Design and Evaluation of Daily Digital Privacy: A game on raising awareness on digital privacy risks

JULIAN DYCAICO, HANS OLAÑO, ROMMEL FERIA, LIGAYA LEAH FIGUEROA, and ROWENA SOLAMO, University of the Philippines, Diliman, Philippines

Game-based learning (GBL) approach has been used in multiple studies in determining or improving its efficiency in teaching its users the specified learning goals. These studies have shown that the approach was conducive to learning. Hence, this study aims to use GBL as a tool for raising awareness on increasing concern on the risks to the Digital Privacy of Filipinos amidst the rapidly growing Social Media usage. Many users unknowingly engage in online behavior that jeopardizes their personal digital privacy concerning their personal data protection, consent, control, and transparency. Lectures and seminars are often present in raising awareness on the said dangers but lack the interactivity and engagement with its audience. Other games also discuss topics such as security and privacy, but lack the specificity to data privacy risks in social media. Hence the researchers implemented the GBL approach and developed Daily Digital Privacy. Investigating the effectiveness of gamification and GBL, Daily Digital Privacy is designed as a situational simulation game immersing players by recreating common online experiences that can potentially exploit user privacy. By employing game elements and mechanics for learning digital privacy risks, increased engagement, motivation, and participation are seen as the expected benefits. Through interactive gameplay, players must navigate through privacy settings and make decisions that either secure or compromise their overall digital privacy. This provides the players with an environment to familiarize themselves with social media privacy settings without harming their personal information. In this project, the researchers sought out if such a video game is capable of effectively raising awareness of these digital privacy risks. To evaluate this, testing was performed on a number of participants in which they responded to two identical questionnaires, answered before and after playing the game. Using paired t-test as the statistical test to analyze the responses, it was found that there was a statistically significant higher level of awareness of these privacy risks after playing the game.

Additional Key Words and Phrases: gamification, video game, data privacy

ACM Reference Format:
Julian Dycaico, Hans Olaño, Rommel Feria, Ligaya Leah Figueroa, and Rowena Solamo. 2023. Design and Evaluation of Daily Digital Privacy: A game on raising awareness on digital privacy risks. 1, 1 (July 2023), 25 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Connectivity through various social media sites has become increasingly popular in the Philippines. As of January 2023, the internet penetration rate, the percentage of the population that has access to the internet in the country, is at 73.1% or 85.16 million people. Out of these, 84.45 million Filipinos are social media users [13]. There was an increase of 6.1% in internet penetration rate and 11.45 million social media users from January 2020 [12]. COVID-19 was a factor in the surge in internet

Authors' address: Julian Dycaico, jbdycaico@up.edu.ph; Hans Olaño, hansfilomeno@gmail.com; Rommel Feria; Ligaya Leah Figueroa; Rowena Solamo, University of the Philippines, Diliman, M339+HC2, Roxas Ave, Diliman, Quezon City, Philippines, 1101.

XXXX-XXXX/2023/7-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

usage as people relied on the internet for work, education, communications, and entertainment during the time of lockdowns and isolation [7].

This increased exposure to the internet among Filipinos poses a risk to their digital privacy. The issue of privacy in this context is the tendency of personal information to be exposed through sharing of content such as location, photos, and videos which are common features in social media platforms. Such data left in the public domain leaves users vulnerable to potential unauthorized access and malicious use of their personal information without their consent.

As the world becomes more digital, companies across industries such as those in business, e-commerce, marketing, and technology, collect these data for consumer insights and employ targeted marketing strategies. This data being collected, may not be consciously provided by the internet users, as these may be data that have been indirectly derived from unrelated interactions [18]. An example of this is a website displaying targeted ads based on a user's search history. These are potential loopholes and gray areas that a person's data is subjected to where their consent does not align with the purpose of the data collection.

Cybercrime is also a concern. Many prey on information being shared online as their means to carry out activities that would exploit users' digital privacy. These include identity theft, where cybercriminals would assume their victim's identity from the personal information they share online. Phishing and social engineering attacks can become highly personalized, exploiting users more effectively by leveraging user information shared online. This enables tailored attacks that match a user's history, relations, interests, preferences, and recent activities, increasing the likelihood of deception and manipulation of these attacks. Children and teenagers are targeted as particularly vulnerable to such privacy violations because of the tendency of these age groups to post information publicly and their susceptibility to being deceived by malicious users [17].

Preventive measures are in place to protect social media users' privacy. These measures involve adjustments to the privacy settings of a user's account. These are but are not limited to; the visibility of the user's profile; the visibility of their content; and settings involving their interactions with other users. However, there are issues with the usage of these settings. In particular, limited knowledge of privacy policies and their controls by the users [17] negates any protection that a social media platform could offer. Thus knowledge and understanding of such privacy settings is a factor to consider when looking into the vulnerabilities of teens in their usage of social media platforms.

With the increasing usage of the internet, it's just as vital that the user literacy of navigating such platforms be addressed. In the Philippines, the Data Privacy Act of 2012 was legislated in response to the concerns of a rise in the digital population of the country brought upon in the 21st century. The goals of the legislation are primarily on the protection of the privacy of individuals without constricting the free flow of information; the regulation on the handling of personal data; and ensuring that the nation complies with the international standards on data protection [2]. For the citizens, a key aspect of this legislation is the data privacy rights of each individual. Each individual has the right to know about any personal information and data that has been gathered, kept, and processed, as well as the right to access, object to, retrieve, and correct it [3]. This act protects its citizens from privacy breaches by establishing a framework for regulating how personal data are handled and ensuring that the rights of the individuals are upheld.

It is necessary for citizens to be informed of their Data Privacy Rights as well as safeguards to their digital privacy while using the internet. This research explores the strategy of using Game-based learning to raise awareness of the risks of internet usage and potentially dangerous online behavior. Game-based learning is a learning technique that incorporates game elements into a unit that is self-contained with its own defined start, gameplay, and ending where learners engage in-game activities as the means of delivery of learning content [11]. Game elements that can be employed are a points system, leaderboards, or rewards to gratify the players, enticing replayability to achieve higher scores and continued learning. Effective gamification efforts highlight story, challenges, feedback, and interactivity to maximize on player engagement for a high positive potential effect on the player's learning [11].

Games are not merely for entertainment purposes. With the proper design, games can be effectively used for learning.Benefit of incorporating game-based elements is the potential for higher engagement and participation among players [5]. These games can be in the form of Educational and Serious games, which are purposely designed for learning. Learnings from games also exist in entertainment games which are games that are commercially available off the shelf or multiplayer games [15]. The main types of game-based learning approaches are flashcard-type games, simulation games, interactives, quiz games, puzzles, strategy games, and reality-testing games [6]. Games that present diverse challenges to players promote collaboration, critical thinking, and problem-solving, providing opportunities for skill development in these areas [15]. By integrating collaboration, role-playing, narrative, exploration, and complexity, games can enhance player engagement and encourage learning.

The rationale for using game elements is to provide users with an environment that promotes active learning engagement whilst providing a safe environment allowing users to make mistakes without significant real-life consequences. Through gamification, enhanced learning outcomes are expected through increased active interaction and engagement, while also providing valuable data and insight for researchers to assess the effectiveness of this approach.

The efficiency of game-based learning as a method for users to achieve learning goals has been demonstrated in studies such as in the study CyberAware [9]. The study aimed to educate and raise awareness on cybersecurity. Pre and post-game questionnaires containing Likert-type questions were used to assess the functionality and learning outcomes of the game. Through the said method, the study found that there was an improvement to the recognition of devices needed for Internet protection. Another study by Balayan et al. exhibits the potential of GBL as a method for reaching the specific learning goals of its participants. [1] aimed to assess SkillVille, a mobile game aiming to teach common visual perception skills. Learning analytics was used to monitor the performance and improvement of the users. They were able to conclude that SkillVille is a potential learning tool recommended for educational enhancement. With the results of the studies and the aforementioned rationale, a game-based learning approach in raising awareness on data privacy concerns was chosen by the researchers.

The premise of the game revolves around scenarios that simulate various interactions in social media. These interactions include setting up a social media account, posting on social media, tagging people in posts, and tweaking privacy settings. The key takeaway for the audience is; on being mindful of what content they share, being sensible of others' consent, and navigating through privacy options. Gamification of the key points of the Data Privacy Act allows for a medium that is rewarding, interactive, and engaging for the target audience with the intention of teaching them how to protect their privacy rights.

