



Project Privacy: A Correlational Study on Immersion and the Level of Perceived Seriousness

Ralf Michael Balatibat¹, Michael Sean Brian B. Omisol¹, Rommel P. Feria²,
Ligaya Leah Figueroa², and Ma. Rowena C. Solamo²

¹ University of the Philippines - Diliman, Quezon City, PH
rsbalatibat@up.edu.ph
mbomisol@up.edu.ph

² University of the Philippines - Diliman, Quezon City, PH
Web Science Group
rpferia@up.edu.ph
llfigueroa@up.edu.ph
rcsolamo@up.edu.ph

Abstract. This study delves into the impact of serious games on individuals' awareness on data privacy seriousness. The game incorporates thriller themes, a pixel art-style, and a point-and-click approach that enhances its immersive experience. With the game at hand, the research examines the relationship between a player's immersion levels and their perceived seriousness of data privacy risks. By utilizing a survey questionnaire to 102 participants, the study was able to identify a moderate positive correlation between these two critical variables. Additionally, respondents' feedback provides opportunities for further exploration on serious games, immersion, and innovative approaches to promoting data privacy awareness.

Keywords: serious games, correlation, immersion, perceived seriousness, data privacy

1 INTRODUCTION

The advent of the Internet has allowed people all over the world to gather and consume information at a high rate. Sites and apps have sprung forth from the far reaches of the world, regardless of geographical location. One such breakthrough is the emergence of social media—allowing more interactive communications as compared to forums.

With 4.95 billion users as of 2024 [23], social media platforms have become a sensation and, to an extent, a way of life. During the period of their emergence, these phenomena coincided with the discussion of another concern: data privacy. In the Philippines, Data Privacy is defined as the state of being free from another person or entity's infringement or imposition of confidential information that one possesses [18].

One way to violate such privacy is through social engineering—hacking humans or “deficient users” [13]. As there is little information on how attackers can gather information from a user, it opens a large gateway for malicious activities. Devious tactics such as phishing and pretexting, exploit human psychology to manipulate individuals into potentially divulging sensitive information. With the vast amount of personal data shared on social media platforms, users become vulnerable to identity theft, cyberbullying, and other forms of online attacks.

This paper explores the potential solution in raising awareness of the seriousness of an individual’s data privacy through a serious video game, focusing on the level of immersion they experienced with the game. In the context of the study, researchers define *perceived seriousness* as the quality of approaching a subject, in this case, data privacy and the risks and implications involved with breaches of such, with careful and vigilant consideration and awareness. The majority of such an exploration is inspired by previous research by Dyaico et al. [7] as they utilize game-based learning in raising awareness for data privacy risks. This study will primarily revolve around answering the question:

”What is the correlation between the level of immersion experienced by a player of the serious game solution and their level of perceived seriousness for their data privacy?”

2 REVIEW OF RELATED LITERATURE

2.1 Perceived Seriousness and the Effectiveness of Serious Games

Perceived seriousness refers to the negative consequences an individual associates with an event or outcome [17]. These consequences may relate to an anticipated event that may occur in the future, or to a current state. Note that Miles defines perceived seriousness in the context of health. The researchers utilize this concept in the context of data privacy, such that it refers to negative connotations an individual associates with threats and events that pose a risk to their data privacy.

Similarly, serious games use the immersive experience provided by games to induce a more thought-provoking atmosphere for the values that the game is trying to relay to the player. Even game-based learning approaches, which include utilization of serious games, serve as effective motivators for students instead of simply providing information to them [21]. They also have the potential to be powerful tools for learning, with their concrete effectiveness in need of further exploration [9], hence the motivation to investigate the matter by implementing it in light of the perceived seriousness of data privacy.

The concept of using serious games in order to educate students is already conducted through various researches with varying degrees of success. This is shown in Kara’s systematic review [12] where various subject areas for the use of serious games are explored which includes computer science, learning science and behavioral science. Not only that, genres that the serious games stated in all of the articles specified are mostly adventure or role-playing game, which

involves a progression-based system in the form of a narrative or objectives. One of the papers noted in Kara's work is a serious VR role-playing game made by Alrehaili & Osman [2], where a player assumes the role of a honeybee for experiential learning. By allowing the player to see through the lens of a honeybee doing its work for its hive as well as the effects their actions do to the hive and to themselves, it allows them to immediately pick up prior knowledge as opposed to traditional learning methods. Given the following, a role-playing game that puts the player through the lens of a character in a first-person view would yield the similarly best results as of the other conducted researches.

2.2 Importance of Immersion in Games

Immersion is the degree of involvement in computer games [10]. With how games are described in previous sections, it is important to point out that there is still the significance of the attention of the player towards the medium of education.

Thus, immersion proves to be a valuable concept in application. As such, emotional involvement is a key factor for a user to be immersed [10]. This means that for a user to be able to focus on a topic or a game in particular, the themes of the game must correspond to the user so that they will immediately understand the emotional weight that it carries, and thus a user can immediately evaluate and realize what it would mean to them in the longer run. This is, however, a hard case to deal with, as Jennett et al.'s study extensively tested games that are not completely serious in context, but otherwise still allow users to be emotionally engaged in the following activities. It is only given, however, if the player's immersion is not broken by any possible external interaction such as loud sounds.

Another interesting point for immersion would be through Ahn's [1] study, wherein a virtual reality environment is used to show the risks of their topic. As the users themselves are immediately exposed to being the subject of the topic—being able to gain weight in real-time through the consumption of carbonated beverages—they immediately see the results and thus become emotionally invested as they perceive themselves as those at risk. While it took a while for users to understand the risks, the fact that by allowing a user to simulate the risks in real-time immediately increases the ability to convey that information without any additional abstractions. Thus, this means that if there is a simulation of the following, regardless that it is VR or not, a user will immediately be able to fill their shoes as the target and thus understand the theme and the risks that should be conveyed.

