge retention. Consequently, further research involving larger participant cohorts is warranted. Additionally, there exist prospects for expanding the game's applicability to various platforms, incorporating personalized adaptivity, and addressing emerging forms of cyberattacks.

In conclusion, this work furnishes compelling evidence that serious games harness the potential of immersive, activity-centered learning to enhance knowledge of phishing threats. Game-based training provides a secure environment for experimentation with common manipulation tactics. Although further endeavors are necessary, gamification demonstrates considerable potential as a supplementary approach to conventional cybersecurity education, particularly with regard to human vulnerabilities.

Implications: **(i)** The outcomes of this research study bear implications for governmental entities, policy formulators, and academic institutions, who can leverage the findings and game to strengthen their efforts in mitigating social engineering, particularly phishing attacks.

CRediT authorship contribution statement

Affan Yasin: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Writing – original draft, Writing – review & editing. **Rubia Fatima:** Conceptualization, Formal analysis, Methodology, Software, Visualization, Writing – original draft. **Zheng JiangBin:** Formal analysis, Project administration, Supervision, Validation, Writing – review & editing. **Wasif Afzal:** Conceptualization, Project administration, Supervision, Validation, Visualization, Writing – review & editing. **Shahid Raza:** Investigation, Methodology, Validation, Visualization, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This paper is partially supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883054 (EU-HYBNET).

Appendix A. Rules or design cards AND phishing website pages

See Figs. A.16–A.18.

Appendix B. Statistical analysis

See Tables B.12–B.23.

References

[1] A. Pollini, T.C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, D. Guerri, Leveraging human factors in cybersecurity: An integrated methodological approach, Cogn. Technol. Work 24 (2) (2022) 371–390.

[2] I. Yaqoob, E. Ahmed, M.H. Rehman, A.I.A. Ahmed, M.A. Al-garadi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges in the Internet of Things, Comput. Netw. (2017) http://dx.doi.org/10.1016/j.comnet.2017.09.003, URL http://eproxy2.lib.tsinghua.edu.cn:80/rwt/33/http/P75YPLUUMNVXK5UDMWTGT6UFMN4C6Z5QNF/science/article/pii/S1389128617303468.

[3] H. Hellaoui, M. Koudil, A. Bouabdallah, Energy-efficient mechanisms in security of the Internet of Things: A survey, Comput. Netw. 127 (Suppl. C) (2017) 173–189, http://dx.doi.org/10.1016/j.comnet.2017.08.006, URL http://www.sciencedirect.com/science/article/pii/S1389128617303146.

[4] W.R. Flores, M. Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, Comput. Secur. 59 (2016) 26–44, http://dx.doi.org/10.1016/j.cose.2016.01.004.

[5] H. Siadati, T. Nguyên, P. Gupta, M. Jakobsson, N.D. Memon, Mind your SMSes: Mitigating social engineering in second factor authentication, Comput. Secur. 65 (2017) 14–28, http://dx.doi.org/10.1016/j.cose.2016.09.009.

[6] F. Mouton, L. Leenen, H.S. Venter, Social engineering attack examples, templates and scenarios, Comput. Secur. 59 (2016) 186–209, http://dx.doi.org/10.1016/j.cose.2016.03.004, URL http://www.sciencedirect.com/science/article/pii/S0167404816300268.

[7] T. Li, C. Song, Q. Pang, Defending against social engineering attacks: A security pattern-based analysis framework, IET Inf. Secur. 17 (4) (2023) 703–726, http://dx.doi.org/10.1049/ise2.12125, arXiv:https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/ise2.12125, URL https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/ise2.12125.

[8] P. Tetri, J. Vuorinen, Dissecting social engineering, Behav. Inf. Technol. 32 (10) (2013) 1014–1023, http://dx.doi.org/10.1080/0144929X.2013.763860, arXiv:http://dx.doi.org/10.1080/0144929X.2013.763860.

[9] L.D. Kimpe, M. Walrave, W. Hardyns, L. Pauwels, K. Ponnet, You've got mail! explaining individual differences in becoming a phishing target, Telemat. Inform. 35 (5) (2018) 1277–1287, http://dx.doi.org/10.1016/j.tele.2018.02.009, URL http://www.sciencedirect.com/science/article/pii/S0736585317304677.

