International Multidisciplinary Research Journal
ISSN: 2424-7073
Available Online at https://imrjournal.info/
Volume:3; November 2025; Page No.32-44
DOI: https://doi.org/10.47722/imrj.2001.52

Research Article

DEVELOPMENT OF A SMARTPHONE GAME APPLICATION FOR INFORMATION SECURITY EDUCATION

Yoshiyuki Kido[1,3]; Kento Fujimoto[1]; Tomohiro Hamano[2]

[1]Graduate School of Science and Engineering, Okayama University of Science, Okayama, Japan
[2]Active Learners Course, Okayama University of Science, Okayama, Japan
[3]D3 Center, The University of Osaka, Osaka, Japan

ARTICLE INFO

Article History:

Received 15.08.2025
Accepted 15.10.2025
Published 20.11.2025

Keywords:

Security Educational Game,
Gaming Education,
Smartphone Game Application

ABSTRACT

The use of information devices on the Internet poses security risks, such as the leakage of personal information and account hijacking. One of the primary causes of these issues is the use of weak passwords and password leakage. However, if users possess knowledge about password strength, they can prevent the creation of weak passwords. In Japan's primary education system, students use information devices to distribute class materials and share contacts. Therefore, providing information security education to young people is of utmost importance today.

On the other hand, there is a field known as gaming education. Gaming education is an instructional method that incorporates games into learning to enhance students' understanding and motivation. In this study, we developed an educational information security game, Mallory in Secured Office, which runs on smartphones and is designed for young users. The game is structured as an escape game set in a corporate office. The objective is to escape from the office while encountering information security challenges that could arise in such an environment. We evaluated the game with 22 participants using completion time measurements and a questionnaire survey. The results showed that players were able to engage with the topic of password management, and survey responses indicated increased interest and understanding of proper password handling.

I. Introduction

Information devices such as computers and smartphones are now widely used, with many people connecting them to the Internet for activities such as using social networking services (SNS) and shopping sites. However, connecting these devices to the Internet poses numerous information security risks, potentially causing harm to users, their families, and the organizations they belong to. Some common information security risks include the leakage of personal information, account hijacking, and identity theft (Blakely *et al*., 2009). These issues often stem from factors such as the use of weak passwords and password leakage. However, the likelihood of such problems can be significantly reduced by following simple security practices, such as avoiding easily guessable passwords and not leaving written passwords in visible places. Therefore, learning about information security is an effective way to minimize potential harm to users, their families, and their organizations.

Information devices are also used in primary and secondary education in Japan for digital textbooks, distributing lesson materials, conducting research during classes, and sharing contact information. However, their use can lead to issues related to information security and ethics in the educational environment.

These problems stem from users' low level of information literacy. As the age at which people begin using information devices continues to decrease, providing information security education to young people is considered extremely important. On the other hand, there is a field known as gaming education. Gaming education is an instructional method designed to enhance students' understanding and motivation by incorporating games into the learning process (Kiilli, 2005). Even when the content is inherently difficult, integrating it into a game allows students to engage with the material while maintaining their motivation to learn. Many analog games have been developed for information security education. However, analog games are constrained by factors such as location and the number of participants, requiring a dedicated space and often necessitating group play. In contrast, digital games can overcome these limitations by offering greater accessibility and flexibility. Password management was chosen as the initial focus of this prototype because it is a universal and foundational security concept that affects all users. Moreover, it lends itself naturally to a puzzle-based game format, making it suitable as the first topic for an educational game. Therefore, in this study, we developed an information security education game, Mallory in Secured Office, aimed at young people. This smartphone-based game focuses on the theme of password management and is designed to provide an engaging and educational experience. The remainder of this paper is structured as follows: Section 2 discusses related research and identifies the challenges and requirements for developing our game. Section 3 details the design and implementation of Mallory in Secured Office. Section 4 evaluates the game using completion times and a questionnaire to assess its effectiveness. Section 5 concludes this paper.

2. Related Work and Problem Identification

This section discusses related research on games designed for information security education and identifies the challenges and requirements for the development of our game.