As such, the player's interest in the form of immersion is a critical component in how the player perceives the game and what they learn from it, as any activity that will bore the player will not be interesting to them [3]. Thus, in order for the player to learn, they must play a game where learning is only a consequence of the actions that they have committed inside the virtual world. An example like *Xiao-Mao*, a 3D role-playing Taiwanese-history game developed by Jheng et. al. [11], measures a player's interactions by adding multiple features to the game such as combat, open world exploration, and NPC interactions depending on the

action done (stealing or attacking an NPC). The addition of freedom within the virtual world reflects deeply into the results of their study, where the existence of the fictional environment that they played in enhanced their cultural awareness.

Hence, this research focuses on measuring the level of immersion, which is essentially measuring the level of involvement a player experiences, with the researcher's developed serious game.

2.3 Existing Game-based Solutions on Data Privacy and Security

The idea of a game to introduce or educate people about anything is not a novel solution to begin with. These serious games have become an avenue for developers to advocate certain ideas, themes, or ideologies. As such, there are game-based solutions that follow the need of data privacy and security in daily life.

The basis of this study, which is the game made by Dyaico et al. [7], focuses on many aspects about data privacy that a user needs to be aware of. Table 1 shows the situations that the player can be involved in, thus increasing the chances of the playing individual to understand what hidden risks are involved when interacting with mechanics that are publicly visible to them. Because of its gamified nature, users can immediately identify the problem at hand and any questions that follow through any of the mechanics can be immediately recognized as problematic. It is also followed through with a results screen that verifies whether the users themselves are aware of the situation, as the game itself is structured as a questionnaire. This structure, of course, does not immediately immerse the player to the virtual environment and thus leading to a lack of interest towards the game's theme and subject.

Another game-based solution is CyberAware: a mobile game app created by Giannakas et al. [8]. Their solution focuses more on a broader scale of cybersecurity such as software (firewall, antiviruses) and hardware (patches) security. However, compared to Dyacaico et al.'s game, CyberAware actively designed its mini-games for players to exert attention towards the app—on the basis that a quiz-like format would cause boredom to students. In CyberAware, students would have to do minigames for specific topics before they tackle the 'Arena Security' minigame of that topic. This form of progression allows players to immediately learn about data privacy topics as well as the cybersecurity technologies discussed in the topic. However, it's on-the-nose design of showing off learning material during gameplay has some of its players skimming or skipping the information. This does lead to a conclusion that a minimalistic approach in showing a volume of information is needed in order to avoid boredom from the player.

A more intriguing game is Immaculacy, an interactive story made by Suknot et. al.[24], where it immerses the player in a slightly dystopian world littered with privacy issues. The novelty in their approach is a narrative to which they assume the role of a character through more realistic scenarios in which their privacy is at risk, as opposed to the mini-game or quiz-based formats as seen in previous examples. Their paper would be a good place to start on what can be

done for players to not only be actively engaged in understanding data privacy but also a long learning process given its more subtle and definitive approach.

3 DESIGN OF PROJECT PRIVACY

The design and philosophies of the implementation referenced and attained insight from existing GBL and Serious Game approaches are discussed in Section 2.2 and 2.1 respectively. The researchers designed the game intending to keep in mind the notions of immersion and data privacy seriousness, and how both are potentially related.

To elaborate further, the novel quality of *Project Privacy* is to create an immersive, serious game that uses subtle clues and contexts that lure the player into scenarios that would potentially risk their privacy throughout the playthrough, using a realistic scenario in which they control a character in a limited first-person perspective. This is elaborated more in the following section.

3.1 Project Privacy Game Rationale

The objective of the development was to make the game as immersive as possible given the capabilities and limitations the researchers are presented with in terms of manpower, time, and resources. The concepts of immersion and perceived seriousness served as the primary guiding factors that allowed the researchers to design and develop the game related to one's data privacy.

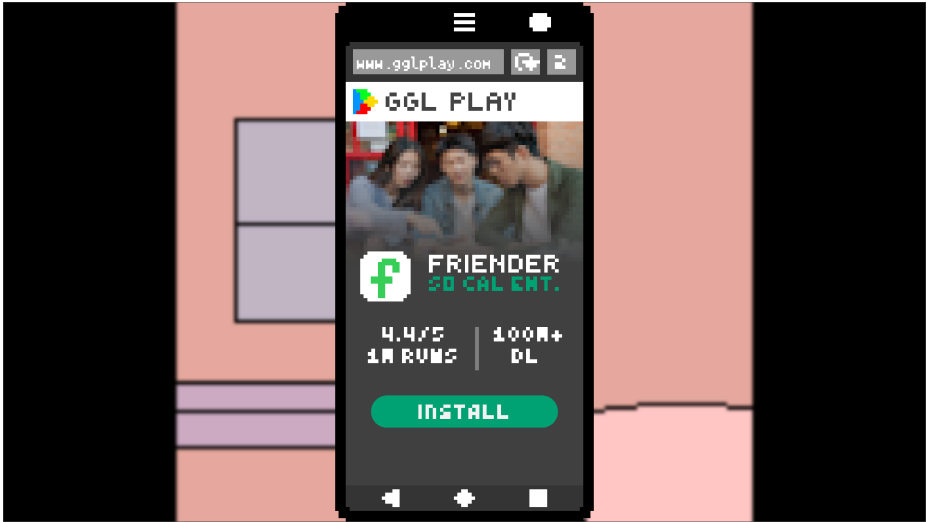


Fig. 1. One of the situational events in the game: the player has the option to install the social media app that the malicious entity wants you to install.

The game incorporating thriller elements serve the purpose of delivering the serious notions of these risks to the player. Such elements provide opportunity to create suspense, intrigue, and emotional investment in the game. In turn, these allow a more immersive and engaging experience to the player as well as relate the in-game situations with the "horrors" of real-life data privacy risks and breaches.

3.2 Narrative and Gameplay

Narrative The game's premise is centered around the player taking the role of a college student living alone in their dorm room during their semester break. Seeking to ward off boredom, the student turns to social media for scrolling and posting, particularly in the fictional Friender app. However, the student learns the inherent risks in social media interaction, especially when their data privacy is disregarded.

