Narrative-Based Interactive Learning for Scam Prevention: Rich Within Reach

Weile Tu, Bryan Zl Lim, Victor Wd Ong, Juay Hee Tan, Ashe Xy Lee, Peisen Xu and Anand Bhojan
Department of Computer Science, National University of Singapore, Singapore, Singapore

Keywords: Gamification, Interactive Learning, Experiential Design, Digital Literacy, Scam Prevention, Fraud Awareness.

Abstract: This paper introduces *Rich Within Reach*, a narrative-driven, decision-based, educational game designed to improve scam identification skills using realistic and interactive scenarios. The game leverages engaging narratives and gameplay mechanics to help players identify phishing, scareware, and invoice scams in email and SMS contexts. Analyzing player performance metrics, the study uncovers improved abilities in scam detection, particularly for phishing emails, while highlighting persistent challenges in SMS-based scam identification, especially for invoice scams. These findings underscore the potential of targeted, gamified interventions to strengthen digital literacy and fraud awareness. By integrating experiential learning principles, Rich Within Reach not only equips users with practical scam prevention skills, but also makes a case for the use of interactive learning to address modern cybersecurity challenges. The paper concludes with insights into the game's design and implications for broader educational applications.

1 INTRODUCTION

In an increasingly digital world, people are often vulnerable to sophisticated scams. In recent years, Singapore has witnessed a significant surge in scam-related activities, with the number of reported scam cases up 46.8% from 31,728 cases in 2022 to 46,563 cases in 2023 (Chua, 2024), underscoring the escalating challenge of scam prevention. Traditional educational campaigns have laid the groundwork for public awareness, with the Singapore Police Force (SPF) at the forefront of interactive anti-scam initiatives such as the Anti-Scam Center established in 2019 (National Crime Prevention Council Singapore, 2024).

However, the dynamic and evolving nature of scams necessitates more engaging and adaptive learning methodologies to educate the public. Interactive learning is a potent strategy to equip individuals with the skills and knowledge to identify and thwart scam attempts using immersive and participatory methods. Academic research further underscores the efficacy of interactive learning in scam prevention, as this allows participants to explore the psychological mechanisms that make individuals susceptible to scams and comparatively evaluate various interventions, including interactive educational tools, to mitigate such vulnerabilities (Tay and Teiw, 2023).

The National Crime Prevention Council (NCPC) has also developed interactive web games designed to test users' decision-making skills in life-like challenges, in collaboration with other major institutions such as banks, telecommunication providers, and government agencies (Dass, 2021). These initiatives highlight the pivotal role of interactive learning in scam prevention, demonstrating its effectiveness and accessibility to the broader population.

Rich Within Reach (**RWR**) takes a narrative-based approach to interactive scam education, with the aim of equipping players with scam identification and prevention skills by role-playing as an entrepreneur. A player is required to distinguish legitimate business and personal opportunities from potential scams on email and SMS mediums. Compared to traditional education delivered unilaterally, *RWR* educates players on scams using engaging, real-world game scenarios.

In summary, our contributions are two-fold:

1. The design and development of *RWR*, an interactive, game-based artefact to scam prevention that offers players a safe and immersive environment to learn to identify and respond to scams effectively.
2. The analysis of player metrics (inputs and responses to real-time game events), which reveals the potential of interactive learning as an innovative tool for educating users on scam prevention.

Tu, W., Lim, B. Z., Ong, V. W., Tan, J. H., Lee, A. X., Xu, P. and Bhojan, A.
Narrative-Based Interactive Learning for Scam Prevention: Rich Within Reach.
DOI: 10.5220/0013436100003932
In *Proceedings of the 17th International Conference on Computer Supported Education (CSEDU 2025) - Volume 1*, pages 581-589
ISBN: 978-989-758-746-7; ISSN: 2184-5026

2 LITERATURE REVIEW

Interactive games have been used for scam education to educate players on recognising and preventing online scams. For example, Scam Busters (MoneySense, 2021) is an interactive web game developed by MoneySense to help younger audiences understand specific types of scams such as fraud and phishing. Players assist a character named Liam and his family to identify potential scams and highlight clues to avoid them. However, Scam Busters targets younger audiences and exclude adult or elderly audiences who are more often targets of scams. The categories are also limited, and do not encompass modern, more complex scams such as ransomware, scareware, and impersonation scams.

