PERMA-RUN: A Persuasive Game to Create Awareness and Promote Secure Smartphone Behaviour

By

Anirudh Ganesh

Submitted in partial fulfilment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
June 2022

DEDICATION

I dedicate this thesis to my aunt
Late Mrs. Kalyani Kalyanaraman
and
my uncle
Late Mr. Raghavan Maruthuvakudi Vaidhyanathan.
Both of you always supported me and motivated me to follow my passion.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Smartphones have become an integral part of people's everyday lives. Due to the ubiquitous nature of smartphone and their functionalities, the data handled by these devices are sensitive. Despite the measures taken by smartphone companies to protect users' data, research has shown that people often do not take the necessary actions to stay safe from security and privacy threats. Sometimes, even people aware of security and privacy threats might not take the needed steps to secure their data. Persuasive games have been implemented across various domains to create awareness and motivate people towards a positive behaviour change. Even though games motivate users, research has shown that the one-size-fits-all approach for persuasive games might not be effective for all users. This thesis reports the design, development, and evaluation of Perma-Run, a persuasive game that aims to educate users and improve their awareness of smartphone security and privacy. We discuss the effect of tailoring Perma-Run according to the user's motivational orientation using the Regulatory Focus Theory.

LIST OF ABBREVIATIONS USED

ANOVA	Analysis of Variance
ARCS	Attention, Relevance, Confidence, Satisfaction
HEP	Heuristic Evaluation for Playability
HUD	Heads-Up Display
IMI	Intrinsic Motivation Inventory
NPC	Non-Playable Character
PMT	Protection Motivation Theory
PSD Model	Persuasive System Design Model
RFQ	Regulatory Focus Questionnaire
RM-ANOVA	Repeated Measure Analysis of Variance
RPG	Role-Playing Game
SSBS	Smartphone Security Behaviour Scale

ACKNOWLEDGEMENTS

Two years ago, I only dreamt of where I am now. If it was not for Dr. Rita Orji's grace, I would not be where I am today. Thank you for trusting me and accepting me as a Research Assistant in your lab. Thanks a lot for your guidance and support during this work. This has been a wonderful journey, and despite the pandemic, you made sure the transition was smooth for everyone and supported us during tough times. Thank you for recommending me for the Dalhousie Research Scholarship. It was helpful during the pandemic.

I also thank my committee members, Dr. Bonnie MacKay and Dr. Rina Wehbe, for volunteering to patiently read my thesis, and I thank Dr. Evangelos Milios for Chairing my Master's Thesis Defense.

Thanks to all my research colleagues (Chinenye, Ashfaq, Ravishankar Subramani Iyer, Ronit, Dinesh, Oladapo, Devansh, Banu, Joseph, Ifeanyi, Victor, Aniefiok, Ruth, Chimamaka, Noora, Mona, Felwah, Pratyasha, Smriti, Jaisheen, Dr. Gerry, Dr. Alaa) at the Persuasive Computing Lab who supported me through this journey and helped me with snowballing the survey. I could not have done it without your help! Thanks to Dalhousie University Library and the Library Staff at Killam for staying open and supporting the students during the pandemic. The library was my second home from where I was able to work in peace.

Finally, I thank my parents, Ganesh and Seetha Rani and my brother Adithya for their moral support throughout this journey. Thanks for motivating me during difficult times. It has been more than two long years, and I cannot wait to see your faces again!

A special thanks to my humble friend Adit(h)ya Balaji for tirelessly playtesting several versions of the game and providing detailed feedback about various bugs and glitches.

Finally, I thank all the gods for getting me through this phase of my life safe and sound.

CHAPTER 1 – INTRODUCTION

Cybersecurity and privacy have always been a topic of interest to researchers from various backgrounds. Usable privacy and security is one such niche under the cybersecurity umbrella that has always intrigued computer scientists. Usable privacy and security cover the users' experience with privacy and security aspects of digital devices [80,83]. User awareness about cybersecurity has been a research problem for a long time, and different interventions for various problems exist. In this age of ubiquitous computing, smartphones have become an integral part of our daily lives. People take their mobile phones with them all the time for their day-to-day tasks, and most of the time, their personal data is involved. In recent times, among other security and privacy issues, smartphone privacy and security have come under the spotlight. Despite the low user awareness around smartphone security and privacy, there are only a few interventions specifically focused on smartphone security and privacy issues. Hence, there is a clear need for interventions in this area. Throughout this thesis, cybersecurity or security, in general, refers to the usable security aspect of digital devices, and smartphone security refers to the usable security aspect of smartphones in general. Although, this thesis focuses only on the Android ecosystem.

1.1 The Problem in Focus

Humans are the weakest link in the chain of cybersecurity [121], and they have been ignored in the initial stages of cybersecurity research. There are various problems in the domain of usable privacy and security. To overcome these problems, many interventions exist and have had successful outcomes. Some of the interventions among these are persuasive games designed to be played by anyone. Compared to traditional educational interventions [122], gameful interventions have shown more success in recent times. For various problems in the domain of cybersecurity, several gameful interventions have been there for a long time [34,98,123,152]. Smartphones have evolved in various ways, and the uniformity in design (both hardware and software) is seen in many phones. The uniformity in design covered some of the common smartphone issues, yet the problem of privacy and security seemed to have evolved along with smartphone advancements. Over the past few years, users' personal information has been compromised in several instances without their knowledge through Android apps [19,124]. Recently, various security flaws were found and patched up [46], but recent research shows that user awareness about smartphone security is low and that there is a need for interventions [20,72,102,121,133]. Surprisingly, only a limited number of interventions for smartphone security and privacy awareness exist, and they cover only a few issues [9,10,160].

1.2 Motivation Behind the Solution

Over the years, users' personal information has been compromised in many instances without their knowledge through Android apps [19,124]. Recent research has shown that interventions are needed to improve user awareness about smartphone security [20,23,72,133,161]. Persuasive games are designed to bring about a positive behaviour change across different domains [17,90,96,98,115], and they have been successful in the past. However, games that educate people about smartphone security practices are few in number. Most existing games focus on other cybersecurity issues, such as detecting phishing links and spam emails and setting strong passwords [34,98,149,152]. Currently, only two games and another mobile app are available for improving user awareness about smartphone security [9,10,160] and only a few smartphone security issues are covered by them.

In addition, none of the existing games were tailored or personalized to the users. Although research has shown that persuasive games have been successful overall, recent research shows that tailored persuasive games are more successful compared to the non-tailored version of the game [105,106,108,110,112,116] for promoting a positive behaviour change and improving the player experience. Despite the existence of various games, it is still unclear what motivates people to follow secure smartphone behaviour.

1.3 The Solution

Video Games have been around for a long time and have evolved tremendously across various platforms. With the evolution in games, there is a distinct difference between older games that invoke nostalgia with their basic game design and modern games with an evolved gameplay, narrative, and improved graphics. These older games are called ***Retro Games*** [164]. With the evolution of game engines and game development tools, many independent developers design games known as indie games ("indie" short for independent) [165]. Existing research has shown that retro games evoke a feeling of nostalgia and gives players the satisfaction that comes with competence [156]. A familiar playstyle also reduces the learning curve of the overall gameplay for the players.

After reviewing various popular game designs and various brainstorming sessions, I developed a 2D retro-themed game called "***Perma-Run***" inspired by other games like Super Mario [166], Dangerous Dave [167], MegaMan [168] and Captain Claw [169] to name a few. I leveraged 2D Level Design patterns developed by Khalifa et al. [70] and Persuasive Strategies from the Persuasive System Design (PSD) developed by Oinas Kukkonen et al. [104] to make the game persuasive and more engaging for the players to play. First, after conducting the literature review, I designed three different prototypes and selected one of the prototypes for further development after receiving feedback from subject matter experts. Following the development of the initial version of the game, I conducted a heuristic analysis with the initial version of the game, and made some design changes according to the results of the study. Second, I conducted a between-subject experiment to compare the game with another educational document. After making the appropriate design changes according to the results of the second evaluation study, I designed, developed, and evaluated two versions of the game tailored according to Regulatory Focus Theory [27,59] to match players' motivational orientation. This thesis describes the iterative process of designing Perma-Run and the effects of tailoring the game according to Regulatory Focus Theory.

1.4 Contributions

In this thesis, the contribution is two-fold:

First, the design and development of the Perma-Run for improving user awareness toward secure smartphone behaviour. The game was designed with an iterative user-centred approach. Two versions of the game were developed for the two motivational orientations according to Regulatory Focus Theory [59]. This would be beneficial for the researchers to experiment more with the idea of tailoring games for users with different motivational orientation across various domains.

Secondly, I conducted an in-the-wild evaluation of the game with 102 participants who played it for ten days. The evaluation results show that overall, the game significantly improved users' security behaviour, self-efficacy, and response efficacy. The game also reduced the user's response cost (perceived effort needed for performing a task). It was also evident that players preferred the game tailored according to their motivational orientation (promotion focus and prevention focus) compared to the non-tailored version of the game. The tailored versions of the game improved their secure smartphone behaviour significantly compared to the non-tailored version.

1.5 Overview of Thesis

This thesis describes the iterative design and development of Perma-Run and various evaluations, in a sequence of seven chapters.

CHAPTER 1 INTRODUCTION: This chapter gives an overview of the thesis, the problem statement, and the solution approach for the problem.
CHAPTER 2 RESEARCH BACKGROUND: This chapter discusses the literature review related to this work and discusses the various designs and evaluations done by other researchers from the HCI community that form a good foundation for this work.
CHAPTER 3 DESIGN & DEVELOPMENT OF PERMA-RUN: This chapter discusses the various stages of the design and development of the game and, the various design frameworks utilized as a part of this research. Mainly, this chapter discusses how the smartphone security aspect is tied to the game mechanics to motivate users.
CHAPTER 4 EVALUATION OF PERMA-RUN: This chapter contains the details of the three evaluations that are part of this iterative user-centric research process.
CHAPTER 5 RESULTS: This chapter answers the research questions with the results of the evaluations in a detailed manner.
CHAPTER 6 DISCUSSION: This chapter discusses the findings from this research, contributions to the persuasive computing and HCI communities, and design recommendations.
CHAPTER 7 CONCLUSION: This chapter discusses the limitations of this work and outlines the future works.

CHAPTER 2 – RESEARCH BACKGROUND

For many years, research has been conducted to evaluate the effectiveness of persuasive messages and various interventions [28]. In this modern era of desktop computers, smartphones, and other devices such as Augmented Reality (AR) and Virtual Reality (VR) headsets, various applications can persuade users for various purposes. For example, persuasive technology spans persuasive applications and other digital interventions that aim to promote a positive behaviour change among users. These can be applications that help to improve user's physical activity [14,57,69,115,148], sleep [63,114], security behaviour [97,152], nutrition [18,32,103,111] to name a few. Smartphone applications [17,97,115], VR/AR applications [2,7,21,24,144], and games are some of the designs utilized to develop a persuasive application. Many times, since persuasive technology is used for promoting a positive behaviour change, behaviour theories have been widely used in the field of persuasion to motivate users. These have also been leveraged to tailor persuasive applications for users.

This chapter discusses the research background that covers the trends in persuasive games, games for cybersecurity awareness and the state of Android smartphone security and privacy. This chapter also highlights the lack of user awareness about secure smartphone behaviour and the lack of interventions for improving secure smartphone behaviour. I collectively refer to the general etiquette and standards to stay safe from smartphone security and privacy issues as secure smartphone behaviour. The chapter concludes with a discussion about the need for interventions for smartphone security and why a persuasive game can be a good solution.

2.1 Literature Review Process

The systematic literature review I conducted is twofold – 1) reviewing persuasive games and 2) reviewing usable smartphone security and privacy issues. This is a helpful guide for the design process to learn from past mistakes and design the game accordingly. I leveraged the ACM Digital Library [170], Google Scholar [171] and Google Search Engine [172] to search for previous academic works and research papers published in journals and conference proceedings. I adapted the coding process outlined by Orji and

Moffatt [107]. Initially, I used the terms “Persuasive Games”, “Security Games”, and “Cybersecurity Games”, “Security Games for User Awareness”. I identified 149 papers, then skimmed and excluded papers that were not interventions related to security, papers that did not cover usable security and privacy, and papers that I had already reviewed. After the exclusion process, I had 40 papers covering persuasive games, games for cybersecurity games, and papers that discussed usable privacy and security issues. From the analysis, I found that interventions for smartphone security were sparse, and this motivated me to continue my literature review using the keywords “Smartphone Security Awareness”, “Smartphone Security User Awareness” and “Smartphone Security Games”. After the exclusion process, I had 48 more papers. Figure 2.1 outlines the literature review process. From the existing surveys conducted by various researchers across various countries, it was evident that there is a need for interventions to improve smartphone security and privacy awareness. We discuss the background details and the need for smartphone security and privacy awareness interventions in the upcoming sections.

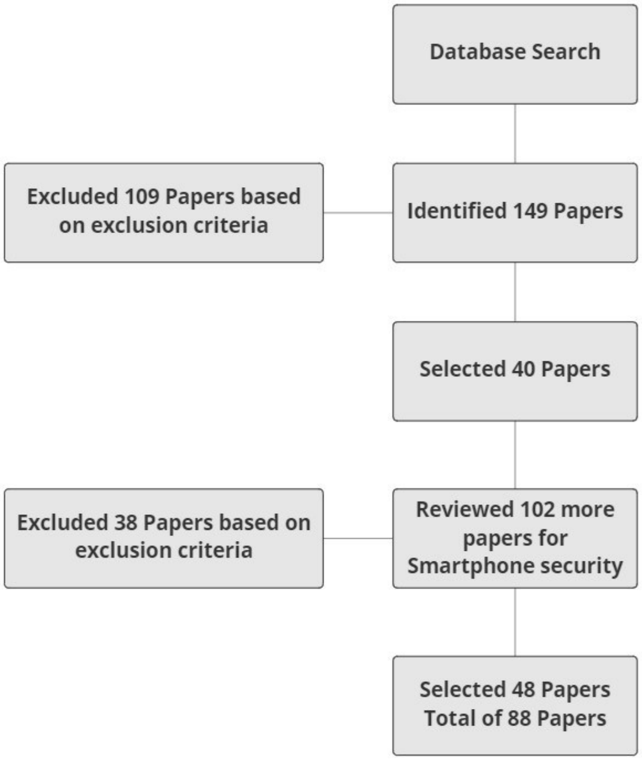

Database Search
Excluded 109 Papers based on exclusion criteria
Identified 149 Papers
Selected 40 Papers
Excluded 38 Papers based on exclusion criteria
Reviewed 102 more papers for Smartphone security
Selected 48 Papers Total of 88 Papers

Figure 2.1: Literature Review Process

2.2 Persuasive Games

Persuasive games have been around for a long time, and they are designed for various purposes across various domains. They are also called games for change and might be confused with serious games. Serious games are games that are not meant for leisure activity and are mostly designed for training purposes. Examples include serious games for cybersecurity professionals [158] and serious games for disaster management training [138]. Games for Change or Persuasive Games are designed to motivate users towards positive behaviour and attitude change. Physical activity [69,115], nutrition [17,32,111], disease prevention [90,95,96], sustainable environment [48,113,151], are some of the domains where persuasive games have been used to motivate behaviour and attitude change. Some of these are discussed below.

TreeCare [115] is a persuasive step tracking game that motivates users to stay physically active. The game leverages a virtual tree which blooms if the user walks frequently and withers if the user is physically inactive for a long time. The game has three modes namely, starter mode, challenger mode and tournament mode. The starter mode tracks the user's steps and simulates their activity using the tree. For the challenger mode, the tree lets the users compete with other users, and the tournament mode allows users to form teams to compete in tournaments. TreeCare also notifies the user when they have been sitting at the same place for more than thirty minutes. The app also reminds the user to walk, if possible, when they travel by vehicle.

BunnyBolt [69] is another app designed to motivate youth to stay physically active. The gamified mobile app employs an interesting story to attract a wide variety of audiences and rewards the users for reaching milestones in the game. The game has four different episodes as part of the story. The game includes a map and guides the users by placing carrot-shaped pins on the map and rewards the users when they reach a carrot pin. The game also notifies the users to vary their walking pace accordingly to keep them active.

PirateBri's Grocery Adventure [17,18] is a game to motivate users towards buying healthy groceries. The game utilizes a situated learning approach to educate the users about nutritional products (also called food literacy) during grocery shopping. The game allows the users to create a character based on information like age and gender to assess their nutritional needs. The game recommends the user to create a shopping list before going to the grocery store. While shopping, the users can input the product they purchase either by scanning the barcode or by manually entering it, and the game uses a traffic signal format to inform the users about the product's nutritional information. The game also has incremental weekly challenges that the users can complete to stay healthy and earn in-game rewards.

Balance Pass [32] is a service design designed to motivate healthy eating behaviour among college students. Balance Pass comprises a student ID holder with a built-in display for the recommender system. Balance Pass records the student's food purchase history when they pay with their card and recommends according to their purchase history, nutritional value, and food price. The recommender system followed the food pyramid as a recommendation guide. The system rewards the users with points for each healthy meal purchase. Users can accumulate points and utilize them to purchase free ice cream or movie tickets.

Similar to Balance Pass, LunchTime [111] is a multiplayer slow casual game that motivates users to make healthy meal choices in a restaurant setting. The game utilizes a goal-setting mechanism, allowing the users to choose their goals before playing the game. Users are grouped in the role-playing game, and everyone in a group gets a notification in the morning to make a healthy meal choice. This is considered one round and lasts for 12 hours. This allows the users to think about and discuss their choice with others before making a decision. Users are rewarded points according to their choices. When users make a healthy food choice, they get more points. The game ranks users from the same group on a leaderboard according to their scores.

In a different context, Orland et al. [113] designed a web-based persuasive game to motivate users to save energy. The game simulates chickens in a farm environment. Each chicken represents a device owned by the user. Each of the device's energy use is simulated using the chicken's health, and every chicken levels up and stays healthy if the user saves energy. If the user does not conserve energy for a specific device, the chicken assigned to that device falls sick. The energy levels and the users' baseline energy are compared and measured over five weeks, and the user gets a graph that shows their energy usage trend after playing the game for a week. The user can also view other farms owned by other users and compare their chickens' health (energy consumption). Healthy chickens lay eggs if the user conserves energy. The players can upgrade their farm and purchase in-game items using the eggs.

Wemyss et al. [151] designed a mobile game called Social Power to motivate households to save electricity. The game utilized two goal-setting features namely competition and cooperation to motivate users. The users either collaborate with their neighbours to save power or compete with their neighbours to see who saves electricity the most. The app provides individual feedback and group feedback, thus contextualizing information according to each individual's usage. The game gives weekly challenges to the user to teach them about sustainable electricity usage. When the users complete a challenge, they earn points. The game also has monthly quizzes with rewards for the users.

STD PONG [95] is a persuasive game to motivate African youth toward risky sexual behaviour change. The game uses the familiar ping pong game mechanism and simulates sexual risks while giving suggestions after the game. The game also employs a pre-post in-game quiz to test the user's knowledge. COVID Pacman [89] is a persuasive game designed to motivate the adoption of Covid-19 precautionary measures among users. The game utilizes the classic Pacman design to simulate the dangers of not following covid precautionary measures. The Pacman maze consists of the covid virus instead of the usual Pacman monsters and static Non-playable characters (NPC) to simulate real-world people. The player should stay away from the covid virus and maintain a safe distance from the NPCs. The game also has collectibles like handwash bottles and sanitizers that the player can collect to increase their health. The game also shows Covid safety tips as suggestions for picking up in-game collectibles. From the existing literature, it is evident that persuasive games leverage various game mechanics and game designs to motivate users towards a positive behaviour change across various research domains.