The basis of the game's narrative is centered around its core game loop. It is a sequence of events or activities repeated by the player that serves as the foundation of a game's design and replayability. It consists of the following steps:

1. Player wakes up (from a dream or nightmare)
2. Player chooses to do daily tasks (based on learning points)
3. Player experiences supernatural repercussions for their earlier actions (when ending the day)
4. At the end, the player gets an ending specific to the action they've made.
5. Repeat 1.

This loop serves as the main sequence of the game throughout the playthrough.

The game starts as the player wakes up from their alarm and wonders what they wish to do for the day. Certain tasks are more mundane than others. To ease off their boredom, they have decided to install and open the Friender app and scroll through, and decide to end the day at some point by going to sleep. Later on, they are suddenly woken up by strange noises in their room. This noise will come from "The Red Man," a character in the game intended to frighten or unnerve the player, telling them the wrong actions they've done that exposed their personal information. The overall narrative of the game will take place through five (5) situations or scenarios that, to a degree, emulate online behavior that potentially risks an individual's privacy.

Gameplay The serious game will be in the form of a point-and-click thriller game, a genre of video games that primarily uses the mouse and its buttons to interact with objects in the game environment, for an immersive gaming and learning experience. The decision to implement the solution as a thriller game is to deliver the impact of the seriousness of an individual's data privacy and the risks that come with it if it were to be breached.

The game is explicitly designed to ensure that the player is unaware of who the threat actor is at the beginning of their first playthrough. At first, 'Alison'

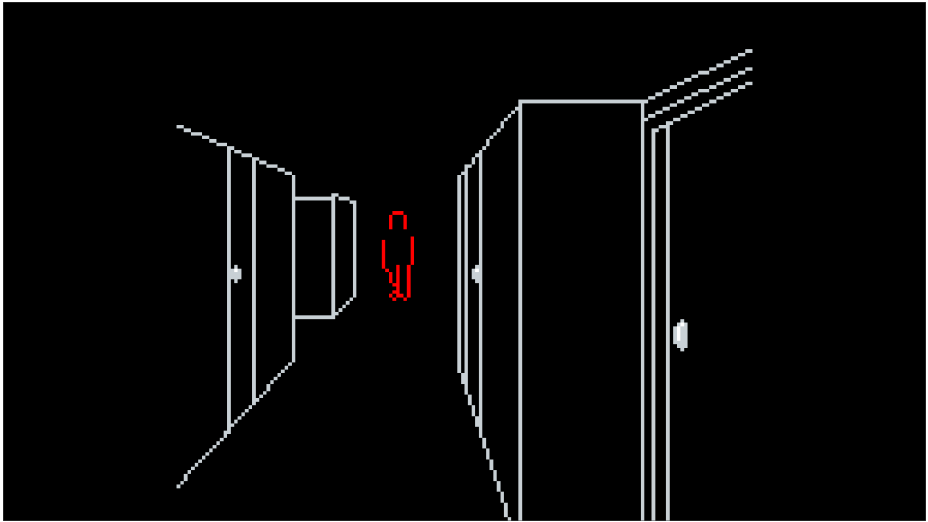


Fig. 2. A nightmare that the player receives in case they have unknowingly given their data privacy to the threat actor, manifesting as a nightmare to show to the player that they have made a mistake in the day before.

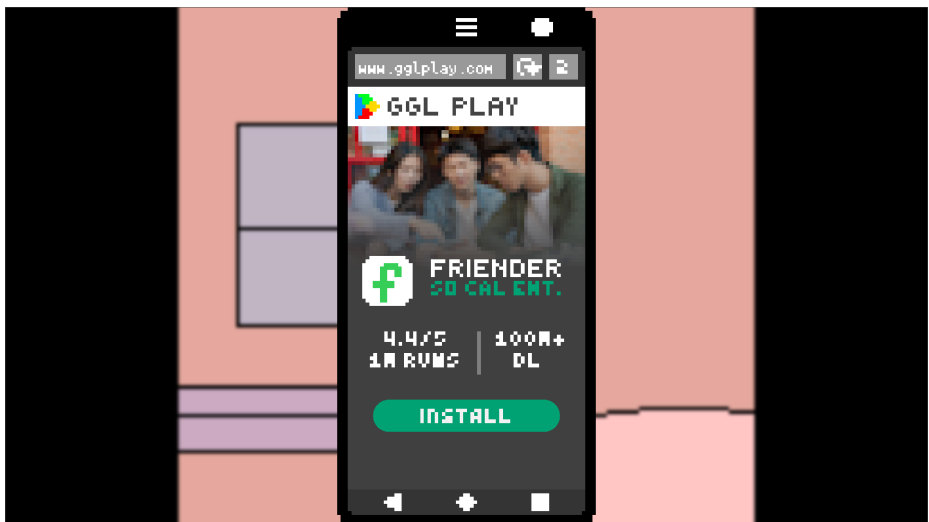


Fig. 3. The player character's phone is one of the diegetic aspects that gives the illusion of immersion for the player. This is where most of the game's interactions center around.



Fig. 4. The Red Man, disguised as 'Alison', attempting to coax the player into actively participating in the app.

is seen as the player character's friend, but subtle hints point out that 'Alison' is, in fact, the 'Red Man', who had gained access to Alison's phone to convince the player to install the application (shown in Figure 4). These hints are shown as subtle coaxing by the threat actor as well as harassing the player into installing the app, taking advantage of the player character's (or rather, Cheryl's) knowledge of their friend Alison.

3.3 Situations

The game incorporates situational events with the objective of providing awareness to the player of the seriousness of their data privacy risks when maneuvering through social media and other platforms. Each mistake or activity that exposes themselves or risks their data privacy will have an equivalent consequence at the end of the day, in the form of a supernatural character called "The Red Man" who will haunt the player, serving as a learning point for the player for the next iteration of their playthrough.

The main learning points introduced in the game are based on the user's rights stated in Sections 12, 16, and 20 of the Philippine Data Privacy Act of 2012. The said points that would serve as the main bases of the game's scenarios and design are as follows:

1. Need for consent in data processing - Section 12.
2. Right to be informed - Section 16A.
3. Right to access - Section 16B.
4. Right to rectification - Section 16D.

