

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

CyQured: Design, Development, and Empirical Evaluation of a Tabletop Game for Personal Cybersecurity Education

Utsho Das and Argha Pratim Saha, *Shahjalal University of Science and Technology;* Md Sadek Ferdous, *BRAC University;* Md Masum, *Shahjalal University of Science and Technology;* Farida Chowdhury, *BRAC University*

https://www.usenix.org/conference/soups2026/presentation/das

This paper is included in the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security is sponsored by USENIX.

CyQured: Design, Development, and Empirical Evaluation of a Tabletop Game for Personal Cybersecurity Education

Utsho Das[†]
Shahjalal University of Science and Technology

Argha Pratim Saha[†]
Shahjalal University of Science and Technology

Md Sadek Ferdous
BRAC University

Md Masum
Shahjalal University of Science and Technology

Farida Chowdhury
BRAC University

Abstract

As reliance on connected home devices grows, human behavior remains a critical vulnerability that is often inadequately addressed by traditional, overly technical educational methods. To bridge this gap, we introduce CyQured, a tabletop board game that models a digital home ecosystem of 16 devices, enabling players to simulate 16 STRIDE-inspired attacks and defenses through structured gameplay. We evaluated CyQured with 50 university students, 13 with prior cybersecurity coursework and 37 without, including 14 with limited tabletop gaming experience. The evaluation was conducted using a mixed-methods approach that included knowledge assessments and user-centered evaluations, including the SUS, TAM, and NASA-TLX scales. While novices without domain or tabletop gaming experience reported higher cognitive load and borderline usability scores, knowledge gains were observed across all cohorts. Thematic analysis revealed that novices encountered initial accessibility barriers and elevated cognitive load due to unfamiliar cybersecurity terminology and gameplay mechanics; however, high engagement and social interaction motivated them to persist. Collectively, these findings suggest that game-based simulations can effectively engage diverse learners in understanding home cybersecurity, while also underscoring the need for accessible game design to support players without prior domain knowledge or tabletop gaming experience.

[†]These authors contributed equally to this work.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

1 Introduction

People today are increasingly surrounded by connected technologies, from smart home appliances and personal devices to always-on cloud services. As reliance on these technologies grows, the human element has become a major source of vulnerability. Even when organizations deploy advanced technical defenses, attacks frequently succeed by exploiting human behavior and decision-making. Systematic data breach research showed that human error is one of the main methods attackers use to cause data breaches [46]. Unlike enterprise environments, home users generally lack access to dedicated security teams, institutional policies, or advanced defensive infrastructure. University students are a particularly relevant population for studying this problem, as they actively manage personal devices and online accounts while exhibiting widely varying levels of cybersecurity knowledge.

Addressing this human factor requires effective education. Traditional cybersecurity awareness programs often rely on passive learning approaches, such as lectures or compliance-driven modules, that focus on information delivery rather than skill development [21, 53]. Evidence suggests such approaches yield limited improvements in real-world security behavior [31]. Learners often struggle to translate abstract advice, such as using strong passwords or recognizing suspicious behavior, into practical decision-making skills [36], especially when they come from non-technical backgrounds.

Serious games and gamification have emerged as promising solutions by providing interactive, experiential learning environments [17, 26]. Security games can teach targeted skills, allowing learners to practice decision-making in simulated environments [28, 41]. However, most tools focus on enterprise contexts, rely on expert facilitation, or target isolated threat vectors rather than the broader home ecosystem.

Research in usable security also shows that non-expert users rely on incomplete or inaccurate mental models when reasoning about security and privacy. Users often misunderstand how their data flows online and how everyday technologies interact, leading to gaps between perceived and actual

risks [13, 32, 35, 55]. While prior security games have improved specific skills, such as phishing detection [7, 39, 48], few interventions support holistic reasoning about interconnected home environments or enable self-directed learning without expert facilitation.

To address these gaps, we introduce CyQured, a tabletop board-and-card game for personal cybersecurity education at home. CyQured models a realistic digital home ecosystem and operationalizes threat categories derived from STRIDE, a widely used threat-modeling framework covering Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [49] into intuitive, facilitator-independent gameplay. Players explore threats, defenses, and trade-offs through collaborative problem-solving. The game specifically targets university students with diverse technical backgrounds, providing an accessible and heterogeneous population for early-stage evaluation.

Our Research Questions are:

RQ1: How effective is CyQured in improving cybersecurity knowledge among university students from different technical backgrounds?

RQ2: How do usability, cognitive load, and technology acceptance of CyQured differ between students with and without prior cybersecurity backgrounds?

To answer these questions, this paper investigates how a tabletop cybersecurity game can support learning and engagement among students with varying technical expertise. We evaluate knowledge gain, usability, cognitive load, and technology acceptance using a mixed-method study.

This paper makes three key contributions:

i. **A home-context tabletop security learning artifact.** CyQured models a connected home ecosystem and maps STRIDE-inspired threats into accessible, facilitator-independent gameplay.

ii. **Empirical evidence of learning and usability trade-offs.** A mixed-methods study with 50 university students demonstrates measurable knowledge gains while revealing usability and cognitive-load challenges for non-expert players.

iii. **Design insights for low-barrier security games.** Our findings highlight how terminology, onboarding, and prior tabletop familiarity affect engagement, extending prior research on mental models and security training.

The remainder of the paper is organized as follows: Section 2 reviews related work, identifies research gaps, and situates CyQured among prior tools. Section 3 and Section 4 explain the game's design and gameplay mechanics. Section 5 presents the evaluation results, Section 6 discusses implications, Section 7 presents limitations, and Section 8 concludes with future directions.

2 Related Work

Security gamification has become a rich research field. Nevertheless, a more detailed examination reveals a notable discrepancy between the tools that are available at present and the requirements of the common users. Numerous games have been effective at imparting specific skills [17, 26, 42], the majority of which were created in enterprise contexts with expert facilitation or in response to a specific security topic. To explain the gap in CyQured records, we analyze the literature regarding these common restrictions.

A major trend in cybersecurity games is their strong organizational focus. Early and influential systems such as CyberCIEGE [33] and Riskio [28] place players in the role of IT managers making budget and policy decisions. Other tools, including Play2Prepare [24] and Protection Poker [56], are built for incident response teams and software development environments. These approaches assume access to security teams, organizational policies, and institutional resources. Such assumptions rarely hold for home users, making it difficult to translate lessons into everyday personal security practices.

The usable security research describes the reasons why this mismatch is significant. There are also informal, incomplete folk models of cybersecurity that non-expert users tend to rely on, based on their own perceptions of cybersecurity safety and protection issues in this field of social life and activity [55]. Such mental models influence decision-making and risk perception online. It has been repeatedly demonstrated that users misinterpret data flows and privacy threats, as users need to be able to create tools that are compatible with a variety of mental models and cognitive capacities [13, 32, 35]. Instructional aids must instead help in learning relationships among various components of the home ecosystem, rather than separate competencies.

Despite this need, many user-focused games remain highly specialized. Tools such as Anti-Phishing Phil [48], PhishGuru [39], and Persuaded [1] effectively teach phishing detection, while GAP focuses on password strength [54]. Other games concentrate on cryptography [23] or smartphone permissions [47]. These tools are effective for micro-learning but do not help players develop a holistic understanding of the connected home environment, in which devices, networks, and physical access interact.

Another barrier is scalability. Several tabletop tools, including Riskio, Security Cards, and Elevation of Privilege [49], rely on expert facilitators to guide discussion and interpret outcomes. While effective in workshops, facilitator-driven experiences are challenging to deploy in everyday settings. This requirement can exclude the very audience most vulnerable to cyber threats, i.e., novice users learning independently at home.

Lastly, most security games are focused on offensive interactions. Games like Hacknet [20], Control-Alt-Hack [16], and d0x3d! [22] advertise their game by playing on the excitement

Table 1: Comparison of gamified cybersecurity tools illustrating the research gap.

Tool	Medium	Audience	Context	Goal	Facilitator
CyberCIEGE [33]	Digital	Expert	Enterprise	IA Risk Mgmt	No
Anti-Phishing Phil [48]	Digital	Novice	Personal	Single Threat	No
PhishGuru [39]	Digital	Novice	Personal	Single Threat	No
GAP [54]	Digital	Novice	Personal	Single Threat	No
Riskio [28]	Tabletop	Employees	Enterprise	Org. Awareness	Yes
EoP [49]	Tabletop	Developers	Software	Threat Model	Yes*
Control-Alt-Hack [16]	Tabletop	Students	Audit	Offense	No
Cyber Threat Defender [9]	Tabletop	K-12	Foundational	Networks	No
Play2Prepare [24]	Tabletop	IT Staff	ICS	Incident Resp.	Yes
Cyber Suraksha [47]	Tabletop	Novice	Personal	Single Threat	No
Protection Poker [56]	Tabletop	Developers	Software	Risk Assess.	Yes*
SREG [57]	Tabletop	Students	Software	Sec. Req.	No
Crypto Go [23]	Tabletop	Mixed	Foundational	Single Threat	No
CyQured (Ours)	Tabletop	Novice	Home	Holistic Defense	No

**Requires an internal team moderator (e.g., Scrum Master) rather than an external instructor.*

of being a hacker. They can be found to be interesting, but can also focus on attack gameplay rather than defensive thinking; the chance to train defensive thought is minimal.

Table 1 highlights how existing tools map to audience, context, and facilitation requirements. Taken together, the literature reveals a clear gap. Few tools are simultaneously (1) centered on the home context, (2) holistic in scope, (3) playable without expert facilitation, and (4) balanced between attack and defense. Existing interventions are either too specialized (e.g., Cyber Threat Defender [9]) or too advanced for novice audiences (e.g., SREG [57]).

CyQured was designed to address this gap. By adapting simplified STRIDE-inspired threat categories into intuitive tabletop mechanics, the game provides a self-contained simulation of the personal cybersecurity ecosystem for novice users without requiring enterprise knowledge or expert guidance.

3 CyQured: Design and Implementation

The game design process followed a clear set of goals and established design principles for serious games to ensure the intended learning outcomes for the target audiences. It also required a well-defined rationale for selecting the game genre and for developing the game's structure and components.

3.1 Design Goals

The main target is to create a learning environment that helps players better understand personal cybersecurity threats and the basic steps needed to defend against them. This goal is supported by three key objectives:

i. **Awareness of personal cybersecurity risks.** To help players identify risks and choose suitable responses, the game exposes players to common real-world attack scenarios and corresponding protective strategies following security standards.

ii. **Security reasoning and trade-off thinking.** By alternating between attacker and defender roles, players experience how vulnerabilities are exploited and how defenses mitigate risk.

iii. **Self-directed and accessible learning.** The game is designed to be playable without expert supervision and can be played in classrooms or informal settings by players from diverse technical backgrounds.