2.3 Interventions for Cybersecurity Awareness

Cybersecurity issues have been around for a long time and across various domains in different contexts. Every security issue cannot be fixed by lines of code. Social Engineering is often used to trick users to extract their sensitive information [22]. Sometimes users are unaware of the preventive measures to protect themselves from malicious cybersecurity attacks. Persuasive games for cybersecurity try to improve users' awareness by implementing game mechanics in various ways for various purposes. Some of the common cybersecurity issues for which persuasive games exist are phishing [52,85,97,149,152], password safety & security [34,123,131], games for cybersecurity training [53,142,158].

Ndulue et al. [97] designed a persuasive game to educate users about phishing links. The author leverages the classic memory match game in which each flashcard displays a phishing link that the users must match before the timer ends. The game has a tutorial that teaches the users how to identify phishing links before the start of the game. The game also has rewards and a leaderboard to motivate the users. What.Hack [152] is a role-playing game (RPG) that educates users in identifying phishing links and various phishing techniques in an email. The player takes the role of an IT expert who works in a bank and must filter the phishing emails from the benign ones without opening the email or the attachments. The game presents emails in an incremental difficulty and has a rule book that states the objectives for each level of difficulty. The game also includes a virtual assistant that the user can use to get tips on a specific email.

In a different study, Scholefield et al. [131] designed a mobile game to educate users about password safety and security. The game quizzes the users about password safety and security. The player competes against a dark knight (NPC) and loses some health for every wrong answer in-game. Chen et al. [34] designed hacked time, an RPG game that educates users about password safety and security. The user takes the role of a detective who must help their college roommate because their social media account was compromised. The player travels back in time and helps their roommate by pointing out the unsafe password practices they have been following and teaches them how to protect their social media account in an effective manner.

Games for cybersecurity training are used in educational institutions that train future cybersecurity professionals or for general awareness. For example, CyberCIEGE [142] is a serious game designed for training cybersecurity students. The course instructors can modify the game to train the students on specific topics. This serious game simulates real-world scenarios to educate the players. In another study, Yerby et al. [158] designed a serious RPG to train digital forensic professionals. The player takes the role of a digital forensic investigator and helps to investigate a cybersecurity incident for a company. The game walks the player through a narrative and simulates the cases. Research shows that serious games are better for training students than traditional classroom-based courses [122]. Apart from digital games, board games are also used for training and improving users' cybersecurity awareness [53].

The research review in this section shows that persuasive games have been used in the cybersecurity research domain to motivate users to adopt safe security and privacy practices. In the upcoming section, the current state of user awareness about smartphone security is discussed followed by a brief description of the existing interventions for smartphone security awareness and why more interventions are needed for smartphone security and privacy.

2.4 Smartphone Security

Smartphone security is a sub-domain under the umbrella of Cybersecurity. With the rise in usage of smartphones for various day-to-day activities, smartphones have become a hotspot for personal data, thus attracting malware. For a long time, Google's Android has been regarded as the less secure smartphone Operating System compared to Apple's iOS [1,5,86]. Apart from the technical security issues, which exist for both the devices, Android is more prone to social engineering attacks compared to iOS due to its design for giving more control to the user [1,86]. Various studies have shown that user awareness about smartphone security needs improvement, and interventions are needed for this purpose [15,16,20,23,72,102,133,161]. From the above discussion about persuasive games for cybersecurity, it is evident that persuasive games motivate users to bring forth a positive behaviour change. But, only a limited number of interventions exist for improving user awareness about smartphone security [9,10,160], and existing research show that users are unaware of smartphone security and privacy, and do not take the necessary steps to protect themselves.

Breitinger et al. [20] conducted a survey to learn about users' smartphone practices. The majority of the respondents were from the USA and South Korea, and the sample was skewed towards the younger generation (18-40 years). The author found that most users were using biometrics for convenience and not for its security features. Users were not using third-party security applications to protect their smartphones, unlike the security software for a desktop which is also facing a decrease in usage. Users are aware of hard security practices like locking their phone and keeping it to themselves but are unaware of soft security practices like turning off GPS, Wi-Fi, and Bluetooth when not in use.

Bitton et al. [15,16] developed a taxonomy for assessing users' awareness of smartphone security and utilized it in a mobile app to monitor users' behaviour in the wild over seven weeks. The author found that self-reported user behaviour data was far different from their actual behaviour measured by the app and by monitoring the network traffic. It was found that users performed risky tasks (dummy tasks set up by the author) in contrast to the self-reported data. Calderwood et al. [23] surveyed the student population in Thailand to gauge smartphone security awareness among youths. The majority of the respondents were female, and most of the survey respondents reported that they click on unknown links and were prone to phishing and social engineering attacks.

Shah et al. [133] conducted a survey to check the level of user awareness about smartphone security among Indian users. The survey questions were based on best practices for smartphone security collated by the researcher. The majority of the survey respondents were Android smartphone users, followed by iPhone users. From the survey results, it was evident that the respondents were not following secure smartphone practices like downloading apps from trusted sources and connecting to secure Wi-Fi networks and they were not backing up their personal data. Furthermore, Zhang et al. [161] conducted an empirical analysis across China and similar to Shah et al.'s [133] findings, their results also showed that most of the users did not follow smartphone security practices such as utilizing the security settings provided by the manufacturer, avoiding data recovery backups, not using antivirus software and downloading apps from untrusted sources.

With the existing survey research [15,16,20,23,64,72,102,125,133,161] that explored the smartphone security and privacy issues across various countries, I conducted a thematic analysis using an affinity diagram and uncovered 12 common security issues as shown in Figure 2.2. I wrote the smartphone security and privacy issues on post-it notes (using Miro Board [173]) and collated the common issues that formed the 12 themes/common security issues. The common smartphone issues were, Lock Screen Basics, Turn off When Not in Use, Unknown Links, VPN & Anti-Virus, Before Installing an App, General App Protocols, Check for Permissions, Do Not Install From 3rd Party, General Recommendations, Safety Routine, Securing Data and Disaster Response. These smartphone security use case scenarios included in the game are described in Appendix F.

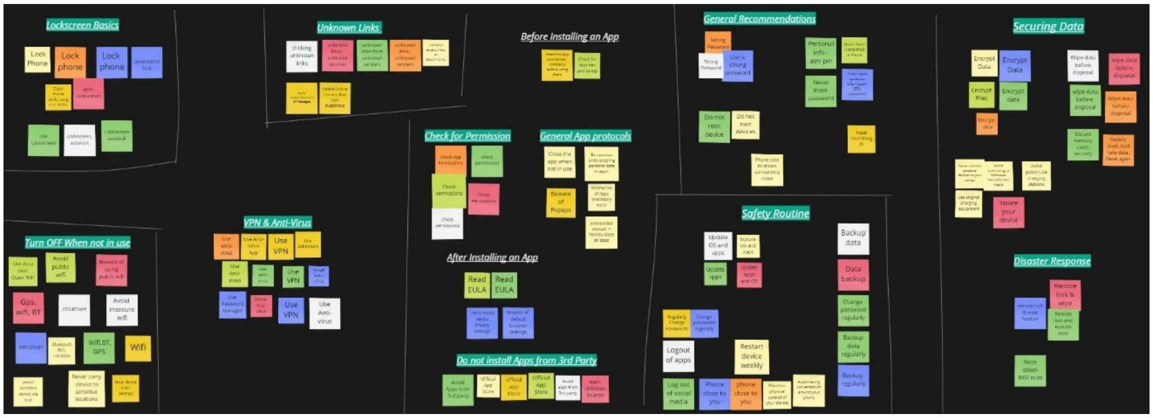


Figure 2.2: Common Smartphone Security Issues – Affinity Diagram

Google’s Android OS [174] enables end-users to control the data they want to share with apps using a mechanism called run-time permissions [175,176]. Before the run-time permission model, Android implemented the install time permission model. In the install time permission model, Android requests permissions when the user tries to install the app, and the user had only two choices, either to install the app and grant all the permissions or not to install the app. There are other types of permissions namely, normal permissions and signature permissions [54]. Normal permissions do not pose any risk to the user data. Retrieving the date and time and accessing the phone’s actuator are some examples of normal permissions. Signature permissions enable apps with the same certificate to share the same permissions. Signature permissions are used by developers who create custom permissions and want to use the custom permission in another app developed by them. Examples of signature permissions are clearing the app's cache and form auto-fill data [54]. Android classifies users' personal data into ten categories (Permission Groups) namely: Activity Recognition, Calendar, Camera, Contacts, Location, Microphone, Phone, Sensors, SMS, and Storage.

With the recent release of Android 12, Google has introduced new runtime permission called Nearby Devices that gives the user the ability to allow or deny the applications' ability to access the device's Bluetooth to discover and connect with other devices. Google also enables Call Log permission only to specific developers for which they must write a letter to the company and explain their app's functionality. Table 2.1 summarizes the runtime permissions and their functionalities. Google introduced permission rationale [176], a way to explain the reason for the requirement of app permissions. But Google does not enforce this on developers and the developers might not contextually request permissions (right before the need for the data) but might request every permission at once. Apart from this, with the recent release of Android 12, Google has introduced one-time permission, permission auto-reset and camera, as well as mic toggles [176,177]. Details of the recent changes after Android 11 can be found in Table 2.3. Despite introducing run-time permissions, apps might still misinform the user and misuse the permissions by requesting unnecessary permissions without providing context, and as a result, users might not pay attention to them [11,15,154,16,23,45,64,74,102,124,133]. Figure 2.3 shows the frequently requested permissions. Figure 2.4 shows the frequently abused Android permissions, also outlined in Table 2.2 with references. I also perused the list of top 20 apps in each app category of the Google Play Store to explore the frequently requested permissions. I excluded the "watch apps", "watch face", and "google cast" app categories because these are related to other devices apart from Android smartphones which have their own permission system.

Table 2.1- Summary of Android Runtime Permissions

Android Run-Time Permissions	**Description**
Activity Recognition	Required for accessing sensors for the purpose of activity tracking like walking, running, and cycling.
Calendar	Required for accessing the calendar attributes like events and reminders.
Call Logs	Required for accessing the user's call logs/call history.
Camera	Required for accessing the device's camera which is used for capturing pictures and videos.
Contacts	Required for accessing user's contacts stored on the device.
Location	Required for accessing the device's location. (Fine grain control for the user is available from Android 12, not required for retrieving Wi-Fi Hotspots from Android 13).
Microphone	Required for accessing the device's Microphone for the purpose of recording and transmitting audio.
Nearby Devices	Required for accessing Bluetooth to scan for nearby Bluetooth devices (Android 12) and for scanning Wi-Fi hotspots (Android 13).
Notifications	Required for permissions associated with posting notifications.
Phone	Required for placing calls and receiving calls.

Sensors	Required for accessing biometric sensors like heartrate monitor.
SMS	Required for reading and writing SMS.
Storage	Required for accessing the device’s internal storage.

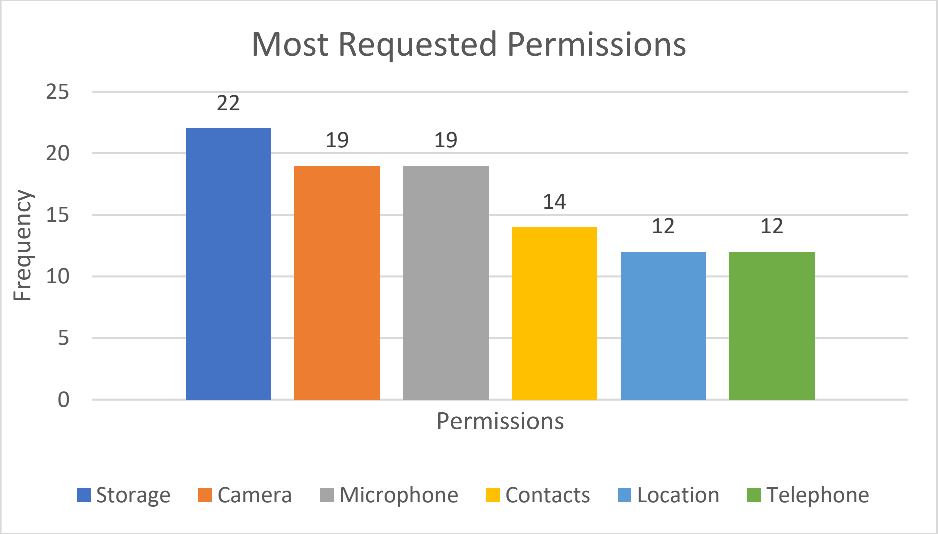


Figure 2.3: Frequently Requested Permissions

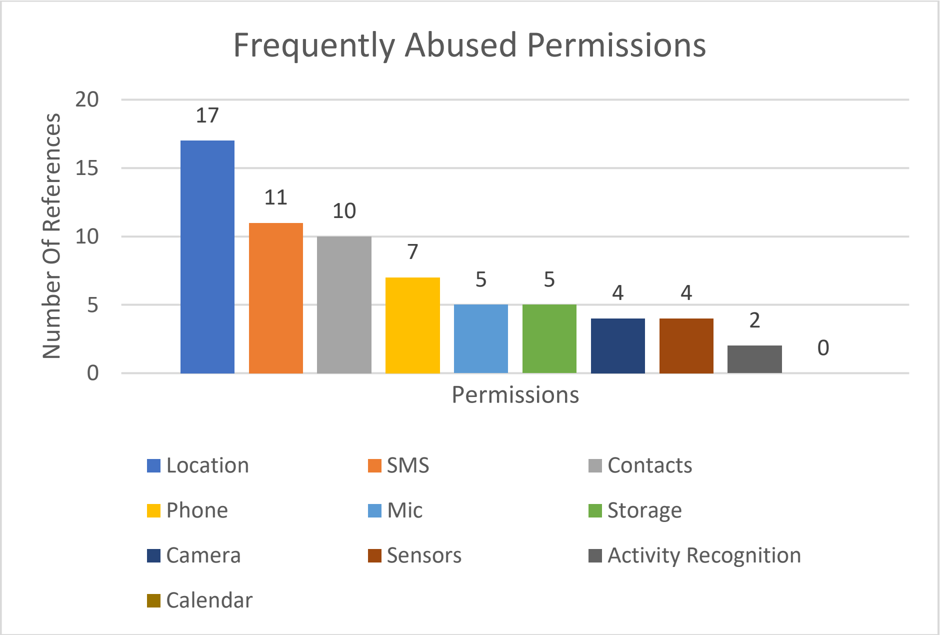


Figure 2.4: Frequently abused Android permissions

Table 2.2 - Android Permission Abuse

Abused Android Permission	**References**
Location	[3,11,124,130,135,153,154,161,163,16,19,37,41,44–46,93]
SMS	[3,16,178,20,44–46,55,130,153,163]
Contacts	[3,16,37,41,44,45,55,135,161,163]
Phone	[3,11,16,20,135,153,161]
Microphone	[16,44–46,162]
External Storage	[3,16,45,46,124]
Camera	[11,16,45,130]
Sensors	[11,16,45,46]
Activity Recognition	[16,46]
Calendar	None

Table 2.3- Recent Changes to Security Features in Android

Security Changes	**Android Version**	**Description**
One time Permission Use	Android 11	User will be able to grant permissions only once while using the app. The user has to grant the permission again for subsequent usage.
Permission Auto-Reset	Android 11	If the user does not open the app for some time, the all the permissions are revoked for that app.
Camera Usage Notification	Android 12	When the camera is being used, a notification pops up to alert the user.

Microphone Usage Notification	Android 12	When the microphone is being used, a notification pops up to alert the user.
Ability to share precise or approximate Location	Android 12	While granting location permission, the user has the option of either sharing precise location or approximate location.
Privacy Dashboard	Android 12	A dashboard is available for the user where they can check permission usage logs.
Runtime Permission for Wi-Fi	Android 13	The runtime Wi-Fi permission for discovering Wi-Fi hotspots is a sub permission that has been moved from Location permission to Nearby Devices permission.
Notifications runtime Permission	Android 13	The notifications permission is required for permissions associated with posting notifications.

Interventions to educate users about smartphone security are sparse, and I was able to find only a limited number of games for improving user awareness about smartphone security. Bahrini et al. [10] designed a role-playing game "MakeMyPhoneSecure" which aims to improve user awareness about smartphone permissions. The player takes the role of a security expert and must help the NPC’s with their security concerns. The player must deny permissions in the app settings according to the scenario. The same authors also designed “HappyPermi” [9], an Android app that simulates the data accessible with each run-time permission. The app had toggles for each permission that the user could toggle on and off to see which data was being retrieved from their phone for each permission. Zargham et al. [160] designed a humorous game to educate users about setting up an Android smartphone phone and using it in a safe manner. The authors conducted a between-subject study with the game, a humorous video and a serious video about smartphone security and privacy. The researchers found that the participants preferred the game over the humorous video.

These existing interventions reviewed in this section only cover some of the smartphone security and privacy scenarios, and existing research shows that user awareness about smartphone security and privacy is low. Hence, there is a need for interventions to bridge this gap. This motivated me to design a game with a refreshing and contextual narrative and game mechanics to cover a wide range of smartphone security and privacy issues. I designed various persuasive game prototypes before proceeding to develop PERMA-RUN, a persuasive game to promote secure smartphone behaviour. Chapter 3 outlines the details of the design and development process.

2.5 Persuasive Systems Design & Game Level Design

Rapid iterative designing and testing are useful to refine the design with the help of potential users at each stage of the iterative design process. This minimizes the delay in evaluating an application as a whole after development, thus saving time, resources, and effort [132,179]. For designing persuasive applications in a user-centred iterative manner, Fogg [47] developed the eight-step process for designing persuasive applications (Table 2.4). I used this process for designing Perma-Run, which is explained later in the upcoming chapter (Chapter 3, Table 3.1). Persuasive applications are designed to bring about a positive behaviour change, and attitude change among users for the greater good.

Table 2.4 - BJ Fogg's Eight Step Design Process for Creating a Persuasive Technology [47]

Eight Steps	Description
1. Target Behaviour	Choosing a simple behaviour for change. Breaking the goal into tiny objectives
2. Target Audience	Choosing the right user base.
3. Identifying Behaviour Change blockers.	Find out what is blocking the behaviour change.
4. Target Device/Technology	Choosing a platform according to the first three steps. (The first four steps can be reordered according to a designer's convenience)
5. Find Existing examples	Find existing persuasive apps that work and learn from them.
6. Imitate examples	Imitate existing example that work.
7. Rapid Test & Iteration	Iterate on design by rapid testing.
8. Expand on Success	Experiment with new audience, try increasing the positive activity, try the same design for a similar behaviour.

Various features motivate different users toward their behaviour goals, and these features are referred to as Persuasive Strategies. The Persuasive System Design (PSD) model was defined by Oinas-Kukkonen et al. [104] that classifies the features that motivate or aid the users' behaviour change journey into four categories - Primary Task Support, Dialog Support, System Credibility Support and Social Support. Each category has seven Persuasive Strategies to motivate the users toward positive behaviour change. The Primary Task Support aids the users' in performing their primary task, and the Dialog Support provides feedback to the users in a verbal format or other forms. The System Credibility Support strategies describe how to make a digital system more credible, and the Social Support strategies utilize the social influence factors to motivate users towards a positive behaviour change. The persuasive strategies are shown in Figure 2.5, and the persuasive strategies used in Perma-Run are described in Table 2.5. The PSD framework can be used to classify the motivational features of an application as persuasive strategies. For example, a gamified step tracking app might display a user's weekly steps, and this can be classified as self-monitoring as this allows the user to monitor their step count and might persuade them to stay physically active. The persuasive strategies for this research were mapped according to the features of the popular games that were implemented in the game.