2.1 Physical Board Game

Henriksen-Bulmer *et al*. (2024) explore the use of game-based learning to teach young people (ages 16–25) about privacy and online safety. Recognizing the increasing exposure of youth to online risks, the researchers developed a physical board game designed to passively educate players about managing information, cyberbullying, online reputation, privacy, and security. Drawing inspiration from games like Trivial Pursuit and Snakes and Ladders, the game integrates quiz-style questions based on real-world concerns gathered through surveys.

The game was tested with 27 university students in focus groups. Pre- and post-game surveys indicated that players' confidence in managing privacy risks improved across all categories, especially in managing personal information and understanding online relationships. Participants found the game easy to play, engaging, and educational. The study concludes that game-based learning is an effective method for raising digital literacy among young people in a fun, non-threatening way.

Although the evaluation was limited to older youth due to COVID-19 restrictions, future plans include developing a digital version and expanding the game to reach broader demographics. Overall, this research demonstrates that gamification can be a powerful tool to improve online safety awareness in young audiences.

2.2 Capture the Flag

Capture the Flag (CTF) is a cybersecurity competition where teams are simultaneously responsible for attacking opponents and defending their own systems (Cowan *et al.*, 2003). Each team is assigned a server that contains a "flag," typically a special file or secret value. The primary goal of the competition is to protect the team's own flag while attempting to compromise and replace the flags on other teams' servers.

In the Defcon CTF 2002 event, the rules made the challenge particularly demanding. Teams were given a deliberately vulnerable reference system at the start of the game without being informed which specific services needed to remain operational. They were required to maintain those hidden services properly while defending against relentless attacks from other teams. To discourage denial-of-service tactics and reckless scanning, penalties were applied for excessive network traffic. Furthermore, teams could only earn points by both maintaining full functionality of their own services and successfully replacing an opponent's flag, emphasizing the need for a balanced approach between offense and defense.

Unlike simple hacking contests that focus only on penetration skills, this form of CtF tests comprehensive cybersecurity abilities, including system hardening, real-time defense under attack, service maintenance, and strategic thinking. It compresses the real-world challenges of cyber defense into an intense and competitive environment.

2.3 Secu-One

Omiya & Kadobayashi, (2019) present Secu-One, a cyber security exercise tool designed to address the shortage of skilled cyber security personnel and the need to maintain their motivation. Unlike traditional technical-focused exercises like CTFs, Secu-One emphasizes management skills necessary for system operation, such as risk assessment, incident handling, and operational security management. Built using the ADDIE instructional design model, Secu-One uses a gamified card-based approach where players match defense cards against cyber attack scenarios. The cards are based on real-world standards and attack libraries like CSC, ATT&CK, and CAPEC.

Through exercises with students and professionals, Secu-One demonstrated effectiveness in improving participants' knowledge and motivation, measured using the ARCS motivational model and MEEGA+ evaluation (Petri *et al.*, 2017). Participants engaged actively, showed increased understanding of cybersecurity management, and benefited from discussion-based learning. Evaluation results showed that Secu-One performed as well as or better than existing tools in terms of motivation and learning impact

Secu-One fills a gap in current cybersecurity training by offering a structured, interactive, and management-focused exercise environment. Future improvements include regular updates to attack and defense libraries, refining materials based on feedback, and developing standalone learning tools for broader use.

2.4 Security Defense & Dungeons

Kido *et al*. (2020) present sD&D (Security Defense and Dungeons), a cybersecurity educational board game designed to raise cybersecurity awareness while offering scalability and flexibility for different scenarios. Developed by Osaka University researchers, sD&D teaches players about cybersecurity threats, network behaviors, and countermeasures through an interactive, team-based game environment. Players navigate rooms (trap, resource, and task rooms), collect and use security tool cards, and experience simulated cyber-attack scenarios such as DNS cache poisoning.

The game focuses on being intuitive and accessible for a broad audience, especially young users and beginners. Unlike traditional cybersecurity competitions like CTFs, sD&D offers a more approachable, scenario-driven way to understand complex concepts like authentication, access control, and attack detection. Scalability is achieved through XML-based configurations, allowing easy addition of new cards and scenarios without modifying the game's core system.