3.2 Target Audience

CyQured is targeted at undergraduate students with diverse technical backgrounds. These students are often exposed to real-world security threats but seldom get formal training on how to detect and deal with them [25]. Our research and validation were conducted exclusively on undergraduate students, who are the main target audience for whom the learning outcomes of the game have been validated.

3.3 Facilitator Independence

The game has been designed to be playable without expert facilitation. All rules and gameplay are self-contained to facilitate independent learning. This design approach allows players to play with friends or classmates wherever they choose and does not require them to rely on someone to serve as a facilitator. During the evaluation, a member of the research team was present solely to clarify gameplay rules upon request and monitor the time, without providing any cybersecurity instruction or guidance.

3.4 Design Principles

To produce a game that educates on cybersecurity on a large scale, the process of game design in accordance with the learning principles and motivation theories was adhered to, as a form of effective learning.

Constructivist Learning [5, 34]: Construction of knowledge occurs through the interactions of players with real-life situations and not through instructions. The game will promote active decision-making and reflection and help players move between the roles of attacker and defender.

Self-Determination Theory [15, 45]: Self-determination theory is a theory that assists players in feeling competent, related, and autonomous as they make strategic decisions, feel their advancement through completed defenses, and learn in a social gameplay environment.

Cognitive Load Theory [50]: The game is designed to balance a challenge with usability by presenting security concepts in structured, simplified forms suitable for novice learners.

These principles guided the design of the layout, card mechanics, and the structure of the turn to ensure that learning about cybersecurity at home is immersive, collaborative, and accessible to players from diverse technical backgrounds.

3.5 Motivation Behind a Role-playing Tabletop Card-and-Board Game

CyQured is designed as a tabletop card-and-board game to prioritize social learning without requiring technical setup [29,

37]. The game mechanics were inspired by Monopoly because it is highly familiar and has pedagogical value [38]. Monopoly is widely known in Bangladesh, with 72% of our participants having played it previously. This provides a cognitive shortcut that lets players direct mental effort toward cybersecurity concepts rather than unfamiliar game mechanics [8, 19]. Alternative formats (cooperative games, trivia decks) were considered but rejected: cooperative play lacks the adversarial tension that simulates real attack-defense decisions, and unfamiliar game structures would compound the cognitive burden of learning new security content simultaneously. Structurally, resource ownership under competitive pressure and consequence-based decision-making map naturally onto cybersecurity reasoning, transforming abstract security principles into practical, memorable [30, 51].

3.6 Game Components

Components of CyQured are divided into two major categories: game cards and the game board. The game also includes a six-sided die, which must be rolled to move along the cells, and token markers are used to indicate each player's current location. These components create a structured environment in which players repeatedly encounter cybersecurity threats, defenses, and trade-offs in decision-making during gameplay.

3.6.1 The Game Board: Architecture and Pedagogical Significance:

The CyQured board (Figure 1) contains a cyclic track of 28 cells inspired by the classic Monopoly game design. The cyclic layout ensures repeated exposure to cybersecurity concepts as players progress through multiple rounds. The 16 devices were selected based on widespread prevalence, inherent security weaknesses, and the high-value data they handle [2,18,43]. These were picked by looking at how often they are used, whether they have had security flaws before, how many outside threats they face, and what tasks they handle inside a local network. Considering the higher vulnerability and the impact of Routers and NAS devices (single-failed-defense: compromising a gateway has a significantly larger blast radius), they were presented as special cells [2, 52]. The Color-Group Immunity mechanic is intentionally borrowed from Monopoly to drive strategic goals and keep players motivated through the "productive struggle." The other special cells introduce structured variation and unpredictability during play (e.g., chance events, scenario challenges, and temporary disruptions). These elements ensure that the game includes both strategic planning and unexpected events to simulate the uncertainty of real-world cybersecurity risk.

We adjusted asset positions using Monte Carlo simulation to handle unpredictability in intricate setups [40]. Instead of fixed trials, we generated around 300 gameplay runs to spot squares most frequently landed on right after GO. Where players ended up most often got linked to essential parts like

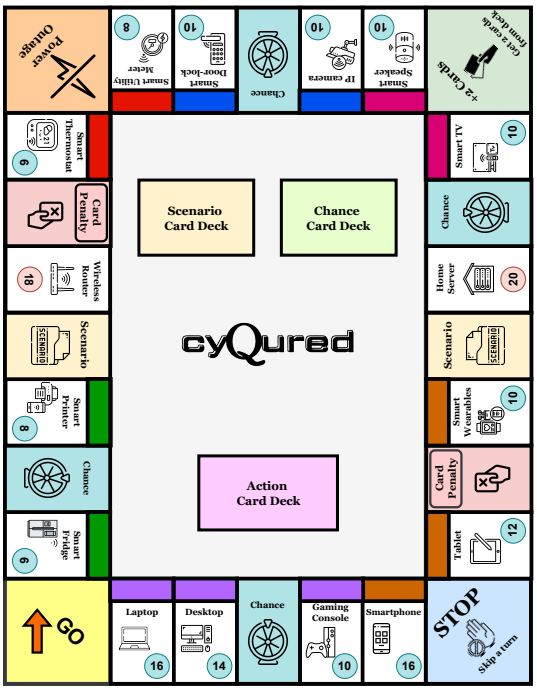


Figure 1: CyQured Game Board

network hardware units. By doing so, learners come across key cyber topics more regularly during play.

3.6.2 The Game Card Elements:

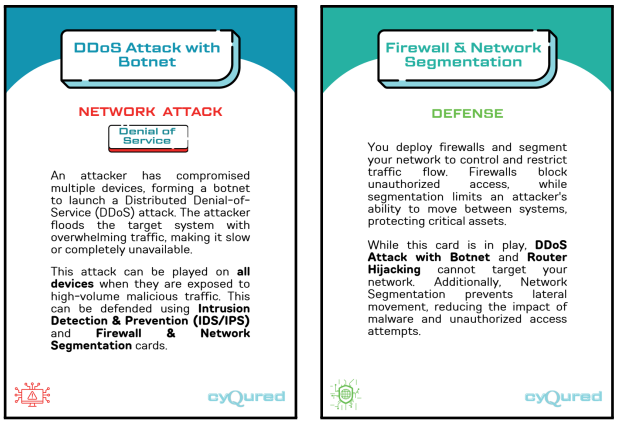
The card system forms the pedagogical core of CyQured. It links threats with defenses and supports scenario-based learning. The game includes four types of cards:

Action Cards: This deck contains attack and defense cards that represent common cyber threats and protective measures. They share the same back design, so players cannot identify the type of card while drawing from the deck. This also conceals opponents' holdings for maintaining uncertainty and strategic tension and making gameplay more engaging.

There are 16 different types of cards for each type: attack and defense. Attack cards describe realistic threats mapped to STRIDE categories and suggest targets and possible defenses as well (Figure 2a). Defense cards follow a layout similar to the attack cards (Figure 2b). They represent practical mitigation strategies and have a list of suggested attacks that can be defended with the card. Continuous use of these cards creates repeated exposure to attack–defense relationships and helps learning through decision-making.

Chance Cards: Chance cards (Figure 3a) add some element of unpredictability to the game. Though not strategy-driven, they provide short narrative contexts that help reinforce security awareness with scenarios.

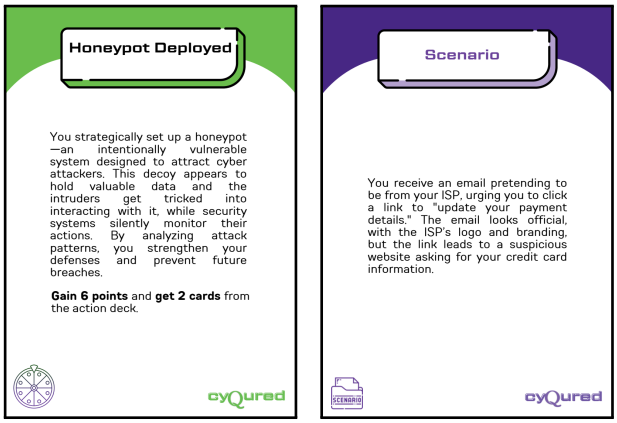
Scenario Cards: Scenario cards (Figure 3b) present open-



(a) Attack Card (b) Defense Card

Figure 2: Attack and Defense Card Layout

ended cybersecurity incidents. These require players to identify the relevant STRIDE threat category. These also encourage recall, interpretation, and discussion.



(a) Chance Card (b) Scenario Card

Figure 3: Chance and Scenario Card Layout

Asset Cards: Asset cards have an asset title and a brief description about that asset. It acts as a token of ownership for a particular asset.

The card system was refined through several rounds of pilot testing. Early versions avoided having attack-defense suggestions and limited the labels, target suggestions, and suggested attack-defense listing to encourage players to follow an open-ended exploration. However, this led the novices to confuse risks, hesitate in decisions, or lean on the game master for help, and resulted in a significantly high cognitive load even for some players from computer science backgrounds. Based on this feedback, the cards were redesigned with clearer titles, short descriptions, asset targets, suggested defenses, and color coding to similar kinds of attacks. Future iterations will add icon-based redundancy to support color-blind players. Later trials revealed better precision, reduced confusion, along with increased independence and assurance during gameplay. These changes were aimed at keeping the game challenging yet manageable. All the cards used in this game are presented in Figure B.1, Figure B.2, and Figure B.3 in the Appendix.

4 Gameplay Mechanics for CyQured

CyQured simplifies cybersecurity concepts through an interactive game where players plan, attack, defend, and react to events. The following subsections describe the game's core mechanics, including turn structures and movement, asset management, the attack-defense resolution system, and other special features. This also includes gameplay walkthroughs to explain the game flow.

4.1 Initial Setup and Turn Flow

The 68-action card deck consists of attack and defense cards, each with 2 copies of 17 types, including 1 ultimate card. Players start with 8 cards each, and the rest are placed on the board along with 30 chance and 20 scenario cards. Each player will also get 50 credit points and will start from the *GO* cell. Players take sequential turns. On each turn, a player rolls a six-sided regular die and moves along the game board, similar to Monopoly.

i. Roll the die and move the corresponding number of cells.

ii. Execute the action of the cell (acquire an asset, engage in attack-defense, draw a chance card, or solve a scenario).

iii. End turn; next player continues.

4.2 Resource Ownership and Attack-Defense Mechanism

Players can claim unowned assets by paying their designated value and acquiring the corresponding asset card. Ownership grants points, while landing on an occupied asset presents a strategic choice: pay partial points or launch an attack using an appropriate attack card.