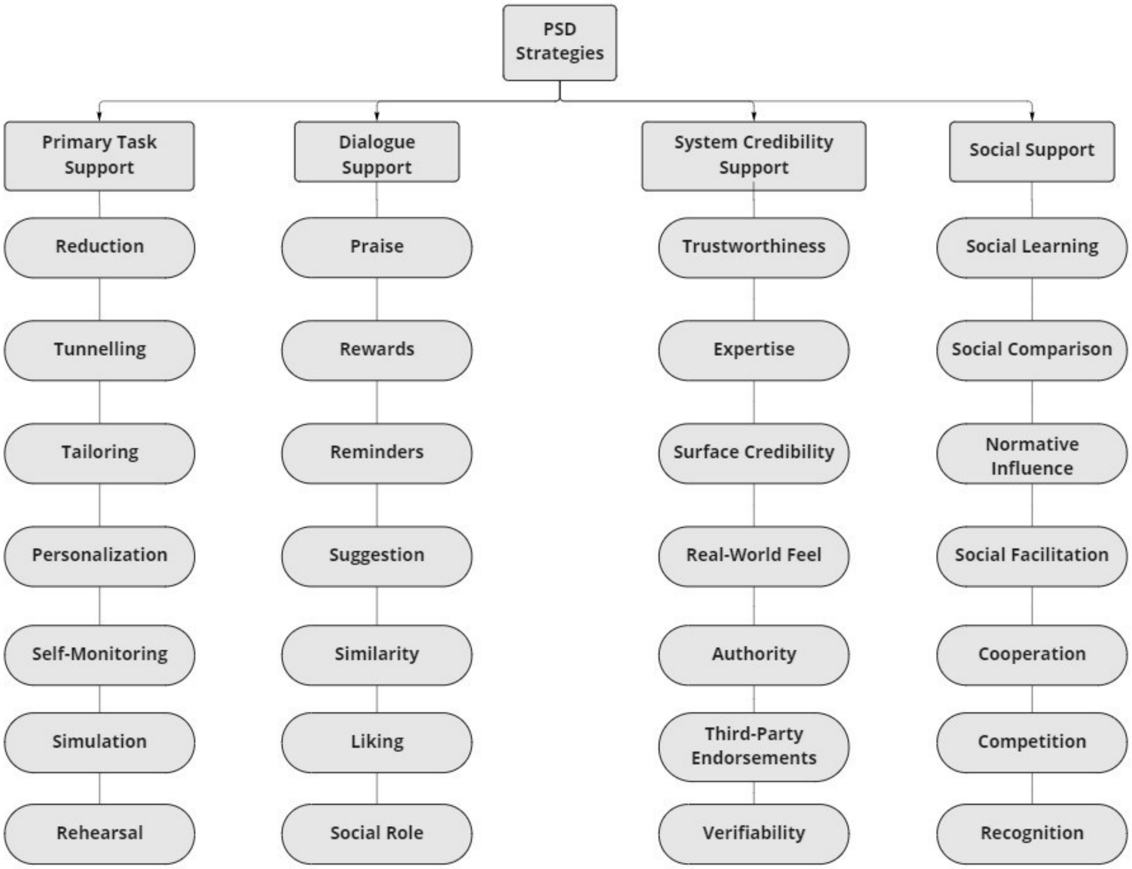


Figure 2.5: Persuasive Strategies from the Persuasive Systems Design Model

Table 2.5- Persuasive Strategies from the PSD model

Persuasive Strategy	**Description**
Self-Monitoring	System helps the user to keep track of their performance.
Simulation	System helps the user to observe

	the link between cause and effect.
Rewards	System rewards the user for performing a behaviour.
Suggestion	System offers appropriate suggestions to the user.
Competition	System leverages user’s drive to compete with others.
Recognition	System recognizes the user’s performance such that it is visible to other users or the public.
Social-Comparison	System enables the users to compare their performance with others.
Reduction	System reduces the workload into simple tasks to help the users perform a target behaviour and might increase the benefit/cost ratio of a behaviour.
Tunnelling	System guides the user through a process or an experience and persuades them along the way.
Praise	System praises the user for performing a target behaviour.
Surface Credibility	System should have a competent feel.
Liking	System is visually attractive to the user.
Real-World Feel	System reveals the details of the designer and the organization responsible for the persuasive application.
Trustworthiness	System provides truthful and unbiased information.

Video games have been around for a long time, and they have been used primarily for entertainment. There are various types of games across various platforms. Recently, with the rise in usage of smartphones, nearly 84% of the world's population (6.6 Billon) has access to smartphones [180,181]. The two popular operating systems for smartphones are iOS and Android, which have a global market share of 99% [182,183]. Android is the more widely used operating system with a 72% global market share followed by Apple with a 27% global market share. Unsurprisingly, the smartphone is frequently used for playing games followed by PC and other consoles like Xbox and PlayStation [184]. Various genres of games have become a classic that has been around for a long time, and multiple researchers have uncovered design patterns that motivate players and invoke their curiosity to play the game. These game design patterns aid the creators to design captivating games and maintain the balance of game experience for a wide range of audiences.

Hullett et al. [65] adapted the software design patterns to analyze the design patterns in First Person Shooter games and put-forth four design patterns with examples for each pattern. Sharif et al. [134] analyzed the game design patterns for feeding them as features to procedural level generation models. The author identified 23 design patterns from 2D games and suggests them for procedural level generation. Inspired by the real-life architectural patterns of buildings, Smith et al. [137] identified 33 quest design patterns and 57 level design patterns from over 20 RPG's each of which was categorized according to five categories of quest design patterns and six categories of level design patterns. Khalifa et al. [70] reviewed games over the past 30 years since the work was published, to identify level design patterns that intrigued the players. Given the deconstruction of motivational features of levels across various 2D games over the past 30 years, I utilized the framework suggested by Khalifa et al. [70] to design Perma-Run. The level design patterns allow a designer to be creative while providing specific guidelines. Table 2.6 outlines the details of the level design patterns.

Table 2.6- 2D- Level Design Patterns [70]

Level Design Pattern	**Description**
Foreshadowing	Player is teased with un-interactable game objects or can be a game element that changes over the course of the game.
Branching	Player has multiple paths to explore in-game. Applying specific conditions to choose another pathway is called conditional branching.
Layering	Introduce challenges by combining multiple game elements or reusing game elements in a different way.
Guidance	Guiding the player towards the goal or in the right direction with non-verbal game elements.
Pace Breaking	Increasing or decreasing the tension in-game is commonly referred to as pace breaking. Pace breaking is usually achieved by introducing bosses or giving the player a break after long combats.
Safe Zone	In-game places where the player is not in danger and where they can take a break from all the tension that was built in-game.

2.6 Protection Motivation Theory

Rogers et al. [82,128] developed the Protection Motivation Theory (PMT) in the 20th Century. Initially, the theory was developed for promoting healthy behaviour like anti-smoking and healthy eating. Some of the popular behaviour theories for behaviour change are the Health Belief Model [129], Technology Threat Avoidance Theory [79] and, Theory of Planned Behaviour [4]. Initially, when Rogers et al. developed PMT [82,128], the major focus was on fear to motivate users to protect themselves. Later, *Self-Efficacy*, which was proposed by Bandura et al. [12] as Self-Efficacy Theory, was added as a construct to PMT. PMT is comprised of five constructs namely, *Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, and Response Cost*. PMT proposes that these constructs give rise to the intention to change behaviour. The first two constructs (*Perceived Severity* and *Perceived Vulnerability*) are referred to as Threat Appeal/ Threat Appraisal, and the other three constructs (*Self-Efficacy, Response Efficacy, Response Cost*) are referred to as Coping Appeal/ Coping Appraisal. Table 2.7 outlines the details of the PMT constructs.

Table 2.7- Description of Protection Motivation Theory Constructs

PMT Construct	**Description**
Perceived Vulnerability	Refers to the user's level of perception towards the susceptibility to negative behaviour outcomes such as health issues due to smoking.
Perceived Severity	Refers to the user's level of perception towards harshness of a negative behaviour outcome such as chances of lung cancer due to smoking.
Self-Efficacy	Refers to the user's level of belief in themselves to work towards a behaviour change.
Response Efficacy	Refers to the user's level of belief in the effectiveness of an action towards achieving a positive behaviour goal.
Response Cost	Refers to the user's perception towards the amount of effort that is needed to perform the actions for a behaviour change.

Macdonell et al. [81] developed a measurement scale for tobacco research based on PMT and validated it with undergraduate students from a Chinese University. Chambers et al. [29] conducted a focus group with American Indian adolescents according to PMT to educate the youth and their parents about safe sexual practices to protect themselves from sexually transmitted diseases. Poong et al. [119,120] developed a presentation based on PMT to persuade tourists to protect and preserve the world heritage site of Luang Prabang [185]. The presentation conveyed the ill effects of not protecting a world heritage site (Threat Appeal) and how to protect it (Coping Appeal). The author developed a survey based on PMT and administered the survey to 238 university students. The results suggested significant mean differences for all the constructs except response efficacy, and self-efficacy had the highest mean difference of all the constructs.

Over the years, PMT has been adapted and applied across various domains. One such domain is cybersecurity, where PMT has been used in various contexts. Bavel et al. [13] designed various nudges according to PMT for motivating users to navigate an e-commerce website safely and securely while making a purchase. The four nudges were – 1) a plain message that served as a control group, 2) a coping message instructing the user how to navigate the e-commerce platform safely, 3) a threat appeal message that conveyed the dangers of shopping on e-commerce platforms and 4) a combination of coping + threat messages. The author found that the threat + coping message performed the best followed by the coping message, threat and control message.

Mwagwabi [91] conducted a 2 x 2 between-subjects experiment for password awareness among users. The author set up a control group and a PMT intervention and measured the PMT constructs in the pre-study and post-study surveys. For the control group, after answering the pre-study survey, the users had to set a password, answer PMT survey questions and then reset the password. After six weeks, the users had to login with the same pre-study survey password for answering the post-study survey. If they had forgotten their password, an alternate password was provided for the user. For the experimental intervention, the users were shown persuasive writings according to each construct of PMT before answering the PMT survey questions.

Meier et al. [84] conducted a 2 (fear appeal vs neural message) x 3 (high norm vs low norm vs no norm) between-subject study to test various design nudges that aimed to motivate users to change their Facebook privacy settings. The authors used fear appeal and perceived behaviour (norm) to persuade users. The authors found that some of the results from the study aligned with past research, yet some did not.

Chittaro et al. [36] designed an interactive serious game to educate users about emergency preparedness during terror attacks. The author designed the game based on the constructs of PMT. For perceived severity, the authors used gory effects, bone-crushing sounds and realistic human screams to induce fear. For perceived vulnerability, the authors simulated public places such as train stations and airports to induce a sense of reality in the user and make them realize the real-world vulnerability. For *self-efficacy*, the player must perform the right action in-game to protect themselves during the catastrophe and for *response efficacy*, the player does not get hurt badly when they performed the right actions in-game. For response cost, the suggestions shown to the player were simple, and the actions to be performed were also simple, closely mimicking real-world actions. The authors compared the interactive version of the game with a non-interactive version in a 2x2 between-study design experiment. Apart from using a survey questionnaire for measuring the PMT constructs, the authors used physiological sensors for correlating with stress, tension, and fear. From the quantitative results, it was evident that the interactive version of the game performed better than the non-interactive version for increasing the *threat appraisal* constructs, emergency preparedness *knowledge* and *self-efficacy*.

Williams et al. [155] designed a game called "(Smart)Watch Out!" to improve user awareness about smartwatch security and privacy. Apart from having a contextual story, the authors modelled the game mechanics according to PMT constructs. The player must go around town answering security questions to citizens and must dodge answering thieves who would try to steal the player's data. Toward the end of the game, the player goes to a shop to make a purchase (the player must collect coins on the way to the shop). The player gains coins for correct answers and has timed challenges while answering the thieves (the number of coins depends on how fast the player answered the questions). The authors highlighted the consequences of not following proper security and privacy practices

(*Threat appraisal*). The users must perform security tasks to protect themselves (coping appraisal) from losing in-game, and to make progress in-game. From the results, researchers found a significant increase in the usage of lock screens and permissions after playing the game.

Yasin et al. [157] designed a card-based RPG called Cyber Security Requirements Awareness Game, according to the PMT for educating users about software security. The game has players grouped into teams of three to four, and each player takes the role of a different type of attacker. This gives the users a chance to think about the security scenarios and the ways security attacks can happen. This team-based game also encourages the teams to discuss and work together. The players must compromise infected devices (*perceived vulnerability*), and during the gameplay, the players might get caught by the security personnel in-game (*perceived severity*). For self-efficacy, the game had rules and objectives for the players and guidance for questions and answers. Players must discuss selecting a viable and feasible attack for compromising the infected devices (Response Efficacy). The results showed that the users self-reported awareness increased significantly.

Various researchers have adapted the PMT by adding different constructs according to the domain to explore usable privacy and security [38,91,147]. For instance, Mwagwabi [91] added *Exposure to Hacking* as a construct to the PMT scale and adapted the scale for compliance with password guidelines. Similarly, Verkijika et al. [147] added *Anticipated Regret* as a construct to the PMT scale and adapted it for smartphone security and privacy. Similar to Verkijika et al.'s [147] PMT scale, Knapova et al. [71] evaluated the determinants of smartphone security behaviour based on the combination of the Health Belief Model and PMT. I adopted the PMT scale validated by Verkijika et al. [147] as this was a scale based on PMT, adopted for smartphone security.

2.7 Regulatory Focus Theory

Regulatory Focus Theory is a goal pursuit theory that emphasizes the motivational orientation of the users and how they pursue their goals [27,59]. The theory states that people try to reach their goals according to their predominant motivational orientation which is categorized as *Promotion Focus* and *Prevention Focus*. Throughout one's lifetime, people are either predominantly promotion focused or prevention focused, and hence adapt to one of the focuses while trying to reach a goal [27,59]. When a person tries to reach a goal because of the advancement, or accomplishment that they might get out of performing the task, they are considered to be *promotion focused*. *Promotion focused* people might often take an eager means (proactively trying to achieve positive outcomes) to achieve their goal. In contrast, a *Prevention focused* individual might take a vigilant means (proactively trying to avoid negative outcomes) to achieve their goal. When a person does not want to lose what they have and wants to follow societal etiquette to reach what they consider as a standard safe goal (concerned about safety and security), they are considered to be *prevention focused*. People might also momentarily switch to their alternate focus in some situations. Higgins et al. [60] developed an 11- item scale to determine the *Regulatory Focus* of a person. When the persuasion matches the users' motivational orientation, users feel right while performing the task, and they experience an increased strength of engagement which is referred to as *Regulatory Fit* [26,27]. Regulatory Fit might also occur due to non-verbal cues or physical actions [26]. Regulatory focus theory has been used in consumer research, to motivate users to buy products and in the health domain to motivate users to make healthy choices [27,60,61,75].

To explore the effects of non-verbal cues tailored according to Regulatory Focus Theory, Cesario et al. [26] conducted an experiment where students were exposed to either a promotion focused video or prevention focused video where a teacher promotes a new after-school program. In the promotion focus video, the actor, while speaking, used an eager delivery style (open wide arms, fast movement), and for the prevention focus, the speaker used a vigilant delivery style (slower movement, leaning backwards). The message in both the videos was identical (introducing a new after -school program). The Regulatory Focus Questionnaire (RFQ) [60] was used to determine the participant's chronic regulatory focus. From conducting quantitative research, the researchers found that participants with a promotion focus orientation understood the eager delivery style easily and the vigilant delivery style was easily understood by prevention focus oriented participants.

To explore the effects of verbal cues in written format, Lee et al. [75] conducted six iterative experiments and found that participants exposed to persuasive messages according to their regulatory fit condition were more persuasive. Similarly, Cesario et al. [25] conducted four iterative studies, in which each study had a promotion focus message and prevent focus message. Participants were assigned randomly to each group according to the RFQ. It was found that the persuasiveness of the message increased when participants felt right about the message in fit conditions.

Elgarf et al. [43] designed an interactive pretend play game (with human-robot interaction) according to the Regulatory Focus Theory to study the impact of Regulatory Focus Theory on emotional induction in children. The researchers designed a pretend play narrative, where the child must work with the robot to escape to planet Mars. The researchers used an EMotive headY System(EMYS) robot [186] and a table interface for priming the users' behaviour. The gameplay was designed according to Regulatory Focus Theory, where the *promotion focus* game version was designed to elicit happiness. The prevention focus game version was designed to elicit fear. EMYS, the robot was set to elicit fear and happiness via facial expressions and sounds. In the pre-test and post-test conditions, the child had to narrate a story to EMYS. After the post-test, they were asked to answer a survey. The results showed that children elicited joy and happiness in the promotion focus version, but the prevention version did not induce fear.

Heeter et al. [58] conducted a quasi-experiment with a shooter gamer which was tailored according to Regulatory Focus Theory. The promotion focus version displayed the number of rounds the player won, and the prevention focus version displayed the number of shots missed by the player overall. The promotion focused players took a greater number of shots (eager approach) and made more mistakes compared to the prevention focus players, who were careful not to make mistakes. The promotion focused players also played the game more than the allotted time limit, and prevention focus players were more likely to comply with external instructions.

Lee et al. [76] explored the effects of regulatory fit for learning with the help of the game "Do I have Right". The game is used for teaching the players about constitutional amendments. The player must win lawsuits in the game and accumulate prestige points. For the eager condition, the players were asked to win as many lawsuits as possible, and for the vigilant condition, the players were asked not to lose prestige points. A dashboard in the game informed the players about their progress. From the study results, it was evident that players in the fit condition played the game for a longer time compared to those in the non-fit condition. Players in the fit condition also spent more time in learning-related behaviour.

From the literature reviewed in this section, it is evident that Regulatory Focus Theory has benefits when there is a Regulatory Fit condition. I tailored Perma-Run according to the Regulatory Focus Theory to improve the game's persuasiveness during fit conditions. To improve users' awareness about smartphone security and privacy, Perma-Run utilizes suggestion in the form of texts to convey about smartphone security and privacy. Regulatory Focus Theory has been used to study the effects of tailored written messages and has been successful in motivating users towards their goals. Hence, I tailored Perma-Run according to Regulatory Focus Theory, and according to my knowledge, Perma-Run is the first game to implement Regulatory Focus Theory in a smartphone security context. The details of the implementation of Regulatory Focus Theory are described in Chapter3, along with the study design. The upcoming section discusses the ARCS model that is used for measuring motivational appeal.

2.8 ARCS model

The ARCS model [68] consists of four major conditions (Attention, Relevance, Confidence, and Satisfaction) that was proposed to keep people motivated. The ARCS model was derived from a powerful macro theory of motivation and expectancy-value theory [68]. The ARCS model combines other motivational theories such as Expectancy Value Theory, Self-Efficacy Theory, Cognitive Evaluation Theory, Reinforcement Theory and Social Learning Theory [66,136,145]. The ARCS model has been used by researchers for measuring motivation and evaluating behaviour change interventions. It has been used across various domains such as health [6,116,140], persuasive games [39,87,159], and education [67,68,78,145]. In the health domain, Oyebode et al. [116] leveraged the ARCS model to measure users' motivation for a tailored persuasive app. The authors designed a quit smoking smartphone app and tailored it according to the Transtheoretical Model's Stages of Change and utilized ARCS to measure users' motivation. From the results, the authors deconstructed which persuasive strategies motivated users at different stages of change.

Similarly, Mulchandani et al. [87,88] leveraged ARCS to measure users' change in motivation to adopt Covid-19 precautionary measures after playing a persuasive game tailored according to Transtheoretical Model. From the results, the authors found that the tailored version of the game was much more effective than the non-tailored version of the game. Derbali et al. [39] measured users' motivation after a serious game session using the ARCS model. The author also used EEG frequencies to correlate with the motivation measurement results from ARCS and found that the EEG patterns correlated with an increase in motivation levels. Based on the positive results of these experiments showing the usefulness of the ARCS model to measure motivational appeal, I also leveraged the ARCS survey scale to measure the user's motivation levels for Perma-Run. Table 2.8 outlines the description of each ARCS motivational construct adapted from Orji et al. [109].