User studies with students showed positive feedback, indicating that sD&D improved their cybersecurity knowledge and awareness, although improvements were suggested for initial instruction clarity. Overall, sD&D demonstrates that game-based learning can effectively teach cybersecurity principles, even in resource-limited environments.

2.5 Identified Problems

The existing research has the following limitations: Secure One or physical board games, a multiplayer analog card game, is restricted in terms of where it can be played. It cannot be played in transit, such as on a bus or train on the way to school. Additionally, it requires three to four players and a game master, imposing strict constraints on the number of participants and location. As a result, it is not suitable for casual play during free time, such as between classes or while commuting. sD&D, a digital PC-based game, can be played alone, making it more flexible in terms of location. However, since it primarily consists of answering quizzes about information security, it does not provide an interactive experience of real security threats. In addition to that, CTF is a highly competitive game, so beginners need a learning phase, such as a tutorial, to learn it. To further clarify the positioning of our work, Table 1 compares existing security education games and tools across platform, multiplayer capability, mechanics, and focus.

Table 1 - Comparison of Security Education Games

Game / Tool	Platform	Multiplayer	Core Mechanic	Educational Focus
Physical Board Game	Board / Analog	Yes (3–4)	Quiz questions, board movement	Online safety, privacy, cyberbullying
Capture the Flag (CTF)	PC / Networked Comp	Yes (Teams)	Attack & defend servers	Advanced cybersecurity skills, penetration & defense
Secu-One	Card-based Exercise	Yes	Defense cards vs. attack cards	Security management, risk assessment, incident handling
sD&D	PC (Digital Game)	Yes (Single available)	Navigate rooms, security cards	Cybersecurity threats, authentication, access control
Mallory in Secured Office (Our Approach)	Smartphone (Android)	No (Single)	Escape game, password puzzles	Password management, basic information security

2.6 Design Requirements

To address these issues, the information security education game Mallory in Secured Office, developed in this study, must meet the following requirements:

I. Accessibility & Flexibility - The game should be playable in short, casual sessions without location restrictions, allowing users to play while commuting or during free time.

II. Interactive Learning of Security Concepts - The game should provide an interactive experience that allows players to encounter and respond to realistic information security threats.

3. Design and Implementation

Mallory in Secured Office is designed as an escape-style smartphone game set in a single office environment. The objective of the player is to escape from the office by solving puzzles while encountering information-security issues focused on password management. The design emphasizes short and accessible sessions that can be played casually, meeting the needs of young learners in everyday contexts. This section explains the game structure, the educational moments, the password list attack mechanic, the implementation details, and how the design fulfills the requirements identified in Section 2.

3.1 Game Structure

The game takes place entirely within an office stage. Players explore different spots within the office, such as desks, PCs, and shelves, interact with objects, and collect password-like strings. Among several candidate strings, only one is the correct password required to unlock the exit door. This structure supports short, repeatable play sessions on smartphones without the need for multiple levels or scenarios.

Screenshots of the game are shown in Figures 1-4. Figure 3 illustrates the play field where the player navigates the office environment to search for password-related clues. Figure 4 shows an event screen that provides explanatory messages when a clue is found. By discovering the correct clues, the player can unlock the exit and successfully escape from the office.