During an attack, the attacker attempts to compromise the asset, while the defender responds using a defense card. A successful defense prevents a point loss, whereas a failed defense allows the attacker to gain points or, in the case of repeated failures, claim the asset. Special assets (e.g., Wireless Router, Home Server) allow ownership transfer after a single failed defense. This mechanic reflects the outsized impact of compromising network gateways: a single router breach can enable lateral movement to other devices.

Owning all assets of a color group provides immunity against attacks and increases point gains, encouraging strategic asset grouping. While not a direct security analog, this Monopoly-derived mechanic provides strategic goals that sustain engagement through the "productive struggle" of learning

complex concepts [19]. However, accumulating assets without adequate protection introduces risk, as poor defense can lead to point loss or elimination.

This attacker–defender exchange encourages players to apply cybersecurity knowledge, evaluate trade-offs, and experience consequences of weak defenses, simulating real-world security decision-making in a controlled environment. Crucially, the game mechanics require players to read the card text aloud and justify their chosen attack or defense to the other players. This forced reading and verbal justification embed active literacy as a pedagogical mechanism, ensuring players engage meaningfully with the security content rather than playing by rote.

4.3 Special Cell Mechanics

Special cells introduce variation and learning opportunities beyond standard asset interactions. The *GO* cell grants points and action cards upon lap completion, rewarding progress. *Chance* cells simulate unexpected cybersecurity events, teaching risk assessment under uncertainty. *Scenario* cells require players to identify the STRIDE threat type from a narrative prompt; correct answers earn points with no penalty for errors, reducing frustration. The *STOP* cell skips a turn (representing forced updates or downtime), the *Power Outage* cell temporarily deactivates all assets, and *Card Penalty/Bonus* cells add randomness by discarding or awarding action cards.

4.4 Role of a Game Master

CyQured was designed to be complete without a facilitator; all players were allowed to follow the rules and interact with the mechanics independently. However, the game allows for an optional Game Master role. A Game Master can be a participant or an external domain expert who can provide additional pedagogical value, such as explaining the details of attacks and defenses during gameplay.

4.5 Game Completion Option

CyQured supports three end conditions: *Elimination* (players with no points or assets are eliminated; last player wins), *Timed* (fixed duration; the highest combined score wins), and *Target Score* (first to reach an agreed total wins). Groups can select the mode to match their available time and desired competitiveness.

4.6 Learning and Engagement Through Game Mechanics

CyQured's mechanics are designed to implement constructivist and experiential learning principles. By alternating roles between attacker and defender, learners gain insight into both offensive and defensive strategies. Strategic choices like deciding which assets to attack or defend encourage players to apply cybersecurity knowledge in realistic contexts. Resource management through cards and points provides cognitive scaffolding. This helps players evaluate trade-offs and consequences of their decisions. Meanwhile, collaborative discussion during decision-making fosters peer learning, debate, and reflection.

Randomization via dice rolls and chance cards prevents rote gameplay and simulates real-world unpredictability. Progressive complexity across rounds maintains engagement while avoiding cognitive overload. An optional Game Master can clarify rules and guide discussion without providing direct answers, preserving learner autonomy.

5 Game Evaluation

To assess the effectiveness of CyQured in terms of knowledge acquisition (RQ1) and usability (RQ2), we conducted a study with university students. Its different aspects are discussed below.

5.1 Study Design

An experimental, pre-/post-test mixed-methods design was used for this study. The independent variable was participants' technical background (CS vs. non-CS). The dependent variables were knowledge acquisition and user experience indexes. The game features were also pilot-tested to reflect the alignment with the learning objectives. We followed a structured workflow for the experiment. The structure is:

i. **Initial Phase:** Participants first gave informed consent and demographic information. They then completed a demographic questionnaire and a 10-item pre-test on cybersecurity knowledge to assess baseline knowledge. The 10-item pre-/post-tests were newly developed for this study, aligned with the 16 attack-defense pairs in CyQured. Pre-test items assessed attack recognition; post-test items assessed corresponding defensive reasoning. This asymmetric pairing was intentional to measure knowledge transfer from threat identification to mitigation strategy selection.

ii. **Game Session:** Participants were split into small groups of four to five students and played the game for one hour or so. A rulebook and a manual with all attacks and defenses used in the game were given to ensure that the game went smoothly, and instructions were the same every time between groups.

iii. **Post-Test, Surveys, and Interview:** After playing the game, a knowledge post-test that consisted of 10 items and a usability survey was performed on the participants. All responses were anonymized by using unique codes associated with players to match pre-test to post-test and survey data. In addition, participants who had not completed any security course participated in semi-structured interviews with four open-ended questions to understand their perception of the game and their experience of learning.

To guard against the test-retest confound inherent in the pre-/post-design, a supplemental baseline study was conducted. Twenty participants of similar demographics and NC-comparable composition completed both the pre- and post-test at a 60-minute interval with no gameplay intervention, allowing direct comparison of score changes attributable to game exposure versus re-exposure to the test format (see Section 5.4 for results).

5.2 Ethics Statement

This study was approved by the Institutional Review Board (IRB) before data collection. Participation was voluntary, and recruitment was done via a Google Form sent to students in a number of different departments where interested students registered for the study. Before engaging in the activities, participants were informed of the purpose of the study, procedures to be employed, and rights of the participants, and informed consent was obtained. Participants were strongly advised that they could withdraw from the study at any time without penalty. No participants were recruited from courses taught by the authors. All students were explicitly informed that participation or non-participation would not affect their academic standing. To ensure strict confidentiality, each participant was given a unique two-digit number upon entry into the study. All materials collected, such as survey responses and audio recordings from the interview phase, were anonymized immediately and linked to these two identifiers only. Furthermore, all data handling, storage, and analysis procedures were strictly adhered to established institutional ethical guidelines to protect participant privacy. All the participants were given a small monetary compensation for their time.

5.3 Study Participants and Sampling

The evaluation was conducted at a renowned university in Bangladesh. Fifty undergraduate students were recruited via convenience sampling because participants were readily accessible on campus. Participants were assigned to one of two primary groups based on prior cybersecurity coursework: 13 students in the Security Coursework (SC) group and 37 in the No Coursework (NC) group. To examine the impact of tabletop gaming literacy, the NC group was further subdivided into two secondary cohorts based on Monopoly familiarity: NC-M (with Monopoly experience, $n = 23$) and NC-NM (without Monopoly experience, $n = 14$). This made direct comparisons of board game literacy between groups infeasible.

Table 2 summarizes participant demographics. Though convenience sampling limits generalizability beyond the university population, the sample provides sufficient diversity in technical backgrounds and gaming experience to evaluate usability, cognitive load, and knowledge gain across subgroups.

Table 2: Participant Demographics ($N = 50$).

Demographic	**SC Group** ($n = 13$)	**NC Group** ($n = 37$)	**Total** ($N = 50$)
Gender			
Male	10 (77%)	28 (76%)	38 (76%)
Female	3 (23%)	9 (24%)	12 (24%)
Monopoly Experience			
Yes	13 (100%)	23 (62%)[a]	36 (72%)
No	0 (0%)	14 (38%)[b]	14 (28%)
Age (years)			
Mean±SD	23.6 ± 1.0	22.0 ± 1.4	22.4 ± 1.5

[a] Designated as the **NC-M** subgroup.

[b] Designated as the **NC-NM** subgroup.

5.4 Evaluation Instruments

A mixed-method approach was followed for the evaluation of the game's effectiveness. Data triangulated from multiple complementary instruments helped to measure objective learning outcomes, perceived usability, cognitive load, technological acceptance, and participants' qualitative reflections.

i. **Knowledge Acquisition (Pre–Post Test).**

Learning gain was measured using a 10-item multiple-choice test covering the cyber threats and defenses represented in the game (the full instrument can be found in Appendix A.1). A paired-samples t-test compared pre- and post-test scores for the full sample and for the different security background groups separately. Learning magnitude was estimated using Cohen's d [12]. To address potential test-retest confounds in the pre-/post-test design, a supplemental control study ($N = 20$) was conducted with demographically similar participants drawn from the NC cohort who did not play the game. These participants completed both the pre- and post-test at a 60-minute interval with no gameplay intervention. No significant score change was observed ($M_{\text{pre}} = 4.05$, $M_{\text{post}} = 3.85$, $\Delta M = -0.20$, SD $= 1.61$; $t(19) = 0.56$, $p = 0.58$, $d = 0.12$, 95% CI $[-0.95, 0.55]$) to confirm that the gains observed in the main study reflect game-induced learning rather than item difficulty differences or repeated exposure effects (see Table 3).

ii. **System Usability Scale (SUS) and NASA Task Load Index (NASA-TLX).** Perceived usability was measured using the 10-item System Usability Scale (SUS) [4]. Cognitive workload was measured using the NASA-TLX, which captures mental demand, physical demand, temporal demand, performance, effort, and frustration [27]. Responses to the SUS questions were recorded on a 5-point Likert scale, while TLX records used 10 points to record input.

iii. **Technology Acceptance.** Acceptance of the game was assessed using a 17-item questionnaire derived from the

Technology Acceptance Model (TAM; measuring Perceived Ease of Use [PEOU], Perceived Usefulness [PU], Intention to Use [ITU], and Attitude Toward Technology [ATT]) [10, 14].

For the TAM question presented in Appendix A.2, user input was recorded on a 5-point Likert scale. Cronbach's α indicated acceptable internal consistency for PU ($\alpha = .84$), ITU ($\alpha = .83$), and ATT ($\alpha = .69$). The lower PEOU reliability ($\alpha = .63$) reflects genuine between-group variability rather than construct invalidity: within-group standard deviations for PEOU were low (SC: $SD = .21$; NC-M: $SD = .18$; NC-NM: $SD = .16$), confirming that participants within each cohort responded consistently. The reduced overall α arises from the polarized usability experiences of gaming-literate versus novice players, a substantive finding rather than a measurement flaw (see Section 5.5.2).

iv. **Semi-Structured Interviews and Thematic Analysis.** To contextualize the quantitative findings, semi-structured interviews guided by four open-ended questions were conducted with a subset of participants after gameplay. Interviews lasted approximately 10 minutes and were audio-recorded and transcribed. Data were analyzed using inductive thematic analysis [11]. To ensure rigor, two researchers independently coded the data and met to discuss and refine the themes.

The pre- and post-test questionnaires were used to explore the research question RQ1–knowledge gain through the game, and the other instruments were used to answer RQ2–the usability of the game, and also to find how impactful it was across participant groups. Statistical significance was determined using a threshold of $p < .05$.