Table 2.8 – ARCS Motivational Constructs Description [109]

Motivational Construct	**Description**
Attention	A system must arouse and sustain a user's attention to motivate them.
Relevance	A system is more likely to motivate the users if it is perceived as useful and in accomplishing their goals. A system should be goal orients, motive matching and must use familiar concepts.
Confidence	Confidence is often correlated with a user's motivation. A system is more likely to motivate users if the user feels confident while using it. Confident people try to achieve their goals despite challenges. If

	its too challenging, the system might demotivate users.
Satisfaction	A system is more likely to motivate a user if it rewards the users to satisfy them for their actions.

2.9 Persuasive games for Smartphone Security Awareness

Currently, only a limited number of games exist for improving user awareness about smartphone security [9,10,160]. These games cover only a handful number of smartphone security use cases, and they do not evaluate users' awareness levels with a proper, validated baseline. Based on the existing literature that we reviewed, it is evident that smartphone security awareness among users across various countries is low, and there is a need for interventions. Persuasive games have been around for a long time and have been used across various domains for motivating users towards a positive behaviour change. Perma-Run [49,50] bridges these research gaps by covering most of the smartphone security use case scenarios contextually with the help of an interesting narrative and gameplay style. Using an iterative and incremental design approach, I conducted a series of evaluation studies to evaluate Perma-Run towards improving players' secure smartphone behaviour. From the literature review, it is also evident that tailored interventions performed much better compared to the non-tailored versions for behaviour change. Regulatory Focus Theory has been widely used to tailor interventions and motivate the users according to their motivational orientation. Hence, I tailored Perma-Run to motivate users according to their motivational orientation.

Chapter 3 - DESIGN & DEVELOPMENT OF PERMA-RUN

This chapter discusses the user-centred iterative design and development process of Perm-Run. This chapter outlines the Game Design, Gameplay, and level design process in detail. There are three versions of the game that are discussed, and each version's design changes were informed by the results of an evaluation study at each stage of the iteration process. Figure 3.1 gives an overview of the iterative design process.

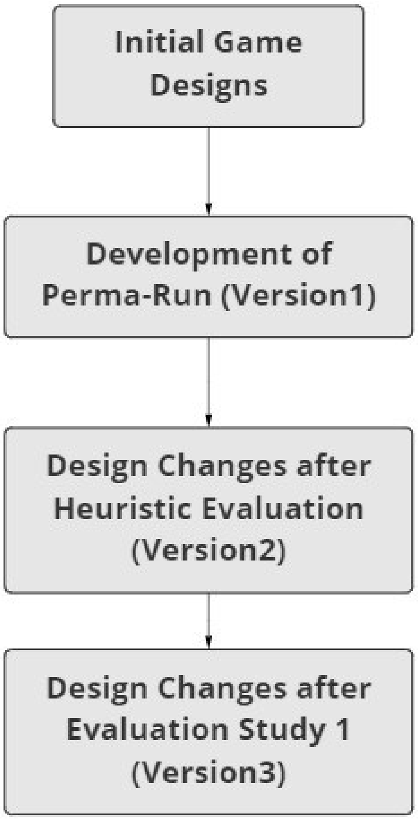

Initial Game Designs
Development of Perma-Run (Version1)
Design Changes after Heuristic Evaluation (Version2)
Design Changes after Evaluation Study 1 (Version3)

Figure 3.1: Overview of the Iterative Design Process

3.1 Game Design

Perma-Run is a 2D side-scrolling platformer inspired by the games like Super Mario [166], MegaMan [168], Captain Claw [169] and Dangerous Dave [167]. Before developing the final version of Perma-Run, the design went through an iterative user-centred design process. I adapted the 8-step design process by Fogg [47] to design the persuasive game. Table 3.1 outlines the eight-step design process in five stages.

Table 3.1 – BJ Fogg's 8-Step Design Process [49]

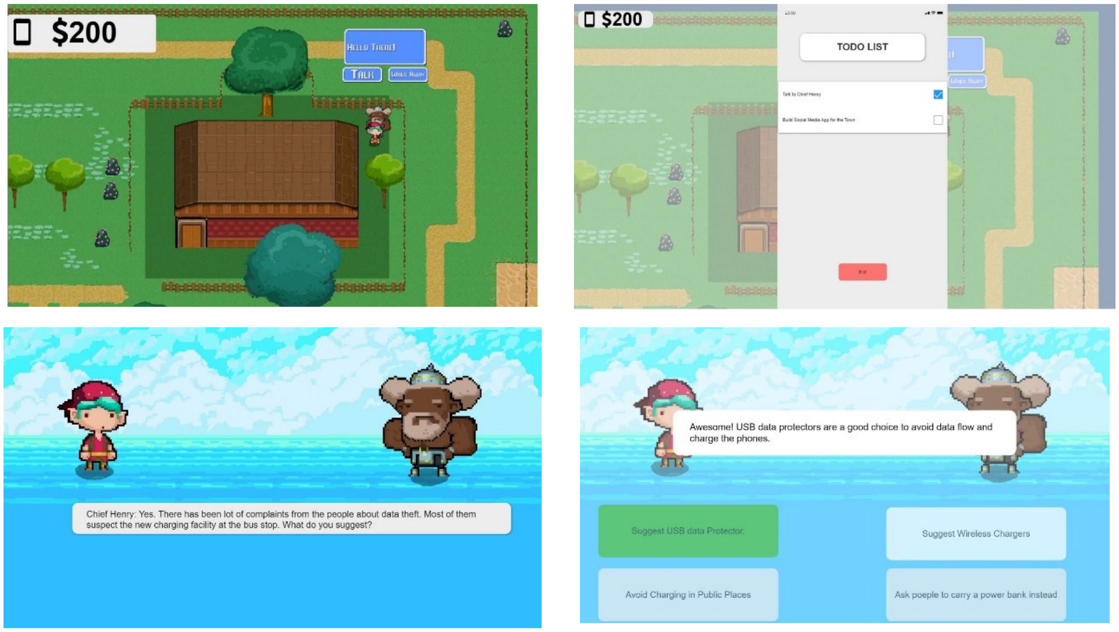
S.No	Design Step Description	Implementation
1.	Choose A Target Behaviour	From the background work, it is evident that there is a scarcity of interventions for secure smartphone behaviour. Hence, I selected the target behaviour as secure smartphone behaviour awareness.
2.	Choose Target Audience	The audience of the intervention is Android smartphone users.
3.	Find the Barriers Hindering Target Behaviour	Users being unaware of secure smartphone behaviour, and dangers of unsecure behaviours are barriers that were identified and discussed in the background chapter.
4.	Choose a Technology Channel	Persuasive games have been widely adopted and have been implemented in various domains. Little or no persuasive games exist for promoting secure smartphone behaviour. Thus, a persuasive game was chosen for this purpose.
5.	Find Existing Examples, Imitate & Iterate	Before starting with the game design, we analyzed various cybersecurity games and persuasive games from other domains. Initially, we had password security and email phishing as a part of our game apart from Android permissions. However, since these have been covered by other games, I focussed on promoting secure smartphone behaviour. The game designs went through an iterative design process and informal feedback from potential users to arrive at the final prototypes.

Following the decision to design a persuasive game for smartphone security, I leveraged the smartphone security and privacy use-case scenarios identified from the thematic analysis (as discussed in Chapter 2) for adding to the game design. Considering the domain of game design, various genres implement various game mechanics and are used for various purposes. For selecting a game genre, I considered the genres that are better for modelling the security use cases considering the development time and feasibility of the game. Role-Playing Games (RPGs) are the most popular genre which is used for simulating real-world scenarios in the form of quests. Quests are tasks that the player must complete in-game to make progress in-game or earn rewards. For a standalone developer, it might take anywhere from 8 months to 1 year to build a simple RPG.

Another popular genre is the 2D platformer which has been around for a long time and has evolved considerably in recent times. People easily recognize games like Super Mario [166] and Mega Man [168]. These games are simple, and the core game mechanic revolves around the player collecting game objects and overcoming obstacles at every level until the end of the game. On the other hand, simulation games are popular for training and educational purposes, and games like cooking simulators have been around for a long time. I initially designed three games around these genres and gauged the feasibility of developing these games and gamifying the security and privacy use cases for each game. All the game design prototypes were designed using Unity Game Engine [146], Inkscape [187] and Proto.io [188].

3.1.1 Design One - Secure My Village

As mentioned before, RPG games are popular because of their ability to model real-world scenarios in the form of quests. Inspired by popular games like Pokemon [189] and Diablo [190], Secure My Village is an isometric RPG game designed around an interesting narrative of saving a village from smartphone security and privacy issues by helping the villagers. The player must go around town and interact with other game characters and help them with their smartphone security or privacy issue. Figure 3.2 shows a few screenshots of the prototype of the game – Secure My Village, which was designed using Unity Game Engine [146] and Proto.io [188]. The quests are added to a To-Do list, and quizzes are included to test the player's knowledge after completing a quest. Figure 3.2 shows the prototype images of Secure the Village.


□ $200
Hello There
Talk
□ $200
TODO LIST
Edit
Suggest USB data Protector.
Suggest Wireless Chargers
Avoid Charging in Public Places
Ask poeple to carry a power bank instead

Talk to Chief Henry ☑

Build Social Media App for the Town □

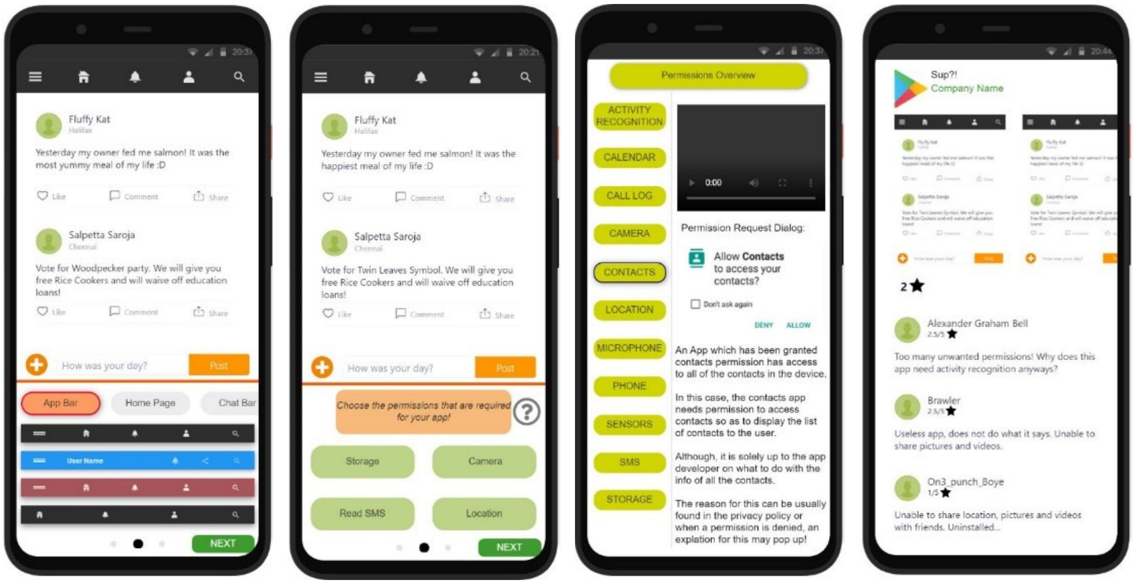
Chief Henry: Yes. There has been lot of complaints from the people about data theft. Most of them suspect the new charging facility at the bus stop. What do you suggest?

Awesome! USB data protectors are a good choice to avoid data flow and charge the phones.

Figure 3.2: *Secure My Village* Prototype

3.1.2 Design Two – CookApp!

"CookApp!" was inspired by simulation games that are used for educating users and entertaining users (eg., cooking games and farm games). This game is similar to the "build by yourself" type of game where the player must perform a task according to the rules to progress in the game or earn rewards. In "CookApp!", the player must build apps and must assign permissions according to the features that they include in the app. Later, the app is published in a simulated Google Playstore, and the user reviews reflect the feedback for the players. If there are too many or too few permissions, they will get bad reviews that outline the problem. Figure 3.3 shows the images of the "CookApp!" prototype.


Fluffy Kat
Halifax
Yesterday my owner fed me salmon! It was the most yummy meal of my life :D

Salpetta Saroja
Chennai
Vote for Woodpecker party. We will give you free Rice Cookers and will waive off education loans!

Fluffy Kat
Halifax
Yesterday my owner fed me salmon! It was the happiest meal of my life :D

Salpetta Saroja
Chennai
Vote for Twin Leaves Symbol. We will give you free Rice Cookers and will waive off education loans!

Choose the permissions that are required for your app!

Permission Request Dialog:

Allow **Contacts** to access your contacts?

□ Don't ask again

An App which has been granted contacts permission has access to all of the contacts in the device.

In this case, the contacts app needs permission to access contacts so as to display the list of contacts to the user.

Although, it is solely up to the app developer on what to do with the info of all the contacts.

The reason for this can be usually found in the privacy policy or when a permission is denied, an explation for this may pop up!

Sup?!
Company Name

2 ★

Alexander Graham Bell
2.5/5 ★
Too many unwanted permissions! Why does this app need activity recognition anyways?

Brawler
2.5/5 ★
Useless app, does not do what it says. Unable to share pictures and videos.

On3_punch_Boye
1/5 ★
Unable to share location, pictures and videos with friends. Uninstalled...

Figure 3.3: CookApp! prototype images

3.1.3 Design Three – Perma-Run

Inspired by 2D platformers like Super Mario [166], Mega Man [168], Captain Claw [169] and Dangerous Dave [167], Perma-Run is a 2D platformer that operationalizes permissions as in-game collectibles (similar to collecting coins in Super Mario). At each level, the player must collect the necessary permissions for an app. The permissions are colour-coded in a traffic signal format (Green: Necessary permission, Red: Unnecessary permission). The permissions to be collected in a level are shown to the play at the bottom of the screen. An interesting story is woven around smartphone security to provide context to the player. The protagonist of the story goes on a camping trip with his friends, and an angry troll appears out of nowhere. The troll was angry with “Humans- the inventor of Smartphones” since it was a victim of data theft. The troll who was unaware of secure smartphone behaviour kidnaps Dillon’s friends and traps them in various parts of the Jungle. The troll promises to release them if Dillon helps the troll by selecting the appropriate permissions for the apps. Figure 3.4 shows the prototype screens of Perma-Run. This initial version of the game was developed, and a heuristic evaluation was conducted to inform the design decisions. Refer to Chapter 4 for more details.

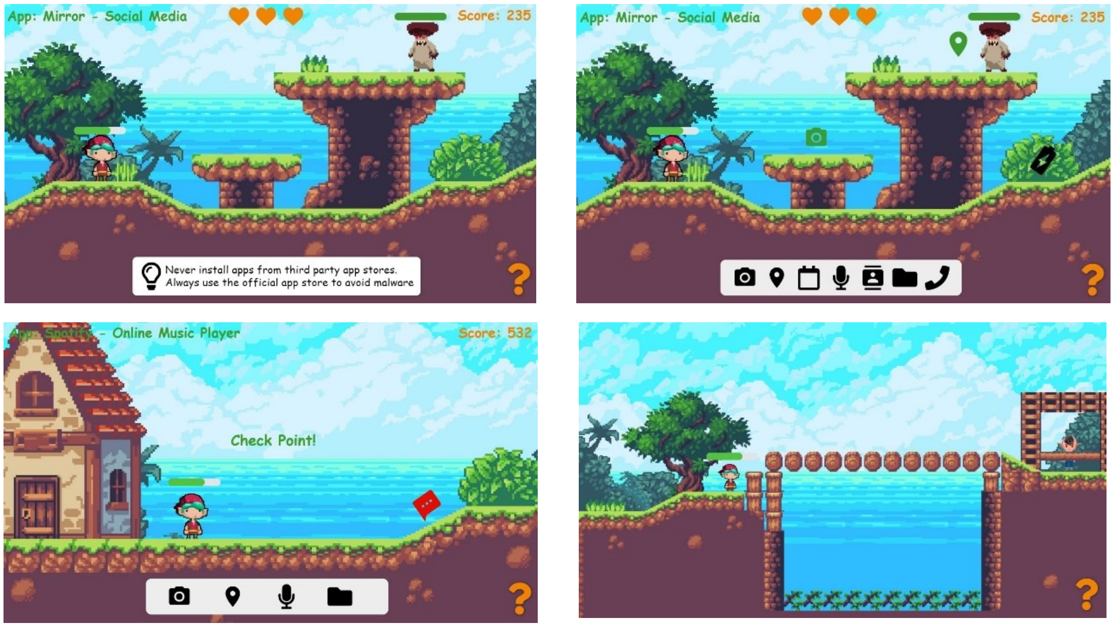

App: Mirror - Social Media
Score: 235
Never install apps from third party app stores.
Always use the official app store to avoid malware
?
App: Mirror - Social Media
Score: 235
?
App: Spotify - Online Music Player
Score: 532
Check Point!
?
?

Figure 3.4: Perma-Run Prototype

3.2 Perma-Run: Final Game Design

Modelling the various smartphone security and privacy use cases for the isometric RPG Secure the Village might sound lucrative, but the time and effort required to design a proper RPG for an iterative development process is a lot. Hence, Secure the Village was not considered for further development. Modelling the use cases for CookApp! might sway away from the main theme of the simulation app since not every security and privacy scenario can be modelled in a similar simulative way. Therefore, CookApp! was also ruled out. 2D platformer games have been around a long time, and recent game engines have smoothened the process of building them so that one can get started with game development easily. Also, smartphone security and privacy use cases can be modelled close to the RPG genre if not the same. The next sub-section lays out the various components of the game *Perma-Run* and the design changes done as part of the iterative process. The mobile game was designed and developed using the Unity Game engine [146], Inkscape [187] and proto.io [188]. Free game assets were used from the Unity Asset store [191] and itch.io website [192]. Free vector images (under the Creative Commons licence) were sourced from the Pixabay website [193], and royalty-free music was sourced from the purple-planet website [194]. Attributions to some of the designers were provided in the credits section of the game.

3.2.1 Perma-Run: Game Story

Just like any other game, providing context to the player is imperative as it sets the scenario and might motivate the player intrinsically. Given the various genres of games, different types of narratives exist for multiple purposes. Research has shown that narrative elements improve users' motivation and engagement during learning [77]. A good contextual narrative helps the players to connect with the game, retain knowledge and positively motivates the players [35,94]. Perma-Run includes a narrative that weaves the context of smartphone security and privacy into the narratives while maintaining a classic storyline similar to the popular 2-D games. The protagonist Dillion, and his friends go on a camping trip to a forest. While setting up their tent, they were invaded by a wild troll who was angry with them. The troll was a new smartphone user and a victim of data theft. Hence, it was angry with "Humans – The inventor of Smartphones". The troll kidnaps Dillon's friends and traps them in various parts of the Jungle. The troll promises to release them if Dillon helps it by collecting appropriate smartphone permissions for an android app on each level. Dillon must help other jungle creatures along the way with their smartphone issues. The game starts with an interesting hook to motivate the users towards playing the game and exploring more. Each level is preceded by a story to maintain the continuity of the game while weaving smartphone security concepts into the story. Further, various NPCs were added to the game with interactable conversations (in the form of quizzes) related to smartphone security and privacy to keep the game interesting and relatable to the main story.

3.2.2 Perma-Run: Gameplay

Considering the design changes from the outcome of the iterative studies, in the upcoming sections, the three versions of the game are discussed in detail.