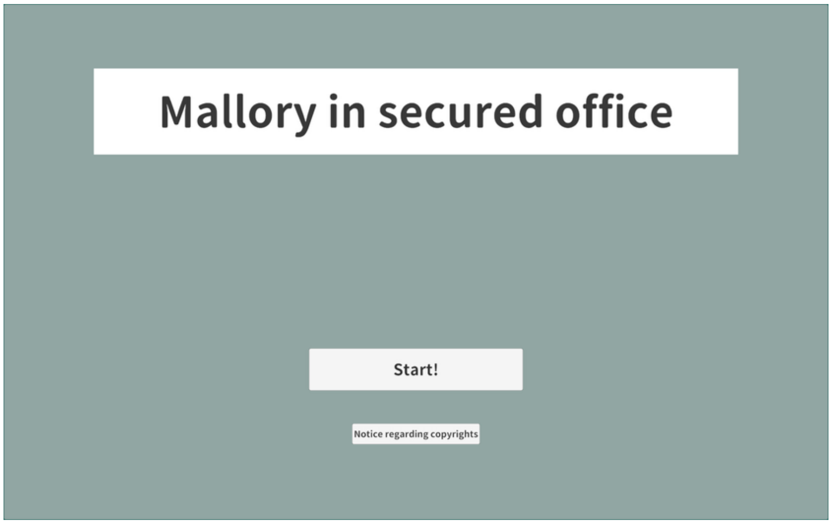
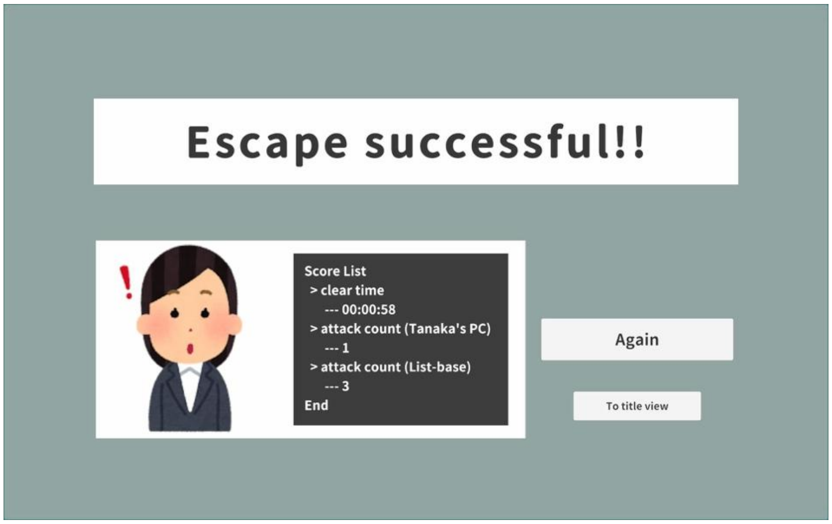


Figure 1: Opening screen



```
Score List
 > clear time
    --- 00:00:58
 > attack count (Tanaka's PC)
    --- 1
 > attack count (List-base)
    --- 3
End
```

Figure 2: Ending screen

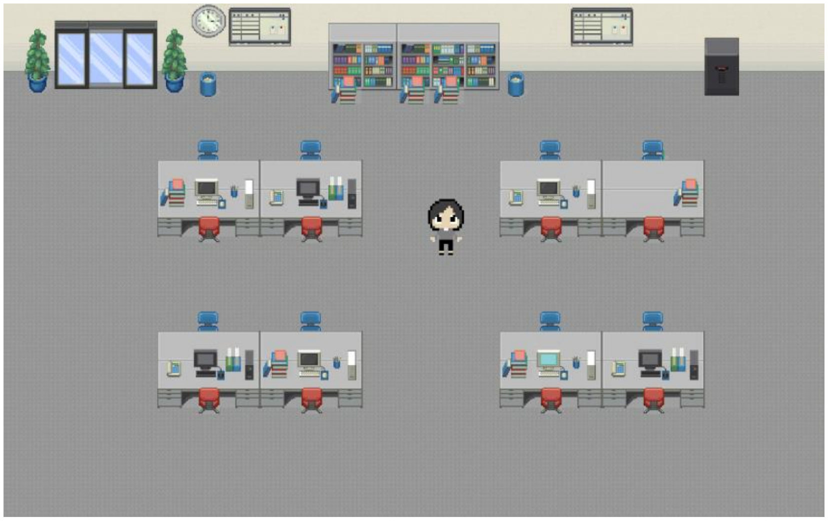
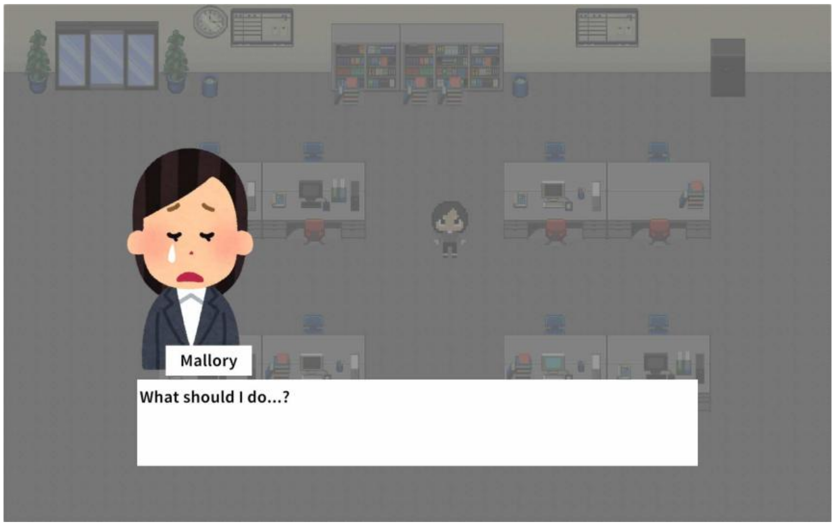