5.5 Result Analysis

This section describes the quantitative and qualitative findings of our evaluation. We structure the analysis around the two main research questions: the assessment of knowledge acquisition (RQ1) and the study of usability barriers (RQ2). Data were analyzed using parametric methods. Although self-reported usability metrics exhibited the expected negative skew, we used t-tests due to their established robustness to non-normality in bounded scales [3], applying Welch's correction for independent subgroup comparisons to account for unequal variances.

5.5.1 RQ1: Effectiveness in Knowledge Acquisition

To assess pedagogical efficacy, we conducted a 10-item knowledge test before and after the game session. Participants in the study were 50 students: 13 had Security Coursework (SC) and 37 had No Coursework (NC).

Pooled data showed a statistically significant improvement in test scores after intervention in the entire sample. Post-test scores were higher than pre-test baselines in all cases, visualized in Figure 4. Disaggregation by cohort shows that learning gains were made regardless of the previous technical background:

- **Security Coursework (SC, $n = 13$):** Despite the higher baseline knowledge, this group had a large mean score increase of $\Delta M = 3.38$ ($SD = 1.80$, 95% CI $[2.40, 4.36]$). The effect size was large ($d = 1.88$), and the level of significance was high ($p < .001$).
- **No Coursework (NC, $n = 37$):** The target audience of home users showed a mean increase of $\Delta M = 1.95$ ($SD = 1.20$, 95% CI $[1.56, 2.34]$). The effect size was also large ($d = 1.62$) and statistically significant ($p < .001$).

Importantly, learning gains were not equivalent between groups. An independent Welch's t-test confirmed that the SC group's gain was significantly larger than the NC group's ($\Delta M_{SC} = 3.38$ vs. $\Delta M_{NC} = 1.95$; $t(16.62) = 2.87$, $p = .01$, $d = 1.08$, 95% CI $[.37, 2.49]$), suggesting that prior domain vocabulary accelerated learning for those with security coursework. To account for non-independence arising from group play (participants seated in groups of 4-5), a Linear Mixed-Effects Model (LMM) with Game Group as a random intercept confirmed a significant overall learning effect ($\beta = 2.32$, $p < .001$, group variance $= 1.90$), indicating that gains occurred robustly across different table environments.

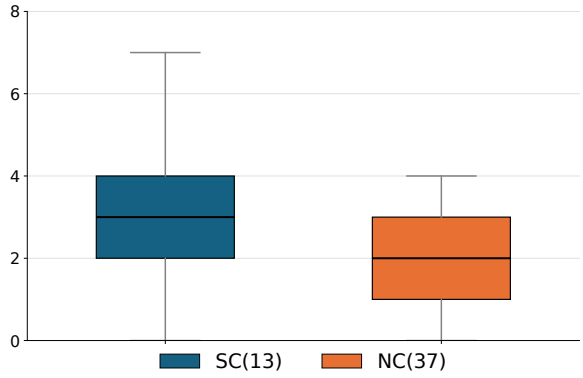


Figure 4: Learning gain distributions (ΔM) for the SC ($n = 13$, blue) and NC ($n = 37$, orange) groups, displayed as box plots. The scale reflects individual point improvements (post-test minus pre-test score out of 10). Both cohorts achieved statistically significant knowledge acquisition ($p < .001$), with the SC group exhibiting a higher average gain ($\Delta M_{SC} = 3.38$ vs. $\Delta M_{NC} = 1.95$).

To investigate whether prior board-game experience affected learning, the NC group was split based on familiarity with Monopoly-style games. NC-M includes participants who

had played such games before, while NC-NM includes those without prior experience. Learning gains were similar across both subgroups ($d = 1.55$ for NC-M, $d = 1.69$ for NC-NM; $t(35) = .07, p = .95$), suggesting that prior familiarity with board-game mechanics did not significantly influence knowledge acquisition.

Table 3: Learning Gain Statistics by Group.

Group	ΔM	SD	d	95% CI	p
SC ($n = 13$)	3.38	1.80	1.88	[2.40, 4.36]	$< .001$
NC ($n = 37$)	1.95	1.20	1.62	[1.56, 2.34]	$< .001$
NC-M ($n = 23$)	1.96	1.26	1.55	[1.41, 2.50]	$< .001$
NC-NM ($n = 14$)	1.93	1.14	1.69	[1.26, 2.58]	$< .001$
All Game ($n = 50$)	2.32	1.46	1.58	[1.90, 2.74]	$< .001$
Control ($n = 20$)	-.20	1.61	.12	[-.95,.55]	.58

5.5.2 RQ2: Usability & Gaming Literacy

Whilst RQ1 demonstrated consistent knowledge gains across cohorts, RQ2 examined accessibility barriers through the System Usability Scale (SUS) [4], the NASA-TLX [27], and the Technology Acceptance Model (TAM) [14].

The Technical Divide (SC vs. NC) We found a difference in perceived usability between technical and non-technical participants (illustrated in Figure 5):

- **SC Group ($n = 13$):** Reported a mean SUS score of 80.6 ($SD = 10.6$, 95% CI $[74.8, 86.4]$), which puts the game in the "Good" to "Excellent" range.
- **NC Group ($n = 37$):** Mean SUS score was reduced to 66.3 ($SD = 14.9$, 95% CI $[61.5, 71.1]$), which is categorized as "Borderline" usability.

This difference in perceived usability between the SC and NC groups was statistically significant ($t(29.74) = 3.73$, $p = .001$, $d = 1.02$), indicating that prior cybersecurity coursework was associated with substantially better perceived usability.

NASA-TLX results explain this gap. From Figure 6, the NC group showed greater Mental Demand and Effort and frustration. However, both groups reported high Performance, implying that the difficulty was seen as a challenging task.

Impact of Gaming Literacy To separate the impact of game mechanics, we divided the NC group into two groups, one with Monopoly experience (NC-M, $n = 23$) and the other without experience (NC-NM, $n = 14$). As illustrated in Figure 7, gaming literacy appears to play a considerable role in perceived usability:

- **NC-M:** Significantly higher ($M = 73.7$, $SD = 12.0$, 95%$CI[68.8, 78.6]$) usability rated, approaching SC scores.
- **NC-NM:** Reported a dramatically lower mean SUS score of 54.1 ($SD = 10.9$, 95% $CI[48.4, 59.8]$), into the "Poor" usability category.

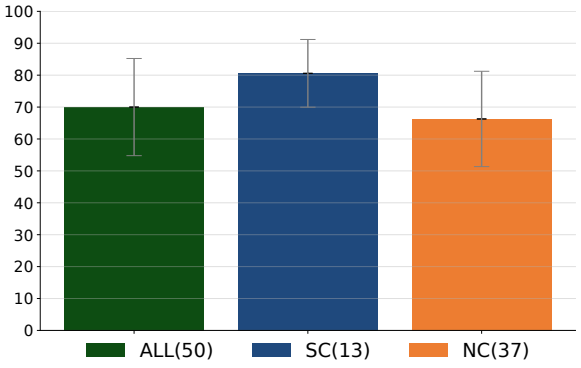


Figure 5: System Usability Scale (SUS) scores: SC vs. NC. Higher scores indicate better perceived usability; 68 is the international benchmark for "acceptable" usability [4].

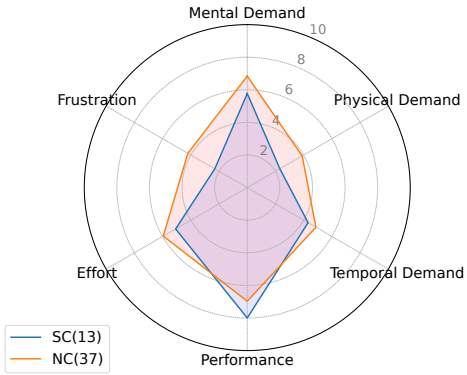


Figure 6: NASA-TLX cognitive load comparison: SC vs NC. Higher subscale scores indicate greater perceived workload; the NC group reported elevated Mental Demand and Effort relative to SC.

This difference was statistically significant ($t(25.65) = 6.13$, $p < .001$, $d = 1.9$, 95% CI $[12.5, 26.7]$) to confirm that prior Monopoly experience substantially reduced perceived usability barriers. This suggests that the demands for concurrent learning, for example, learning of the game rules and security concepts, may have heightened the perceived usability barriers amongst non-gamers.

This is supported by the breakdown of the findings by the NC-NM subgroup, which experienced the most Mental Demand and Effort according to the study conducted by the US National Aeronautics and Space Administration (NASA-TLX), as shown in Figure 8.

Technology Acceptance (TAM) Despite usability challenges, TAM results showed high acceptance across groups. PU and ITU scores were high (means > 4.2) with no signifi-

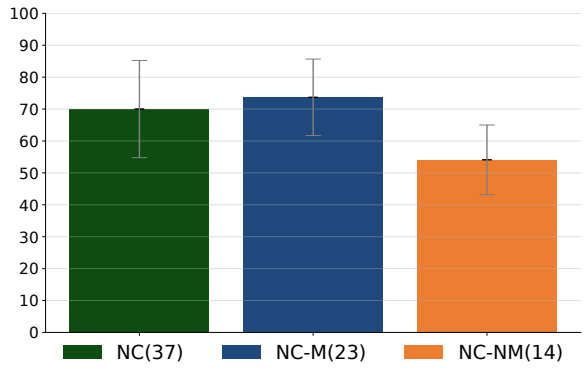


Figure 7: Impact of gaming literacy on perceived usability in the NC group (NC-M vs. NC-NM). Participants without prior Monopoly experience (NC-NM) rated usability significantly lower, falling in the "Poor" SUS category.

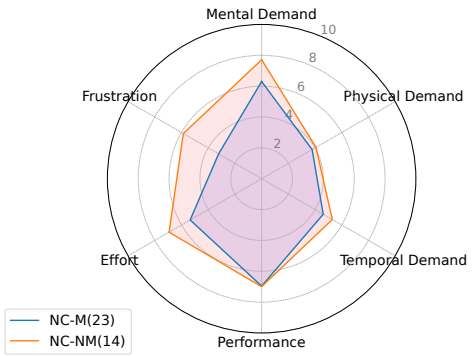


Figure 8: Cognitive load breakdown: NC-M vs. NC-NM. The NC-NM subgroup experienced the highest Mental Demand and Effort, consistent with the simultaneous learning of game mechanics and security concepts.

cant differences. This suggests that usability barriers did not reduce perceived usefulness or willingness to use the game. However, SC participants rated PEOU higher ($M = 4.42$ vs 4.09), a significant difference ($t(48) = 2.93$, $p = .005$, $d = .64$). The large standard deviation in the NC group ($SD = .60$) compared to the SC group ($SD = .21$) indicates high variability in how non-technical users experienced the game's complexity. This variance suggests that the NC cohort is not a monolith, motivating our deeper investigation into the specific impact of gaming literacy (NC-M vs. NC-NM) on ease of use. Notably, ATT scores were uniformly high ($M > 4.6$), indicating participants experienced CyQured as genuinely enjoyable rather than merely instructional, a finding corroborated by qualitative feedback as presented in Section 5.5.3.