Another initiative is ScamSpace (ScamSpace, 2024), which is a platform designed to help users avoid scams on social media platforms like TikTok. It offers a gamified approach to learning about scam detection, where a player progresses through a module-based learning tree and navigates a simulated interactive TikTok feed, differentiating between scams and legitimate content. *RWR* takes a broader approach, presenting scams on multiple common media formats such emails and SMSes as opposed to solely being focused on specific social media platforms. This multimodal engagement allows players to develop nuanced scam detection skills that adapt to various contexts.

RWR is also differentiated from other initiatives by weaving scam prevention skills into an engaging narrative-driven game. Unlike traditional educational tools that deliver content unilaterally, *RWR* provides dynamic, time-sensitive scenarios that mimic real-world scams, and challenges players to identify and avoid them. By blending experiential learning and entertainment, *RWR* makes scam prevention education active, memorable, and enjoyable, while fostering a players practical scam-identification skills.

3 GAME DESIGN AND DEVELOPMENT

RWR is a single-person role-playing game (RPG) where players are required to distinguish between scams and legitimate opportunities in order to progress. The game was designed to equip players with real-world skills in a simulated, risk-free environment. This section will cover the design and development of *RWR* with an emphasis on creating an interactive, narrative-driven environment.

Figure 1: Scenario development in tutorial for Macs upon game start.

3.1 Narrative and Scenario Development

RWR starts by introducing the Macs, an entrepreneur (Figure 1) who is presented with numerous "investment opportunities". Some are legitimate and will make Macs wealthier while others are scams that will drain Macs of his hard-earned wealth. The player's objective is to grow Macs' wealth to $100,000 from a starting capital of $25,000 by identifying and avoiding scams while responding to legitimate opportunities within a time limit. Scams range from impersonation, phishing, bogus investments and ransomware that mimic common scam tactics in Singapore documented in recent studies (Singapore Police Force, 2024). These scenarios allow players to experience the subtleties of real scams in a safe setting, while learning transferrable skills to recognize similar scams in their personal lives.

3.2 User Interface and Experience (UI/UX) Design

RWR was designed to simulate real-life devices and contexts. Interfaces were designed to resemble real-world interfaces, using similar themes, fonts and art styles. A sketch-inspired style was used for a more casual feel compared to traditional modes of education. Interfaces were also intentionally kept minimal and user-friendly for clarity, allowing a player to focus on the core gameplay - reading and making decisions on text-based content. Interactive objects are marked with a simple orange outline. Game directions are provided through an interactive tutorial that is loaded upon game start (Figure 2). Overall, the game was designed to be minimal and clear, to increase accessibility for different audiences. This is supported by previous research indicating that well designed UI/UX in educational games can significantly enhance knowl-

edge retention by reducing cognitive load and increasing engagement (AnNing et al., 2024).

Figure 2: User interface design in tutorial for Macs upon game start.

3.3 Gameplay Mechanics

RWR employs time-bound, decision-making tasks to simulate real-world scams. The time element is added to add gameplay pressure and simulate real-life, where an individual is presented with scams while occupied with other tasks. Players are thus required to quickly analyze in-game prompts to distinguish between legitimate opportunities or fraudulent scams and progres in the game (Figure 3).

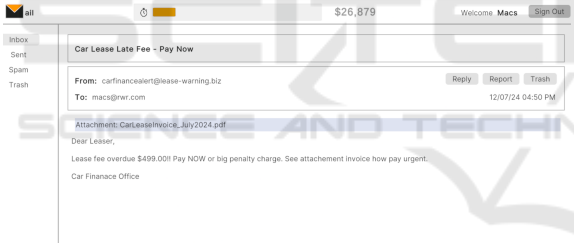

Figure 3: A fraudulent email example of an invoice scam.

This mechanic aligns with active learning principles, where engagement in decision-making boosts memory retention and real-world application (Laine and Lindberg, 2020). Progress is measured using an in-game money system that rewards players for correctly identifying legitimate opportunities and penalizes players for ignoring legitimate opportunities or responding to fraudulent scams. This also encourages re-playability and enhances learning through a frequent feedback loop.

3.4 Content Generation

A mix of manual writing and various algorithms is used for content generation.

3.4.1 Newspaper Content

The Newspaper interface presents static content which a player can access through the main scene to learn about common scams types that show up in the game. This is manually written from research conducted by the team.

3.4.2 Email & SMS Challenges

Email & SMS challenges are randomised using a generative algorithm that randomly selects and mutates content from a repository of template emails/SMSes generated using GPT-4 and manually vetted by the authors.