3.2.2.1 Perma-Run: Version One

The game starts with a contextual story followed by a tutorial that explains the controls of the game and how to progress in the game. The players are briefed about the features of the android app for which they must collect necessary permissions in-game according to the app feature in each level. This is followed by a list of all the permission symbols that are shown to the player with a simple explanation of their functionality. After this, a quiz is shown to the player before starting each level. The players are questioned about the required permissions for the app for which they would be collecting permissions in-game. This is also shown to the user after completing the level, and the players get appropriate feedback for their quiz answers, explaining why certain permissions might or might not be required for the app. The necessary permissions that are to be collected in-game are coloured in green, and the unnecessary permissions are coloured in red. These collectible permissions are similar to collectible coins in video games.

Appropriate permission symbols are used in the game, same as the Android Permission symbols displayed to the user. The permissions to be collected in a level are displayed via a Heads-Up Display (HUD) to the user at the bottom of the screen. When the player collects the permissions, secure smartphone behaviour tips are shown to the player over the HUD (Figure 3.5 (i)). The player must collect all the necessary permissions along their way to rescue Dillon's friends at the end of the level. The player gains safety points (score) while collecting the necessary permissions, and they lose safety points and some health for collecting unnecessary permissions and the game character's movement speed is reduced nearly by 80% for about 3 seconds. The reduction of players' health and movement speed after picking up unnecessary permissions is done to reinforce awareness about the importance of necessary app permissions. There are obstacles and enemies that patrol the areas of the jungle to keep the game interesting. The player's safety score increases when the enemies are destroyed, and there are hidden areas and health bonuses to help the players progress in the game. The player has three lives and a health bar. The players lose health when they are attacked by an enemy or when they pick the wrong permission. When the player loses all their health, they lose a life (indicated by a heart symbol). The players lose a life when they fall on thorns/spikes or when they miss jumping on a platform and fall into the river. The design of Perma-Run: Version One was published at the Persuasive Conference Workshop, Ganesh, Ndulue and Orji [49].

3.2.2.2 Perma-Run: Version Two

Following the game's Version One, I conducted a Heuristic Evaluation for Playability (HEP) to evaluate the initial game design with six HCI and Persuasive Technology researchers. Heuristic analysis can be conducted during the early stages of the development of a design since it is considered to be cheap in terms of time and effort [40,100]. The number of evaluators for the heuristic analysis was in line with the recommendation of Nielsen et al. [100]. The details of the heuristic evaluation and the results are described in Chapter 4. I iterated the game design according to the Heuristic Evaluation of Playability results. The design changes are outlined in Table 3.2 for each heuristic. Apart from this, I added two more levels to the game. At each level of the game, the player must collect appropriate permissions for each smartphone app according to the features outlined in the story. Table 3.3 outlines the apps for each level, their features and the permissions required for each of them.

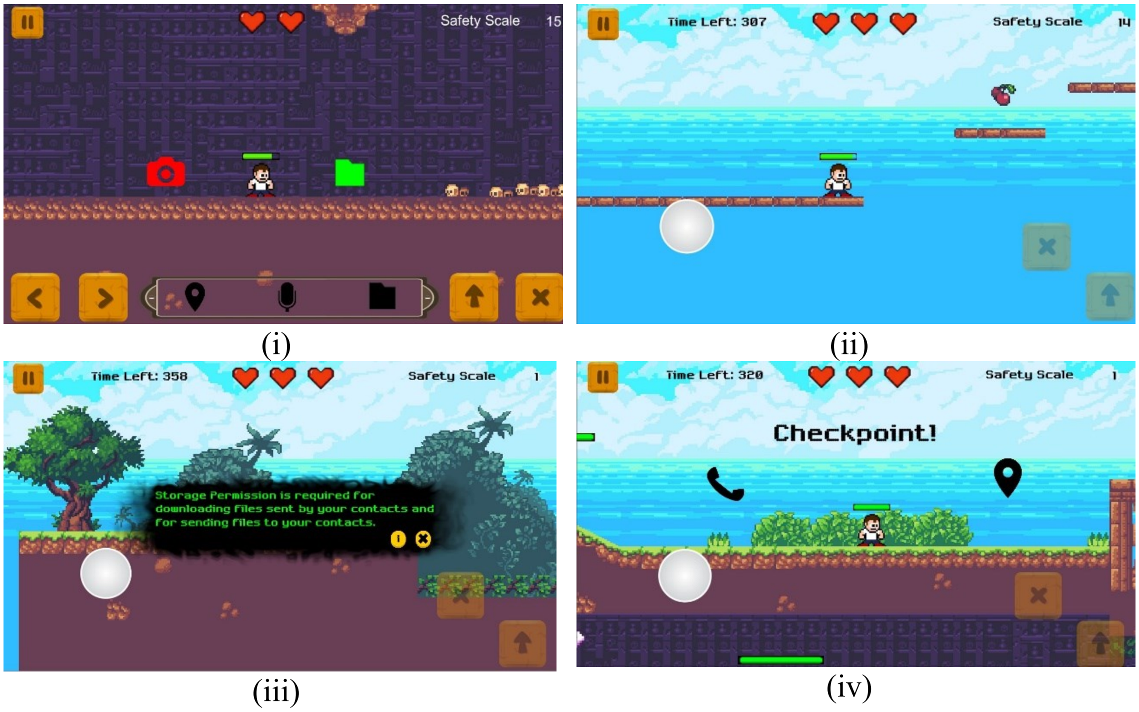
Table 3.2 - Design Changes according to the results of Heuristic Evaluation

Heuristic	**Design Changes**
Gameplay, Game Usability	Centered the suggestions and paused the game while displaying them (Figure 3.5 (iii)) so that users do not avoid reading the suggestions.
Game Usability	Removed the HUD from the bottom of the screen since it was hindering jumps and visibility of platforms.
Game Mechanic	Removed the color coding of collectible permissions (Figure 3.5(iv)) in-game as per feedbacks from conferences.
Game Story	*No Change*

Table 3.3 – Description of App Features and Permissions required in each level

Level	**App & Features**	**Permissions**
1.	*Communication App* – Video Chat, Sharing Media Files, Sharing Location, Messaging your contacts, SMS, Phone Dialler.	Camera, Storage, Location, Contacts, SMS, Phone, Microphone

2.	*Activity Tracking App* – Activity Tracking, Heart Rate Tracking, Fitness Blog, Popular running routes around you	Sensors, Activity Recognition, Location, Storage, Camera
3.	*Event Booking App* – View events happening around you, Save event reminders on your calendar, Store offline tickets on your phone.	Storage, Location, Calendar

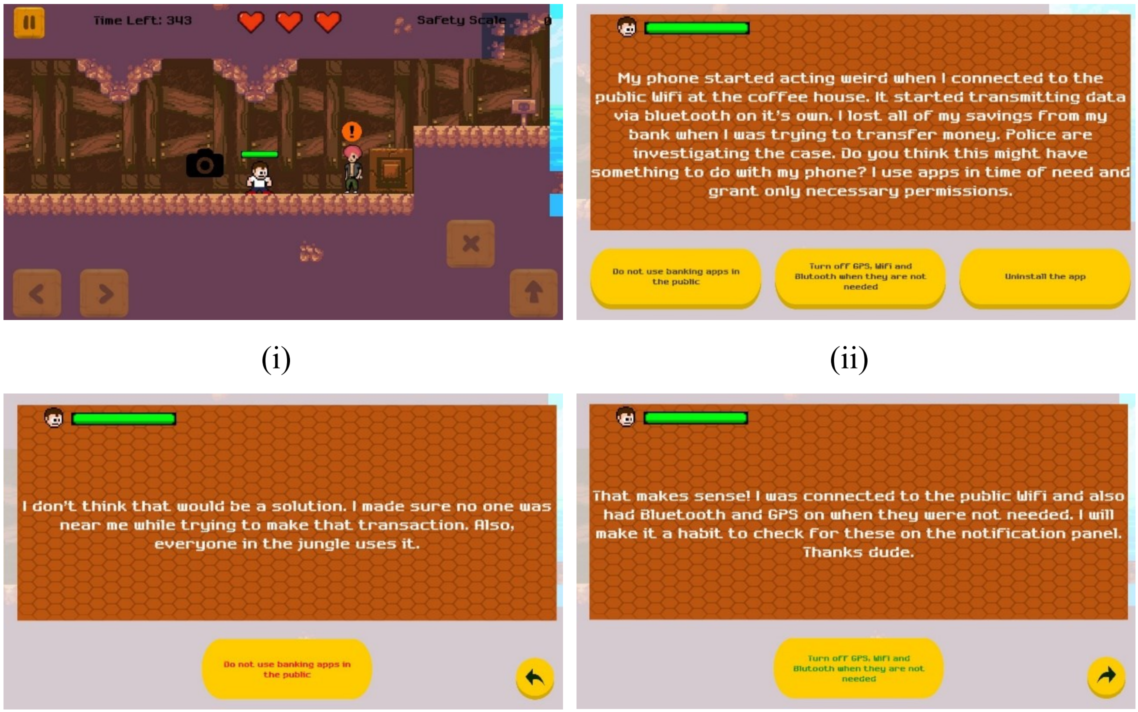


Storage Permission is required for downloading files sent by your contacts and for sending files to your contacts.

(i) (ii) (iii) (iv)

Figure 3.5: (i) Coloured Permissions with HUD at the bottom; (ii) A health boost fruit to help the player progress in the game; (iii) Centered Suggestion panel; (iv) Permissions of same colour

Following the changes according to the results of the Heuristic Analysis, I included other smartphone security and privacy scenarios according to the thematic analysis results from the background section. I added Friendly jungle creatures throughout the game (Figure 3.6), and the player must help them with their security and privacy issues while progressing in-game. A security or privacy scenario is displayed to the player in a quiz format along with three options. Appropriate feedback was provided to the players when they answer for the scenario. A wrong answer reduces the player’s health. The details of the smartphone security and privacy scenarios are described in Appendix F, with the feedback and response for each option.



(i)

My phone started acting weird when I connected to the public Wifi at the coffee house. It started transmitting data via bluetooth on it's own. I lost all of my savings from my bank when I was trying to transfer money. Police are investigating the case. Do you think this might have something to do with my phone? I use apps in time of need and grant only necessary permissions.

Do not use banking apps in the public
Turn off GPS, Wifi and Blutooth when they are not needed
Uninstall the app

(ii)

I don't think that would be a solution. I made sure no one was near me while trying to make that transaction. Also, everyone in the jungle uses it.

(iii)

That makes sense! I was connected to the public Wifi and also had Bluetooth and GPS on when they were not needed. I will make it a habit to check for these on the notification panel. Thanks dude.

(iv)

Figure 3.6: (i) A friendly jungle character waiting for the player's help; (ii) A security scenario with 3 options to choose from; (iii) Feedback for choosing a wrong option; (iv) Feedback for choosing the correct option

3.2.2.3 Perma-Run: Version Three

I conducted a between-subject study with the Perma-Run: Version Two to compare the game's efficacy with another education document published by the NSA [199] to promote smartphone security and privacy awareness. I collected the player's in-game lives loss data (coordinates of in-game locations when they lose a life) and the number of attempts taken to answer the in-game quiz questions (jungle character's security scenario). After analyzing the game's log data (details of the analysis are described in Chapter 4), I made a few tweaks to the levels to adjust the game's difficulty. Existing research has shown that platform size, scroll speed, and jump complexity affect a game's difficulty significantly [150]. The game's difficulty was primarily due to the jump distance between the platforms and strategic placement of obstacles (thorns/spikes) in-between jumps, along with the platforms. This was evident from the game's log data and qualitative data from the interview. For Version Three of the game, some of the gaps between platforms (where the players lost lives frequently) were reduced, and some of the obstacles in-between jumps were removed to reduce the difficulty of the game. If a game is too easy, it might not be engaging to play, and if it is too tough, players might stop playing altogether and hence they might not be exposed to the persuasive component. Finding the right balance to make games interesting requires iterative evaluation and experience with game design [195]. As mentioned in the background section, tailoring persuasive applications has been shown to yield better results. Different people might have various approaches towards achieving their goals. To tailor the game according to the user's motivational orientation, I leveraged the Regulatory focus theory and designed two variants of the game – The Promotion Focus Version, and the Prevention Focus Version. I consider both variants as Version Three of Perma-Run. Table 3.4 outlines the design changes implemented in line with Regulatory Focus Theory.

Table 3.4 – Game Design changes according to Regulatory Focus Theory

Variant	**Design Changes**
Promotion Focus (PRF)	• The suggestions of the security scenarios were tailored to reflect the gains or the positive outcome that the users would achieve when they take precautionary measures for safeguarding their smartphone from security and privacy issues. • Players gain a bit of health for picking up necessary permissions. • Players gain a bit of health for correct in-game quiz answers. • Players do not lose movement speed or health upon picking up an unnecessary permission.
Prevention Focus (PVF)	• The suggestions of the security scenarios were tailored to reflect the losses or the negative outcome that the users would face when they do not take precautionary measures for

	safeguarding their smartphone from security and privacy issues. - Players lose a bit of health for picking up unnecessary permissions. - Players lose a bit of health for wrong in-game quiz answers. - Players lose about 80% of movement speed and a bit of health upon picking up an unnecessary permission.

3.2.3 Perma-Run: Level Design

Apart from the gameplay and story, one of the important features of a 2D platformer is level design. Monotonous content might not be interesting for the players, and popular 2D games utilize level design to motivate players to progress through the game. I leveraged the 2D level design patterns developed by Khalifa et al. [70] to design the levels in an interesting manner. The level design patterns and their implementation details are outlined in Table 3.5.

Table 3.6 outlines the persuasive strategies of the initial version (Version One) of the game and their implementation details. Table 3.7 outlines the other persuasive strategies implemented in the other versions (Version Two and Version Three) of the game. Figure 3.7 and Figure 3.8 outline the overview of various game screens for Perma-Run Version One, Perma-Run Version Two and Version Three.

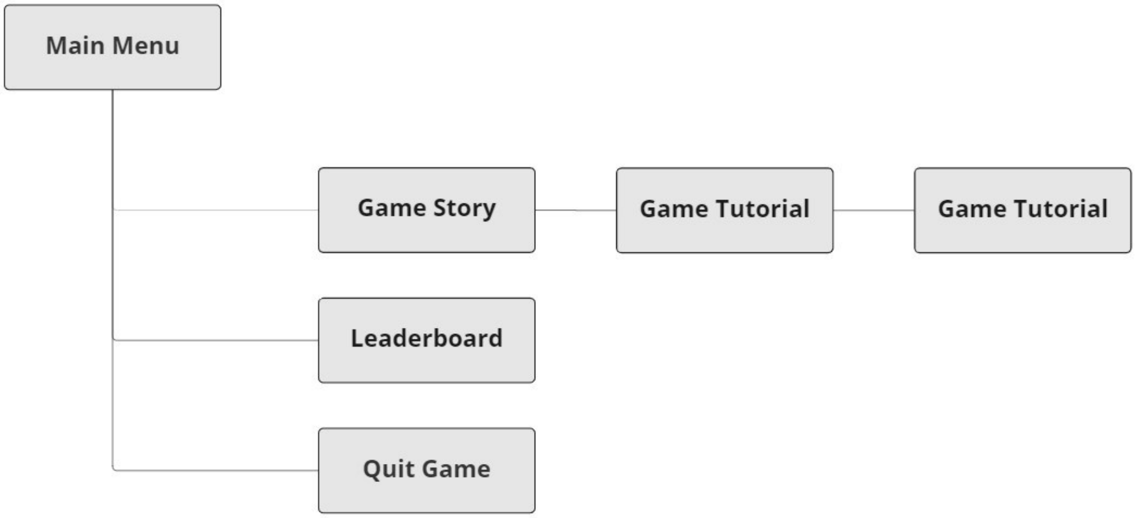


Figure 3.7: Overview of Perma-Run: Version One Game screens

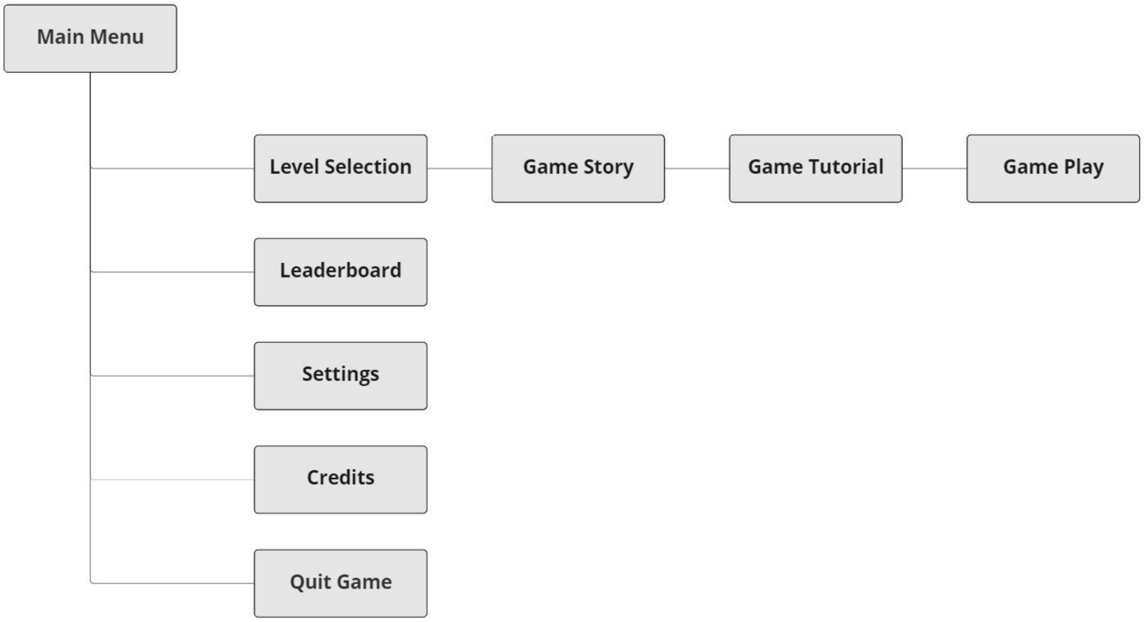


Figure 3.8: Overview of Perma-Run: Version Two and Version Three Game screens

Table 3.5 – Implementation of 2D Level Design Patterns [50,70]

Level Design Pattern	**Implementation**
Branching	We implement both branching and conditional branching. For branching, we give an alternate path to the player for exploration, and for conditional branching, the player is teleported to another

	location if they pick up a gem. This makes the game more interesting and increases the curiosity of the player.
Guidance	We used pathways to guide the player. We placed enemies and collectibles to guide them towards a specific path.
Foreshadowing	We tease the players with hidden areas or inaccessible game items that would be accessible as they progress through the game. We introduce enemies in a stationary way, followed by patrolling enemies at a later stage. This makes the game more interesting to play and might increase the players' curiosity [143].
Safe Zone	For safe zones, we have checkpoints (Player restarts the game from a particular point if they lose) in our game, where the player is not in danger and would feel safe. We have three checkpoints in our game. The player can plan their next moves or can just rest before progressing in the game. This breaks the tension in the game.
Layering	We placed enemies in-front of collectibles, positioned app permission symbols near enemies, placed obstacles in the pathway, and players can reach some areas only through a moving platform. This makes the game challenging.
Pace Breaking	We implement pace breaking by introducing enemies and then by giving the player a brief break from combat. We mix the Layering game pattern with Pace Breaking by adding obstacles to the paths to keep the game interesting, and the players engaged.