Figure 3: Play field



Mallory

What should I do...?

Figure 4: Event screen

3.2 Educational Moments

"Educational moments" are embedded at points of interaction. When a player inspects an object or acquires a candidate password, a concise, context-aware message is displayed to explain the (in)security of that choice.

- Example 1: On acquiring "Company123"
  "Using the company name makes a password easy to guess. Avoid including personal or publicly known information."
- Example 2: On acquiring "12345678"
  "Simple numeric sequences are highly vulnerable. Use a mix of letters, numbers, and symbols."
- Example 3: On acquiring "Qwerty2024!"

> "Keyboard patterns are predictable even with a year or symbol. Prefer passphrases with unrelated words."

These immediate, localized explanations connect in-game actions to security principles at the moment of decision, reinforcing correct practices.

3.3 Password List Attack Mechanic

After gathering several candidate strings, players attempt to use them as a password list to unlock the exit. This mechanic is not intended to train offensive techniques. Instead, it simulates the attacker's perspective in a simplified and controlled way. By observing how weak passwords are quickly compromised once they are included in the list, learners gain an appreciation of the importance of creating strong and unique passwords.

3.4 Password List Attack Mechanic

The prototype was implemented as a smartphone game for Android devices. The office environment and interactable objects were developed as modular components, each with hooks for triggering explanatory messages and generating candidate passwords. The explanatory-text subsystem and the password-list module were designed to be extensible, so that additional content such as phishing scenarios or multi-factor authentication can be incorporated in the future. The system also records anonymized interaction logs (e.g., object inspected, message displayed, password candidate chosen) to support evaluation and analysis.

3,5 Compliance with Design Requirements

Requirement I: Accessibility and Flexibility.

The smartphone-first design and the single-office stage allow gameplay in short sessions without restrictions on location or the number of participants. All interactions are touch-based and suitable for small screens, which ensures ease of access for young learners.

Requirement II: Interactive Learning of Security Concepts.

The game design emphasizes interactive learning. Immediate feedback through educational moments connects in-game exploration with security knowledge, while the password list mechanic provides an intuitive understanding of how attackers exploit weak passwords. Together, these elements make abstract concepts concrete through experiential learning.

4. Evaluation

In this section, we evaluate the preliminary usefulness of Mallory in Secured Office by measuring the game's completion time and conducting a questionnaire. In the experiment, 22 undergraduate participants (aged 19–22) played Mallory in Secured Office. During the session, we recorded their completion times and collected responses through a questionnaire survey.

4.1 Completion Time

Participants were asked to play Mallory in Secured Office, and their completion times were recorded. The measurement period for completion time was defined as the interval from when the game screen first appeared until the player examined the opened exit. The completion time results are shown in Table 2. The maximum, minimum, average, and variance of the recorded completion times are also presented. Note that the variance is calculated in minutes. The average completion time was 7 minutes and 7 seconds, but the variance was large, at 15.96.