Table 4: Analysis of TAM Constructs (Mean ± SD). Comparisons were conducted using Welch's t-test.

Construct	SC Group ($n = 13$)	NC Group ($n = 37$)
PEOU	$4.42 \pm .21$	$4.09 \pm .60$
PU	$4.26 \pm .41$	$4.25 \pm .61$
ATT	$4.85 \pm .32$	$4.61 \pm .61$
ITU	$4.54 \pm .32$	$4.43 \pm .69$

5.5.3 Qualitative Findings

To better understand the usability gap in RQ2, open-ended survey responses and semi-structured interviews were analyzed using inductive thematic analysis. Two researchers independently coded the data using the codebook presented in Table 5 and resolved disagreements through discussion.

Participants frequently described early confusion (Table 5, Theme 1), but reported that interaction and discussion helped them overcome it. These findings are consistent with the SUS and NASA-TLX results, suggesting a pattern of "productive struggle" in which engagement helped sustain learning despite initial barriers.

5.5.4 Results Synthesis

Across all measures, participants demonstrated good knowledge gains regardless of technical background or gaming experience. While non-technical players with limited board-game literacy faced initial usability barriers, their high perceived usefulness and qualitative feedback indicate that collaborative gameplay helped them overcome early confusion. Ultimately, CyQured is an effective educational tool, though future iterations must prioritize accessible onboarding for novices.

6 Discussion

The evaluation of CyQured reveals a critical tension between pedagogical efficacy and user experience. While evaluation demonstrated substantial post-game knowledge gains across all cohorts, it also revealed notable usability challenges for its primary target audience. This section interprets these findings through the lens of the "CyQured Paradox" and offers design implications for inclusive security education tools.

6.1 Interpretation: The CyQured Paradox

The results of RQ1 indicate substantial knowledge gains following gameplay across all cohorts, though gains were not uniform: the SC group showed significantly larger improvement ($\Delta M = 3.38$, $d = 1.88$) than the NC group ($\Delta M = 1.95$, $d = 1.62$), suggesting that prior domain vocabulary amplifies learning rather than being a prerequisite for it. Both effect sizes are large, consistent with meaningful game-induced learning regardless of technical background.

However, the HCI analysis regarding RQ2 highlights a distinct accessibility divide. While both groups demonstrated significant knowledge gains, the SC group's larger improve-

Table 5: Thematic Analysis of User Feedback.

Core Theme	Sub-Theme	Representative Evidence	Interpretation
1. Initial Barriers	Perceived Complexity	P27 (NC): "There are just too many rules to remember right at the start."	High entry-level cognitive load for non-gamers.
	Terminology	P33 (NC): "At first, concepts like spoofing were really confusing to me."	Domain terminology acts as a language barrier. Future iterations may benefit from plain-language glossaries for non-expert players.
2. Learnability	Gradual Adjustment	P1 (NC): "It was confusing in the beginning, but it got easier as we played."	Learning emerged through iterative gameplay.
	Productive Struggle	P15 (NC): "It was confusing, sure, but I actually learned a lot of things."	Difficulty did not prevent knowledge acquisition.
3. Engagement	Social Interaction	P27 (NC): "The fun part was everyone sitting together and playing."	Social play buffered the negative effects of complexity.
	Peer Scaffolding	P9 (SC): "It was engaging to have such good discussions with everyone."	Collaborative environment helped resolve confusion.

ment ($\Delta M = 3.38$ vs. $\Delta M = 1.95$; $t(16.62) = 2.87$, $p = .01$, $d = 1.08$) suggests that prior domain vocabulary accelerated learning for those with security coursework; independent of this difference, the NC group reported significantly higher workload on the NASA-TLX. While the SC group rated usability as "excellent" ($SUS = 80.6$), the NC-NM group without gaming experience rated it as "poor" ($SUS = 54.1$). This highlights an apparent methodological tension: How did participants in the NC-NM group achieve substantial knowledge gains ($d = 1.62$) despite a usability score of $SUS = 54.1$ that is typically associated with poor acceptance?

We refer to this tension as CyQured Paradox. Our data suggest the presence of a compensatory dynamic where high Perceived Usefulness (PU) and Attitude (ATT) may have acted as a "motivational reserve" that helped participants persist despite mechanical friction. While the Technology Acceptance Model (TAM) posits that both PU and $PEOU$ influence adoption, our findings indicate that in high-motivation learning contexts, strong domain relevance ($PU > 4.2$) can temporarily offset the negative impact of low ease of use. This pattern is consistent with the theory of "desirable difficulties," which suggests cognitive strain can support deeper processing when learners remain engaged. In CyQured, the game's social nature may have helped sustain engagement during periods of "productive struggle" (a known concept in serious games where moderate difficulty supports deeper learning when learners remain engaged [19]). Qualitative feedback supported this interpretation: participants described the game as "competitive" and "fun" (P20, P28), with several stating they would play it informally with family, not solely as a structured exercise.

6.2 Implications for Low-Barrier Design in Security Education

Our findings offer transferable design implications for the usable security community. By "Low-Barrier," we refer to reducing interaction and cognitive barriers for players with limited prior gaming or domain experience.

Decouple Interaction Cost from Domain Complexity: The "CyQured Paradox" suggests that pedagogical success and usability are distinct constructs. A tool can be educationally effective (high recall) yet present significant usability barriers (low SUS). Future tools should scaffold the *mechanics* of the intervention as rigorously as the *security content*, ensuring that the interaction-induced workload does not compete with the cognitive resources required for learning.

Design for Asymmetric Literacy: Our findings suggest a potential double burden for the general audience: they lack both domain literacy (security) and interaction literacy (tabletop mechanics). Designers should assume an asymmetry where the user cannot leverage existing mental models for either the content or the interface. This requires *progressive disclosure*, where mechanics are introduced sequentially (e.g., "Round 1: Movement only") to prevent cognitive overload before the security concepts are even encountered.

PEOU as a Barrier to Long-Term Adoption: While PU drove the immediate willingness to learn (efficacy), low $PEOU$ remains a threat to long-term voluntary adoption. In educational contexts, motivation may be extrinsic; however,

in home-user tools, high interaction costs can lead to "security fatigue." *PEOU* may therefore be an important predictor of whether a security intervention will survive beyond the initial novelty phase.

7 Limitations

This study has several methodological limitations. First, our convenience sample of university students may introduce tech-savvy bias. Prior work identifies a socio-technical divide in security knowledge, where users with lower digital literacy rely disproportionately on informal advice sources [44]. Future work should evaluate CyQured with more diverse, non-student populations. Second, the large effect sizes observed (SC: $d = 1.88$; NC: $d = 1.62$) should be interpreted with caution given the modest sample size ($N = 50$). Small samples are susceptible to upward bias in effect size estimation, sometimes referred to as the "winner's curse" [6], and these gains may not fully replicate in larger or more diverse samples. Furthermore, the ad-hoc, 10-item multiple-choice knowledge assessment immediately after playing the game and without formal psychometric validation only measures short-term recall, not long-term behavioral changes or complex real-world decision-making.

Third, our use of subjective measures (SUS, TAM, NASA-TLX) gives rise to possible social desirability bias and common method variance. For the 5-point Likert TAM questionnaire (Appendix A.2) internal consistency was acceptable for PU ($\alpha = .84$), ITU ($\alpha = .83$), and ATT ($\alpha = .69$) but considerably less acceptable for PEOU ($\alpha = .63$). This decreased PEOU reliability is a direct reflection of the incredible usability divide and the variance between our gaming-literate and non-literate cohorts, not an invalid construct. Additionally, the high levels of cognitive load experienced by individuals with limited prior exposure to strategy games suggest that measured mental effort often resulted from the friction of learning game mechanics rather than grappling with cybersecurity concepts.

Fourth, conducting the sessions in a controlled research environment, with an experimenter present, limits ecological validity. Although this game is intended to be facilitator-independent, in unsupervised real-world deployments in homes or classrooms, the motivational dynamics of those environments may differ. In addition, the qualitative inductive thematic analysis approach is inherently interpretive. Finally, our knowledge assessment measured immediate recall only; long-term retention and behavioral transfer to real-world security practices remain open questions for future longitudinal study.

8 Conclusion and Future Work

This paper introduced *CyQured*, a facilitator-independent tabletop game designed to support experiential learning of home cybersecurity concepts. In a mixed-methods evaluation with university students of varying technical backgrounds, we observed short-term knowledge gains alongside a clear tension between usability and learning: novice players reported a higher cognitive load, especially during the first round of the game, despite strong perceived usefulness and engagement.

Beyond the immediate study context, these findings highlight an important implication for usable security research: educational outcomes and usability are distinct dimensions of intervention success. Learners may remain motivated to engage with complex security content even when interaction costs are non-trivial, but such friction can threaten inclusivity and long-term adoption.

For designers of security education tools, this suggests three priorities: scaffold interaction mechanics as carefully as domain concepts, minimize early onboarding barriers for non-technical users, and treat perceived ease of use as critical for voluntary adoption beyond structured study settings.

Future work should examine long-term retention, compare gameplay against alternative training approaches, and evaluate deployment across more diverse populations and real-world contexts to better understand scalability and sustained impact.

References

[1] Dina Aladawy, Kristian Beckers, and Sebastian Pape. Persuaded: fighting social engineering attacks with a serious game. In *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15*, pages 103–118. Springer, 2018.

[2] Bitdefender. The 2025 IoT security landscape report. https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/10/2025_iot_security_report.pdf, 2025. Accessed: 2026-05-22.

[3] C. Alan Boneau. The effects of violations of assumptions underlying the t test. *Psychological bulletin*, 57(1):49–64, 1960.

[4] John Brooke. Sus-a quick and dirty usability scale. *Usability evaluation in industry*, 189(194):4–7, 1996.

[5] Jacqueline Grennon Brooks and Martin G Brooks. *In search of understanding: The case for constructivist classrooms*. Association for Supervision Curriculum Development, 1999.

[6] Katherine S. Button, John P. A. Ioannidis, Claire Mokrysz, Brian A. Nosek, Jonathan Flint, Emma S. J. Robinson, and Marcus R. Munafò. Power failure: why small sample size undermines the reliability of neuroscience. *Nature reviews neuroscience*, 14(5):365–376, 2013.

[7] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza. Nophish: an anti-phishing education app. In *International workshop on security and trust management*, pages 188–192. Springer, 2014.