2 REVIEW OF THE STATE OF THE ART

Gamification is the use of game elements and mechanics in traditionally non-game contexts. Gamification offers enhanced interaction and engagement between the audience and the medium through various game modes making the learning experience more encouraging. There's also the element of gratification through awarding of points or virtual rewards by accomplishing tasks within the game giving a sense of progress.

2.1 Effectiveness of Gamification

In a study conducted by Dicheva et al. on the directions and tendencies of applications of gamification to education, published empirical research on game elements used in educational contexts was reviewed. The researchers of this study noted that there is a lack of empirical research on the effectiveness of gamification in an educational setting. In this study, however, there is a consensus that gamification has the potential to enhance learning granted that it has undergone proper development and is used as intended. [5] reported the following benefits of gamification. A significantly higher engagement and participation from its students. The benefits of increased class contributions, percentage of passing students, participation in voluntary activities, and a reduction in the gap between the bottom and top graders were also noted behaviors of the students. Gratification from in-game rewards was also noted to have an impact on student performance even if it had no direct impact on their final grading. It was also the students' opinion that the gamified instances were more motivating, interesting, and easier to learn than their other courses [5]. These would be target outcomes from employing GBL in this research.

2.2 Visual Novel as a Situational Simulation

The work of Gensheimer et al. is an example of situational simulation as an application of gamification for educational contexts. In [8], the gamification of the Waterfall model topic in Software Engineering was implemented in the form of a Visual Novel. A visual novel is a genre of interactive fiction video games that rely primarily on text and illustrations to tell a story. The user interaction varies from button clicks to progress the story, selecting dialogue options, entering text, and choosing decisions that could affect the outcome of the story. Visual novels allow for a medium of complex topics to be conveyed playfully supporting the learning process of the students [8]. The design philosophy of the visual novel is that it consists of several scenes each with target learning outcomes from the players with varying levels of interaction. It was emphasized that visual novels used in an educational context should focus on specific topics, thus the story should revolve around the topic that is intended to be taught [8]. The potential of visual novels to simplify complex topics through a text-based narrative while offering a high level of interaction with its players makes it a suitable medium for gamification in an educational context. In their study, the researchers were able to develop a visual novel game with a story that revolves around teaching the topic of the Waterfall model. It is intended to be used as additional material in teaching the topic, however, its effectiveness was not evaluated, and the researchers suggested that further work should be done to survey the acceptance level of the game [8].

2.3 Existing GBL Solutions on Data Privacy and Security

This subsection is a review on existing solutions (2.3.1,2.3.2,2.3.3) that utilize game-based learning to address Cyber Security and Cyber Wellness topics. A commonality in these solutions is the development of specific game scenarios to tackle a specific objective point of learning about the overlying topic of Cyber Security / Wellness. In line with these, this research will adopt a similar approach to developing game events to address specific digital privacy concerns. This will enable the researchers to evaluate the awareness raised on a specific privacy concern by isolating them into specific scenes as learning objectives.

In the evaluation of the developed solution, these solutions employed pre and post-questionnaires. These were used as the basis for the improvement in the respondents' performance by comparing their responses before playing the solution and then after. Two of the works were able to administer a post-questionnaire and their results suggest that the game approach was conducive to learning. As the research aims to evaluate the effectiveness of the developed solution for raising awareness of digital privacy risks, a similar approach to a pre and post-questionnaire method will be used with the appropriate modification to address the issue.

2.3.1 Game-based learning platform to enhance cybersecurity education . [14] is a GBL solution that is targeted to address the constantly evolving threat of cyberattacks. The objective of the solution was to provide the players with tools to learn about cybersecurity challenges at their own pace. The categories of cybersecurity challenges tackled were reverse engineering, cryptography, web security, forensics, and binary exploitation. The implementation is composed of two components. To evaluate their solution, a pre-questionnaire was administered to gain insights into the participant's knowledge level regarding game-based cybersecurity consisting of yes or no questions. The responses from the pre-questionnaire indicated a low level of knowledge regarding computer security problems but found that there is a high level of motivation for learning through games and challenges. A post-questionnaire was also prepared for future evaluation of the platform, however, this was not administered

While [14] was able to create a solution that induced motivation for learning about cybersecurity challenges (reverse engineering, cryptography, web security, forensics, and binary exploitation) through GBL, the research was unable to cover certain Data Privacy and Security aspects. Specifically, the scope did not include Data Privacy dangers that users expose themselves to while using Social Media, the main focus of this study. It focused more on hacking skills with ethics taken in mind.

2.3.2 CyberAware: A mobile game-based app for cybersecurity education and awareness. [9] is also a solution targeted at cybersecurity education and awareness that utilizes game-based activities for learning. The implemented solution is Cyberaware, which was developed to address cybersecurity among young people because of the evident increased internet penetration in this age group. In particular, Cyberaware is designed for K-6-aged children. The game is comprised of mini-games that are either categorized as security or privacy. Successful completion of the mini-games unlocks "shields" motivating the player. With this approach, learning is expected to be self-administered as the discovery of knowledge is entirely by the student. The topics tackled are on firewall technologies, antivirus software, security patches, and email spam filters. A strong consideration for this implementation is the Bring Your Own Device which meant that CyberAware was designed to be easily accessible. Evaluation was also conducted in the form of pre and post-questionnaires which are designed to be administered before and after playing Cyberaware, assessing the functionality and learning outcomes from playing the game. This was in the form of Likert-type questions with choices of answers ranging from strongly disagree to strongly agree. The evaluation highlighted an improvement of 15% regarding recognition of protection for Internet-connected devices.

The solution mainly focused on cybersecurity education and awareness. The scope included specific learning goals for Data Security but lacks topics for Data Privacy. Additionally, the solutions proposed by Giannakas et al. did not directly address security and privacy topics. Hence, they recommended case-based scenarios that relate to security and privacy learning and awareness.

2.3.3 Effects of Digital Game-Based Learning on Students' Cyber Wellness Literacy, Learning Motivations, and Engagement. [19] is another GBL solution that addresses cyber wellness literacy, mainly tackling Internet addiction. It's designed as an educational escape room with the narrative objective of saving a friend from gaming addiction. The game is spread through various scenes in which the player must collect "knowledge points" on Internet addiction symptoms. Its gameplay follows a storyline that progresses by clicking and selecting the player in interactable sections. The game also provides immediate feedback by providing tips and prompting the right answer and an explanation for these answers. The game was developed on Articulate Storyline3 and deployed as a web-based game on a Tencent Cloud Server allowing for cross-platform access. The researchers have noted the cross-platform accessibility of the game as a criterion for developing the game.

Pre and post-questionnaires were also designed to measure the cyber wellness literacy of the respondents. Two groups of respondents were formed, a group learning about cyber wellness through traditional lessons and another through the developed digital game, answering the same set of questionnaires. Similarly, the questionnaires consisted of Likert-like questions regarding the awareness of the respondents on rational use and their views on technology.

Regarding the effectiveness of methods, an independent t-test was used to compare the post-test literacy of the two groups. The result was that those who were part of the group who learned through the digital gaming approach scored significantly higher than those who learned through traditional methods. To compare the pre and post-questionnaire responses, a paired sample statistical t-test was performed. The results indicated a significantly greater cyber literacy among the respondents in the post-game responses suggesting a positive learning effect after the course. There were also higher reported levels of intrinsic and extrinsic motivation to learn from playing the game.

These positive results of the GBL approach mainly covers the topic of Internet addiction. The utilization of interactive graphic novel for the design of GBL, the use of pre and post-game questionnaires, and paired t-test can be further applied into more topics such as in digital privacy risks in social media usage.

3 OUR PROPOSED SOLUTION

Digital privacy is a growing concern as the population of internet users increases in this digital age. That is why our research group is proposing a video game aimed at raising awareness of online behavior that is potentially harmful to one's digital privacy due to the use of social media platforms.

From the shortcomings noted and insights sought on the existing GBL approaches in 2.3, the proposed video game aims to revolve around digital privacy issues on social media, to directly address the said issues, and utilize the visual novel design and useful aspects of existing solutions.

The solution will be in the form of a simulated social media platform with the objective of guiding the audience on what content they share, essentially using visual novels for GBL in 2.3.3 on the topic of digital privacy. The video game will show them how to navigate through various privacy and permission settings ensuring that no excessive personal information is released to the public. Similar to the considerations of the study in 2.3.1, but applied to the topic of digital privacy. The choice of situational simulation as the mode of GBL is so that the players are immersed in an environment that would be familiar to real-life social media platforms without the consequence that come with its usage. The idea being that they would apply what they've learned in playing the game to the real-life experience.