[10] L.K. Marett, J.F. George, Deception in the case of one sender and multiple receivers, Group Decis. Negot. 13 (1) (2004) 29–44, http://dx.doi.org/10.1023/B:GRUP.0000011943.73672.9b.

[11] D.B. Buller, J.K. Burgoon, Interpersonal deception theory, Commun. Theory 6 (3) (1996) 203–242, http://dx.doi.org/10.1111/j.1468-2885.1996.tb00127.x, URL http://eproxy2.lib.tsinghua.edu.cn:80/rwt/99/http/MS6C63DQNEYG86UH/10.1111/j.1468-2885.1996.tb00127.x.

[12] A. Bergholz, J.D. Beer, S. Glahn, M. Moens, G. Paaß, S. Strobel, New filtering approaches for phishing email, J. Comput. Secur. 18 (1) (2010) 7–35.

[13] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M.A. Blair, T. Pham, School of phish: A real-world evaluation of anti-phishing training, in: Proceedings of the 5th Symposium on Usable Privacy and Security, SOUPS '09, ACM, New York, NY, USA, 2009, pp. 3:1–3:12, http://dx.doi.org/10.1145/1572532.1572536.

[14] M. Bada, J.R.C. Nurse, Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs), Inf. Comput. Secur. 27 (3) (2019) 393–410.

[15] M.D. Workman, J.A. Luévanos, B. Mai, A study of cybersecurity education using a present-test-practice-assess model, IEEE Trans. Educ. 65 (1) (2021) 40–45.

[16] C.A. Dykman, C.K. Davis, Online education forum: Part two-teaching online versus teaching conventionally, J. Inf. Syst. Educ. 19 (2) (2008) 157.

[17] R. Fatima, A. Yasin, L. Liu, J. Wang, What should abeeha do? An activity for phishing awareness, in: 2022 IEEE 22nd International Conference on Software Quality, Reliability, and Security Companion, QRS-C, 2022, pp. 756–757, http://dx.doi.org/10.1109/QRS-C57518.2022.00120.

[18] R. Beuran, D. Tang, C. Pham, K.-i. Chinen, Y. Tan, Y. Shinoda, Integrated framework for hands-on cybersecurity training: CyTrONE, Comput. Secur. 78 (2018) 43–59.

[19] C. Vogeler, Game-based learning with OER in higher education: Development and evaluation of a serious game, in: European Conference on E-Learning, Academic Conferences International Limited, 2018, pp. 592–XX.

[20] I. Dunwell, P. Petridis, S. Arnab, A. Protopsaltis, M. Hendrix, S. de Freitas, Blended game-based learning environments: Extending a serious game into a learning content management system, in: 2011 Third International Conference on Intelligent Networking and Collaborative Systems, IEEE, 2011, pp. 830–835.

[21] M. Host'oveckỳ, M. Novák, Game-based learning: How to make math more attractive by using of serious game, in: Computer Science on-Line Conference, Springer, 2017, pp. 341–350.

[22] U. Güleç, M. Yilmaz, M.A. Gozcu, Bireylerin programlama yeteneklerini ve bilgi seviyelerini arttirmak amaciyla dusunulmus ciddi oyun tabanli ogrenme catisi - cengo(serious game-based learning framework to improve programming skills and knowledge levels of individuals - CENGO), in: Ç. Turhan, A. Coskunçay, A. Yazici, H. Oguztüzün (Eds.), Proceedings of the 11th Turkish National Software Engineering Symposium, Alanya, Turkey, October 18-20, 2017, in: CEUR Workshop Proceedings, vol. 1980, CEUR-WS.org, 2017, pp. 171–183, URL http://ceur-ws.org/Vol-1980/UYMS17_paper_8.pdf.

[23] M. Freese, Game-based learning: An approach for improving collaborative airport management, in: European Conference on Games Based Learning, Academic Conferences International Limited, 2016, p. 835.

[24] N. Micallef, N.A.G. Arachchilage, Changing users' security behaviour towards security questions: A game based learning approach, in: 2017 Military Communications and Information Systems Conference, MilCIS, IEEE, 2017, pp. 1–6.