One reason for this large variance is the success or failure of the password list attack performed within the game. Among the password-like strings collected by exploring the office, only one is the correct password. Participants who discovered the correct password early had shorter completion times, while those who took longer to find it required more time to finish. When the completion time is short, participants collect fewer password-like strings, resulting in fewer opportunities to read the explanatory texts displayed with each string. Therefore, based solely on the completion times, it cannot be concluded that all participants engaged in equally effective learning.

Table 2 - Completion Time

	Completion Time
Maximum	19:54
Minimum	02:58
Average	07:07
Variance	15.96

4.2 Analysis of Questionnaire Results

To verify whether playing Mallory in Secured Office helped maintain or enhance participants' motivation to learn about password management, we prepared a questionnaire. After gameplay, all 22 participants were asked to complete the questionnaire. The questionnaire content is shown in Table 3, and the results are presented in Figure 5. Questions Q1 to Q4 were answered using a five-point Likert scale (from 1 to 5), while Q5 was an open-ended question requiring a free-text response. In Figure 5, the Y-axis indicates the number of responses. The Likert scale is defined as 1 = Strongly Disagree and 5 = Strongly Agree.

Table 3 - Questionnaire List

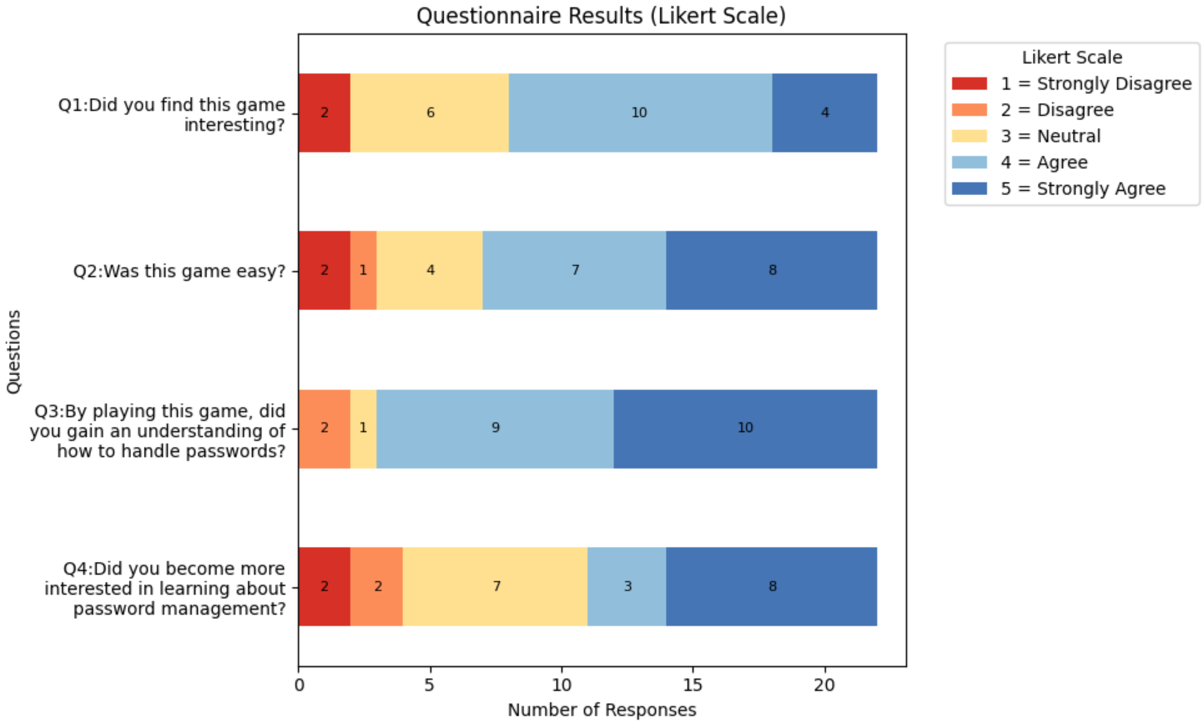
No.	**Question**
Q1	Did you find this game interesting?
Q2	Was this game easy?
Q3	By playing this game, did you gain an understanding of how to handle passwords?
Q4	Did you become more interested in learning about password management?
Q5	Please freely describe your impressions of the game.