The proposed solution will incorporate learning objectives to the events in the game. Specifically, each event will have a corresponding digital privacy risk to tackle, enabling the GBL design to directly address digital privacy issues and essentially supplement the limitation in 2.3.2 (Cyber-Aware). These events will be evaluated by performing a pre-test and post-test on a single group of respondents. Similar to the works mentioned, the pre-test will assess the respondent's preconceived awareness on digital privacy risks whereas the post-test will assess whether there was an improvement on their awareness after playing the game solution. This will be verified using a paired t test which would verify whether the improvements, should there be any after playing the game are statistically significant.

3.1 Game Overview

The game will be in the form of a visual novel, a genre of video games that emphasizes narrative storytelling with player interaction for an enhanced learning experience.

3.1.1 Premise. The game's premise revolves around the player taking the role of the main character who is invited to their friend's birthday party. At the party, their other friends invite them to install the new trending social media app, which makes it easier to take pictures and videos and then share them with friends. Once installed, the player is guided in the process of setting up the social media application, using it to take pictures, then sharing their post on social media.

3.1.2 Narrative. The narrative of the game will take place through 10 scenarios, 8 of which simulate online behavior that is potentially a risk to their digital privacy. In these scenarios, the players are to make decisions in the game that would affect their digital privacy positively or negatively. These decisions are tracked and would be reviewed at the end of the game, recapping the negative decisions the player made, along with a discussion on why these decisions are potentially harmful.

3.1.3 Scenes. As the game is intended to develop the player's awareness of privacy risks regarding their digital privacy, each scene is designed such that it has a target privacy risk to address which will be referred to as **privacy risk pointers**. The table below is an overview of these implemented scenes in the current implementation of the game. This describes the event or setting, the target privacy risk pointer being addressed, and the objective of each scene. For a more detailed discussion of each scene along with illustrations of gameplay mechanics, refer to the Scene Analysis and Gameplay subsection of the Appendix 6.

Table 1. Scenes Overview

Scene	**Event**	**Privacy Risk Pointers**	**Objective**
1	Player opens the invitation to their friend's party.	None	Scene serves as the player's profile/creation setup. Player chooses their name and appearance.
2	Arrival at friend's party / Installation of social media application.	App Permissions	Awareness of what services are given permission to the application. Differentiate the kinds of permissions or access a user can give to an application.
3	Creation of username.	Username Selection	The player selects a username from a set of choices. Usernames can contain a person's real name or full name which can lead to doxxing of the person.
4	Trying the app / Taking pictures of friends during the party.	None	The player interacts with the app, taking pictures of their friends using the camera.

Table 1 – continued from previous page

Scene	Event	Privacy Risk Pointers	Details
5	Selecting a photo to post / Tagging of friends.	Photo Selection Tagging of Friends	Player selects a photo to post from the photos they have taken. These photos can contain sensitive information such as disclosing a person's whereabouts. Player tags their friends in the photo. Incorrect tagging in posts can lead to concerns to the affected person's privacy, even possibly lead to defamation.
6	Selecting a caption.	Caption selection.	A caption can explain in detail the contents of the photos. This can include full names, the nature of the event, location, and other sensitive information. The objective of this scene is for players to be sensitive to what information they disclose.
7	Additional Settings. Location Data	Post Visibility	Set whether to include the location of where photos were taken. Set the visibility of the post whether to friends only, friends of friends, or the public.
8	Tags consent	Removal of Tags	Teaches the player to respect the digital privacy of others as well. In this case, respecting the consent of a person not to be tagged in a post.
9	Removing a tag from a friend's post.	Persuasive Features	Introduces players to deceptive design, coercing them to keep a feature, in this case, their tags. In this scenario, when a player attempts to remove their tag from a friend's post, they are prompted with a message from the app explaining that they will be missing out on features/experiences.
10	Tags Review	Tagging Behavior	As a user, it is in their rights and authority to review any information posted of you. This is shown through a scenario in which the player is tagged in a photo they didn't know was taken. A person can revoke their tags on this photo. They can also adjust the behavior of tagging for future posts.

3.2 Architecture

3.2.1 Game Architecture. Daily Digital Privacy follows a Model-View-Controller Architecture or MVC [4]. As the proposed solution is to be developed as a game, adopting MVC architecture will allow for better organization during development. It also allows for scalability should this research be continued. MVC consists of three components, the Model, View, and Controller. The Model component mainly handles game logic and scripting. This includes game functionalities involving the definition of rules and tracking of player decisions, scores, and progress. It is also responsible for handling the game state such as the status and state of the entities but not necessarily concerned with what is being displayed. The View component is responsible for rendering the current game state from the Model and displaying it on the screen of the player. The Controller receives and interprets user input and translates the actions of the player into events that affect the Model and effectively the game state.

3.2.2 Research Design. The methodology of this research revolves around investigating how the game “Daily Data Privacy” changed the level of awareness of the users regarding the potential risks on their data privacy when using social media.

The experimental research involved making a game that aims to expose the participants to different data privacy concerns in using social media and asking the participants to answer a pre-game and a post-game questionnaire to measure the difference in their awareness of the said concepts. The design principles of making the game are detailed below. The creation of the game mainly revolved around the points on the rights of the users as stated in Sections 12, 16, and 20 of the Data Privacy Act of 2012. The chosen points to be used as the fundamentals of the game 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 rights and pointers listed above became the basis of making the game. The researchers then came up with different scenes with important points denoting different real-life situations that also relate with the pointers above. The resulting scenes that tackle these data privacy risks and concerns are shown in the table below.

Table 2. Privacy Risk Pointers and Relevant Items

Privacy Risk Pointer	**Item no. in Data Privacy Knowledge List Covered/Relevant**
App Permissions	1, 2, 6
Username Selection	4
Photo Selection	7
Tagging of Friends	4, 7
Caption Selection	7
Location Data	3, 7
Post Visibility	3, 7
Removal of Tags	5, 6, 7

Table 2 – continued from previous page

Privacy Risk Pointer	Item no. in Data Privacy Knowledge List Covered/Relevant
Persuasive Features	2, 3, 4, 5, 6
Tagging Behavior	2, 3, 4, 5, 6, 7

Shown above is the table denoting both the risks and concerns along with the data privacy pointers that come along them. These are the concepts that were used to assess the awareness of the respondents. The said concepts cover aspects of modern social media usage that have potential risks in people's data privacy.

Pre-game and post-game questionnaires were also created to measure the awareness of the participants of the study. The pre-game questionnaire was answered by the respondents before the game to measure their initial awareness on the topics, while the post-game questionnaire was answered afterwards to measure their new awareness. The questionnaire consists of a Likert scale to quantitatively assess their knowledge on the data privacy risk concepts. Qualitative assessment was also added to the questionnaires which includes a question about the respondents' knowledge on the Data Privacy Act in the pre-game questionnaire as well as the participants' realizations and possible learnings after playing the game in the post-game questionnaire.

These questionnaires aim to find the difference in their awareness before and after playing the game quantitatively and qualitatively.

4 DISCUSSION

4.1 Game Development

The current implementation of Daily Digital Privacy is developed using the Godot engine. Godot is a free cross-platform game engine that allows the development of 2D and 3D games. Its features, versatility, and existing frameworks set it as a good candidate to be the engine of choice.

A major consideration for the choice of engine was the Dialogic plugin. As the game is designed as a visual novel, the Dialogic plugin is utilized for facilitating the construction and display of dialogue sequences in the game. Dialogues in the game between the player, guide, and other characters will be the main driver for the story-telling of the game.

As Godot follows Object Oriented Programming design principles [10], the project was developed in accordance with these principles. Daily Digital Privacy's architecture follows OOP architecture. The narrative scenes 1 in the planned story are implemented as objects called Godot scenes. A Godot scene is comprised of nodes that define the positioning and properties of assets and interactable controls by the player. Each scene and node can then be called or extended as needed. These scenes are what is displayed on the player's screen while playing the game.

For simplicity, a node can be an asset such as a player's icon or background image. It may also be an interactable object such as a clickable button or a drop down menu. A scene is a collection of these nodes which comprises what would be shown on the screen of the player. These nodes can be extended or used by other scenes as well. The controller of the game, particularly the scenes, is implemented in Godot's proprietary gdscript. The gdscript defines the game logic such as the functionality, scripting, calling, and order of appearance of the scenes.