Each email is broken into descriptive fields of “sender”, “title”, “body”, “date”, “attachment” (optional), and functional fields of “isScam”, “hackable”, “daysLeft” etc. which allows for both content and logic to be generated based on a single email object in the repository, and also allows for field-specific mutations to be made by the email generation algorithm. Mutations include randomly creating typographical errors (e.g. modifying an email’s local part before the symbol, modifying a legitimate sender’s name that closely resembles the original name) The algorithm also tags each email object generated with a category (e.g. phishingScam), which allows the team to implement game and separate database logic to track and analyze a player’s response to different scam types.

Similarly, each SMS is also composed of descriptive and game logic fields such as “sender”, “recipient”, “body”, “isScam” etc. Likewise, this allows for field-specific mutations to be applied, and game-logic to be created from an SMS object in the repository.

Lastly, the frequency of email & SMS generation is also randomized using an exponential probability function which increases the likelihood of challenges as the game day progresses. The reward/penalty of an challenge response is randomly determined at “runtime”, i.e. when a player makes a decision.

3.5 Iterative Development and Testing

RWR was developed iteratively across three phases - Alpha, Beta and Gold. Each iteration was tested by the authors’ coursemates. The feedback was used to improve narrative, game mechanics and overall gameplay flow. A weekly development blog was also maintained. Iterative development has been shown to enhance user satisfaction in educational games, particularly when feedback is used to adjust game complexity and usability (Viudes-Carbonell et al., 2021).

3.6 Education Framework

The game's design is grounded in experiential learning theory, which posits that individuals learn best by transforming theoretical knowledge into practical skills, thereby enhancing the likelihood of real-world application (Kolb, 1984). The narrative-driven design of *RWR* maps seamlessly onto Kolb's (Kolb, 1984) Experiential Learning Cycle. Players are introduced to realistic scam scenarios (Concrete Experience), encouraged to reflect on their choices through directed feedback (Reflective Observation), equipped with abstract principles for scam detection via in-game content (Abstract Conceptualization), and challenged to apply these strategies in progressively complex situations (Active Experimentation). This alignment ensures that the learning experience is not only engaging but also theoretically grounded, promoting deeper knowledge retention and real-world applicability. Research has further shown the efficacy of experiential learning in educational settings, with a study suggesting that experiential learning activities have significantly improved student's ability to apply theoretical concepts in practice (Sarah Yardley and Dornan, 2012). Similarly, a meta-analysis has demonstrated that interactive learning methods, such as simulations and role-playing, effectively enhance learners' critical thinking and problem-solving skills (Rogers, 2015). In the context of scam prevention, interactive learning tools have been shown to increase awareness and preparedness. With academic literature on game design framework revealing that mobile games designed to teach phishing awareness led to a significant improvement in users' ability to identify fraudulent emails (Arachchilage and Love, 2013).

The following were implemented to achieve the learning objectives:

1. **Concise, Static Newspaper Content.** In the Newspaper of the Main Scene, the team has included extremely concise information about different types of scams. By focusing only on: (i) What are these scams; (ii) How they manifest; and (iii) How to avoid them; Players can read about scams and refer to this for gameplay aid.
2. **Scam Detection as Core Gameplay.** The core gameplay mechanic replicates real-life scams, allowing players to train their "scam detection" instincts; this lets them respond to actual scams better. The game is also intentionally fast-paced, to replicate real life conditions - where a player is often presented with scams in their hectic lives. Lastly, the game also simulates for a player what happens in reality should they fall for a scam - they lose more money than they've earned.
3. **Directed, Instantaneous Feedback.** The game also provides directed, informative feedback immediately after the player makes a decision, i.e. if a player falls for a scam, the game explains to the player in the post-decision prompt about why the Email or SMS was a scam and how they could have detected it. This directed feedback allows players to be more aware of the scams they are likely to fall for, and how they can detect and avoid it in the future.

4 EVALUATION FRAMEWORK

The evaluation framework assesses *RWR*'s effectiveness in educating players on scam awareness and prevention strategies. This section outlines the key metrics and the methodology used to gauge the educational impact of the game.