Table 3.6 – Implementation of Persuasive Strategies for Perma-Run: Version1 [50]

Persuasive Strategy	**Implementation**
Simulation	When the user picks up a necessary permission, their score increases, but when they pick up an unnecessary permission, their

	score decreases, and the player’s movement speed reduces for a short duration.
Competition	We rank the players according to their in-game score on a leaderboard. This score is affected by various factors like the type of permissions the player collects in-game, items that they pick up (E.g., Fruits), and the number of enemies they destroy.
Rewards	When the players pick up the correct permission or if they destroy an enemy, their score increases. When the player picks up fruits, their health increases. There are also extra lives in hidden areas for the player to collect.
Suggestion	We give immediate feedback and tips regarding secure smartphone behaviour. Whenever the player picks up a permission, we show suggestions about secure smartphone behaviour.
Liking	We added sound effects for the game character, background music followed by other in-game features and animations.
Tunnelling	We have three instances of tunnelling in our game – (a) before the start of the game, where the player gets an instruction screen that explains how to play the game. (b) In-game Collectibles to guide the player to the end of the level. (c) Providing information about the run-time permissions to the players to give them context about the permissions.
Self-Monitoring	The player has a Heads-Up Display (HUD) in between the in-game controls, which is displayed throughout the game that shows the necessary permissions that are needed to complete a level.
Reduction	We consider in-game checkpoints as a reduction strategy because the player need not repeat the whole level if they make a mistake and lose a life in the middle of the game.
Praise	The users receive praise (in the form of text) if they get the right answers in the post-game quiz after playing the game.

Table 3.7 – Implementation of Persuasive Strategies for Perma-Run: Version2 and Version3

Persuasive Strategy	**Implementation**
Recognition	Badges are awarded to players for in-game achievements.
Surface Credibility	The 2-D game was designed and developed in-line with popular 2-D platformers.
Real-World Feel	The information of the developer and the organization was provided in the credits screen along with links for game assets.
Trustworthiness	The security scenarios were provided with reasoning and appropriate feedback.
Social Comparison	The top five scores are displayed on the leaderboard.

3.2.4 Perma-Run: Game Development

I developed the game using Unity Game Engine [146] and programmed the scripts using C#. I designed some of the game assets like the buttons and the menu components using Inkscape [187]. Apart from this, I wrote separate game manager scripts for various functionalities of the game. This helps to maintain separate scripts while maintaining a few master scripts to integrate functionalities (inheriting functions from other classes) from various other scripts. This is helpful during the iterative design since editing the code according to the design changes was easy.

Chapter 4 – EVALUATION PROCESS OF PERMA-RUN

The evaluation of Perma-Run is three-fold, which matches the number of design iterations. As mentioned in the previous chapter, for the Version One of the game design, I conducted a Heuristic Evaluation for Playability (HEP) [40] with six HCI and Persuasive Technology researchers to identify initial design issues with the early version of the game before expanding upon it. Following this, I compared Version Two of the game with an educational document published by the National Security Agency (NSA) [199] with a between-subject study to compare which intervention performed better for improving smartphone security awareness. The document published by the NSA outlines smartphone security and privacy tips for the readers with the help of a pictorial representation of a smartphone. For the last study, evaluation study two, after tailoring the game according to the literature, I compared the two tailored versions (Version Three) of the game with a 2x2 between-subject study. Figure 4.1 outlines the evaluation stages along with the game version for reference. The study details are outlined in this chapter, and the results are presented in the following chapter.

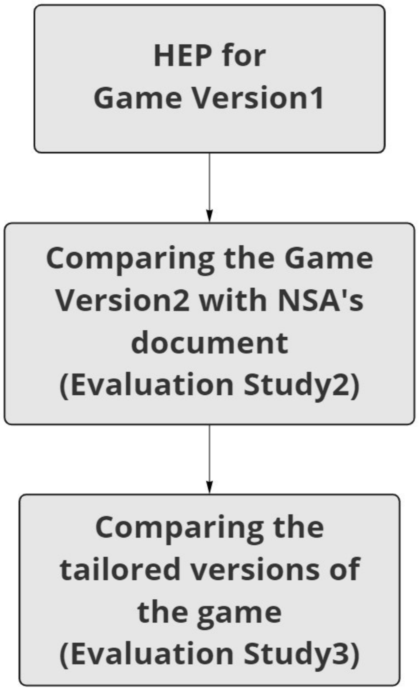


Figure 4.1: Evaluation stages of Perma-Run

4.1 Heuristic Evaluation for Playability (HEP) for Game Version One

Heuristic evaluations are useful for researchers during the initial stages of design to identify design-related and usability issues [40]. Usually, subject matter experts conduct a heuristic evaluation to identify usability or design issues in a digital application. The subject matter experts use a list of heuristics provided to them, according to which they would evaluate the digital application. To avoid personal bias, I conducted the heuristic evaluation for playability with six HCI and Persuasive Technology researchers (in-line with the recommended number of evaluators [99]) from the Persuasive Computing Lab at Dalhousie University. The convenience sampling was done by word of mouth. The researchers played the game for 20 minutes on average and rated the four heuristics (adapted from the HEP [40]) on a 5-point Likert scale. The HEP outlines four core heuristics – Game Mechanics, Game Usability, Game Play and Game Story. Apart from this, they also responded to a survey that measured their perceived persuasiveness, perceived self-efficacy, and perceived smartphone security awareness. The results of this study were published as part of the CHI Late-Breaking Work (LBW), Ganesh, Ndulue and Orji [50] and are discussed in the following chapter. Following this evaluation, the game was redesigned according to the results of the analysis as Perma-Run: Version Two.

4.2 Perma-Rum: Evaluation Study One

To understand the effectiveness of an intervention, it is a common practice to compare it with another intervention that is available to the general public. Recently, Wen et al. [152] compared *What.Hack*, a novel role-play based phishing game with *Anti-phishing Phil*, a popular non role-play based intervention. The author conducted a between-subject study to compare the two interventions, and from the results, it was evident that *What.Hack* performed better than *Anti-phishing Phil*. Similarly, Raptis et al. [123] designed *GamePass* a gamified graphical user authentication to improve users' password choices. The author conducted a between-subject study and compared *GamePass* with *Oripass,* a web-based graphical user authentication interface that uses a background image as a cue. From the results, it was evident that the gamified intervention GamePass, performed better than Oripass. After redesigning Perma-Run according to the results of the HEP evaluation, I compared it with an existing intervention for improving smartphone security awareness.

I conducted a between-subject study with Perma-Run: Version Two and an educational document published by the NSA [199]. From the literature review, it was evident that Protection Motivation Theory (PMT) has been widely used in the domain of cybersecurity to measure users' overall intention to protect themselves from threats. PMT outlines five core constructs (self-efficacy, response efficacy, response cost, perceived vulnerability, and perceived severity) that contribute toward peoples' intention to protect themselves from threats. I adopted the PMT scale for smartphone security developed by Verkijika et al. [147] to measure the players' intention to protect themselves from smartphone security threats. I also leveraged the Intrinsic Motivation Inventory (IMI) to measure the game's play experience and the reader's experience with the educational document. Along with this, I included a permission scenario, where the users are asked to select the required permissions for a music app out of the ten dangerous permissions. For the study design, I conducted a between-subject study to compare the game (Version Two) and the security document. A total of sixteen participants answered a pre-study survey which included PMT, Permission Scenario and IMI. The participants were recruited from the persuasive computing lab through word of mouth. They were given seven days to interact with the interventions (either the game or educational material) randomly assigned to them. One group of users (n = 9) played the game while the other group (n = 7) read the educational document. After that, they took the post-study survey which had the same scales as the pre-study survey for repeated measurement. To get a deeper understanding of the participants' experience, I interviewed eight participants who played the game and five participants who read the document after the post-study survey. From the results of evaluation study one (discussed in the upcoming Chapter), it was evident that overall, the game performed better than the educational document. Apart from this, the players' game data (coordinates of the place where they lose a life, in-game quiz answer attempt number, health remaining) were logged in the background during gameplay using Unity's WWW library. With the game log data, the levels' difficulty was adjusted accordingly by removing some obstacles and adjusting the distance between various platforms in-game. Table 4.1 outlines the research questions and the respective survey scales used in Evaluation Study One, and Figure 4.2 outlines the overview of Evaluation Study One. The results are outlined in the upcoming chapter. Evaluation Study One was published as part of the conference proceedings of the International Conference on Persuasive Technology, Ganesh, Ndulue and Orji [51].

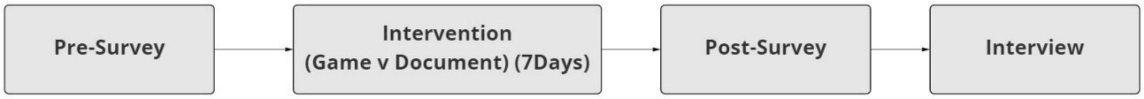


Figure 4.2: Overview of Evaluation Study One design

Table 4.1 – Research Questions and Survey scales for Evaluation Study One

Research Questions	**Survey Scales**
RQ1: Does Perma-Run improve user's intention to protect themselves from smartphone security threats compared to the educational document?	Protection Motivation Theory (PMT) [147] scale
RQ2: How does Perma-Run's user experience compare to the educational document?	Intrinsic Motivation Inventory (IMI) [126] scale
RQ3: Does Perma-Run improve user's awareness about smartphone permissions compared to the educational document?	Permission Scenario

4.3 Evaluation Study Two

From the literature review, it was evident that tailored interventions and persuasive games were much more effective in bringing forth a positive behaviour change compared to non-tailored versions. I tailored the game according to the Regulatory Focus Theory [59], which states that people develop a predominant motivational orientation to reach their goals over their lifetime. People with a Promotion Focus orientation prefer the presence of positive outcomes or positive gains while working towards their goals. People with a Prevention Focus orientation prefer the absence of negative outcomes while trying to reach their goals. The design changes done according to the Regulatory Focus Theory for Version Three of the game are described in Chapter 3. For Evaluation Study Two, the users answered a pre-study survey followed by gameplay for at least ten days after which they filled a post-study survey. For the pre-study survey, I collected the players' demographics, gaming habits, Protection Motivation [147], Security Behaviour using the smartphone security behaviour scale (SSBS [64]), Permission Scenario and Regulatory Focus Questionnaire (RFQ [60]). The SSBS is used to measure smartphone security behaviour over two factors namely technical aspect and social aspect [64]. The technical aspect of SSBS covers the technical steps or knowledge that is needed (e.g., Using a VPN or Anti-Virus) to secure one's smartphone. The social aspect of SSBS covers the users' ability to identify social cues (e.g., Deleting suspicious communication, verifying the app's source) to identify smartphone security threats. The RFQ is an 11-item questionnaire used to identify a user's chronic orientation. For the post-study survey, Protection Motivation, Security Behaviour and Permissions Scenario were measured again. Apart from these, the players' perceived persuasiveness (adapted from [42,141]), their overall play experience (IMI) [126] and motivational appeal (ARCS) [68] were also measured. After the post-study survey, I interviewed some of the players (n = 25) to understand more about their experience with the game. All the scales, tables and interview questions are included in Appendix B&C. Figure 4.3 shows the overview of Evaluation Study Two. Table 4.2 outlines the research questions and the respective survey scales used for Evaluation Study Two. Table 4.3 shows the number of participants for each 2x2 between-subject study design.

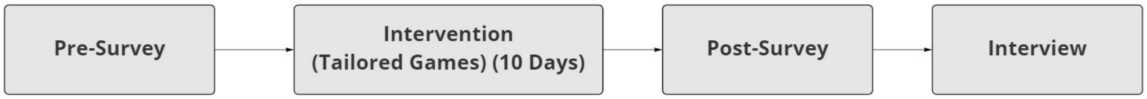


Figure 4.3: Overview of Evaluation Study Two design

Table 4.2 - Research Questions and Survey scales for Evaluation Study Two

Research Questions	**Survey Scales**
RQ4: Does Perma-Run motivate users to protect themselves from smartphone security threats? (PMT)	Protection Motivation Theory (PMT) [147] scale (Pre-Post study design), SSBS, Permission Scenario
RQ5: Does the tailored version of Perma-Run improve players' intention to protect themselves?	PMT

RQ6: How does Perma-Run perform with respect to the motivational appeal.	ARCS scale [68,109]
RQ7*:* How effective is Perma-Run with respect to promoting a positive user experience?	Intrinsic Motivation Inventory [126]
RQ8: How persuasive is Perma-Run with respect to motivating players to follow secure smartphone behaviour?	Perceived Persuasiveness [42,141]
RQ9: How does the tailored version of Perma-Run affect the player's intrinsic motivation?	IMI
RQ10: How does the tailored version of Perma-Run affect the players' motivational appeal?	ARCS scale
RQ11: Does the tailored version of Perma-Run have an effect on the game's persuasiveness?	Perceived Persuasiveness

Table 4.3 – 2x2 between-subject study design for Evaluation Study Two

	Total N = 102	
	Promotion Focus Game version	Prevention Focus Game version
Promotion Focus players	25 (tailored)	24 (non-tailored)
Prevention Focus players	26 (non-tailored)	27 (tailored)

For this second evaluation study, I used snowball sampling [196] for recruiting participants, and the recruitment notice was shared using university email lists, and social media sites like Reddit, LinkedIn and Facebook. A participant's data was included in the analysis if they had played the game for at least 10 mins per day, over the course of 10 days and this was ensured with the help of the game's log data. A total of 26 participants played the game but did not complete the post-study survey, and a total of 156 participants did not play the game after completing the pre-study survey. Apart from this, I also filtered the pre-study survey data that were filled within 5 minutes. Based on the participants' RFQ responses, they were divided into two groups – Promotion Focus and Prevention Focus. To eliminate the possibility of bias, a total of 284 participants were randomly assigned to one of the two versions of the game – the Promotion Focus version or the Prevention Focus version. From this, four groups of participants were formed - Promotion Focus users who played the promotion focus game version (*Promotion focus tailored*), Promotion Focus users who played the prevention focus version of the game (*Promotion focus non-tailored*), Prevention Focus users who played the promotion focus version of the game (*Prevention focus non-tailored*), *and* Prevention Focus users who played the prevention focus version of the game *(Prevention focus tailored)*. A total of 102 participants completed the study (by completing the post-study survey after 10 days). After the post-survey study, I conducted a lucky draw (random wheel spinner), and four random participants were awarded a sum of CAD 25. The results of Evaluation Study Two are discussed in the upcoming chapter.

4.3.1 Participant's Demographics

Looking at the participants' demographics, there were a total of 102 participants overall, 69 of them were male (68%), and 33 were female participants (32%) as shown in Figure 4.4. Although there has been a considerable rise in the number of female gamers in general, male gamers still dominate, and this might be a reason for the skewed number of participants [73,197]. There was a total of 52 participants who had completed a bachelor's degree, 2 participants who had completed a college diploma, 3 participants with doctoral degrees, 18 participants had completed high school or equivalent, 1 participant who had completed less than high school and 26 participants who had completed Master's. These are outlined in Figure 4.5. A total of 22 participants were married, and 80 participants were single. Looking at the participant's age ranges, 54 participants were in the age range of 18-25 years, 37 of them were 26-35 years, 5 of them were 36-45 years, and 6 participants were in the range of 46-60 years. This is shown in Figure 4.6.