The project primarily consists of 3 components: the world.gd file, world.tscn file, and the dialogic directory.

world.gd. The world.gd file, written in Godot's proprietary gdscript language, handles the logic of the game. It manages the game environment, controls the scenes displayed on the screen, and calls the necessary assets and dialogues from the world.tscn file and the dialogic directory. As each scene has a learning objective and corresponding player decision, this file also facilitates the tracking of the player's decisions and tracking their scores throughout the game. In each scene from 1 that has a corresponding Risk Pointer, players are presented with the choice of making a positive, negative, or neutral option. These decisions are weighted accordingly and are tracked. The summary of scores is presented at the end of the game during the review section shown.

world.tscn. The world.tscn stores the data structures that define the scenes or nodes used in the game. It contains the positioning and properties of assets, resources, and interactable controls.

dialogic directory. The dialogic directory contains all the characters and dialogues used in the game. Using the dialogic screen, the developer can define characters and timelines which contain the content of the dialogues.

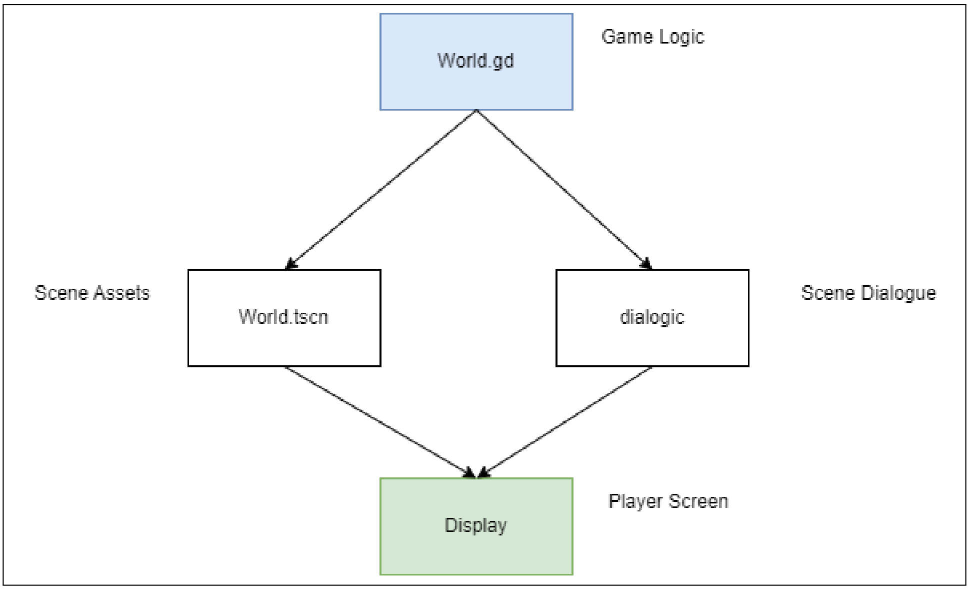


Fig. 1. Game Design Structure

4.2 Game Deployment

4.3 Testing

4.3.1 Participants. The game was published on gotm.io and 4 millennial adults (1977-1995) and 39 respondents belonging to Gen Z (1996-2010) participated according to the data that they provided in the questionnaire. No requirements were given to the participants aside from their ability to participate in the research.

4.3.2 Data Collection Methods. As mentioned above, the researchers used a questionnaire to gather the pre-game and post-game data of the participants. Below is a table that enumerates the data collected, the type of data, the measure used in collecting the data, along with a short description of the data.

Table 3. Data Collection and Measurement Used

Data Collected	**Data Type**	**Measurement Used**	**Short Description**	**Questionnaire that Measured**
User Consent	Required	N/A	Consent of users in participating in the study and collection of data for research.	Pre-game
Name	Optional, Qualitative	Text	Name of the participant	Pre-game
Email	Required, Qualitative	Email formatted text	Required data to verify users across the two questionnaires	Pre-game
Year of Birth	Required, Quantitative	Date: Year	Used to identify the generation category of the participant	Pre-game
Time Spent on Social Media	Required, Quantitative	Likert Scale, Usage frequency	Denoting the frequency of social media	Pre-game
Social Media Platform used	Required, Qualitative	Enumeration (text)	Social media used (e.g., Facebook, Instagram)	Pre-game
Knowledge on Data Privacy Act	Required, Qualitative	Yes/No Option with Short essay	Asks the users if they know the Data Privacy Act of 2012. Essay asks to elaborate, if answered yes.	Pre-game
Level of Awareness on Privacy Risk Pointers	Required, Quantitative	Likert Scale	Scale ranging from 1 (Not aware) to 5 (Well aware) on the pointers in the Privacy Risk Pointers Table[2]	Pre-game and Post-game
Participant Realization	Optional, Qualitative	Short essay	Short essay asking the participants regarding the risks after playing the game.	Post-game

The table above shows the data that were collected using the questionnaire, the type of data, the measurement used, and which questionnaire measured the said data. From the collected data, the researchers proceeded with the analysis of the data.

4.3.3 Data Analysis. The data analysis was conducted by processing the Google Sheets obtained from the responses in both the questionnaires using Python in Google Colab.

The data was first pre-processed to remove the responses in the pre-game and post-game questionnaires that did not use the same email in answering, as these responses cannot be compared in-between questionnaires.

The next step was the analysis of the demographics. The respondents' generations were analyzed using the date of the year that they provided. The categorization of the generations used was based on [16]. The social media usage of the users along with the platforms that they use were also graphed to show the most used social media. Lastly, the participants' knowledge was also analyzed.

Afterward, the number of participants that improved was counted based on the scores that they provided with their level of awareness. The labels for the scores to show improvement are: "Improved", "Unchanged", and "Lowered". The analysis on the improvement was done per topic to see which topics the game had the most impact on.

For the overall analysis of the awareness, the means of the scores of each data privacy risk pointer were taken, pre-game and post-game. The difference between each means were graphed to show the topics that the game had the most impact on, in terms of level of awareness.

In line with the approach done in 2.3.3, Paired sample t-test was used to determine if there is a significant change to the two tests. The null hypothesis is stated as: The means of the two tests have no significant difference; and the alternative hypothesis: The means of the two tests have a significant difference. The significance level 95% was compared with the p-value to accept/reject the null hypothesis.

In [20], a paired sample t test is a comparison of measurements for related units. It cites the comparison of pre-test and post-test scores as a valid use of the statistical test. Its purpose is to determine whether there is statistical evidence that the mean difference between paired observations is significantly different. For the purpose of this research, This test will determine the statistical significance of any differences in the scores of the respondents in the post-game questionnaire against the pre-game questionnaire. This would validate any improvement should there be any observed in the improvement of the respondents' score. It is noted that a requirement of the paired t test is that the units be paired, continuous, and normally distributed.

Lastly, the answers of the participants on the realization essay were used to verify their responses on the awareness level, as well as provide qualitative data for reference.

The overall procedure that was conducted by the researchers are as follows.

- Assessment of game requirements The specific requirements and details of the target players were given importance to the game: especially the method of access, the age group, their initial knowledge, along with the relevance of the players with the goal of the game. The visual novel type was chosen as the class of game to be created in consideration of the intuitiveness to the players, the ease of creation, and the expandability of the coverage of the game, in terms of the scope of topics.
- Creating the Storyboard for the game Before proceeding to the creation of the game, the researchers designed a storyboard for the said visual novel game. The aforementioned data privacy risk topics listed in 2 was used as the basis for creating the storyboard for the game.
- Game development via Godot Engine Godot Engine was used for the development of the game. The software had the capacity for exporting in different forms. HTML5 was used for the exportation to enable publishing on websites.
- Bugfix and game refinement The game underwent multiple bug fixes, refinement, and re-calibration of elements and components based on internal feedback on its scope, clarity, and other possible improvements.