4.1 Evaluation Metrics

To measure *RWR*'s impact quantitatively, our team has developed 45 key metrics (shown in Table 1l) that aligns with both educational and interactive learning goals in three broad categories:

1. **Scam Detection Skills**, which focuses on evaluating players' abilities to recognize and respond to scams. These include the accuracy of scam identification, frequency of legitimate emails correctly identified, the different platforms (e-mail or SMS) being engaged, and the total number of emails and SMS sent within an in-game day;
2. **Time Element**, which analyzes the time taken for player to respond to an email or SMS event generated, number of in-game days that the player has spent within the game (as retention rate), and time taken to respond correctly. These provide insights into how time constraints influence learning retention and decision-making speed, which complements with the Scam Detection Skills category metrics and is essential in real-life scam prevention where quick decisions are needed;
3. **Overall Gameplay**, which evaluates the broader aspects of player engagement by tallying whether the player has been able to achieve the goal objective easily with the UI/UX design and scenario development. These metrics ensure that the game remains user-friendly and engaging, as a high score indicates that the game has provided an effective and enjoyable learning experience for players.

[1] Available at https://metaverse.comp.nus.edu.sg/projects/rwr.

Table 1: Excerpt of part of the 45 metrics suite collected into MongoDB. Full list of variables available in Table A1 of the appendix [1].

GameDay	TotalEmails-Received	CorrectEmails-Identified
ScamEmails-Identified	MissedEmails	TotalPhoneSMS-Received
CorrectPhone-SMSIdentified	ScamPhoneSMS-Identified	MissedPhone-SMS

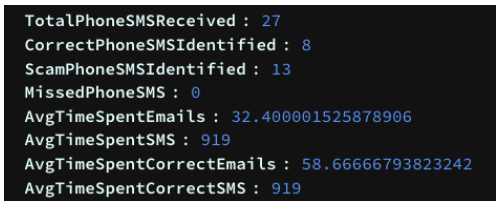

Figure 4: Example of the actual data collected for some of the metrics.

At the end of every game day, all evaluation metrics for that game day are collected and stored in an online MongoDB Atlas NoSQL database, preparing the dataset for further processing and analysis (Figure 4). By implementing real-time data collection alongside conventional survey methods, this measure improves both the volume and accuracy of data gathered for analysis. This layered approach enables a more consistent and quantitative understanding of player performance, reducing biases which may arise from conventional survey methodologies.

4.2 Evaluation Methodology

The learning outcomes were evaluated using quantitative in-game metrics and pre- and post-game surveys, to accurately assess users' before and after understanding of scams using specific scenario-based quiz questions (Figure 5).

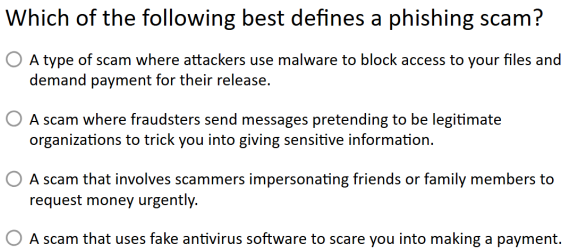

Figure 5: Pre-survey and post-survey quiz question on phishing scams.

The pre- and post-surveys included technical questions, such as identifying the warning signs of ransomware and recognizing the deceptive nature of scareware and incorporated scenario-based questions where players were asked to respond to situations like receiving an email about a suspicious login attempt on their account, testing their ability to identify the appropriate next steps.

The surveys also gauged players' self-reported understanding of different scams before and after playing the game, giving insight to whether players each feel that the game has "subjective helped" them understand scams better.

In combination, the surveys provided both objective (e.g. most effective educational elements in the game) and subjective (self-reported learning "gains") learning outcomes to gauge the effectiveness of *RWR* as a reliable interactive learning platform for scam awareness and prevention.

5 RESULTS

The results demonstrate that *RWR* has objectively and subjectively improved players' understanding and ability to identify scams. This section summarizes key findings from empirical data collected through in-game metrics, pre- and post-game surveys, and qualitative feedback, along with limitations and potential areas of improvements for future research on the use of interactive learning. 21 pre-survey responses and 12 post-survey responses for *RWR* and 74 player records were used to analyse player engagement and learning outcomes.

5.1 Pre-Game Survey Analysis

In the pre-survey, majority of respondents (47.6%) reported a very high level of understanding of common scam types, rating their knowledge as "very well" (5 out of 5-point scale). This response, along with 33.3% of respondents rating their understanding "well" (4 out of 5-point scale), reflects that the participanst are relatively confidence with their foundational awareness of scams prior to playing *RWR* (Figure 6).