[8] Jordi Carenys. Competing to Learn: The Role of Competition in Students‘ Flow, Cognitive Load, and Learning Gains in Game-Based Learning. *International Journal of Learning, Teaching and Educational Research*, 24(5):174–197, 2025.

[9] Center for Infrastructure Assurance and Security (CIAS). Cyber threat defender (CTD). https://cias.utsa.edu/ctd/, 2024. Accessed: 2024-12-31.

[10] Mohammad Chuttur. Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *All Sprouts Content. 290*, 9(37), 2009.

[11] Victoria Clarke and Virginia Braun. Thematic analysis. *The journal of positive psychology*, 12(3):297–298, 2017.

[12] Jacob Cohen. *Statistical power analysis for the behavioral sciences*. routledge, 2013.

[13] Kovila PL Coopamootoo and Thomas Groß. Mental models: an approach to identify privacy concern and behavior. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 9–11. USENIX Association USA, 2014.

[14] Fred D Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, pages 319–340, 1989.

[15] Edward L Deci and Richard M Ryan. The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. *Psychological inquiry*, 11(4):227–268, 2000.

[16] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-alt-hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 915–928, 2013.

[17] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke. From game design elements to gamefulness: defining “gamification“. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, pages 9–15, Tampere, Finland, 2011. ACM.

[18] Dexpose. Iot hacking statistics. https://www.dexpose.io/iot-hacking-statistics/, 2026. Accessed: 2026-05-22.

[19] Tjitske JE Faber, Mary EW Dankbaar, Walter W van den Broek, Laura J Bruinink, Marije Hogeveen, and Jeroen JG van Merriënboer. Effects of adaptive scaffolding on performance, cognitive load and engagement in game-based learning: a randomized controlled trial. *BMC Medical Education*, 24(1):943, 2024.

[20] Fellow Traveller. Hacknet. https://www.hacknet-os.com/, 2015. Accessed: 2026-05-31.

[21] Scott Freeman, Sarah L Eddy, Miles McDonough, Michelle K Smith, Nnadozie Okoroafor, Hannah Jordt, and Mary Pat Wenderoth. Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the national academy of sciences*, 111(23):8410–8415, 2014.

[22] Mark Gondree and Zachary NJ Peterson. Valuing security by getting {[d0x3d!]}: Experiences with a network security board game. In *6th Workshop on Cyber Security Experimentation and Test (CSET 13)*, 2013.

[23] Ana I González-Tablas, María I González Vasco, Ignacio Cascos, and Álvaro Planet Palomino. Shuffle, cut, and learn: Crypto go, a card game for teaching cryptography. *Mathematics*, 8(11):1993, 2020.

[24] Ingrid Graffer, Maria Bartnes, and Karin Bernsmed. Play2prepare: A board game supporting it security preparedness exercises for industrial control organizations. NIK: Norsk Informatikkonferanse, 2015.

[25] Anderson Kevin Gwenhure. University students’ security behavior against email phishing attacks: insights from the health belief model. *Journal of Cybersecurity*, 11(1):tyaf034, 2025.

[26] Juho Hamari, Jonna Koivisto, and Harri Sarsa. Does gamification work?–a literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences*, pages 3025–3034. Ieee, 2014.

[27] Sandra G Hart and Lowell E Staveland. Development of nasa-tlx (task load index): Results of empirical and theoretical research. In *Advances in psychology*, volume 52, pages 139–183. Elsevier, 1988.

[28] Stephen Hart, Andrea Margheri, Federica Paci, and Vladimiro Sassone. Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95:101827, 2020.

[29] Maxwell Hartt, Hadi Hosseini, and Mehrnaz Mostafapour. Game on: Exploring the effectiveness of game-based learning. *Planning Practice & Research*, 35(5):589–604, 2020.

[30] Khondokar Fida Hasan, William Hughes, Adrita Rahman Tory, Chris Campbell, and Selen Turkay. Game on: A developmental approach to unsw cyber escape room for cybersecurity governance and policy education. *Education Sciences*, 16(1), 2026.

[31] Grant Ho, Ariana Mirian, Elisa Luo, Khang Tong, Euyhyun Lee, Lin Liu, Christopher A Longhurst, Christian Dameff, Stefan Savage, and Geoffrey M Voelker. Understanding the efficacy of phishing training in practice. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 37–54. IEEE, 2025.

[32] Adam Houser and Matthew L Bolton. Formal mental models for inclusive privacy and security. In *SOUPS*, 2017.

[33] Cynthia E Irvine, Michael F Thompson, and Ken Allen. Cyberciege: gaming for information assurance. *IEEE Security & Privacy*, 3(3):61–64, 2005.

[34] David H Jonassen and Lucia Rohrer-Murphy. Activity theory as a framework for designing constructivist learning environments. *Educational technology research and development*, 47(1):61–79, 1999.

[35] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, Canada, 2015. USENIX Association.

[36] David A Kolb. *Experiential learning: Experience as the source of learning and development*. FT press, 2014.

[37] Maria Kordaki. A constructivist, modeling methodology for the design of educational card games. *Procedia-Social and Behavioral Sciences*, 191:26–30, 2015.

[38] Tan Ming Kuang, Ralph W Adler, and Rakesh Pandey. Creating a modified monopoly game for promoting students' higher-order thinking skills and knowledge retention. *Issues in Accounting Education*, 36(3):49–74, 2021.

[39] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[40] Nicholas Metropolis and Stanislaw Ulam. The monte carlo method. *Journal of the American statistical association*, 44(247):335–341, 1949.

[41] Barack Onduto, R Ali, and AJ Smed. Gamification of cyber security awareness–a systematic review of games. *Computing, Faculty of Technology*, 2021.

[42] Omid Pahlavanpour and Shang Gao. A systematic mapping study on gamification within information security awareness programs. *Heliyon*, 10(19), 2024.

[43] G. Paparis, A. Zarras, A. Farao, and C. Xenakis. Crashed: Cyber risk assessment for smart home electronic devices. *Journal of Information Security and Applications*, 91:104054, 2025.

[44] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. Where is the Digital Divide?: A Survey of Security, Privacy, and Socioeconomics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 931–942, Denver, Colorado, USA, 2016. ACM.

[45] Richard M Ryan and Edward L Deci. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist*, 55(1):68, 2000.

[46] Hamza Saleem and Muhammad Naveed. Sok: Anatomy of data breaches. *Proceedings on Privacy Enhancing Technologies*, 2020.

[47] Pintu Shah and Anuja Agarwal. Cyber suraksha: a card game for smartphone security awareness. *Information & Computer Security*, 31(5):576–600, 2023.

[48] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth 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*, pages 88–99, 2007.

[49] Adam Shostack. Elevation of Privilege: Drawing Developers into Threat Modeling. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[50] John Sweller. Cognitive Load During Problem Solving: Effects on Learning. *Cognitive science*, 12(2):257–285, 1988.

[51] Giorgia Tempestini, Sara Merà, Marco Pietro Palange, Alexandra Bucciarelli, and Francesco Di Nocera. Improving the Cybersecurity Awareness of Young Adults through a Game-Based Informal Learning Strategy. *Information*, 15(10):607, 2024.

[52] Trend Micro. Backing your backup: Defending nas devices against evolving threats. https://documents.trendmicro.com/assets/pdf/wp-backing-your-backup-defending-nas-devices-against-evolving-threats.pdf, 2022. Accessed: 2026-05-31.

[53] William J Triplett. Addressing Cybersecurity Challenges in Education. *International Journal of STEM Education for Sustainability*, 3(1):47–67, 2023.

[54] Harshal Tupsamudre, Rahul Wasnik, Shubhankar Biswas, Sankalp Pandit, Sukanya Vaddepalli, Aishwarya Shinde, CJ Gokul, Vijayanand Banahatti, and Sachin Lodha. GAP: A Game for Improving A wareness About Passwords. In *Serious Games: 4th Joint International Conference, JCSG 2018, Darmstadt, Germany, November 7-8, 2018, Proceedings 4*, pages 66–78. Springer, 2018.

[55] Rick Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–16, 2010.

[56] Laurie Williams, Andrew Meneely, and Grant Shipley. Protection Poker: The New Software Security "Game". *IEEE Security & Privacy*, 8(3):14–20, 2010.

[57] Affan Yasin, Lin Liu, Tong Li, Jianmin Wang, and Didar Zowghi. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Information and Software Technology*, 95:179–200, 2018.

A Questionnaire Instruments

A.1 Knowledge Assessment (Pre/Post Test)

Pre-Test Questions

1. You receive an email from your "CEO" urgently requesting you to buy gift cards for a client reward. The email looks official but feels off. What type of attack are you most likely facing?
   A) Firmware Attack B) Phishing Attack C) DDoS Attack D) Wireless Sniffing
2. While working at a coffee shop, you notice someone looking over your shoulder as you type your laptop password. What is this attack called?
   A) Router Hijacking B) Shoulder Surfing C) Credential Stuffing D) ARP Spoofing
3. Your computer starts running very slowly and a message appears demanding payment to unlock your files. Which attack has occurred?
   A) Trojan Horse B) Session Hijacking C) Ransomware D) Zero-Day Exploit
4. A hacker gains access to your router and changes its DNS settings to redirect your banking website to a fake one. What attack is this?
   A) Network Jamming B) Router Hijacking C) Wireless Sniffing D) Activity Log Manipulation
5. You download a free game online, but it secretly installs a program that gives a hacker remote access to your computer. What type of malware is this?
   A) Ransomware B) Trojan Horse C) Firmware Attack D) Phishing
6. An attacker floods your company's website with so much traffic that legitimate customers cannot access it. What is this called?
   A) DDoS Attack B) Password Cracking C) ARP Spoofing D) Caller ID Spoofing
7. Someone uses automated software to try thousands of common passwords to break into your online account. What attack is this?
   A) Session Hijacking B) Credential Stuffing C) Password Cracking D) Wireless Sniffing
8. An attacker secretly listens to data being sent over an unsecured public Wi-Fi network. What attack is this?
   A) Network Jamming B) Wireless Sniffing C) Router Hijacking D) Firmware Attack
9. After a meeting, you realize your login session for an online service was taken over without your password being changed. What likely happened?
   A) Phishing Attack B) Session Hijacking C) Trojan Horse D) Ransomware
10. An attacker pretends to be from IT support over the phone and tricks an employee into revealing their login details. What social engineering tactic is this?
    A) Shoulder Surfing B) Caller ID Spoofing C) Wireless Sniffing D) ARP Spoofing

Post-Test Questions

1. To prevent employees from being tricked by fake emails from the CEO requesting money transfers, which defense should be implemented?
   A) Wired Connections B) Email Filtering C) VPN D) Secure Firmware Updates
2. What is the most effective defense to protect against someone stealing your password by watching you type it in a public place?
   A) Strong Password Policy B) Account Lockout C) Privacy Screen D) Immutable Logging
3. After a ransomware attack encrypts a department's files, what is the primary method to restore operations without paying?
   A) Anti-Virus Scan B) Data Backup & Recovery C) Firmware Update D) Network Segmentation
4. To prevent a hacker from changing your router's DNS settings to redirect your traffic, which defense is most relevant?
   A) Secure DNS B) WPA3 Encryption C) IDS D) Email Filtering
5. Which defense is specifically designed to prevent malicious programs disguised as legitimate software from being installed via email?
   A) Firewall B) Email Filtering C) VPN D) Secure Session Management
6. Your online store is under a DDoS attack. Which defense can help mitigate the flood of traffic from thousands of hacked devices?
   A) Account Lockout B) Strong Password Policy C) Wired Connection D) Immutable Logging
7. To protect against automated brute-force login attempts on your website, what should you enable?
   A) VPN B) Account Lockout & Rate Limiting C) Secure DNS D) Data Backup
8. To protect sensitive data like login credentials when using public Wi-Fi, what should you always use?
   A) WPA3 B) VPN & Network Encryption C) Anti-Virus D) Firewall
9. Which defense helps ensure that even if a session token is stolen, an attacker cannot easily take over a user's logged-in account?