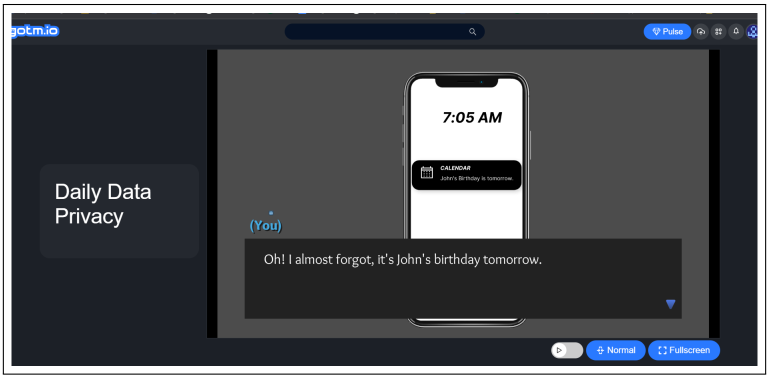
- Creation of questionnaires The questionnaires were formulated to measure the awareness of the participants in the game's data privacy pointers as shown in 2. Additionally, the demographics' information on their social media usage, year of birth, knowledge on the Data Privacy Act, and game realizations were also asked in the said questionnaire. These were collected to gain more insights on the demographic and obtain qualitative data to support the quantitative data.
- Online publishing of the game and questionnaires The HTML5-exported version of the game was published by researchers on the online game hosting platform Gotm.io. This allowed the participants to access the game using a link that will redirect their browser to the said game. Gotm.io was used as the platform because of its zero-price hosting and its ability to support the game, enabling players to play it in the browser, translating to availability to participants regardless of the device or OS that they are using.
- Data analysis The researchers used the responses from the questionnaires that the participant filled up to analyze the data and gather insights regarding the impact of the game in terms of the change of awareness in the participants after playing the game.
- Drafting of Paper Lastly, the researchers proceeded to the drafting and making of the paper.

With respect to the rights of the participants regarding their data, the survey asked for their consent on using the data for the research before participating. Additionally, access to the responses of the data were secured privately, only to be disclosed to the researchers and relevant advisers on the research matter.

4.3.4 Limitations. · The game was published online and through Facebook and Discord, which might create a bias on the participants' demographic. · Additionally, the participants consisted mostly of Generation Z participants, with some Gen Y included. Other generations such as Baby Boomers and Gen X were not covered in the study.

4.3.5 Reproducability. To enable reproducibility of the study, the link for the game is available in the Appendix sections6. Should there be a need for more information, the researchers could be contacted through the provided email addresses.

Another consideration for the choice of game engine was the options for deployment. Gotm.io is a free-hosting platform for Godot-based games allowing deployment of the researcher's project that is accessible to a wide range of audiences or players. Once published in Gotm.io, the game can be shared given a provided link that a user can open on compatible browsers, allowing them to play the game on desktops and mobile devices.



Oh! I almost forgot, it's John's birthday tomorrow.

Fig. 2. Game Deployment on Gotm.io

4.4 Results

4.4.1 Demographics.

Number of Responses. A total of 43 respondents participated in the testing of the project. Among the respondents, 39 were identified to be **Gen-Z** age group, accounting for 90.7% of the respondents. The remaining 9.3% belonged to the **Gen-Y** age group with 4 respondents. These age groups are based on the generational groups defined in [16].

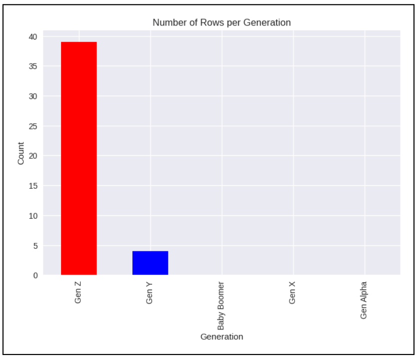


Fig. 3. Age Group Generations

Social Media Platforms Used. Among the respondents, the three most popular social media platforms were **Facebook, Instagram, and Twitter**, with 35, 32, and 26 users, respectively. It is important to note that respondents were allowed to mention multiple platforms. These were followed by **TikTok and YouTube**, with 12 and 9 users, respectively. The other platforms are shown in the graph below.

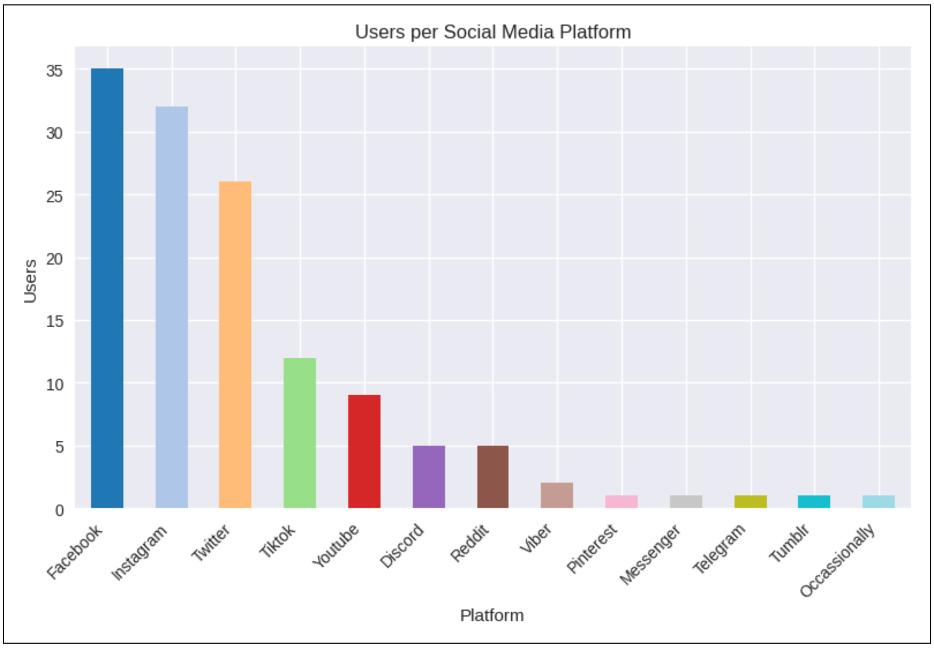


Fig. 4. Social Media Platforms Used

Knowledge on the Data Privacy Act. On whether the respondents know the Data Privacy Act of 2012, 33 of the respondents responded yes, while 10 responded no.

4.4.2 Respondent Improvement Levels. To evaluate the extent to which users' awareness of privacy risk pointers has improved, their responses from the Level of Awareness on Privacy Risk Pointers from the pre-game and post-game will be examined. By comparing their self-perceived level of awareness in the pre-game and post-game questionnaires, any improvement will be determined based on whether they reported a higher level of awareness after the game.

Pre-processing: To ensure that the pre-game and post-game responses being compared belong to the same respondent, the respondent's email is utilized as a unique identifier or key for the data. After matching the pre-game and post-game responses based on the unique email, it is found that there are a total of 35 responses. The decrease in the number could be due to respondents either using different emails for each questionnaire or not completing both questionnaires as instructed.

Individual Level of Awareness Comparison. The respondent's post-game and pre-game responses are compared for each privacy risk pointer. Their improvement for each pointer is classified as follows:

(1) If their level of awareness in the post-game is higher than their pre-game level of awareness, then this is labeled as: **Improved**
(2) If their level of awareness in the post-game is the same as their pre-game level of awareness, then this is labeled as: **Unchanged**
(3) If their level of awareness in the post-game is lower than their pre-game level of awareness, then this is labeled as: **Lowered**

The improvement scores are summarized in the table below:

Table 4. Privacy Risk Pointer Improvement Summary

Privacy Risk Pointer	**Improved**	**Unchanged**	**Lowered**
App Permission	12	21	2
Username Selection	19	14	2
Photo Selection	12	20	3
Caption Selection	21	12	2
Location Data	7	24	4
Post Visibility	9	23	3
Removal of Tags	14	18	3
Persuasive Features	13	18	4
Tagging Behavior	16	14	5

Along with the plot to visualize the improvement of the respondents on each Privacy Risk Pointer.

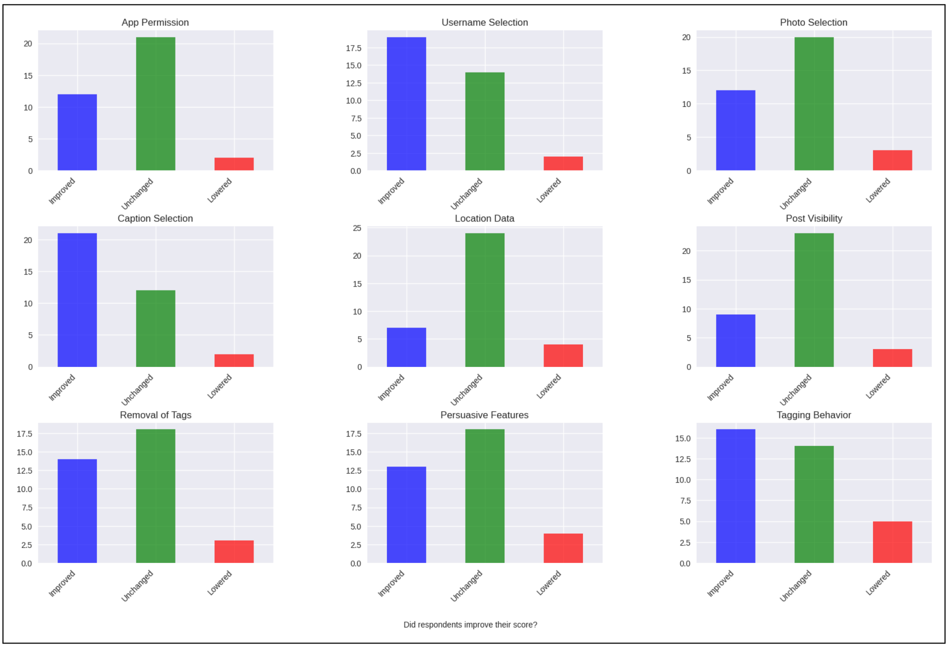


Fig. 5. Privacy Risk Pointers Improvement

Per topic, the average number of respondents whose **awareness level lowered is 3**. There were generally more respondents whose level of awareness improved or was unchanged in each pointer. On average **13 respondents improved** their awareness level while those whose awareness level **was unchanged was an average of 18 respondents**.