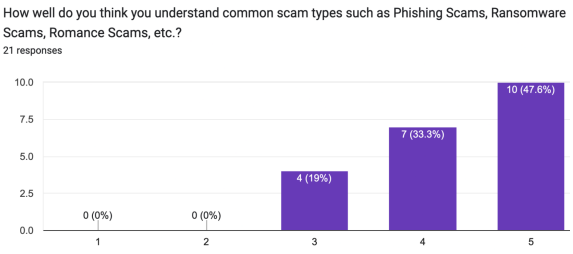

Figure 6: Pre-survey results for level of understanding of scams.

Prior to playing *RWR*, majority of respondents have encountered phishing (81%), fake invoices

(66.7%), scareware (61.9%), and impersonation (61.9%) scams (Figure 7). This shows that most players start with a certain level of real-world scam awareness. The game's design, therefore, builds on this familiarity by training players to respond faster and more accurately to scams they encounter.

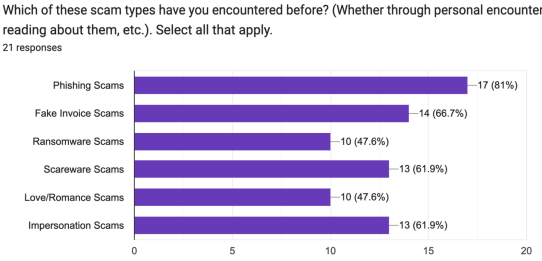

Figure 7: Pre-survey results for common scams encountered.

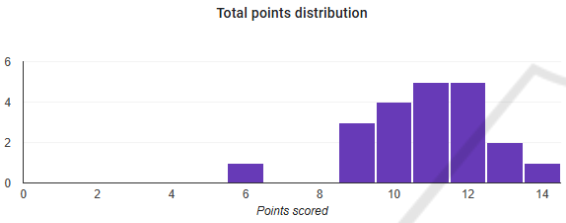

Figure 8: Pre-survey score distribution of scenario-based questions.

The pre-survey also assessed respondents' foundational knowledge of scams through a set of 15 multiple-choice questions, shown in Figure 7. The results showed a mean score of 10.86 and a median score of 11, suggesting that respondents generally possessed a good understanding of scams (Figure 8) before playing *RWR*.

5.2 In-game Survey Analysis

5.2.1 Scam Identifications by In-Game Days

To evaluate the progression in players' ability to correctly identify email scams across different days, we analyzed the distribution of the percentage of correctly identified emails for Day 1 and Day 2. Figure 9 illustrates this distribution, with separate histograms for Day 1 and 2.

The distribution of correct email identification percentages on Day 1 shows a wide spread, with prominent peaks around 20%, 40%, and 60%. The distribution indicates varied performance among players, with clusters of lower (20%) and moderate (40–60%) correct identifications. This spread suggests that players on Day 1 had mixed success in identifying email scams accurately, with a concentration around moderate success rates. The mean and median for Day 1 are 49.73% and 50%, respectively, indicating a relatively symmetrical distribution centered around the midpoint.

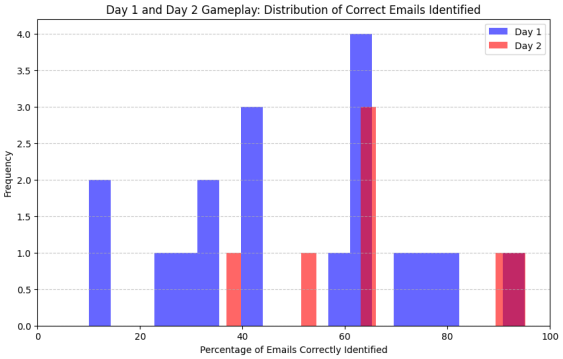

Figure 9: In-game survey results for correct emails identified.

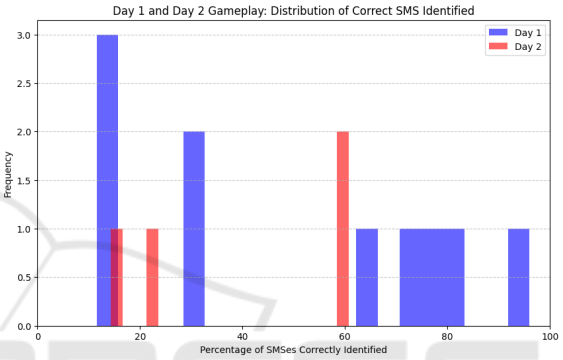

Figure 10: In-game survey results for correct SMS identified.