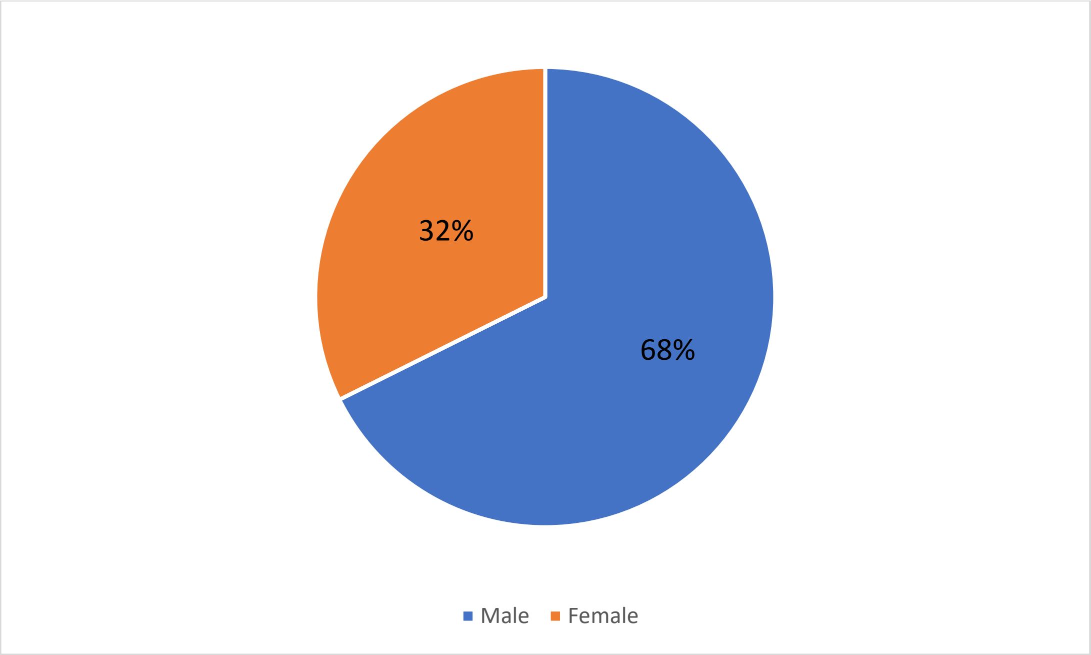


Figure 4.4: Demographics by gender

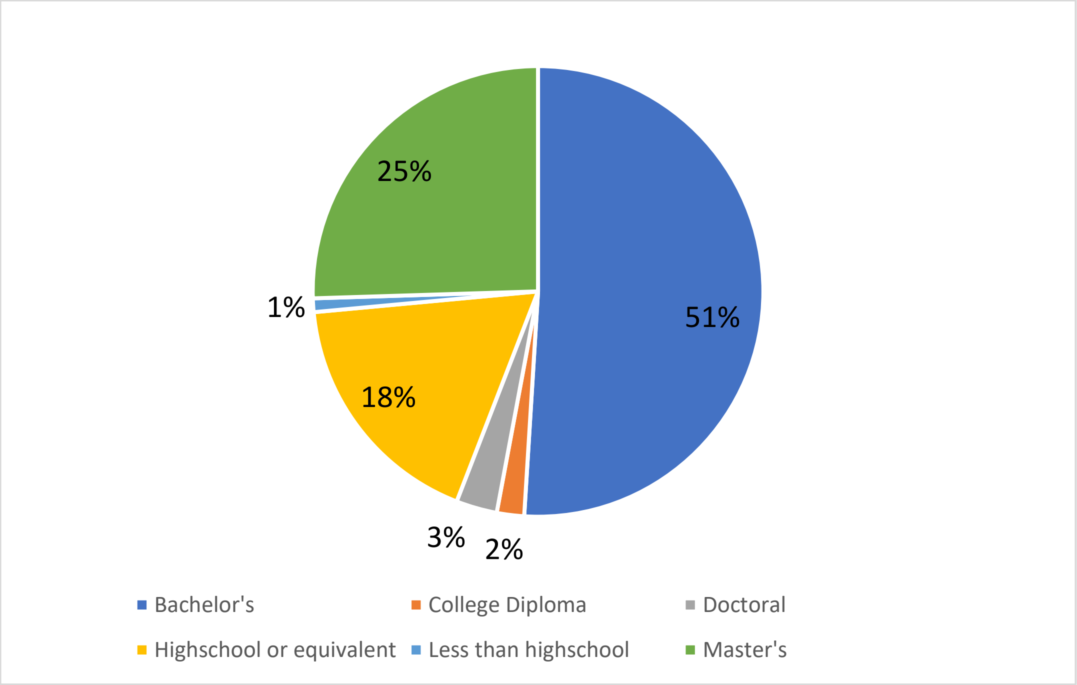


Figure 4.5: Demographics by highest level of education

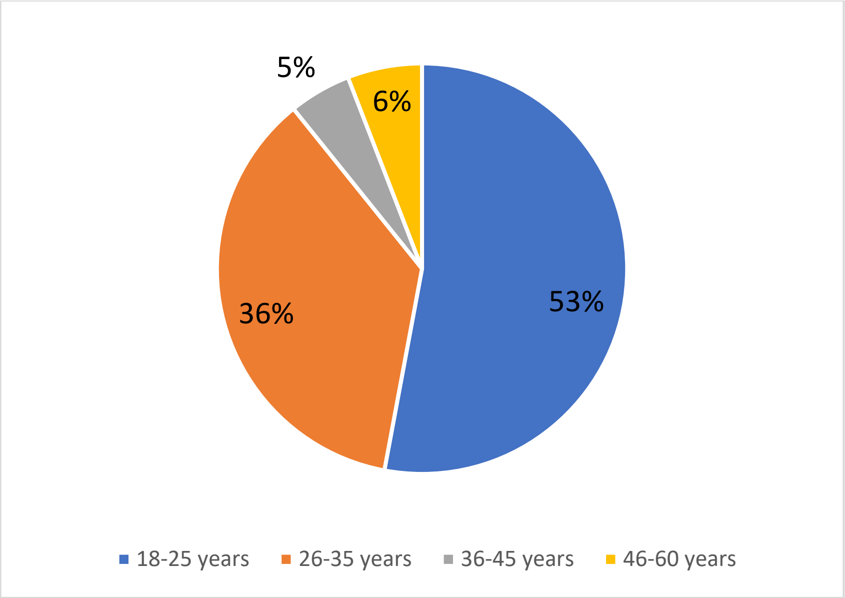


Figure 4.6: Demographics by Age

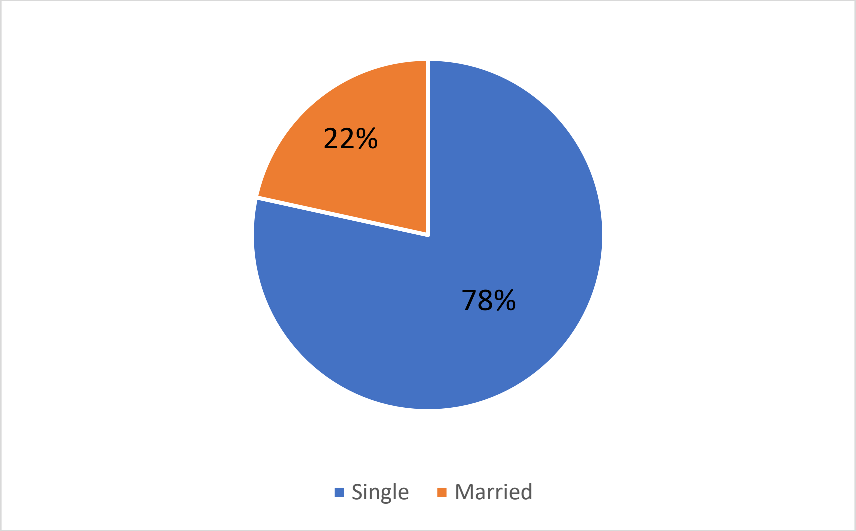


Figure 4.7: Demographics by Marital Status

Looking at the devices used by players for playing games, 96 participants reported that they play games on smartphones, 85 participants played on PC, 51 participants played console games, and 5 participants marked other as their choice, and some of them were portable consoles like Sega hand-held console and head-mounted display (HMD). This is shown in Figure 4.8. When players were asked about their average gameplay time per week, 16 participants answered that they do not play games, 51 participants played 1-2 hours, 18 participants played 3-5 hours, 10 participants played 6-8 hours, and seven participants played 8+ hours. This is outlined in Figure 4.9. Table 4.4 outlines the overall participants' demographic data.

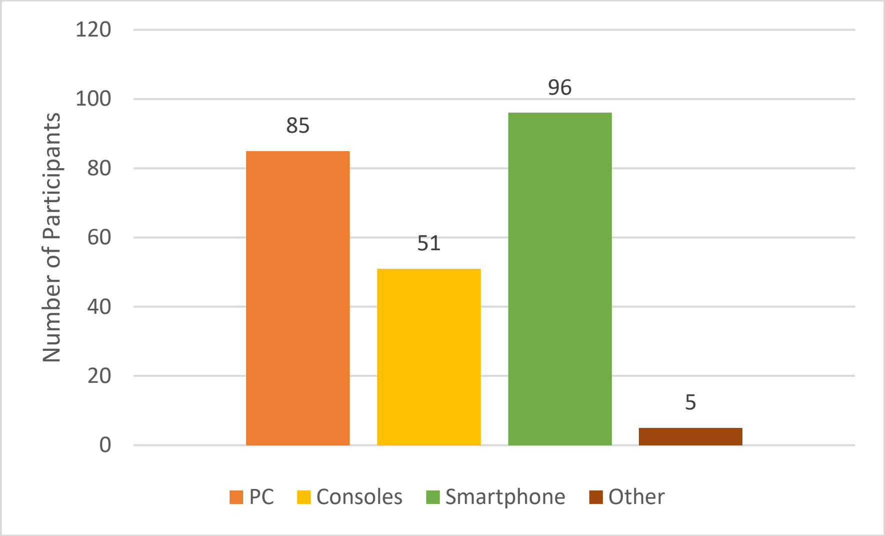


Figure 4.8: Demographics by frequently used devices for gaming

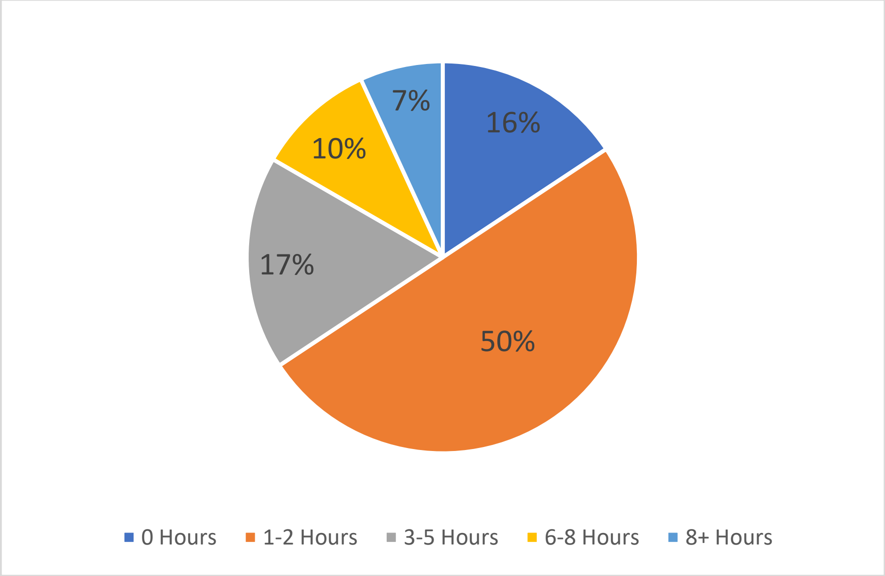


Figure 4.9: Demographics by average gameplay time over a week

Table 4.4 – Overall Demographics of Participants

Total Participants = 102	
Gender	Male (68%), Female (32%)
Age	18-25 Years (53%), 26-35 Years (36%), 36-45 Years (5%), 46-60 Years (6%)

Marital Status	Single (78%), Married (22%)
Education	Bachelor’s (51%), College Diploma (2%), Doctoral (3%), Highschool or Equivalent (18%), Less than High School (1%), Master’s (25%)
Gameplay Time	0 Hours (16%), 1-2 Hours (50%), 3-5 Hours (17%), 6-8 Hours (10%), 8+ Hours (7%)
Frequently Used Devices for Gaming	PC (85), Smartphone (9), Console (51), Other (5)

Chapter 5 – RESULTS

In this chapter, I present the results of the Heuristic Evaluation for Playability (HEP), Evaluation Study One and Evaluation Study Two of Perma-Run. Each study's outcomes are discussed, along with design changes incorporated in each game version, as mentioned in Chapter 3.

5.1 Results of Heuristic Evaluation for Playability (HEP)

After conducting the HEP with six HCI and Persuasive Technology researchers from the Persuasive Computing Lab, Dalhousie University, I prepared the survey data and the open-ended feedback for analysis. For analyzing the survey data, I averaged the scores of each heuristic and compared the average scores of perceived persuasiveness, perceived smartphone security awareness and self-efficacy against the neutral value of 3. Since the data did not have a normal distribution and the sample size was low, a t-test was not feasible. The mean scores of the heuristics are shown in Table 5.1, and the mean scores of perceived persuasiveness of the persuasive strategies are shown in Table 5.2. Both perceived smartphone security awareness (M = 4.30, SD = 0.47) and perceived self-efficacy (M = 4.00, SD = 0.81) mean scores are above the neutral score of 3. Figure 5.1 shows the boxplot for the heuristics. Figure 5.2 shows the bar chart for perceived smartphone security awareness and perceived self-efficacy.

Table 5.1 – Mean and Standard deviation for Heuristic Evaluation for Playability

Game Heuristics	**Mean (M), Standard Deviation (SD)**
Game Mechanic	M = 4.09, SD = 0.42
Game Usability	M= 4.02, SD = 0.41
Game Play	M = 3.93, SD = 0.50
Game Story	M = 3.75, SD = 0.61

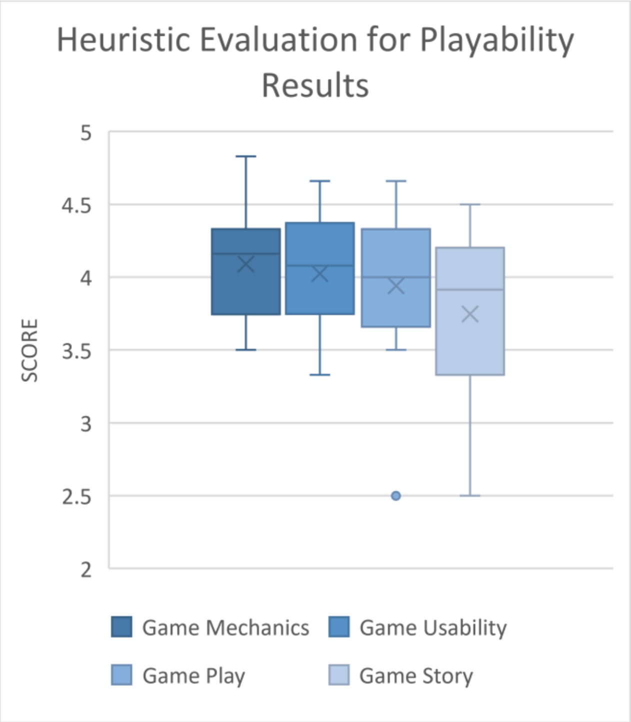


Figure 5.1: Box and Whisker Plot for Heuristic Evaluation for Playability Results

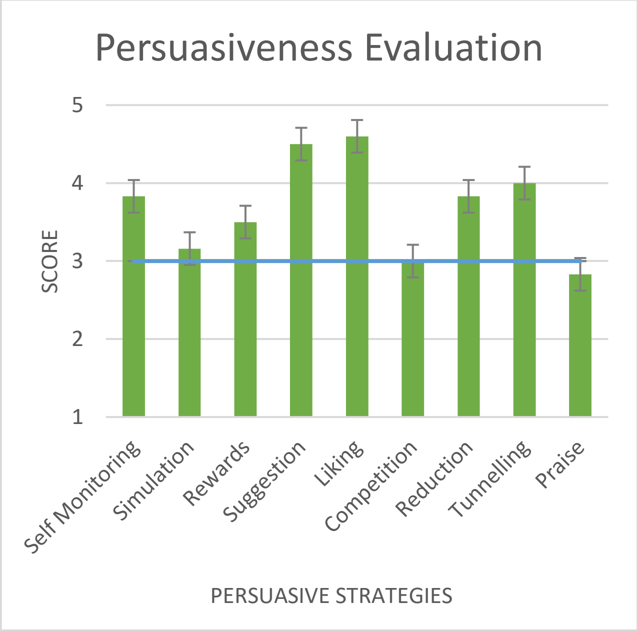


Figure 5.2: Bar Chart for Persuasiveness Results

Table 5.2: Mean and Standard deviation for Persuasive Strategies

Persuasive Strategies	**Mean (M), Standard Deviation (SD)**
Self-Monitoring	M = 3.83, SD = 1.34
Suggestion	M = 4.50, SD = 0.50
Tunnelling	M = 4.00, SD = 1.82
Reduction	M = 3.16, SD = 1.46
Rewards	M = 3.50, SD = 1.80
Simulation	M = 3.16, SD = 1.46
Praise	M = 2.80, SD = 1.86
Liking	M = 4.60, SD = 0.47
Competition	M = 3.00, SD = 1.15

For analyzing the evaluator's qualitative feedback, I used the affinity diagram method (Figure 5.3) to perform a thematic analysis. This helped to uncover usability issues and the evaluator's thoughts about the game. Some of the evaluators reported that they felt ***nostalgic*** when they played the game for the first time. They also reported that they felt a ***sense of achievement*** when they finished the game. *Evaluator(6)* commented: *"I could quickly relate it to Mario"*. Recent research suggests that nostalgia is directly impacted by past memories, and satisfaction of competence, especially with retro games that focus on challenging and fast gameplay [156]. The ability to relate the game with the player's past experience is essential for persuasive games since it lowers the learning curve and improves the feeling of competence, which is in line with the Self-determination theory [156]. This also makes sure that the players associate the game with their past experience, which increases the game's relevance, and relatedness and might ensure that players would play the game. This also confirms that our design decision to make the gameplay resemble a well-known game Super Mario [166], to attract a diverse audience and reduce the learning curve paid off.

Most of the evaluators uncovered at least one of the hidden areas in the game. The hidden areas can be classified under the foreshadowing level design pattern [70], which creates a sense of uncertainty or a knowledge gap that makes the user curious about a visual cue. This is called *perceptual curiosity,* which leads to increased attention to the game [143] and motivates the players to play further. Some evaluators felt that the ***game was challenging to play.***

Evaluator(3) commented - "Considering the level has a timer, reading the tips is against the gameplay, and I barely read even one tip to save time." The same evaluator also stated that *"The HUD overlaps the map in many places, I died twice because I couldn't see what I'm jumping at due to the interface on the bottom-middle".*

Evaluator(4) stated - *"While the player is collecting the icons (whether green or red), you can pause the gameplay, with an OK button, so that after the player reads the message, they can then press the OK button to resume the game".*

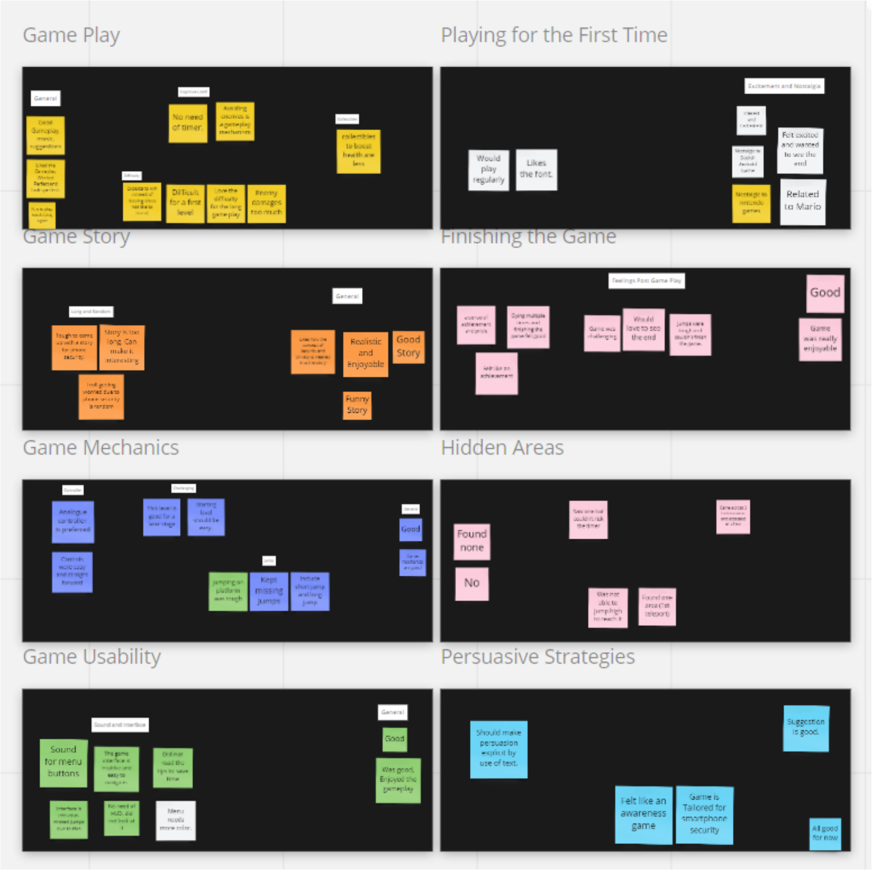

Game Play
General
Good Gameplay, music, suggestions
No need of timer.
Avoiding enemies is a gameplay mechanism
Collectibles
collectibles to boost health are less
Difficulty
Difficult for a first level
Love the difficulty for the long game play
Enemy damages too much
Playing for the First Time
Excitement and Nostalgia
Would play regularly
Likes the font.
Felt excited and wanted to see the end
Nostalgic to nintendo games
Related to Mario
Game Story
Long and Random
Tough to come up with a story for phone security.
Story is too long. Can make it interesting
General
Realistic and Enjoyable
Good Story
Funny Story
Finishing the Game
Feelings Post Game Play
Felt like an achievement
Game was challenging
Would love to see the end
Good
Game was really enjoyable
Game Mechanics
Controller
Analogue controller is preferred
Controls were easy and straight forward
Challenging
This level is good for a later stage
Starting level should be easy.
General
Good
Jump
Jumping on platform was tough
Kept missing jumps
Include short jump and long jump
Hidden Areas
Found none
No
Was not able to jump high to reach it
Found one area (Tet teleport)
Game Usability
Sound and Interface
Sound for menu buttons
The game interface is intuitive and easy to navigate.
Did not read the tips to save time
No need of HUD, did not look at it
Menu needs more color.
General
Good
Was good. Enjoyed the gameplay
Persuasive Strategies
Should make persuasion explicit by use of text.
Suggestion is good.
Felt like an awareness game
Game is Tailored for smartphone security
All good for now

Figure 5.3: Affinity Diagram for HEP comments

Ideally, games should pose some level of challenge to sustain players' interest; if it is too easy, players might get bored, and stop playing the game. However, if persuasive games are too challenging, players may drop off before they are exposed to all the persuasive content that would lead to behaviour change. With this feedback in mind, design changes were made to the game accordingly, and this led to Perma-Run: Version Two. The design changes were:

- *Removal of the HUD to increase visibility in-game (Game Usability)*
- *Removal of colour coding of permission collectibles (Game Mechanic)* and *centring the suggestions while pausing the game (Game Usability, Game Play)*.

These design changes are also mentioned in Chapter 3, Table 3.2. Apart from these changes, I added a quiz element to cover other smartphone security and privacy concepts apart from permissions. These changes are depicted in Chapter 3, Figure 3.6.

5.2 Results of Evaluation Study One

After making the design changes to the game following the HEP analysis, I compared Perma-Run: Version Two with an existing educational document published by NSA [199] that promotes mobile device best practices. The research questions are as follows:

RQ1: Does Perma-Run improve users' intention to protect themselves from smartphone security threats compared to the educational document?

RQ2: How does Perma-Run's user experience compare to the educational document?

RQ3: Does Perma-Run improve users' awareness about smartphone permissions compared to the educational document?

To answer ***RQ1:*** *Does Perma-Run improve users' intention to protect themselves from smartphone security threats compared to the educational document?*- I adapted the PMT scale from Verkijika et al. [147] for measuring the player's intention to follow secure smartphone behaviour. The PMT scale has eight constructs namely, Self-Efficacy, Response Efficacy, Response Cost, Perceived Vulnerability, Perceived Severity, Anticipated Regret, Security Intention and Security Behaviour. The users responded to the PMT scale during the pre-study survey and post-study survey. Due to the low number of participants in each group and the non-normal data, a paired t-test was not feasible in this case. Hence, I explored the descriptive statistics for both interventions which are described in Table 5.3. Some of the constructs have been omitted from this table since they did not yield significant results (< 1% change) for both the interventions.