The Likert scale results showed generally positive evaluations. The average scores were 3.9 for Q1 (interest), 4.2 for Q2 (ease of play), 4.5 for Q3 (understanding of password handling), and 3.7 for Q4 (increased interest). The median response was 4 for all four questions, indicating that most participants agreed or strongly agreed with the statements. These results suggest that the game was perceived as engaging and easy to play, and that it contributed to learners' understanding of password management.

Free-text responses to Q5 were obtained from 21 participants (one response was N/A). A thematic analysis was conducted to identify common categories of comments. The responses were grouped into four major themes: learning outcomes (11 responses), enjoyment or novelty (2 responses), usability and interface issues (7 responses), and game design improvement requests (4 responses). Examples of learning outcomes included comments such as "I realized that simple numeric passwords are insecure" and "I relearned the importance of password management in modern society." Enjoyment-related comments noted the novelty of the storyline, such as "collecting passwords and opening the door felt fresh." Usability issues highlighted difficulties with touch response or unclear controls, while design improvement requests suggested additional variation in gameplay or more suitable scenarios for younger learners. The full set of free-text responses to Q5 is provided in the Appendix for reference.

Overall, the majority of comments emphasized learning outcomes, supporting the quantitative results that indicated the game improved understanding of password management. At the same time, several responses pointed out usability challenges and suggested improvements, which provide useful directions for refining the prototype in future development.

Figure 5: Questionnaire Results



5. Conclusion

In this study, we developed Mallory in Secured Office, a prototype smartphone-based educational game aimed at introducing young people to information security, with an initial focus on password management. The game was designed as a short-session escape game that provides immediate educational feedback, making abstract security concepts more tangible through interactive gameplay. Our preliminary evaluation with 22 undergraduate participants demonstrated that the game was easy to play, engaging, and capable of raising awareness about the importance of password management. Quantitative results from the questionnaire showed average Likert scores of around 4 across all questions, with particularly high ratings for understanding password handling (Q3). Thematic analysis of free-text responses further supported these findings: most participants commented on what they had learned, while some pointed out usability challenges and suggested improvements to the gameplay design.

These results suggest that Mallory in Secured Office can serve as an effective introductory tool for raising security awareness among young learners. In particular, the game addresses two important requirements: accessibility and flexibility through a smartphone-first design, and interactive learning through the integration of contextual feedback and a simplified attacker's perspective. The ability to motivate players while simultaneously teaching secure password practices highlights the educational potential of serious games in the information security domain.

At the same time, several limitations of this study must be acknowledged. The evaluation involved only a small number of participants, and no pre- and post-test measures of learning outcomes were conducted. In addition, some participants reported difficulties with controls and interface usability, indicating that refinement of the game's design is necessary to maximize its educational effectiveness.

In future work, we plan to address these limitations by conducting larger-scale evaluations with more diverse participant groups, incorporating pre- and post-tests, and applying statistical analyses such as t-tests to more rigorously assess learning outcomes. We also intend to enhance the usability of the game interface and expand the educational content to include broader security topics, such as phishing awareness, multi-factor authentication, and the risks of social engineering. Through these improvements, we aim to further develop Mallory in Secured Office into a comprehensive and practical tool for information security education.

Acknowledgments

A part of this research work was supported by the JSPS KAKENHI Grant Number JP18K1135

References

Blakely, G., Skirton, H., Cooper, S., Allum, P., & Nelmes, P. (2009). Educational Gaming in the Health Sciences: Systematic Review. Journal of Advanced Nursing, 65(2), 259–269.

Cowan, C., Arnold, S., Beattie, S., Wright, C., & Viega, J. (2003). DefCon Capture the Flag: Defending Vulnerable Code from Intense Attack. Proceedings DARPA Information Survivability Conference and Exposition, 1, 120-129.