The privacy risk pointers with the **most numbers of improved scores was on Photo Selection** where 21 respondents improved on their post-game assessment, with 12 whose scores were unchanged, and 2 with lower scores. This indicates that a significant number of individuals who experienced improvements may not have been aware of the potential privacy risks associated with the photos they choose to post. These risks could include inadvertently sharing sensitive information through the images they share.

Most numbers of respondents whose **level of awareness lowered was 5, which is on the risk of Persuasive Features**. Those who improved their score was 16 while those whose scare was unchanged was 14. A possible reason for the respondents having a lower level of awareness of this pointer is that they might have a higher initial level of preconceived awareness regarding that topic, which may have changed after it was tackled during the game, a realization that they had lower awareness regarding this pointer. It is also possible that the implementation of these persuasive features was not implemented well in the game and may have led the respondents to have a lower level of awareness.

Overall Improvement on Awareness Level. To evaluate the respondents' overall improvement level, their improvement levels on each pointer are collected and weighted. An improved score is weighed positively, unimproved has zero weight, and a lowered score is weighted negatively. The overall improvement level for each respondent is determined by summing these weights.

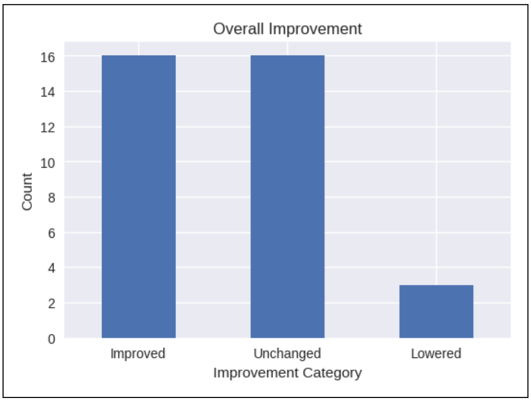


Fig. 6. Privacy Risk Pointers Overall Improvement

The overall improvement levels of the population are: **16 respondents improved**,**16 respondents awareness level unchanged** and **3 respondents awareness level lowered** on their post-game assessments.

4.4.3 Pre-Game and Post-Game Means. This section looks at the performance of the respondents by analyzing the means of their self-perceived awareness levels. This was done by calculating the average awareness level of the respondents for each privacy risk pointer for the pre-game and post-game responses. The averages, rounded to 4 decimal places, are summarized in the table below:

Table 5. Privacy Risk Pointer Means

Privacy Risk Pointer	**Pre-Game Average**	**Post-Game Average**	**Difference**
App Permission	4.4571	4.8571	0.4
Username Selection	3.4286	4.4	0.9714
Photo Selection	4.1714	4.5714	0.4

Table 5 – continued from previous page

Privacy Risk Pointer	**Pre-Game Average**	**Post-Game Average**	**Difference**
Caption Selection	3.3143	4.5143	1.2
Location Data	4.5714	4.6857	0.1143
Post Visibility	4.4	4.5143	0.1143
Removal of Tags	3.8286	4.4571	0.6286
Persuasive Features	3.1143	3.6	0.4857
Tagging Behavior	3.4	4.2	0.8

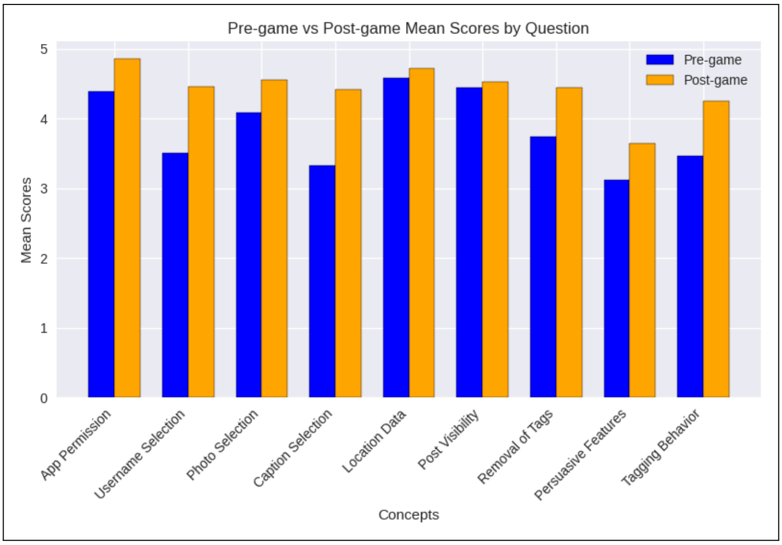


Fig. 7. Pre-Game and Post-Game Means for Each Privacy Risk Pointer

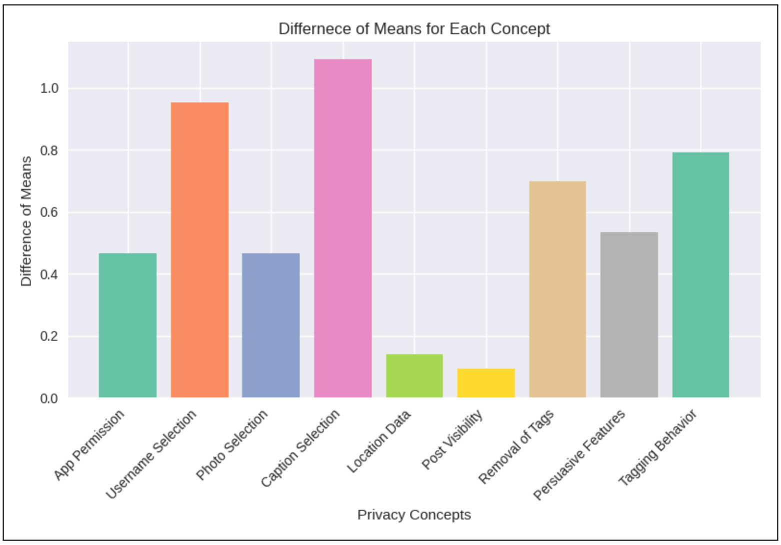


Fig. 8. Difference of Means for Each Privacy Risk Pointer

Across the privacy risk pointers, the difference in averages of the post-game and the pre-game responses are positive. This indicates that in all privacy risk pointers, the respondents on average scored higher in their responses after playing the game. Notable pointers where respondents had a higher average awareness level are on **Caption Selection, Username Selection, and Tagging Behavior** where the average level is higher by **1.2, 0.97, and 0.8** compared to the pre-game averages respectively. This would indicate that respondents improved their level of awareness regarding these privacy risk pointers the most after playing the game.

The lowest differences in means were on the **Location Data and Post Visibility** pointers which may indicate that the respondents already had a strong level of awareness prior to playing the game, hence the low level of improvement.

Although awareness levels improved on all pointers, it is noted that the responses for the pointer **Persuasive Features** are still relatively low with an average post-game awareness level of **3.6**. As mentioned in the previous subsection, this could be attributed to the pointed not being adequately contextualized or discussed in the game.

4.4.4 Statistical Test.

Paired T-test. The assessment of a pre-test and post-test qualifies this research to be evaluated using a **Paired T-Test** as discussed in 4.3.3. The intent of this test is to evaluate the impact of the game on raising awareness of the defined data privacy risk pointers. What the test indicates is whether there is a **significant statistical difference between the average scores of the respondents in the pre-game and post-game responses**. For this test, a **confidence level of 95%** is used. Positive statistical significance on the responses would indicate raised awareness caused by playing the game.