[25] A. Yasin, L. Liu, T. Li, J. Wang, D. Zowghi, Design and preliminary evaluation of a cyber security requirements education game (SREG), Inf. Softw. Technol. 95 (2018) 179–200, http://dx.doi.org/10.1016/j.infsof.2017.12.002, URL https://www.sciencedirect.com/science/article/pii/S0950584917301921.

[26] M. Qian, K.R. Clark, Game-based learning and 21st century skills: A review of recent research, Comput. Hum. Behav. 63 (Suppl. C) (2016) 50–58, http://dx.doi.org/10.1016/j.chb.2016.05.023, URL http://www.sciencedirect.com/science/article/pii/S0747563216303491.

[27] C.-C. Chang, C. Liang, P.-N. Chou, G.-Y. Lin, Is game-based learning better in flow experience and various types of cognitive load than non-game-based learning? Perspective from multimedia and media richness, Comput. Hum. Behav. 71 (Suppl. C) (2017) 218–227, http://dx.doi.org/10.1016/j.chb.2017.01.031, URL http://www.sciencedirect.com/science/article/pii/S0747563217300377.

[28] S.S. Tseng, K.Y. Chen, T.J. Lee, J.F. Weng, Automatic content generation for anti-phishing education game, in: 2011 International Conference on Electrical and Control Engineering, 2011, pp. 6390–6394, http://dx.doi.org/10.1109/ICECENG.2011.6056921.

[29] N.A.G. Arachchilage, M. Cole, Design a mobile game for home computer users to prevent from phishing attacks, in: International Conference on Information Society, I-Society 2011, 2011, pp. 485–489.

[30] R. Zhao, S. John, S. Karas, C. Bussell, J. Roberts, D. Six, B. Gavett, C. Yue, Design and evaluation of the highly insidious extreme phishing attacks, Comput. Secur. 70 (2017) 634–647, http://dx.doi.org/10.1016/j.cose.2017.08.008, URL http://eproxy2.lib.tsinghua.edu.cn:80/rwt/33/http/P75YPLUUMNVXK5UDMWTGT6UFMN4C6Z5QNF/science/article/pii/S0167404817301633.

[31] A. Aleroud, L. Zhou, Phishing environments, techniques, and countermeasures: A survey, Comput. Secur. 68 (2017) 160–196, http://dx.doi.org/10.1016/j.cose.2017.04.006, URL http://www.sciencedirect.com/science/article/pii/S0167404817300810.

[32] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, E. Nunge, 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, SOUPS '07, ACM, New York, NY, USA, 2007, pp. 88–99, http://dx.doi.org/10.1145/1280680.1280692.

[33] M. Junger, L. Montoya, F.-J. Overink, Priming and warnings are not effective to prevent social engineering attacks, Comput. Hum. Behav. 66 (2017) 75–87, http://dx.doi.org/10.1016/j.chb.2016.09.012, URL http://www.sciencedirect.com/science/article/pii/S0747563216306392.

[34] J. Bullee, L. Montoya, M. Junger, P.H. Hartel, Spear phishing in organisations explained, Inf. Comput. Secur. 25 (5) (2017) 593–613, http://dx.doi.org/10.1108/ICS-03-2017-0009.

[35] K. Beckers, S. Pape, A serious game for eliciting social engineering security requirements, in: 24th IEEE International Requirements Engineering Conference, RE 2016, Beijing, China, September 12–16, 2016, IEEE, 2016, pp. 16–25, http://dx.doi.org/10.1109/RE.2016.39.

[36] C.C. Yang, S.S. Tseng, T.J. Lee, J.F. Weng, K. Chen, Building an anti-phishing game to enhance network security literacy learning, in: 2012 IEEE 12th International Conference on Advanced Learning Technologies, 2012, pp. 121–123, http://dx.doi.org/10.1109/ICALT.2012.174.

[37] M. H. A. Khan, S. Tanveer, M.A. Shah, MITRE att&ckTM based language for effective training in cyber range, in: Competitive Advantage in the Digital Economy, vol. 2022, CADE 2022, 2022, pp. 105–110, http://dx.doi.org/10.1049/icp.2022.2049.