The distribution for Day 2 shows a noticeable shift, with higher concentrations in the 40–60% range, indicating an improvement in players' performance in correctly identifying emails. The clustering around these percentages suggests that more players were able to recognize email scams more accurately by Day 2, indicating a potential learning effect or familiarity with the game mechanics and scam cues. The mean and median for Day 2 were calculated as 66.75% and 63.16%, respectively, both values higher than those for Day 1. The increase in both mean and median points to an overall improvement in correct email identification skills.

The findings demonstrate an improvement in players' ability to identify email scams. The concentration of Day 2 results around the higher percentages, along with increased mean and median values, suggests that players were able to more accurately identify email scams over time; this reflects learning and/or adaptation, where repeated gameplay or feedback may have enhanced players' detection skills.

In addition to email identification, we analyzed players' performance in identifying SMS scams across both days. Figure 10 provides a distribution of the percentage of correct SMS identifications for Day 1 and Day 2.

The distribution of correct SMS identification percentages on Day 1 is highly variable, with peaks around 20% and 60%. The clustering at 20% indicates that a significant portion of players had difficulty in accurately identifying SMS scams, suggesting that they may have struggled with recognizing scam indicators in SMS messages. However, there are also players with higher correct identification rates, up to 60%, indicating some players were relatively successful despite the general challenges.

The distribution for Day 2 shows a concentration around the same lower and moderate percentages, with fewer instances above 60%. Despite the slight presence of players who achieved moderate success, the distribution reveals a lack of significant improvement from Day 1, as reflected in the overlapping clusters at lower ranges. This consistency across days implies that players' ability to identify SMS scams may have reached a plateau, or that SMS scams were inherently more challenging to identify compared to email scams. Both the mean and median for SMS identification across days remained relatively indifferent, further supporting the observation of minimal progression in SMS identification skills.

The analysis of SMS identification results indicates limited improvement between Day 1 and Day 2. Unlike email identification, where players demonstrated noticeable progress, the SMS identification data reveals continued challenges, with little indication of a learning effect. This finding suggests that identifying SMS scams requires more nuanced understanding or targeted support, as players did not show the same level of adaptation observed in email identification.

Notably, the majority of real-time records were concentrated in the early stages of gameplay, with 27 entries from the first in-game day (17 entries on emails, and 10 on SMSes) and 11 from the second (7 on emails and 4 on SMSes). This distribution indicates a natural decline of player count as the game progresses. The players are also more willing to engage with the email contents as compared to SMSes. We mention this in Section 5.5.

These findings suggest that players may inherently find email scam cues more discernible, whereas SMS scams require more nuanced interpretation, which may not be readily learned through simple repetition.

5.2.2 Scam Identification by Type

The in-game metrics also examines the frequency of incorrect identifications by scam category in both email and SMS formats, (Figure 11 and Figure 12).

In email challenges, **Phishing** (10 errors), **Scareware** (12 errors), and **Impersonation** scams (10 errors) were the most challenging for players, reflecting the deceptive nature of these scams. The high error rates suggest that players found it difficult to distinguish these scams from legitimate emails. In contrast, Invoice scams were incorrectly identified only once, suggesting they were more easily recognized, likely due to distinct indicators relating to financial documentation.

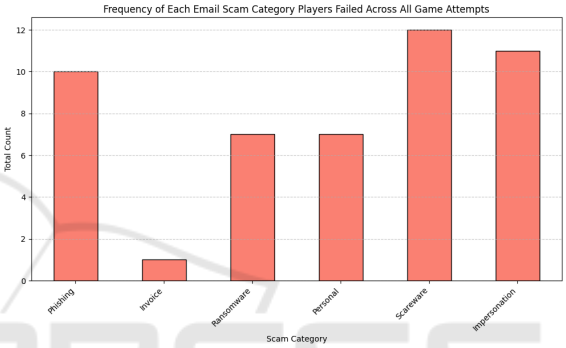

Figure 11: In-game survey results for common e-mail scam mistakes by players.

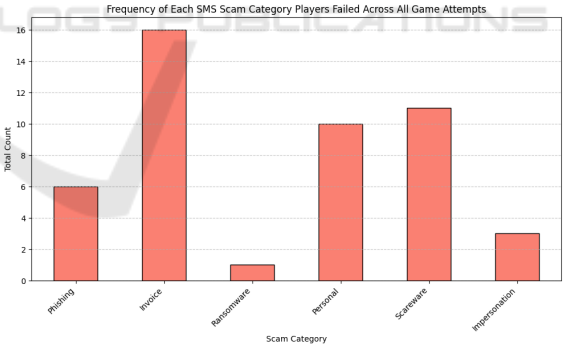

Figure 12: In-game survey results for common SMS scam mistakes by players.