Hypotheses Definition. Before performing the test, the hypotheses are defined as follows:

(1) **Null Hypothesis:** There is no significant difference between the mean scores of the pre-game and post-game responses.

(2) **Alternative Hypothesis:** There is a significant difference between the mean scores of the pre-game and post-game responses.

Using the Shapiro-Wilke test, the means of both pre and post-responses were found to be normally distributed and continuous. This meets the qualifications for using the paired t test.

The results of the paired t test are as follows:

- **T-Statistic:** -4.6087205316313975
- **P-Value:** 0.0017355633470949611

The obtained t-statistic of -4.609 suggests that the mean of the post-game scores is higher than the mean of the pre-game scores. The significance of this difference is assessed by the p-value. In this case, the calculated p-value is 0.0017356, which is smaller than the chosen significance level of 5% (corresponding to the 95% confidence level). These statistical values provide sufficient evidence to **reject the null hypothesis**. Therefore there is a significant difference in the levels of awareness among the respondents before and after playing the game.

Based on these results, it can be concluded that the project, a video game designed to raise awareness of various digital privacy risks, achieved its objective as the difference in the mean scores of the responses is statistically significant.

5 CONCLUSION

5.1 Summary

Daily Digital Privacy is a Game-Based Learning solution aimed to raise awareness of the potential risks to personal digital privacy stemming from today's continuous growth of internet penetration and social media use. Developed as a situational simulation game, Daily Digital Privacy reproduces scenarios in social media that elicit potential privacy risks. These risks are termed by the researchers as Privacy Risk Pointers, privacy concepts that the solution targets to address. Namely, these pointers are *App Permissions, Username Selection, Photo Selection, Tagging of Friends, Caption Selection, Location Data, Post Visibility, Removal of Tags, Persuasive Features, and Tagging Behavior.* The game solution was developed on the Godot Game Engine and was deployed on the gotm.io platform. To evaluate the game's objective of raising awareness, pre and post-games were designed using Likert scales to measure the respondent's conceived awareness of each of the privacy risk pointers before and after playing the game. A call for respondents was conducted online through Facebook and Discord, totaling 43 respondents, reduced to 35 after matching the pre-game and post-game responses using the respondents' unique email. The results from the post-test showed benefits from playing the game. Regarding the improvement levels of the respondents, for each pointer, an average of 13 respondents had an improved score, 18 remained unchanged, and 3 would have a lower score. When comparing the mean scores of the pre and post-game responses, the mean scores of the post-game responses were higher for all of the risk pointers than its pre-game counterpart.

5.2 Insights

From the statistical tests, it can be concluded that the game Daily Data Privacy positively impacted the respondents' level of awareness of the listed Data Privacy Risk pointers. The awareness level of each respondent showed a positive increase on the said pointers. Further inspection of the specific pointers shows that most of the respondents showed an unchanged or improved awareness, which shows the game's potential as a tool for raising awareness. The photo selection pointer showed the highest number of improvements that may imply either great efficacy on the Daily Data Privacy and/or low initial awareness of the respondents to the risks of sharing images through social media. Further studies could be conducted in investigating the said Privacy Risk Pointer. Another insight gained from the results was the relatively low perceived awareness of Persuasive Features.

Numerous implications could be sought including respondents assessing that the said topic was more complex than initially thought or ineffective implementation on the part of the Daily Data Privacy game. The analysis of the pre-game and post-game means also shows more insight into these pointers, specifically the amount of improvement. The highest differences in the average awareness were observed in *Caption Selection, Username Selection, and Tagging Behavior.* This indicates the high amount of awareness developed among the respondents. The lowest difference was observed in *Location Data and Post Visibility.* This implies that the respondents already had a high awareness of risks in the said pointers. Lastly, the pointer *Persuasive Features* had the lowest mean in both pre-game and post-game, indicating that the sample population has a low awareness of the risk of their information on features on social media that are persuasive.

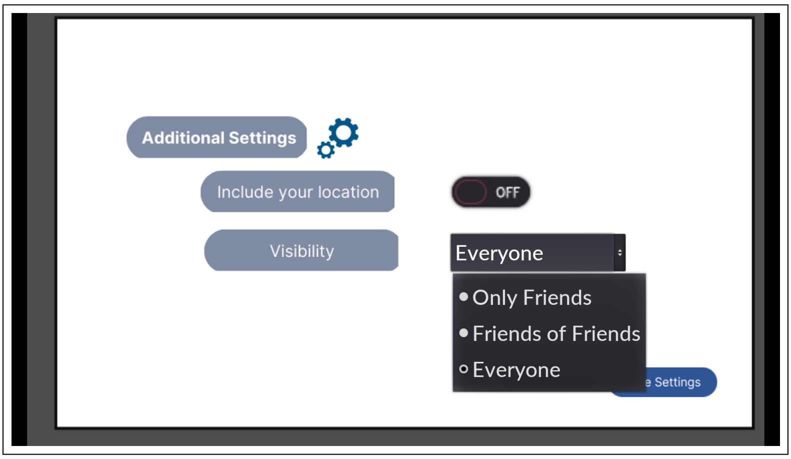
5.3 Limitations and Recommendations

With regards to the existing solutions, the current solution is novel given that it tackles the topic of personal digital privacy whereas the other works focused on cyber security and cyber wellness. The researchers were also able to statistically determine a significant improvement in the respondents' awareness on digital privacy risks after playing the game. As previously mentioned, the demographic of the participants of the study mostly represented the Gen-Z group, while having low representation for the Gen-Y and no representatives for the other generations. It is highly recommended for future research to study the awareness of these other groups not included in the research. In addition to having a different generation of participants, different Privacy Risk Pointers could be designed to incorporate different aspects of the Data Privacy Act as well as a different type or theme of the game. The researchers have noted *Persuasive Features* as the pointer that requires more contextualization as this is the pointer that received the lowest mean of improvement as well as the lowest mean score among the privacy risk pointers. With regard to evaluation, Wang et al. conducted tests on two distinct groups: one group used traditional methods, while the other group employed the game solution for learning [19]. This provided them a basis for whether game-based learning would be more effective than traditional learning methods. The researchers of Daily Digital Privacy were unable to conduct testing using traditional learning methods for teaching digital privacy concepts. As a recommendation, the researchers propose a further investigation into learning digital privacy concepts through traditional methods to gain insight into the benefits of Game-Based Learning. By comparing the effectiveness of Game-Based Learning with that of traditional methods in terms of topic comprehension and student motivation, this additional research could shed light on the benefits of each approach.

6 APPENDIX

6.1 Demonstration of Current Implementation

This subsection demonstrates the appearance and gameplay mechanics of Scene 7 of the current implementation of Daily Digital Privacy. In this scene, the player is preparing to post in the social media app. The player is prompted to an additional settings menu which includes location and post visibility settings. The player will decide whether they will include the location data in their post. They will also decide whether to set the visibility setting of their posts to *Only Friends, Friends of Friends, or Everyone.* The ideal settings would be for the player not to include location data and to limit the visibility of their posts to their friends only.



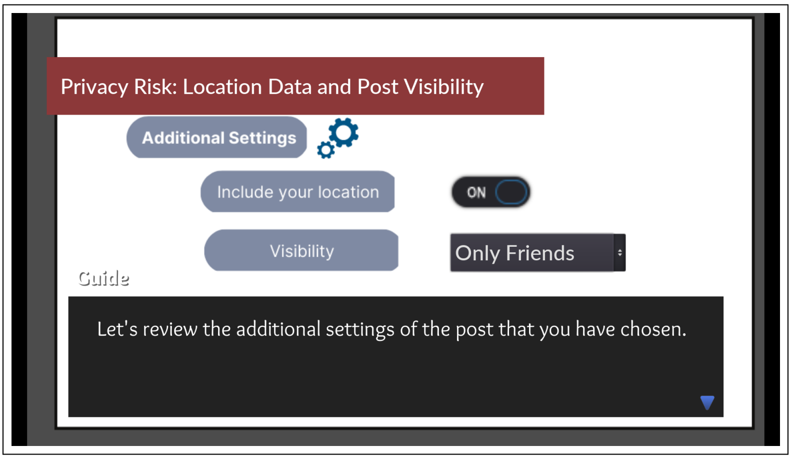
Include your location: OFF

Visibility: Everyone

● Only Friends
● Friends of Friends
○ Everyone

Fig. 9. Scene 7 Gameplay

At the end of the game, a review of the decisions the player made is conducted. Actions that are deemed potentially risky are recapped accompanied by a description as to why it is considered as such. In the case of scene 7, if the player chooses to include their location data, allow their post to be visible to those who are not their friends, or select both options, the review of scene 7 will be prompted to discuss these decisions. The intent of this review is to give an explanation as to how such online behavior can compromise personal digital privacy.