A) Secure Session Management B) Wired Connection C) Bluetooth Security D) Immutable Logging

10. To defend against phone-based social engineering where attackers fake their caller ID, what is the best practice?
A) Enable WPA3 B) Verify caller identity C) Use a VPN D) Install Anti-Virus

Answer Key:
Pre-Test: 1-B, 2-B, 3-C, 4-B, 5-B, 6-A, 7-C, 8-B, 9-B, 10-B
Post-Test: 1-B, 2-C, 3-B, 4-A, 5-B, 6-A, 7-B, 8-B, 9-A, 10-B

A.2 TAM-Based Questionnaire

ID	Question
Perceived Ease of Use (PEOU)	
PEOU1	I found the CyQured game easy to understand.
PEOU2	I found the CyQured game easy to play.
PEOU3	I found CyQured easy to use for identifying cyber threats on my personal devices.
PEOU4	I found CyQured easy to use for identifying cybersecurity defenses on my personal devices.
Perceived Usefulness (PU)	
PU5	Playing CyQured improved my ability to identify cybersecurity threats on my personal devices.
PU6	Playing CyQured improved my ability to identify cybersecurity defenses on my personal devices.
PU7	Playing CyQured enhanced my cybersecurity knowledge.
PU8	CyQured is an effective way to identify cyber threats and defenses.
PU9	CyQured helped me discover new cyber threats I hadn't noticed before.
PU10	CyQured helped me discover new cybersecurity defenses.
PU11	CyQured increases cybersecurity awareness for personal use.
PU12	CyQured is a helpful way to teach cybersecurity.
Intention to Use (ITU)	
ITU13	I would use CyQured to improve my cybersecurity awareness.
ITU14	I would recommend CyQured to identify cyber threats.
ITU15	I would recommend CyQured to identify security defenses.
Attitude Toward Use (ATT)	
ATT16	I found CyQured enjoyable.
ATT17	I remained engaged while playing CyQured.

Table 6: TAM-based questionnaire items used in the study.

A.3 SUS Questionnaire

SUS1 I would like to play this game frequently.
SUS2 I found the game unnecessarily complex.*
SUS3 I thought the game was easy to use.
SUS4 I think I would need the support of a technical person to play this game.*
SUS5 I found the various features in this game were well integrated.
SUS6 I thought there was too much inconsistency in this game.*
SUS7 I would imagine that most people would learn to play this game very quickly.
SUS8 I found the game very cumbersome to use.*
SUS9 I felt very confident playing the game.
SUS10 I needed to learn a lot of things before I could get going with this game.*

* *Indicates reverse-scored items.*

A.4 NASA-TLX Questionnaire

#	Question	Dimension
1	How mentally demanding was the task?	Mental Demand
2	How physically demanding was the task?	Physical Demand
3	How hurried or rushed was the pace of the task?	Temporal Demand
4	How successful were you in accomplishing what you were asked to do?	Performance*
5	How hard did you have to work to accomplish your level of performance?	Effort
6	How insecure, discouraged, irritated, stressed, and annoyed were you?	Frustration

* Indicates reverse-scored item.

Table 7: NASA-TLX workload questionnaire items.

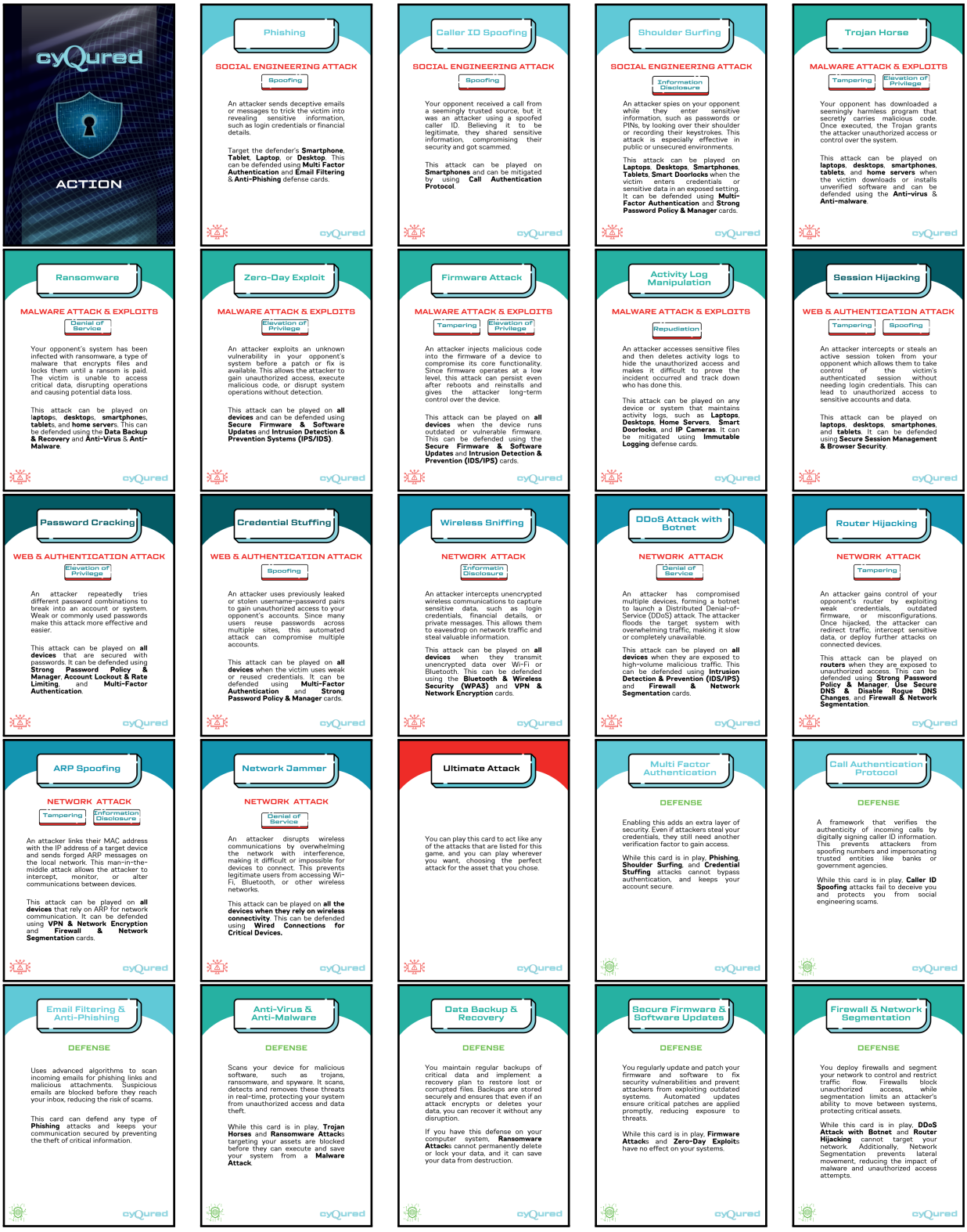
A.5 Open-Ended Feedback Questions

#	Question
1	What did you like most/least about the game?
2	Was there anything confusing?
3	How do you think this game helped you learn about cyber threats?
4	Do you have any suggestions for improving it?

Table 8: Open-ended feedback questions used in the post-game interview.

B CyQured Game Cards

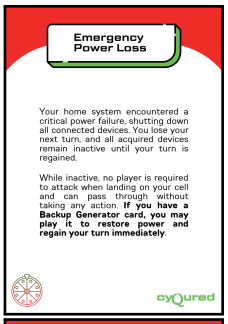
B.1 Action Cards



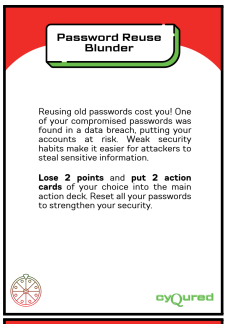


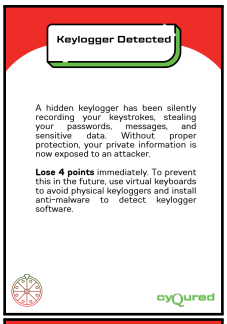
B.2 Chance Cards

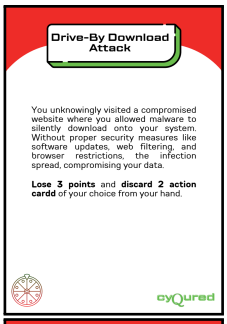


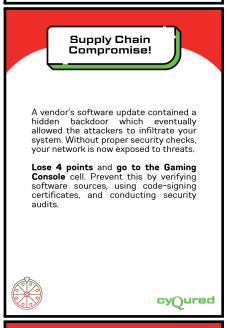

Emergency Power Loss
Your home system encountered a critical power failure, shutting down all connected devices. You lose your next turn, and all acquired devices remain inactive until your turn is regained.
While inactive, no player is required to attack when landing on your cell and can pass through without taking any action. If you have a Backup Generator card, you may play it to restore power and regain your turn immediately.
cyQured

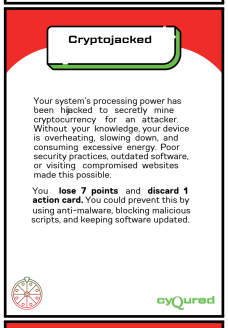

Social Engineering Exploited
An attacker tricked you into revealing sensitive login credentials through a deceptive phone call. With this information, they gained unauthorized access to your system and your security got compromised.
Lose 7 points and discard 1 card from your hand. To prevent this in the future, always verify requests for sensitive information, enable multi-factor authentication, and stay cautious of unsolicited messages or calls.
cyQured