5. Right to erasure - Section 16E.
6. Right to object - Section 16E.
7. Need for security measures for the obtained personal information - Section 20.

The situations the player will be presented in are triggered by the initial actions they decide on during the playthrough. Various situations have equivalent learning points or present risks related to disregarding data privacy. The situations, equivalent data privacy risk pointer, and their relevant learning points are presented in Table 1.

Table 1. Data Privacy Scenarios

Situation #	Data Privacy Risk Pointer	Learning Point
(1) Installing a new social media app and immediately agreeing to the permissions without reading them thoroughly or checking which permissions to deny	App Permissions (Installation)	1, 2, 6
(2) Posting on Friender with your location turned on	Location Data	3, 7
(3) Interacting/entertaining a scam text/chat and clicking on the link it contains	Scam Texts/Chats	2, 6, 7
(4) Player is persuaded by the app through their deceptive design to share more than they should	Persuasive Features	2, 3, 4, 5, 6
(5) Connecting to a public Wi-fi without properly knowing the source	Unsecured Wi-Fi	2, 6, 7

These situations and their associated pointers were based heavily on Dyaico et. al.'s [7] Data Privacy Risk Pointers:

1. Situation #1 focuses on the player having the option to install the application that 'Alison' wants you to download: with the overarching theme of being able to progress the game without ever installing it. While it does not activate any parameters in the game that would immediately lock you into the endings where the player's identity is exposed: it leads to the following data privacy risks.
2. Situation #2 is expected to be the most subtle out of the data privacy risks, with the location settings of the app when posting to be on by default. The player would have to manually disable it on their own in order for their location to not be at risk.
3. Situation #3 is the last ditch effort by 'Alison' to get the player's interest should they not reveal their location in the app via posting or if player considers not installing the app as stated in Situation #1.

4. Situation #4 is done by allowing the player to post online with or without their location being revealed. It is to be noted that the following situation does not influence any endings in the game, but is similar to that of Situation #2 of being an indirect consequence of using the app.
5. Situation #5 is as similarly subtle to that of Situation #2, given that a freely accessible Wi-Fi puts the player at risk of being hacked at any time possible.

It is worth noting that, in the interest of time, only the five given scenarios and their incorporated learning points are implemented within the game. The discussion on unimplemented scenarios and learning points that could be explored will be elaborated more at Section 7.

3.4 Technology Stack

The technology used in implementing the game along with its assets include the Godot Engine and Aseprite. Godot is a free, open-sourced, and lightweight cross-platform game engine that allows its developers to create games using various programming languages such as GDScript, C#, and C++. Aseprite is an image editor that specializes in pixel art and animation.

Game Architecture The Godot Engine utilizes object-oriented design, wherein elements of the engine such as Nodes and scenes act as objects that interact with each other and each has respective sets, properties, scripts, and instructions given to the object either immediately or in reaction to an event. The engine also leans on the aspects of the Entity-Component-System (ECS) architecture, a software design architecture that is most commonly used in video game development.

Deployment The game is exported to Windows and Linux, alongside a web version that is uploaded to itch.io, an online platform for hosting, selling, and downloading mainly video games and various assets, where it is publicly hosted. Knowledge of the game is then disseminated through a social media post in both Facebook and Twitter, as well as contacting interested individuals. The game and its description can be accessed at <https://theredswarm.itch.io/project-privacy>.

4 METHODOLOGY

The methodology conducted in the study combines quantitative methods with an analysis of open-ended questions provided within the survey.

4.1 Target Participants

Participant recruitment was done through an opportunity sample, a sampling method based on the availability of their participants. The study and recruitment were publicized through online platforms including Facebook and Itch.io. Participants were informed in advance that the game included thriller themes to avoid misleading those who do not enjoy such games.

4.2 Project Privacy: Post-Game Survey Questionnaire

For this study, a self-report survey, entitled "Project Privacy: Post-Game Survey, was utilized to gather post-game data centering on immersion and perceived seriousness. It has the following key segments:

- Demographic Profile. This includes inquiring about their gender, which age group they are in, and their current level of education.
- Self-Assessment on the Game's Level Immersion. Participants rated their immersion experience during gameplay using a 5-point Likert scale, with 5 meaning the participants felt immersed in that question's aspect and 1 meaning the participants felt the least immersed.
- Self-Assessment on Perceived Seriousness of Data Privacy Risks. Participants indicated their perception of Data Privacy risks associated with the game scenarios using a similar 5-point Likert scale, with 5 representing the participant feeling the most serious about their data privacy and risks, and 1 being the opposite.

Perceived level of immersion-related questions in the instrument were heavily based on Jennett et al.'s [10] questionnaire about immersion, particularly from their third experiment, modified to fit the context of the game. Questions about the level of perceived seriousness of data privacy were curated by the researchers keeping in mind the general principles of questionnaire design, common themes related to data privacy risks, and the established learning points of the game.

The Cronbach's Alpha test was conducted on the questionnaire, with $N = 12$, to assess the reliability of questions related to the Level of Immersion and Perceived Seriousness. The obtained values were 0.8293 for immersion and 0.8380 for seriousness. These results indicate that the survey questionnaire is reliable, meeting the minimum threshold of 0.70.

Google Forms was utilized to implement the questionnaire and acquire respondent data for its accessible and convenient setup and data visualization.

4.3 Data Analysis

The statistical data analysis uses Spearman's rank correlation due to the ordinal nature of the variables: level of immersion and perceived seriousness. Spearman's correlation assesses the strength and direction of their relationship without assuming linearity.

Survey responses are stored in Google Sheets obtained via Google Forms and processed using Python in Google Colab. Data is immediately sanitized to remove any duplicate data for immediate analysis.

Given the exploration of the relationship between immersion and perceived seriousness, the study postulates the following hypotheses:

- H_0 : There is **no significant correlation** between the proposed serious game's level of immersion and perceived seriousness of data privacy.

- H_A : There is a **significant correlation** between the proposed serious game’s level of immersion and perceived seriousness of data privacy.

A significance level $\alpha = 0.05$ is compared with the p-value to accept/reject the null hypothesis.