Privacy Risk: Location Data and Post Visibility

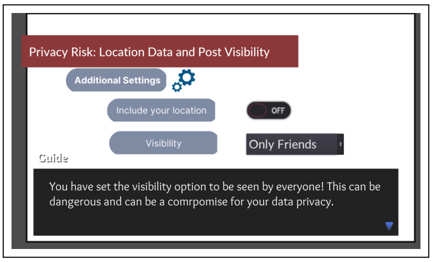
Include your location: ON

Visibility: Only Friends

Guide

Let's review the additional settings of the post that you have chosen.

Fig. 10. Scene 7 Review: Start



Privacy Risk: Location Data and Post Visibility

Include your location: OFF

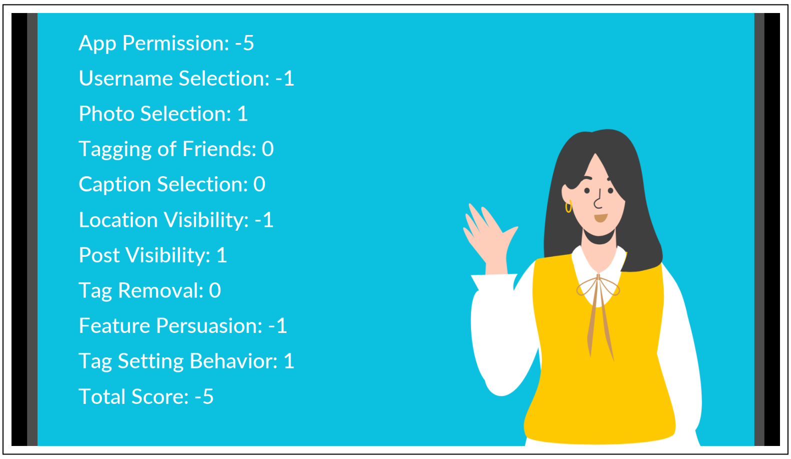
Visibility: Only Friends

Guide

You have set the visibility option to be seen by everyone! This can be dangerous and can be a comrpromise for your data privacy.

Fig. 11. Scene 7 Review: Visibility Settings

As mentioned in the Development of the game, these decisions are also weighted and have a corresponding score. The score for each scene is collected and displayed during the score summary at the end of the review.



App Permission: -5
Username Selection: -1
Photo Selection: 1
Tagging of Friends: 0
Caption Selection: 0
Location Visibility: -1
Post Visibility: 1
Tag Removal: 0
Feature Persuasion: -1
Tag Setting Behavior: 1
Total Score: -5

Fig. 12. Review: Score Summary

6.2 Questionnaires

To gain access to the pre-game and post-game questionnaires, you may contact the researchers using the given contact details.

6.3 Deployed Game

The game is currently deployed and accessible through this link Daily Digital Privacy.

6.4 Data Analysis

To view the codes used in the Data Analysis section, the viewable link of the Google Colab Python notebook can be accessed through this link Data Analysis.

REFERENCES

[1] Maricia Polene A. Balayan, Vanessa Viel B. Conoza, Jasmine Mae M. Tolentino, Rowena C. Solamo, and Rommel P. Feria. 2014. On evaluating skillville: An educational mobile game on visual perception skills. In *IISA 2014, The 5th International Conference on Information, Intelligence, Systems and Applications*. 69–74. https://doi.org/10.1109/IISA.2014.6878828

[2] National Privacy Commission. 2017. Data Privacy Act Primer. https://www.privacy.gov.ph/data-privacy-act-primer/

[3] National Privacy Commission. 2017. Know Your Rights. https://www.privacy.gov.ph/know-your-rights/#:~:text=Underthelawyouhave

[4] John Deacon. [n. d.]. Model-View-Controller Architecture – John Deacon. http://www.johndeacon.net/john-deacon/articles/model-view-controller-architecture/#:~:text=A%20controller%20is%20an%20object

[5] Darina Dicheva, Christo Dichev, Gennady Agre, and Galia Angelova. 2015. Gamification in Education: A Systematic Mapping Study. *Journal of Educational Technology & Society* 18, 3 (2015), 75–88. http://www.jstor.org/stable/jeductechsoci.18.3.75

[6] Kirstavridou Dimitra, Kousaris Konstantinos, Zafeiriou Christina, and Tzafilkou Katerina. 2020. Types of Game-Based Learning in Education: A Brief State of the Art and the Implementation in Greece. *European Educational Researcher* 3, 2 (2020), 87–100. https://eric.ed.gov/?id=EJ1265904

[7] Anja Feldmann, Oliver Gasser, Franziska Lichtblau, Enric Pujol, Ingmar Poese, Christoph Dietzel, Daniel Wagner, Matthias Wichtlhuber, Juan Tapiador, Narseo Vallina-Rodriguez, Oliver Hohlfeld, and Georgios Smaragdakis. 2021. A Year in Lockdown: How the Waves of COVID-19 Impact Internet Traffic. *Commun. ACM* 64, 7 (jun 2021), 101–108. https://doi.org/10.1145/3465212

[8] Matthias Gensheimer, Florian Huber, and Georg Hagel. 2020. Gamification in Software Engineering Education through Visual Novels. In *Proceedings of the 4th European Conference on Software Engineering Education* (Seeon/Bavaria, Germany) *(ECSEE '20)*. Association for Computing Machinery, New York, NY, USA, 1–5. https://doi.org/10.1145/3396802.3396808

[9] Filippos Giannakas, G. Kambourakis, and S. Gritzalis. 2015. CyberAware: A mobile game-based app for cybersecurity education and awareness. *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)* (2015). https://doi.org/10.1109/IMCTL.2015.7359553

[10] Godot. [n. d.]. Godot's design philosophy. https://docs.godotengine.org/en/stable/getting_started/introduction/godot_design_philosophy.html#object-oriented-design-and-composition

[11] Karl Kapp. 2014. *42 Chief Learning Officer • March 2014 • www.* https://www.cedma-europe.org/newsletter%20articles/Clomedia/Gamification%20-%20Separating%20Fact%20from%20Fiction%20(Mar%2014).pdf

[12] Simon Kemp. 2020. Digital 2020: The Philippines. https://datareportal.com/reports/digital-2020-philippines

[13] Simon Kemp. 2023. Digital 2023: The Philippines. https://datareportal.com/reports/digital-2023-philippines

[14] Manzoor Ahmed Khan, Adel Merabet, Shamma Alkaabi, and Hesham El Sayed. 2022. Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies* (Jan 2022). https://doi.org/10.1007/s10639-021-10807-6

[15] Meihua Qian and Karen R. Clark. 2016. Game-based Learning and 21st century skills: A review of recent research. *Computers in Human Behavior* 63 (Oct 2016), 50–58. https://doi.org/10.1016/j.chb.2016.05.023

[16] Beresford research. 2023. Age Range by Generation. https://www.beresfordresearch.com/age-range-by-generation/

[17] Cristiana S. Silva, Glívia A.R. Barbosa, Ismael S. Silva, Tatiane S. Silva, Fernando Mourão, and Flávio Coutinho. 2017. Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case Study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference* (Troy, New York, USA) *(WebSci '17)*. Association for Computing Machinery, New York, NY, USA, 63–71. https://doi.org/10.1145/3091478.3091479

[18] Jordi Soria-Comas and Josep Domingo-Ferrer. 2015. Big Data Privacy: Challenges to Privacy Principles and Models. *Data Science and Engineering* 1, 1 (Sep 2015), 21–28. https://doi.org/10.1007/s41019-015-0001-x

[19] Ke Wang, Panpan Liu, Junyi Zhang, Jinping Zhong, Xianfei Luo, Jingxiu Huang, and Yunxiang Zheng. 2023. Effects of Digital Game-Based Learning on Students' Cyber Wellness Literacy, Learning Motivations, and Engagement. *Sustainability* 15, 7 (Jan 2023), 5716. https://doi.org/10.3390/su15075716

[20] Kristin Yeager. 2022. LibGuides: SPSS Tutorials: Paired Samples t Test. https://libguides.library.kent.edu/spss/pairedsamplesttest#:~:text=The%20Paired%20Samples%20t%20Test