As for SMSes, **Invoice scams** had the highest error rate (16 errors), significantly higher than in emails, indicating that players struggled to recognize financial scams in SMS form. **Scareware** (10 errors) and **Personal scams** (8 errors) also had high failure rates, similar to email results, suggesting consistent difficulty across formats. **Phishing** (6 errors) was somewhat easier for players to identify in SMS, while **Impersonation** and **Ransomware scams** had lower error rates (3 and 1 errors, respectively).

Players found Phishing, Scareware, and Impersonation scams challenging across formats, while SMS-specific challenges were prominent in Invoice scams. These findings therefore suggest a need for targeted guidance in recognizing scams that exploit different mediums. Enhancing in-game cues for complex scam types, particularly in SMS format, may improve players' scam detection skills and overall learning outcomes.

5.3 Post-Game Survey Analysis

In the post-survey, a majority of respondents (66.7%) reported a very high level of understanding of common scam types, rating their knowledge as "very well" (5 out of 5 on a 5-point scale). Additionally, 25% of respondents in the post-survey rated their understanding as "well" (4 out of 5). This reflects an improvement of distribution from the pre-survey, indicating enhanced awareness and confidence (Figure 13). These results suggest that *RWR* has contributed meaningfully to deepening players' foundational knowledge of scams, with a clear increase in participants reporting a high or very high level of understanding after gameplay.

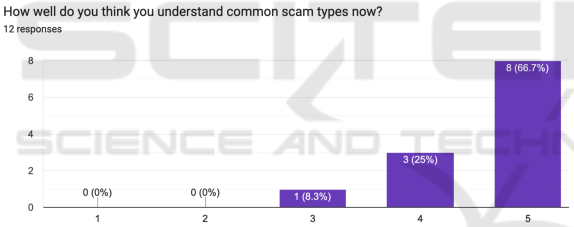

Figure 13: Post-survey results for level of understanding of scams.

Furthermore, reflecting on their knowledge before playing the game, a majority of respondents (50%) admitted that their foundational understanding of scams had been only moderate (3 out of 5 on a 5-point scale) (Figure 14). This retrospective assessment, contrasted with the pre-survey data, where the majority were confident about their understanding (47.6% rated as "very well", or 5 out of 5), suggests that *RWR* provided meaningful learning experiences that helped participants' increase the scam awareness. The shift in awareness underscores the game's effectiveness in enhancing players' confidence and understanding of common scam types.

The post-survey also evaluated respondents' foundational knowledge of scams using the same set of fifteen multiple-choice questions. The results revealed a mean score of 11.17 and a median score of 12, showing a slight improvement from the pre-survey mean

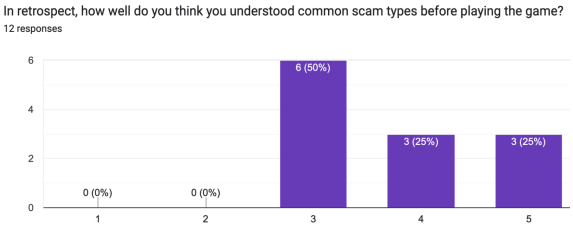

Figure 14: Post-survey results for level of understanding retrospectively.

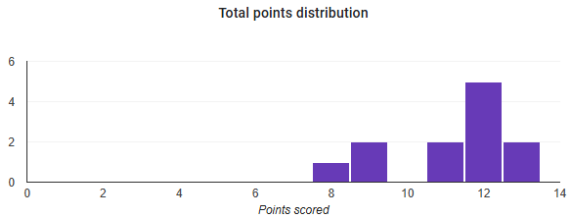

Figure 15: Post-survey score distribution of scenario-based questions.

of 10.86 and median of 11 (Figure 15). This increase suggests that participants not only retained their baseline knowledge but also enhanced their understanding of scams and their mechanisms after playing *RWR*.

5.4 Observational Findings and Hypothesis

The main hypothesis was that playing *RWR* would objectively improve players' ability to discern scams from legitimate communications. This was tested by comparing players' accuracy in scam identification over two Game Days. The in-game metrics support this - players showed a slight improvement in response accuracy (Correct responses to emails/SMS-es out of total responses) on Game Day 2 versus Game Day 1. Likewise, pre- and post-survey data supported these findings, where respondents' minimum mean and median scores increased after gameplay, which indicates player learning and improvement in scam identification. As such, *RWR* did improve players' abiity to discern scams.