5 RESULTS AND ANALYSIS

The results are divided into the following sections: Demographics (Section 5.1), Level of Immersion (Section 5.2), Perceived Seriousness (Section 5.3), Spearman Correlation (Section 5.4) and Analysis (Section 5.5).

5.1 Demographics

102 participants participated in the study as the result of the opportunity sampling. There were 70 male (69%) and 26 female (25%) participants, with 1 being non-binary (.9%) and 6 prefer not to disclose their gender (6%). For the age ranges, there are 28 16-20-year-olds (27%), 67 21-25-year-olds (65%), and 7 over the age of 26 (6%). As for the highest attained education among participants, 75 are from college (73%), 12 are from high school (11%) and 15 are post-graduates (14%).

The profile of the sampling is that most of the participants are male, college-level individuals with ages 21-25 years old.

5.2 Level of Immersion

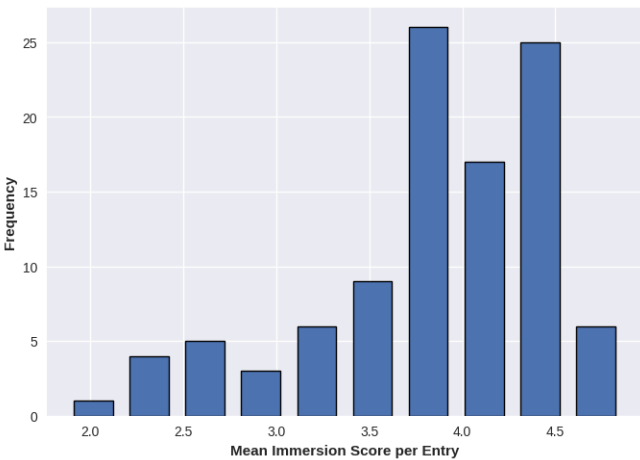


Fig. 5. Mean level of immersion per entry.

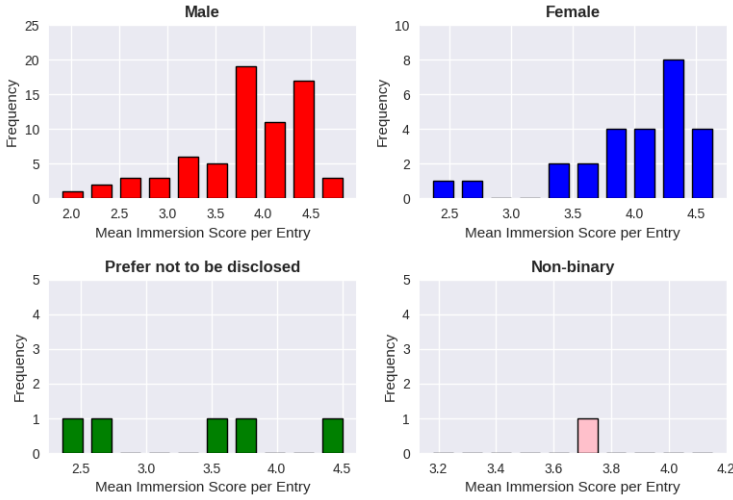


Fig. 6. Mean level of immersion per entry by gender.

For the level of immersion shown in Figure 5, the mean level per entry skews to the right as shown in Figure 9. Analyzing how the male and female participants answered for the following section in the questionnaire shows that there is no difference in how both answered, with how distributed the mean scores are per participant (Figure 6). Considering the low sample size for both those non-binary and would not disclose their gender, that means that all genders answered the same way.

The following trend continues when comparing the mean scores by categorizing participants by their education (Figure 7) as well as by their age (Figure 8). While it can be noted that those 26 years old and above balance towards the middle, the small number of participants for that category shows no difference.

In general, the result of the sampling shows that the overall mean level of immersion is high as predicted, with no interesting differences when checking through groupings of the participants.

5.3 Perceived Seriousness

Compared to the levels of immersion of participants, participants are shown to be more understanding of the risks regarding their digital data privacy (Figure 9). Comparing the seriousness scores by their groupings, like the previous section, shows how similar all participants are in answering the questions, as seen in Figures 10, 11 and 12.

5.4 Spearman Correlation

Spearman's rank correlation was conducted to assess the relationship between the level of immersion and perceived seriousness ($N = 100$). There was a positive

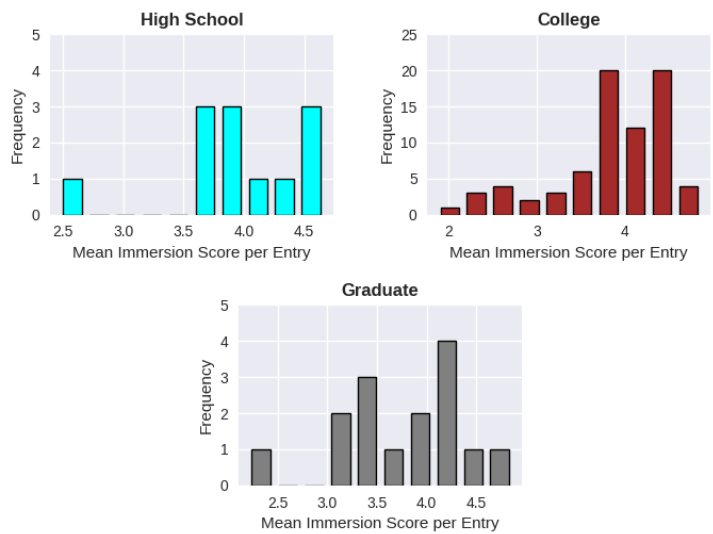


Fig. 7. Mean level of immersion per entry by educational attainment.



Fig. 8. Mean level of immersion per entry by age range.