[38] D. Alt, Assessing the benefits of gamification in mathematics for student gameful experience and gaming motivation, Comput. Educ. 200 (2023) 104806, http://dx.doi.org/10.1016/j.compedu.2023.104806, URL https://www.sciencedirect.com/science/article/pii/S0360131523000830.

[39] C.-M. Chen, L. Ming-Chaun, C.-P. Kuo, A game-based learning system based on octalysis gamification framework to promote employees' Japanese learning, Comput. Educ. 205 (2023) 104899, http://dx.doi.org/10.1016/j.compedu.2023.104899, URL https://www.sciencedirect.com/science/article/pii/S0360131523001768.

[40] R. Fatima, A. Yasin, L. Liu, J. Wang, How persuasive is a phishing email? A phishing game for phishing awareness, J. Comput. Secur. 27 (6) (2019) 581–612, http://dx.doi.org/10.3233/JCS-181253.

[41] J. Hamari, D.J. Shernoff, E. Rowe, B. Coller, J. Asbell-Clarke, T. Edwards, Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning, Comput. Hum. Behav. 54 (2016) 170–179, http://dx.doi.org/10.1016/j.chb.2015.07.045, URL https://www.sciencedirect.com/science/article/pii/S074756321530056X.

[42] N.L. Laakso, T.S. Korhonen, K.P.J. Hakkarainen, Developing students' digital competences through collaborative game design, Comput. Educ. 174 (2021) 104308, http://dx.doi.org/10.1016/j.compedu.2021.104308, URL https://www.sciencedirect.com/science/article/pii/S0360131521001858.

[43] G. Boström, J. Wäyrynen, M. Bodén, K. Beznosov, P. Kruchten, Extending XP practices to support security requirements engineering, in: Proceedings of the 2006 International Workshop on Software Engineering for Secure Systems, ACM, 2006, pp. 11–18.

[44] C. Haley, R. Laney, J. Moffett, B. Nuseibeh, Security requirements engineering: A framework for representation and analysis, IEEE Trans. Softw. Eng. 34 (1) (2008) 133–153.

[45] L. Nielsen, Personas - User Focused Design, in: Human-Computer Interaction Series, vol. 15, Springer, 2013, http://dx.doi.org/10.1007/978-1-4471-4084-9.

[46] W. Xiong, R. Lagerström, Threat modeling — A systematic literature review, Comput. Secur. 84 (2019) 53–69, http://dx.doi.org/10.1016/j.cose.2019.03.010.

[47] H. Liang, Y.L. Xue, et al., Understanding security behaviors in personal computer usage: A threat avoidance perspective, J. Assoc. Inf. Syst. 11 (7) (2010) 1.

[48] A. Yasin, L. Liu, T. Li, J. Wang, D. Zowghi, Design and preliminary evaluation of a cyber security requirements education game (SREG), Inf. Softw. Technol. 95 (2018) 179–200, http://dx.doi.org/10.1016/j.infsof.2017.12.002.

[49] C. Wohlin, P. Runeson, M. Höst, M.C. Ohlsson, B. Regnell, A. Wesslén, Experimentation in software engineering, in: Experimentation in Software Engineering, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 123–151.

[50] K. Petersen, C. Gencel, Worldviews, research methods, and their relationship to validity in empirical software engineering research, in: 2013 Joint Conference of the 23rd International Workshop on Software Measurement and the 8th International Conference on Software Process and Product Measurement, 2013, pp. 81–89, http://dx.doi.org/10.1109/IWSM-Mensura.2013.22.

[51] R. Fatima, A. Yasin, L. Liu, J. Wang, W. Afzal, Retrieving arxiv, SocArXiv, and SSRN metadata for initial review screening, Inf. Softw. Technol. 161 (2023) 107251, http://dx.doi.org/10.1016/j.infsof.2023.107251, URL https://www.sciencedirect.com/science/article/pii/S0950584923001052.

[52] I. Kirlappos, M.A. Sasse, Security education against phishing: A modest proposal for a major rethink, IEEE Secur. Priv. 10 (2) (2011) 24–32.

[53] N.A.G. Arachchilage, M. Cole, Design a mobile game for home computer users to prevent from "phishing attacks", in: International Conference on Information Society, I-Society 2011, IEEE, 2011, pp. 485–489.