Henriksen-bulmer, J., Rosenorn-lanng, E., Corbin-clarke, S., Ware, S., Melacca, D., & Fenge, L. (2024). Using Game-Based Learning to Teach Young People about Privacy and Online Safety. Interactive Learning Environments, 32(10), 6430–6450.

Kido, Y., Tou, N. P., Yanai, N., & Shimojo, S. (2020). SD&D: Design and Implementation of Cybersecurity Educational Game with Highly Extensible Functionality. Advances in Information and Communication: Proceedings of the 2020 Future of Information and Communication Conference (FICC), 1, 857–873.

Kiili, K. (2005). Digital Game-Based Learning: Towards an Experiential Gaming Model. The Internet and Higher Education, 8(1), 13–24.

Omiya, T., & Kadobayashi, Y. (2019). Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill. Proceedings of the 2019 7th Inter- National Conference on Information and Education Technology, 259–268.

Petri, G., Gresse-von-Wangenheim, C., & Ferreti-Borgatto, A. (2017). A Large-scale Evaluation of a Model for the Evaluation of Games for Teaching Software Engineering. Proceedings of the 39th International Conference on Software Engineering: Software Engineering and Education Track, 180-189.

How to cite this article:
Kido Y. “et al.” (2025) ‘Development of a Smartphone Game Application for Information Security Education’, *International Multidisciplinary Research Journal*, Volume:3; November 2025; Page No.32-44 DOI: https://doi.org/10.47722/imrj.2001.52

Appendix: Responses to Q5 (Free-text Impressions of the Game)

1) I thought I should avoid storing passwords in places where others can see them.
2) I realized that writing "pass" in a place visible to others is not acceptable. For elementary and junior high school students, a different situation might be more appropriate, such as falling for a malicious website, which seems more realistic for them.
3) Because the operation was not intuitive, I could not progress through the game alone. The touch area was too strict, and I often did not know where to tap. Since this is an educational game, I felt it would be better if the character moved or events were triggered more intuitively through tapping, with clearer visual cues.
4) I had some difficulty only with the operation method.
5) I learned about how to handle passwords, so I think it was a good game.
6) I was not able to successfully investigate some of the searchable places, but I felt the content of the game itself was good.
7) The game was simple and easy to play, and I was able to clearly understand the importance of password management. However, being able to re-check the same place made it a little difficult to play.
8) I think it would be better if places that have already been checked could not be checked again.
9) I thought I should treat passwords carefully.
10) I came to think that passwords should not consist of only numbers, but should combine numbers and letters.
11) I understood what kind of passwords are good, but when asked whether I wanted to know more, I felt I had already learned enough from this game, so I did not feel the need for more.
12) I felt that there was no need for the animation when obtaining a password that had already been collected.
13) I almost got stuck.
14) I thought it was very good that the game showed realistic office scenarios of password leakage and taught the risks of password settings one by one. Sometimes the touch did not respond properly, perhaps because it was recognized as a slide gesture. It was also difficult to tell whether a flag had been set, so I felt that sound effects or similar feedback would make it better.
15) The guidance in the game was clear, and I found it useful that it showed concrete examples, such as why having a password in a visible place is dangerous. Regarding password handling, I felt I should be more careful about what was shown, but I did not feel much beyond that.
16) It was difficult to find the paper with the birthday, and I had to go around the office once. I realized that setting simple passwords is not good, and I also understood the importance of managing passwords.
17) I was able to straightforwardly learn useful knowledge, and it was very educational. However, as a game, it was mainly just searching and exploring, so I felt it could use a bit more variety. I also wondered if there were hints about where the correct password was located.
18) The content of the game itself was simple, but there were no instructions for the controls, so I did not know what allowed me to move or what triggered an action. I think it was possible to understand how to handle passwords.
19) I was able to relearn the importance of information management, such as passwords, in modern society.
20) I found the story of collecting passwords, attacking, and opening the door to be novel.
21) I thought that personal information should definitely be shredded.