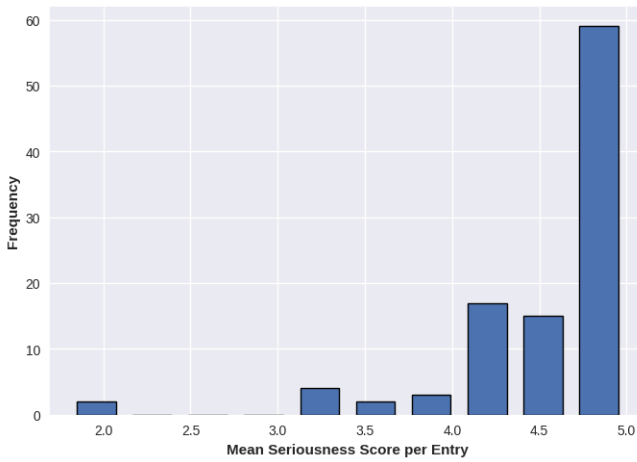


Fig. 9. Mean level of perceived seriousness per entry.

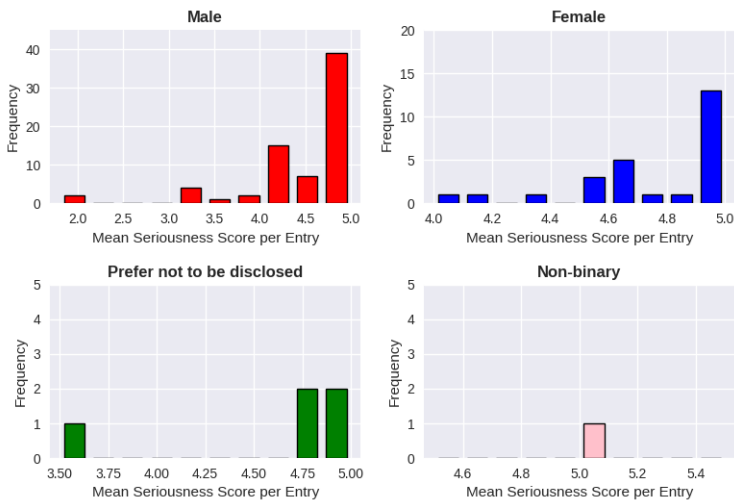


Fig. 10. Mean level of seriousness per entry by gender.

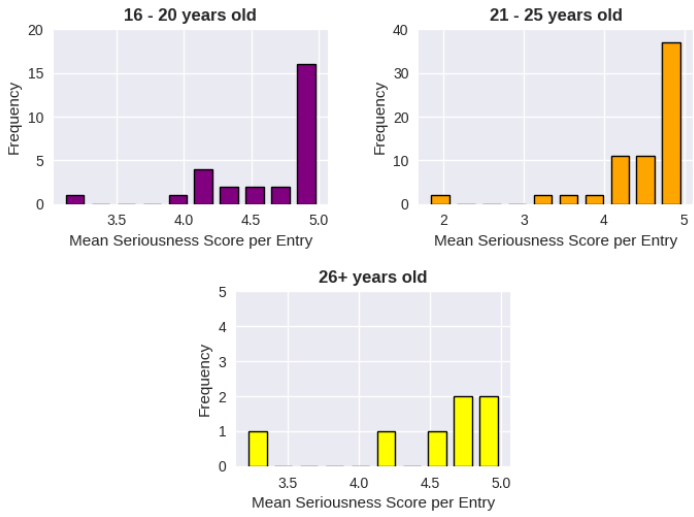


Fig. 11. Mean level of age per entry by age range.

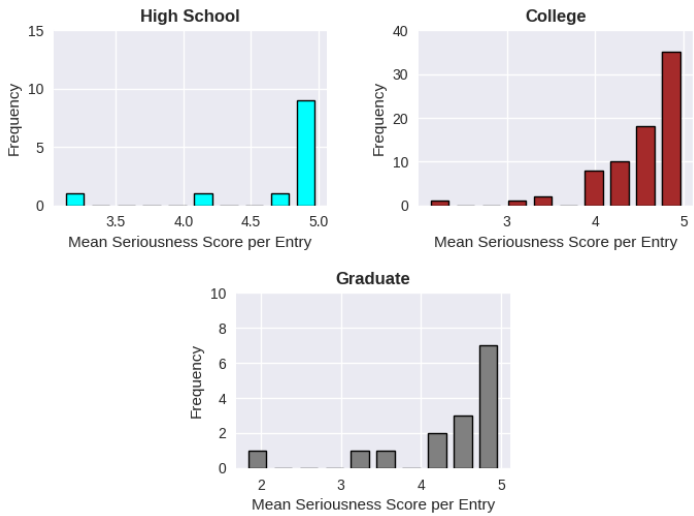


Fig. 12. Mean level of seriousness per entry by educational attainment.

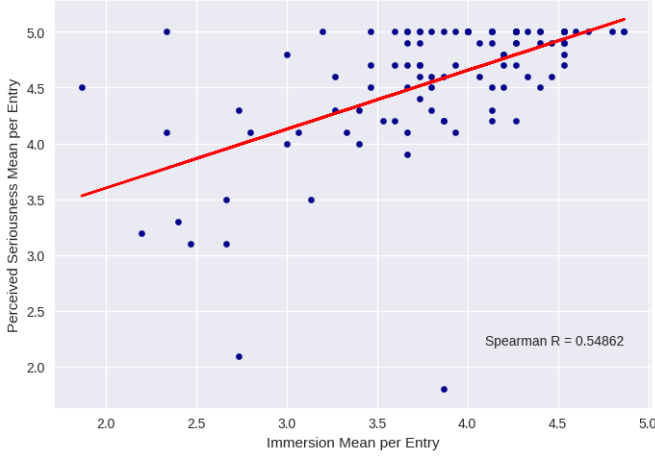


Fig. 13. Correlation between immersion and perceived seriousness.

correlation between two variables $r_s(100) = .55, p = .197$, thus H_0 is rejected. This indicates that a player with a high level of immersion perceives the negative consequences and risks of their data privacy, and vice versa.

These findings appear reliable, as seen in previous sections that a participant's gender, age and educational attainment have no significant correlation to either the mean level of immersion or perceived seriousness. However, with consideration of a few trends in how participants answered in the questions, as well as outliers, the following section is added to discuss further details.