[54] N.A.G. Arachchilage, S. Love, A game design framework for avoiding phishing attacks, Comput. Hum. Behav. 29 (3) (2013) 706–714.

[55] N.A.G. Arachchilage, S. Love, K. Beznosov, Phishing threat avoidance behaviour: An empirical investigation, Comput. Hum. Behav. 60 (2016) 185–197.

[56] M. Xenos, V. Maratou, I. Ntokas, C. Mettouris, G.A. Papadopoulos, Game-based learning using a 3D virtual world in computer engineering education, in: 2017 IEEE Global Engineering Education Conference, EDUCON, IEEE, 2017, pp. 1078–1083.

[57] G. Baral, N.A.G. Arachchilage, Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour, in: 2019 Cybersecurity and Cyberforensics Conference, CCC, IEEE, 2019, pp. 102–110.

[58] K. Beckers, S. Pape, A serious game for eliciting social engineering security requirements, in: 2016 IEEE 24th International Requirements Engineering Conference, RE, IEEE, 2016, pp. 16–25.

[59] M. Baslyman, S. Chiasson, "Smells phishy?": An educational game about online phishing scams, in: 2016 APWG Symposium on Electronic Crime Research, ECrime, IEEE, 2016, pp. 1–11.

[60] M.A. Khan, A. Merabet, S. Alkaabi, H.E. Sayed, Game-based learning platform to enhance cybersecurity education, Educ. Inf. Technol. (2022) 1–25.

[61] M. Hendrix, A. Al-Sherbaz, B. Victoria, Game based cyber security training: Are serious games suitable for cyber security training? Int. J. Serious Games 3 (1) (2016).

[62] B.D. Cone, C.E. Irvine, M.F. Thompson, T.D. Nguyen, A video game for cyber security training and awareness, Comput. Secur. 26 (1) (2007) 63–72.

[63] C.C. Fung, V. Khera, A. Depickere, P. Tantatsanawong, P. Boonbrahm, Raising information security awareness in digital ecosystem with games-a pilot study in Thailand, in: 2008 2nd IEEE International Conference on Digital Ecosystems and Technologies, IEEE, 2008, pp. 375–380.

[64] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, E. Nunge, 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, 2007, pp. 88–99.

[65] M. Silic, P.B. Lowry, Using design-science based gamification to improve organizational security training and compliance, J. Manage. Inf. Syst. 37 (1) (2020) 129–161.

[66] Z.A. Wen, Z. Lin, R. Chen, 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, 2019, pp. 1–12.

[67] S.-S. Tseng, K.-Y. Chen, T.-J. Lee, J.-F. Weng, Automatic content generation for anti-phishing education game, in: 2011 International Conference on Electrical and Control Engineering, IEEE, 2011, pp. 6390–6394.

[68] R. Roepke, U. Schroeder, The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education, in: CSEDU (2), 2019, pp. 58–66.

[69] P. Weanquoi, J. Johnson, J. Zhang, Using a game to improve phishing awareness, J. Cybersecur. Educ. Res. Pract. 2018 (2) (2018) 2.

[70] F. Giannakas, G. Kambourakis, S. Gritzalis, CyberAware: A mobile game-based app for cybersecurity education and awareness, in: 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL, IEEE, 2015, pp. 54–58.

[71] T. van Steen, J.R.A. Deeleman, Successful gamification of cybersecurity training, Cyberpsychology Behav. Soc. Netw. 24 (9) (2021) 593–598.

[72] R. Raman, A. Lal, K. Achuthan, Serious games based approach to cyber security concept learning: Indian context, in: 2014 International Conference on Green Computing Communication and Electrical Engineering, ICGCCEE, IEEE, 2014, pp. 1–5.

[73] D. Ki-Aries, S. Faily, Persona-centred information security awareness, Comput. Secur. 70 (2017) 663–674, http://dx.doi.org/10.1016/j.cose.2017.08.001, URL http://www.sciencedirect.com/science/article/pii/S0167404817301566.

[74] R. Heartfield, G. Loukas, D. Gan, You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks, IEEE Access 4 (2016) 6910–6928, http://dx.doi.org/10.1109/ACCESS.2016.2616285.