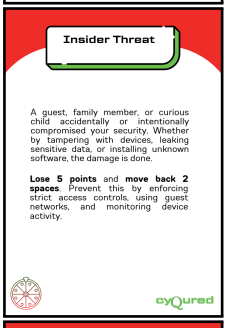

Password Reuse Blunder
Reusing old passwords cost you! One of your compromised passwords was found in a data breach, putting your accounts at risk. Weak security habits make it easier for attackers to steal sensitive information.
Lose 2 points and put 2 action cards of your choice into the main action deck. Reset all your passwords to strengthen your security.
cyQured

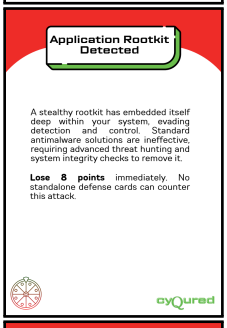

Keylogger Detected
A hidden keylogger has been silently recording your keystrokes, stealing your passwords, messages, and sensitive data. Without proper protection, your private information is now exposed to an attacker.
Lose 4 points immediately. To prevent this in the future, use virtual keyboards to avoid physical keyloggers and install anti-malware to detect keylogger software.
cyQured

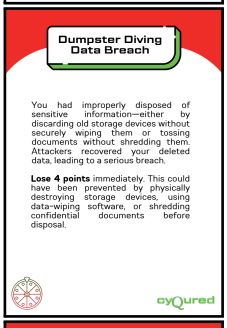

Drive-By Download Attack
You unknowingly visited a compromised website where you allowed malware to silently download onto your system. Without proper security measures like software updates, web filtering, and browser restrictions, the infection spread, compromising your data.
Lose 3 points and discard 2 action cardd of your choice from your hand.
cyQured

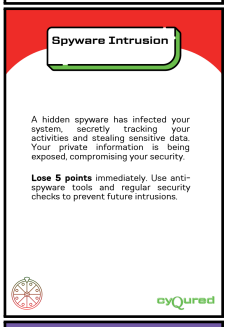

Supply Chain Compromise!
A vendor's software update contained a hidden backdoor which eventually allowed the attackers to infiltrate your system. Without proper security checks, your network is now exposed to threats.
Lose 4 points and go to the Gaming Console cell. Prevent this by verifying software sources, using code-signing certificates, and conducting security audits.
cyQured

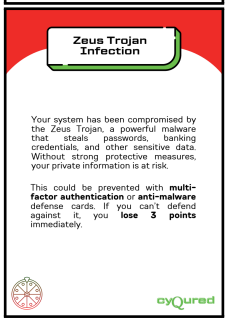

Cryptojacked
Your system's processing power has been hijacked to secretly mine cryptocurrency for an attacker. Without your knowledge, your device is overheating, slowing down, and consuming excessive energy. Poor security practices, outdated software, or visiting compromised websites made this possible.
You lose 7 points and discard 1 action card. You could prevent this by using anti-malware, blocking malicious scripts, and keeping software updated.
cyQured

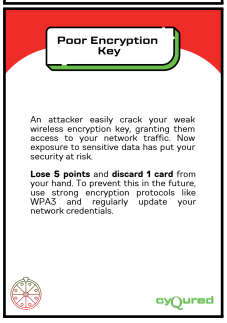

Insider Threat
A guest, family member, or curious child accidentally or intentionally compromised your security. Whether by tampering with devices, leaking sensitive data, or installing unknown software, the damage is done.
Lose 5 points and move back 2 spaces. Prevent this by enforcing strict access controls, using guest networks, and monitoring device activity.
cyQured

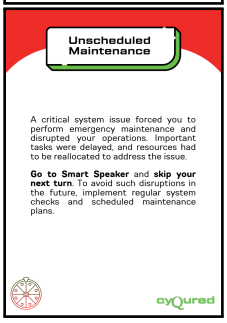

Application Rootkit Detected
A stealthy rootkit has embedded itself deep within your system, evading detection and control. Standard antimalware solutions are ineffective, requiring advanced threat hunting and system integrity checks to remove it.
Lose 8 points immediately. No standalone defense cards can counter this attack.
cyQured

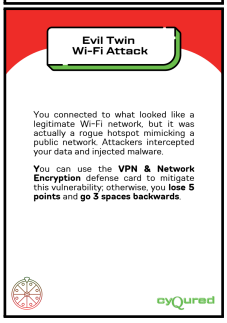

Dumpster Diving Data Breach
You had improperly disposed of sensitive information—either by discarding old storage devices without securely wiping them or tossing documents without shredding them. Attackers recovered your deleted data, leading to a serious breach.
Lose 4 points immediately. This could have been prevented by physically destroying storage devices, using data-wiping software, or shredding confidential documents before disposal.
cyQured

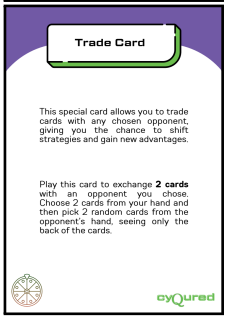

Spyware Intrusion
A hidden spyware has infected your system, secretly tracking your activities and stealing sensitive data. Your private information is being exposed, compromising your security.
Lose 5 points immediately. Use anti-spyware tools and regular security checks to prevent future intrusions.
cyQured


Zeus Trojan Infection
Your system has been compromised by the Zeus Trojan, a powerful malware that steals passwords, banking credentials, and other sensitive data. Without strong protective measures, your private information is at risk.
This could be prevented with multi-factor authentication or anti-malware defense cards. If you can't defend against it, you lose 3 points immediately.
cyQured


Poor Encryption Key
An attacker easily crack your weak wireless encryption key, granting them access to your network traffic. Now exposure to sensitive data has put your security at risk.
Lose 5 points and discard 1 card from your hand. To prevent this in the future, use strong encryption protocols like WPA3 and regularly update your network credentials.
cyQured


Unscheduled Maintenance
A critical system issue forced you to perform emergency maintenance and disrupted your operations. Important tasks were delayed, and resources had to be reallocated to address the issue.
Go to Smart Speaker and skip your next turn. To avoid such disruptions in the future, implement regular system checks and scheduled maintenance plans.
cyQured


Evil Twin Wi-Fi Attack
You connected to what looked like a legitimate Wi-Fi network, but it was actually a rogue hotspot mimicking a public network. Attackers intercepted your data and injected malware.
You can use the VPN & Network Encryption defense card to mitigate this vulnerability; otherwise, you lose 5 points and go 3 spaces backwards.
cyQured


Trade Card
This special card allows you to trade cards with any chosen opponent, giving you the chance to shift strategies and gain new advantages.
Play this card to exchange 2 cards with an opponent you chose. Choose 2 cards from your hand and then pick 2 random cards from the opponent's hand, seeing only the back of the cards.
cyQured

B.3 Scenario Cards



Scenario

You receive an email pretending to be from your ISP, urging you to click a link to "update your payment details." The email looks official, with the ISP's logo and branding, but the link leads to a suspicious website asking for your credit card information.

cyQured

Scenario

You receive a call from someone claiming to be from your bank. They say there's suspicious activity on your account and ask for your account details to "verify your identity." The caller ID shows your bank's official number, which makes the call seem legitimate.

cyQured

Scenario

You type your bank's official URL into your browser, but instead of the real website, you're redirected to a fake site that looks identical. The fake site asks you to log in with your credentials.

cyQured

Scenario

You receive an alert that someone tried logging into your email from an unfamiliar location. You realize you've reused the same password on multiple sites, and one of those sites was recently breached.

cyQured

Scenario

Your internet slows down, and you notice unfamiliar devices connected to your router. When you check the router settings, you see changes you didn't make, like a new admin password or DNS settings.

cyQured

Scenario

Your indoor security camera starts moving independently, and you notice unfamiliar logins to the camera's admin panel. Even after resetting the camera, the issue persists, and you can't regain control.

cyQured

Scenario

You open an email attachment, and suddenly all your files are encrypted. A message pops up demanding payment in cryptocurrency to unlock your files. The message warns that your files will be permanently deleted if you don't pay within 48 hours.

cyQured

Scenario

While entering your PIN at an ATM, you notice someone standing unusually close to you. Later, you find unauthorized transactions on your account, and the bank confirms that your PIN was used at another ATM.

cyQured

Scenario

You download a free game from an untrusted website. Soon after, your device starts behaving strangely—pop-ups appear, and you notice unauthorized programs running in the background. Your antivirus software detects malware.

cyQured

Scenario

You try to access your favorite online gaming platform, but it's unavailable. Later, you hear that the platform was overwhelmed by a massive surge in traffic, causing it to crash. The platform confirms it was a targeted attack.

cyQured

Scenario

You're logged into your online banking account when suddenly you're logged out. When you try to log back in, you see unfamiliar transactions. The bank confirms that someone accessed your account using your active session.

cyQured

Scenario

You notice that your internet connection is slow, and some websites load strange content. When you check your network, you see unfamiliar devices listed as connected. Your router's ARP table shows incorrect IP-MAC mappings.

cyQured

Scenario

You receive multiple failed login attempt notifications for your social media account. Later, you find that your account has been accessed, and spam messages were sent to your contacts.

cyQured

Scenario

Your Wi-Fi suddenly stops working, and none of your devices can connect. When you check, you notice that your router's signal is being disrupted by a nearby device emitting strong radio signals.

cyQured

Scenario

Your smart utility meter starts sending incorrect usage data to your provider, showing abnormally high consumption. You later discover a nearby attacker spoofed your meter's communication to inflate usage, possibly to trick you into overpaying or causing billing chaos.

cyQured

Scenario

You notice your smart printer printing strange documents at random times. Investigation reveals a hacker accessed the printer remotely through an exposed port and used it to store and print malicious material.

cyQured

Scenario

Your smart refrigerator displays ads and redirects your mobile phone to phishing sites when connected to its app. You find that malware has infected the fridge's firmware, acting as a proxy to intercept traffic.

cyQured

Scenario

Your smart door lock unlocks automatically without your command while you're away. Reviewing the logs, you see access tokens were reused by an attacker intercepting previous traffic.

cyQured

Scenario

Your smartwatch battery drains rapidly and gets hot. A diagnostic app shows it has been constantly sending location and health data to an unknown IP. Malware was installed through a third-party app.

cyQured

Scenario

You're playing an online game on your gaming console, and suddenly, the system freezes and restarts. Upon reboot, all your saved data is gone. A vulnerability in the console OS was exploited to cause system-wide corruption.

cyQured