5.5 Analysis

Immersion Section Answer Trends There are questions that, while not significant factors to the mean immersion scores per participant, show interesting takeaways. Graphing the specific answer count for each stated question shows a bell curve. This has led to a more extensive look at the answers of each participant, to which the following questions in the immersion section are stated in bullet form:

- **Question 1:** "To what extent was your sense of being in the game environment stronger than your sense of being in the real world?"
- **Question 2:** "At any point, did you find yourself become so involved that you wanted to speak to the game directly?"
- **Question 3:** "To what extent did you feel as though you were moving through the game according to your own will?"
- **Question 4:** "To what extent were you distracted from your surroundings?"

Questions 1 & 3 are whether the participant has a defined goal for them to move forward to, as presented by the game's design, while Questions 2 & 4 are

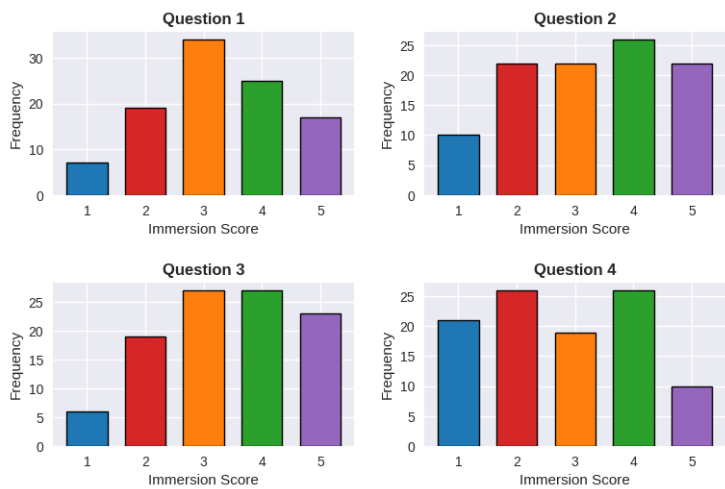


Fig. 14. Questions (Section 5.5) and their scores from correspondents.

if the player has their entire attention towards the game instead of their current environment. These questions would have an immediate impact as frustration can lead to players wondering what the next goal is, just as being distracted by the environment would cause them to snap out from what is defined in this paper as 'immersive' either by sounds or frustration over design.

However, it is quite contradictory given the right skew in answers for the question "To what extent did the game hold your attention?"—where there are only 5 participants below scoring it 3 (and none answering 1)—as well as other questions. This meant that intrigue over the game holds as a larger factor to the mean immersion score of a participant as well as its art style, given that there are participants that played the game during a noisy environment (ie. a noisy colloquium). While the following questions aren't significant due to the nature of the questionnaire, future work could have the following questions as primary factors when it comes to immersion.

Feedback Checking the comments from the participants in the sampling shows positive feedback with regards to the game. One that is commonly pointed out is how the horror theme of the game, alongside the simplistic graphics, proves effective in immersing (as well as scaring) participants. This lines up with the expectation that the pixel art style forces the imagination of the player during the game's tense sequences, as the sudden shift from calm to suspense creates a shock value that puts their attention immediately towards the game, thus also increasing perceived seriousness. The same goes for how the first-person perspective that participants are forced to play on makes the consequences much more relatable and realistic, such as how the players have to wave their cursors

to access the phone section of the game or how they have to navigate around the main character's room.

However, as seen in Section 14, the participants point out with what was seen from the questions that have an equal or left-skewed distribution of answers in the immersion parts. The game's subtle design towards its narrative, while proven effective in bringing psychological horror to the narrative, confuses players. Participants pointed out that they have no clue as to what was going on and what they would have to do, confirming the speculations from the previous section. However, it is unfortunately expected as the players have no clue as to who is the hacker (or in this case, the one hacked) in the narrative.

In the end, participants still state that they learn about data privacy once they reach the endings, thus requiring multiple replays of the game to understand what choices they could've made to avoid the following events.

Outliers Curiosity aside, there are two outliers when observing Figure 13: a participant with a mean immersion score of 3.867 and a mean seriousness score of 1.8, and another with a mean immersion score of 2.73 and a mean seriousness score of 2.1.

Looking further through their feedback, the former (21-25-year-old male with post-graduate-level education) states that the game is immersive and its scenario being as close as to their daily life. Giving insight into this vague comment, the participant may have given a low seriousness score as they presume the following events as 'trivial' to them due to experiencing a digital data privacy attack (with how the statement is worded).

The latter (21-25 year old male with college-level education) is also similar given the context. Looking over how they answered the questionnaire, they pay attention to the game but have low scores on questions pointed towards how they perceive progress as well as their emotional investment in the game. This pattern does not show up in the perceived seriousness portion, as any answer is either in the range of 2 or 3. This may prove to be a similar case as the former, but their comments state otherwise. Instead, the following comment shows that the participant is someone who is knowledgeable about their data privacy and understands the negative aspects of it. Their low scores are attributed towards how the game is designed to be subtle, stating that to quote, "a regular person who doesn't know what not to do, the lesson is a bit confusing since it's not very clear what happened". The following insight may prove to be a possible future work to those who have already experienced similar events in their life, or for those who have adequate knowledge about data privacy risks.

6 CONCLUSION

Project Privacy is a serious game designed to see if there is a correlation between one's immersion in a game to their perceived seriousness of digital data privacy risks. The study shows that there is a moderate positive correlation between the proposed serious game's level of immersion and the perceived seriousness

of data privacy among respondents, thus rejecting the null hypothesis. Despite the majority of the participants being young, college-level males, specifics in the demographic show no factors towards the mean scores for both immersion and perceived seriousness.

In addition, the graphics and the horror elements of the game proved effective in taking the player's attention towards the game. The game and the research were also able to provide valuable insight that immersion is an important aspect of any game-based learning and serious game implementations in providing impact to the player and their intended learning outcomes, portraying the risks that come alongside ignoring data privacy.

However, there are still possible improvements to the game as stated by players. As such, these directions for any future works associated with this paper will be highlighted in the next section.

7 FUTURE WORKS

In light of the study's findings and the overall research process, several opportunities, recommendations, and directions emerge for future research.