The second hypothesis proposes that players will better understand common scam types after playing *RWR*. Compared to the previous hypothesis which was observed objectively, this hypothesis is supported by subjective observations - respondents expressed an improvement in their self-assessed understanding of common scam types post-game, and indicate that they earlier overestimated their understanding of scams.

Both hypotheses are supported by the in-game metrics and surveys, suggesting that *RWR* is effective in educating players on scams and scam identification.

5.5 Areas of Improvements

An initial hypothesis was that playing the *RWR* would train players to respond faster to scams they encounter. However, player metrics do not show a marked improvement in response times between Game Day 1 versus Game Day 2. From the extremely short response times, players could also have reacted impulsively rather than thoughtfully. Further development is required to increase engagement, and more data is required for analysis.

Due to time constraints, a major limitation is the relatively small dataset for analysis - only 27 entries were recorded for Day 1 and 11 for Day 2. Some players also only engaged with one medium (SMS or email), distorting the data collected. More player testing is required to bolster the findings.

RWR can also be developed to include progressive difficulty depending on the player's progress and response times. This can improve retention rate by posing more challenging scenarios to well-informed players, and reduce impulsive decision-making by posing longer prose to players who react impulsively (short response time + incorrect answer). Data collected will be more reflective of a player's learning progress.

A more well-developed narrative with a branching storyline dependent on the player's decisions (akin to "personality tests" or "determine your fate" style of games can also be implemented to engage a player better, and in turn increase retention and reinforce learning over time.

Lastly, more comprehensive in-game feedback can be provided to a player to reinforce learning, retain players, and make players feel a better sense of enrichment. For example, in-game metrics can be analysed and shown to a player at the end of every Game Day - their improvement in response time, scams most vulnerable to, etc.

6 CONCLUSIONS

RWR is a significant step towards the field of interactive learning for scam prevention, by contributing to the growing body of research on the intersection of gamification and cybersecurity education. *RWR* also demonstrates the tangible impact that thoughtfully designed educational games can have on societal challenges. Through its engaging narrative, realistic scenarios, and decision-based gameplay, the game equips players with the practical skills needed to recognize and respond well to various scams. Empirical studies reaffirm the success of *RWR* in enhancing scam awareness and its response, which demonstrates the overall effectiveness of interactive learning as a platform to raise public awareness on scams. Our team hopes that *RWR* serves as a prelude to help liaise with related authorities to increase the impact of combating the proliferation of fraudulent scams.

REFERENCES

AnNing, Ahmad, M., and Ibrahim, H. (2024). User-centered mobile app design for education: Enhancing engagement and learning outcomes. *ESP International Journal of Advancements in Science & Technology*, 2(1).

Arachchilage, N. A. G. and Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706–714.

Chua, N. (2024). Scam victims in s'pore lost $651.8m in 2023, with record high of over 46,000 cases reported.

Dass, D. (2021). Police life: The anti-scam centre: A collaborative approach against scams.

Kolb, D. (1984). *Experiential Learning: Experience As The Source Of Learning And Development*, volume 1. Prentice Hall.

Laine, T. H. and Lindberg, R. S. N. (2020). Designing engaging games for education: A systematic literature review on game motivators and design principles. *IEEE Transactions on Learning Technologies*, 13(4):804–821.

MoneySense (2021). Scam busters.

National Crime Prevention Council Singapore (2024). Xiam the scams.

Rogers, D. T. (2015). Further validation of the learning alliance inventory: The roles of working alliance, rapport, and immediacy in student learning. *Teaching of Psychology*, 42(1):19–25.

Sarah Yardley, P. W. T. and Dornan, T. (2012). Experiential learning: Transforming theory into practice. *Medical Teacher*, 34(2):161–164. PMID: 22288996.

ScamSpace (2024). Your child's safety on tiktok starts here.

Singapore Police Force (2024). Mid-year scams and cybercrime brief 2024.

Tay, S. and Teiw, Y. K. (2023). Phishing for a job? investigating scam victimisation and interventions in singapore.

Viudes-Carbonell, S. J., Gallego-Durán, F. J., Llorens-Largo, F., and Molina-Carmona, R. (2021). Towards an iterative design for serious games. *Sustainability*, 13(6).