A potential direction that could be taken is based on how the majority of the samples in the study included respondents from Gen Z, with another smaller portion being in the Millennial generation. It could be a comparative analysis on other generations' experience in playing the game and the influence on their perceptions on data privacy. An alternative comparative study could also be done based on participants' different age ranges.

An additional direction future research could take could rely on creating a different game, with the same topics in mind, and conducting a comparative study between both games and their effectiveness in measuring correlation or promoting data privacy awareness.

It is also recommended to consider a bigger development team for creating new serious game implementations. This could allow for conveying topics and provide better learning points in a more refined light. This allows for a more streamlined game development process compared to the current implementation due to limitations in time and manpower.

A final recommendation in terms of conducting the study would be the addition of objectively recording immersion from players similar to Jennett et. al.'s [10] study. This could include tracking participants' reaction time, heart rate and facial reactions, and eye movements—incorporating these elements to measure them within the game. This could effectively create more concrete data that would supplement questionnaires with direct feedback from a participant.

References

1. Ahn, S. Incorporating immersive virtual environments in health promotion campaigns: A construal level theory approach. *Health Communication*. **30**, 545-556 (2015)

2. Alrehaili, E. & Osman, H. A virtual reality role-playing serious game for experiential learning. *Interactive Learning Environments*. **30**, 922-935 (2022), <https://doi.org/10.1080/10494820.2019.1703008>
3. Barbosa, A., Pereira, P., Dias, J. & Silva, F. A new methodology of design and development of serious games. *International Journal Of Computer Games Technology*. **2014**, 817167 (2014)
4. Becker, K. What's the difference between gamification, serious games, educational games, and game-based learning. *Academia Letters*. **209** pp. 1-4 (2021)
5. Brooke, J. SUS: A quick and dirty usability scale. *Usability Eval. Ind.*. **189** (1995,11)
6. Dimitra, K., Kousaris, K., Christina, Z. & Tzafilkou, K. Types of Game-Based Learning in Education: A brief state of the art and the implementation in Greece. *The European Educational Researcher*. **3**, 87-100 (2020,6,15), <https://doi.org/10.31757/euer.324>
7. Dycaico, J., Olaño, H., Feria, R., Figuera, L. & Solamo, M. Design and Evaluation of Daily Digital Privacy: A game on raising awareness on digital privacy risks. (University of the Philippines - Diliman, 2023)
8. Giannakas, F., Kambourakis, G. & Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. *2015 International Conference On Interactive Mobile Communication Technologies And Learning (IMCL)*. pp. 54-58 (2015)
9. Girard, C., Ecalle, J. & Magnan, A. Serious games as new educational tools: how effective are they? A meta-analysis of recent studies. *Journal Of Computer Assisted Learning*. **29**, 207-219 (2012,6)
10. Jennett, C., Cox, A., Cairns, P., Dhoparee, S., Epps, A., Tijs, T. & Walton, A. Measuring and defining the experience of immersion in games. *International Journal Of Human-computer Studies*. **66**, 641-661 (2008)
11. Jheng, S., Shih, J. & Wang, Y. Creating simulations in history game that enhance players' sense of cultural reality. *Proceedings Of The AECT International Conference On The Frontier In E-Learning Research 2013 (AECT'13)*. (2013)
12. Kara, N. A Systematic review of the use of serious games in science education. *Contemporary Educational Technology*. **13**, ep295 (2021,1,20), <https://doi.org/10.30935/cedtech/9608>
13. Klimburg-Witjes, N. & Wentland, A. Hacking humans? Social engineering and the construction of the "Deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*. **46**, 1316-1339 (2021,2,10), <https://doi.org/10.1177/0162243921992844>
14. Lee & Jeong A Study on the Serious Games Design Framework via Potential Outcomes - Focused on Construal Level Interventions. *International Journal Of Contents*. **10**, 53-62 (2014,12)
15. Marcial, D., Peña, L., Montemayor, J. & Dy, J. The design of a gamified responsible use of social media. *Frontiers In Education*. **6** (2021,3,30), <https://doi.org/10.3389/educ.2021.635278>
16. Martínez, K., Menéndez, I. & Bustillo, A. A new measure for serious games evaluation: Gaming Educational Balanced (GEB) model. *Applied Sciences*. **12**, 11757 (2022,11,19), <https://doi.org/10.3390/app122211757>
17. Miles, A. Perceived Severity. <https://cancercontrol.cancer.gov/brp/research/constructs/perceived-severity>, Accessed: May 27, 2024
18. National Privacy Commission Republic Act 10173 - Data Privacy Act of 2012 - National Privacy Commission. (2022,2,12), <https://privacy.gov.ph/data-privacy-act/>

19. Pilote, B. & Chiniara, G. The many faces of simulation. *Clinical Simulation*. pp. 17-32 (2019)
20. Qian, M. & Clark, K. Game-based Learning and 21st century skills: A review of recent research. *Computers In Human Behavior*. **63** pp. 50-58 (2016,10,1), <https://doi.org/10.1016/j.chb.2016.05.023>
21. Schrader, C. Serious games and game-based learning. *Handbook Of Open, Distance And Digital Education*. pp. 1255-1268 (2023)
22. Serrano-Laguna, Á., Manero, B., Freire, M. & Fernández-Manjón, B. A methodology for assessing the effectiveness of serious games and for inferring player learning outcomes. *Multimedia Tools And Applications*. **77**, 2849-2871 (2017,2,15), <https://doi.org/10.1007/s11042-017-4467-6>
23. Shewale, R. Social media users and statistics for 2024 (Latest data). (2024,1,9), <https://www.demandsage.com/social-media-users/>
24. Suknot, A., Chavez, T., Rackley, N. & Kelley, P. Immaculacy: a game of privacy. *Proceedings Of The First ACM SIGCHI Annual Symposium On Computer-human Interaction In Play*. pp. 383-386 (2014)
25. Wang, K., Li, P., Zhang, J., Zhong, J., Luo, X., Huang, J. & Zheng, Y. Effects of Digital Game-Based Learning on Students' Cyber Wellness Literacy, Learning Motivations, and Engagement. *Sustainability*. **15**, 5716 (2023,3,24), <https://doi.org/10.3390/su15075716>

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