Table 5.3 – Mean changes of PMT constructs for the game and educational document

Survey Items	**Mean Change (Pre to Post - Game)**	**Mean Change (Pre to Post - Document)**
Self-Efficacy	72%	14%
Response Cost	-78%	-32%
Perceived Severity	38%	-14%
Perceived Vulnerability	11%	-18%
Security Behaviour	66%	57%

To answer ***RQ2:*** *How does Perma-Run's user experience compare to the educational document?*- I leveraged the IMI scale [126] to measure the participants' experience with the game and the document. Overall, for the IMI, Perma-Run: Version Two performed slightly better (M = 4.37, SD = 0.845) compared to the educational document (M = 4.24, SD = 0.769). To answer ***RQ3:*** *Does Perma-Run improve users' awareness about smartphone permissions compared to the educational document?* **-** the participants answered a permission scenario question in both the pre-study survey and the post-study survey. The participants had to select the required permissions according to the features of an online music player out of the ten dangerous permissions. The game recorded a mean change of 33% for selecting correct permissions and -56% for selecting wrong permissions (participants selected less number of unnecessary permissions in the post-test). The document scored a mean change of 0% for correct permissions and -15% for wrong permissions.

5.2.1 Thematic Analysis of Evaluation Study One Interview Data

I also interviewed the users after the post-study survey, and I analyzed this qualitative data using thematic analysis (Affinity Diagram, Table 5.4) for both the game (Figure 5.4) and the educational document (Figure 5.5). I interviewed 8 participants who played the game and 5 participants who read the educational document. Participants' comments were concisely written on post-it notes, and I collated similar comments to form themes. The key themes for both interventions are discussed here. When players' were asked how they felt about the game when they opened it for the first time, most of them described being ***nostalgic and were able to relate it*** with Super Mario [166] and other retro games.

Player-2 chuckled while stating, *"Mario. It gave me the feeling of playing 2-D Sega games. It was more like walking back into memory lane and enjoying the game"*.

Recent research shows that retro games invoke nostalgia by invoking past memories and satisfaction of competence [156]. For the intervention presented as a document, most of the readers ***struggled*** to understand the document and needed some time to understand it.

Reader-3 said, "*I was confused about what to look for the first time because everything was on one page with a lot of text, signs, and arrows… I found it was too much of an overload*".

Reader-2 mentioned, "*...But for the second page, it took me a while to understand what the symbols were all about*". Some of the readers were ***not familiar with cybersecurity terminologies***.

Table 5.4 – Themes for Evaluation Study One Thematic Analysis

Themes For Game	**Themes For Educational Document**
Nostalgic and Relatable	Suggestions
Self-Realization and Retrospection	Self-Realization and Retrospection
In-Game Quiz	Security
Security	Positive comments for Document
Struggles with Game	Struggles with Document
Positive comments for Game	Recommendation to others
Suggestions	Overview of Document

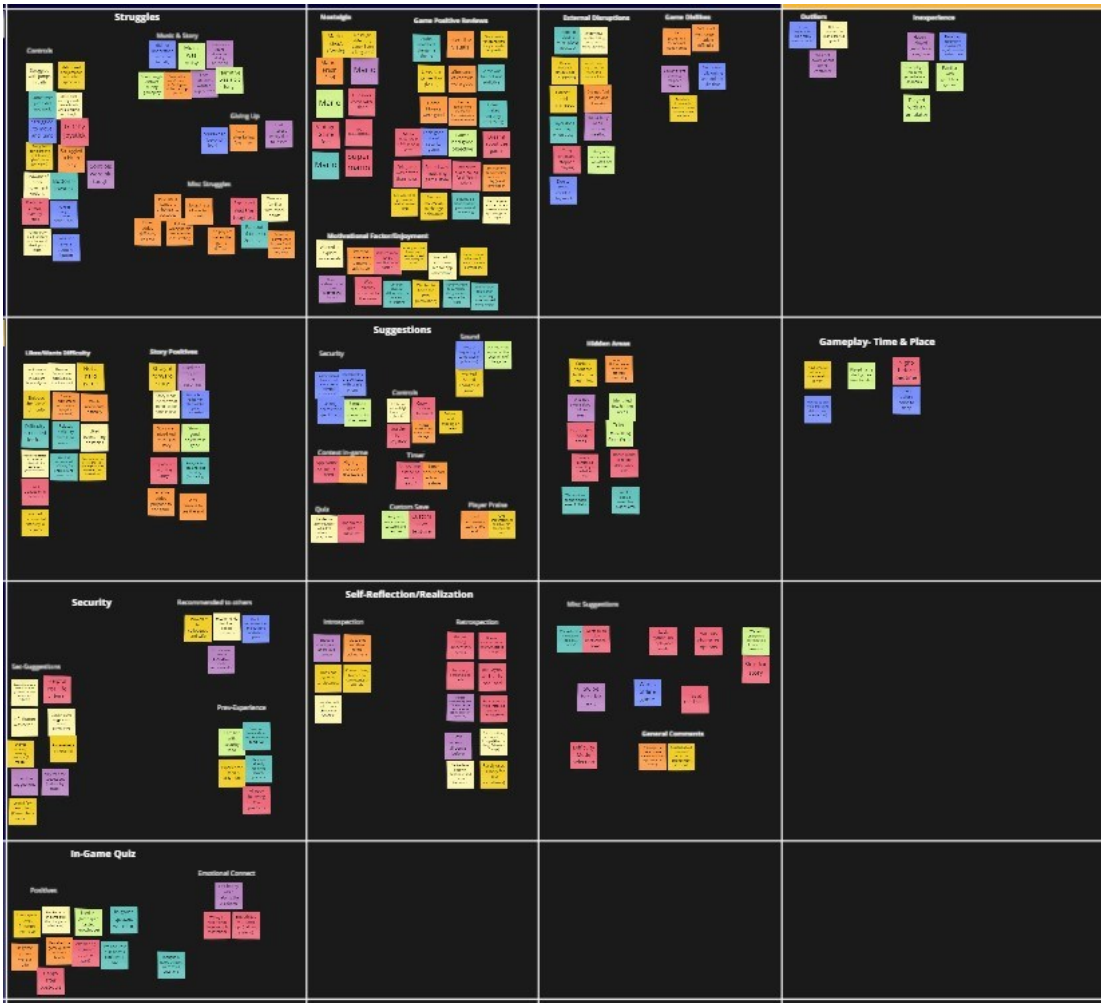


Figure 5.4: Affinity Diagram for Game Version2

For most of the players, difficulty was one of the ***motivational factors*** for this game. Player-8 related the difficulty to a popular game and stated "*…It's down to the difficulty of the game. I'd compare this to GTA Vice City's helicopter mission where you try, stop for a while, and try again later. At least some level of difficulty is needed in a game else what is the point. If it is difficult, you get a **sense of achievement***".

Despite the appreciation for the game's difficulty, it is imperative to keep in mind that persuasive games should not be too difficult to play but should also be interesting and challenging with the right balance to keep the players engaged [118] and expose them to the necessary persuasive contents.

Looking at the ***positive comments*** for the document:
Reader-5 mentions that *"It was very organized, and I knew what went with what… It's kind of like on your face and you can choose where you want to start…".*
Reader-3 states that *"...It was easy to follow...", "I liked the icons used here...the avoid, disable, do, do-not, I love them…".*

The foreshadowing level design pattern (hidden areas) ***increased players' curiosity***. Player-2 said, *"At the first time, I noticed a fruit, but I couldn't figure out how to reach there, and I kept trying".* These unusual visual cues create uncertainty that invokes perceptual curiosity and increases attention among players [143].

Players found ***in-game quizzes to be fun and informative***. When asked about their favourite game mechanic, Player-6 said while chuckling *"the questions… if you are wrong, it is going to give you more information after testing your knowledge. That's the good thing".* Humour is widely used not only in games but also in advertisements [139]. Previous research shows that humour can boost intrinsic motivation and learning [160].

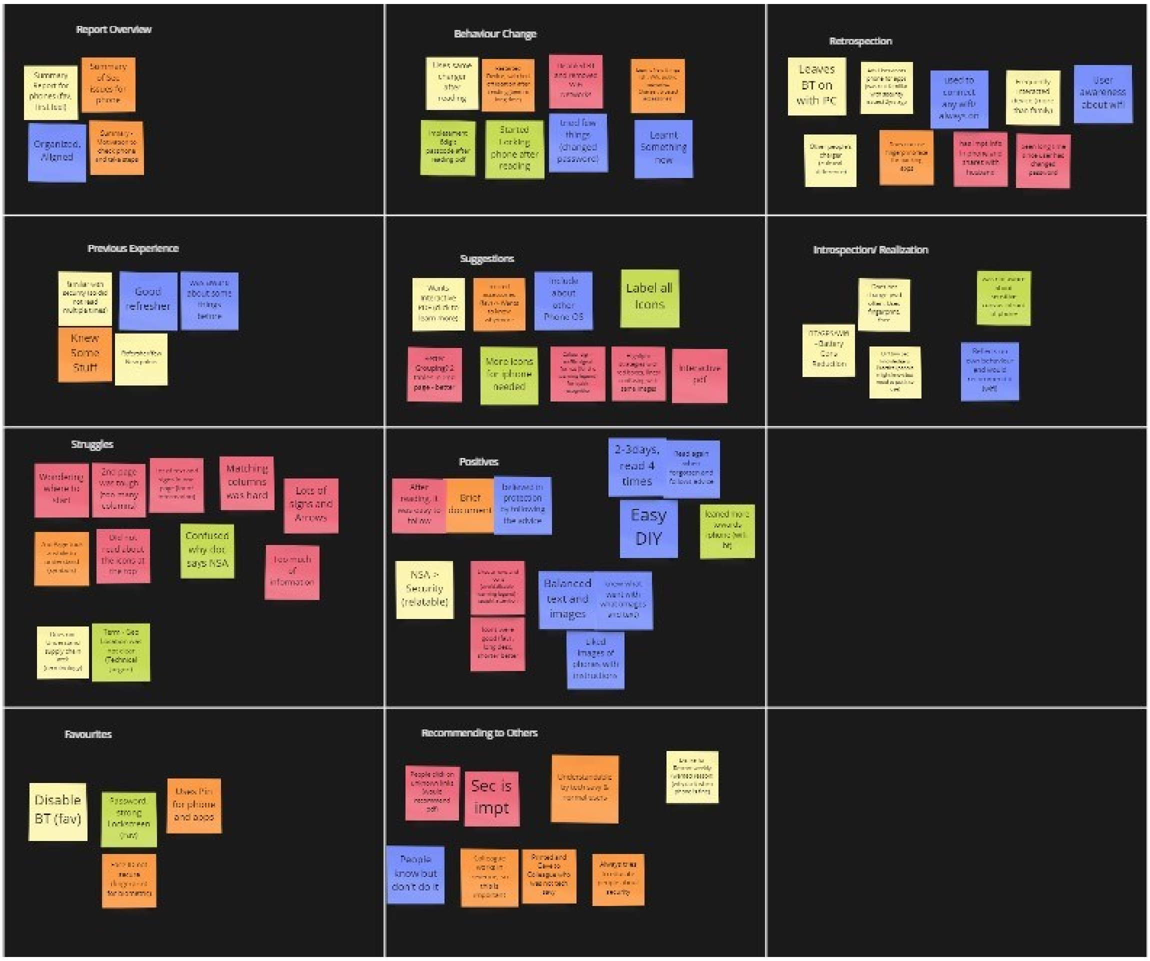
When the readers were asked about the changes they would make to the document, most of them wanted an ***interactive version of the document***. Reader-3 said, *"The icon descriptions can be hidden and shown while clicking on the icons. This might reduce the amount of information on the page".* All the readers learnt something new from the document, and some of them tried a few security measures while reading it or after reading it. For the game, the players suggested that they ***wanted more levels***.

For both the game and the educational document, the reason for behaviour change was either ***retrospection or realization of threat severity***. Reader-4 described their experience as *"… Since I am always with my phone, what is the use of using the passwords. But after this, I implemented the 6-digit lock screen password".*
Some of the players ***implemented in-game security suggestions*** after playing the game. Player-4 commented, *"… after playing the game, I have started the habit of seeing what I am downloading and its source".*

Player-1 shared their experience stating *"I have actively started to notice what permissions are required, and I deny or allow accordingly… earlier I did not pay much attention to it. I have also started turning off the Wifi when it is not needed"*.

Players thought about their actions before making in-game decisions. Player-4 said, *"… when I got the option, I had to think… instead of selecting everything, I stopped and thought about it. Before, I used to accept all… this was insightful"*.

Individuals who try to averse regret are more likely to make secure decisions to avoid negative consequences [147]. In Perma-Run: Version Two, players had a chance to think about their decision among other possible answers.



Report Overview
Summary of Sec issues for phone
Organized, Aligned
Behaviour Change
Started Locking phone after reading
Tried few things (changed password)
Learnt Something new
Retrospection
Leaves BT on with PC
Used to connect any wifi always on
User awareness about wifi
Previous Experience
Good refresher
Knew Some Stuff
Suggestions
Include about other Phone OS
Label all Icons
More Icons for iphone needed
Interactive pdf
Introspection/ Realization
Struggles
Wondering where to start
Matching columns was hard
Lots of signs and Arrows
Confused why doc says NSA
Too much of information
Positives
2-3days, read 4 times
Brief document
Easy DIY
NSA > Security (relatable)
Balanced text and images
Liked images of phones with instructions
Favourites
Disable BT (fav)
Password strong Lockscreen (fav)
Uses Pin for phone and apps
Recommending to Others
Sec is impt
People know but don't do it

Figure 5.5: Affinity Diagram for the Educational Document

5.2.2 Analysis of Game Logs

I also collected players in-game play data using game logs. Whenever the players lose a life in-game, the coordinates of that place and the particular level where they lose a life are logged in the background. Apart from this, when they answer a quiz question, the number of answer attempts is logged along with the amount of health left for the player. On average, the players had a gameplay time of ten minutes. With the coordinates data, I generated frequency maps to identify where the players lost lives often to tweak the game accordingly. In Figure 5.6, each red dot corresponds to an instance when a player lost life at that point (more images are included in Appendix E). This is helpful for game designers who want to balance the game's difficulty while keeping it challenging and interesting [195]. Some of the places in the game were intended to be difficult to keep the game interesting according to the level design patterns. Hence, not all the places in the game were tweaked after the frequency analysis of game logs. From Figure 5.7, we can infer that most users were able to figure out about third-party apps in the first attempt followed by a secure lock screen and other security issues.

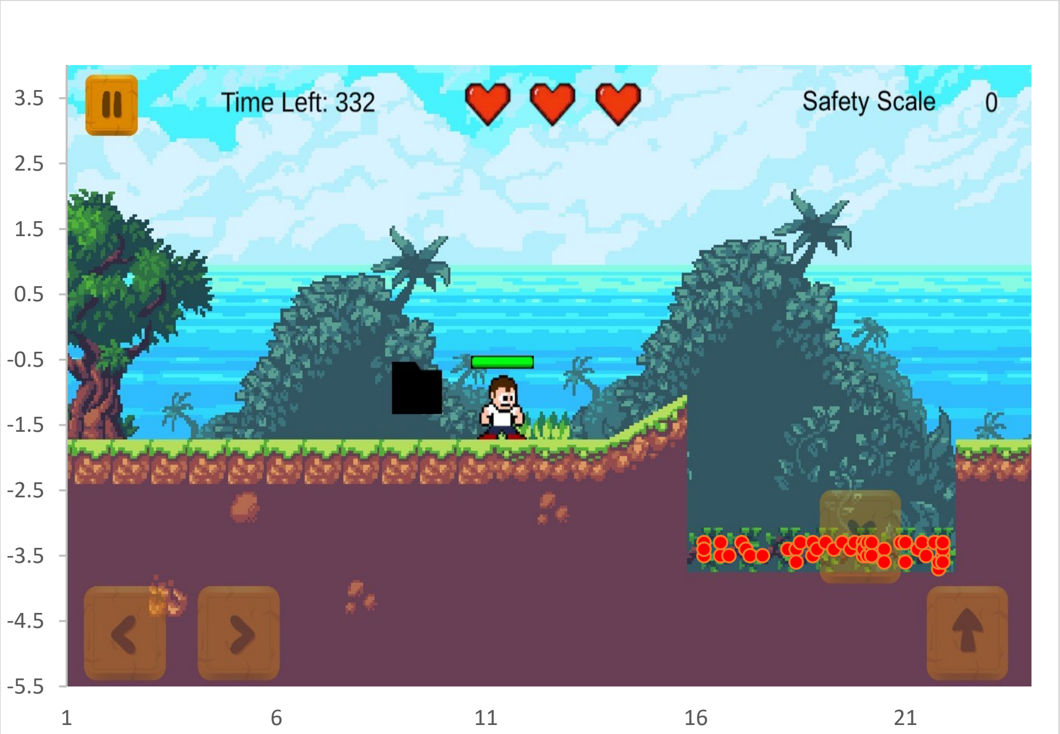


Figure 5.6: Frequency map of Player Losing Lives in-game

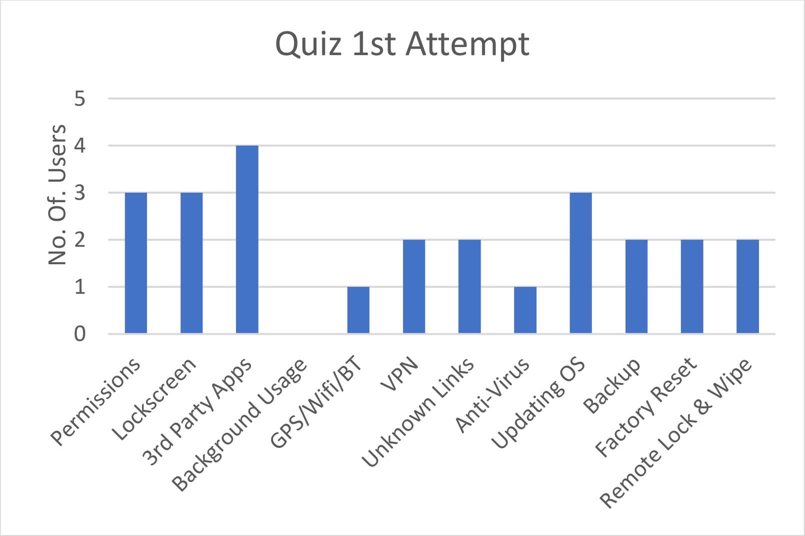


Figure 5.7: Frequency Analysis of in-game quiz answers

5.3 Results of Evaluation Study Two

After Evaluation Study One, I made some tweaks to the level designs according to the results of the frequency map of players losing lives in-game (Figure 5.6). Apart from this, according to the literature review, I tailored the game with Regulatory Focus Theory, thus resulting in two versions of the game namely, the promotion focus version and the prevention focus version. Regulatory Focus Theory states that people who are *promotion focused*, are sensitive to gains or achievements while trying to reach their goals. On the other hand, *prevention focused* people are sensitive to negative scenarios or losses while trying to achieve their goals [27,59]. In the game, the suggestions for the PRF version were tailored to reflect the positives or gains that the user would benefit from following secure smartphone behaviour. The suggestions for the PVF version were tailored to reflect the negatives or losses that the user would face if they do not follow secure smartphone behaviour. Apart from this, for the PVF version, the users lost health for collecting unnecessary permissions or for selecting wrong quiz answers. For the PRF version, the users gained some health for collecting the required permissions and for answering the in-game quiz correctly. These design changes are described in Chapter 3, Table 3.4.

5.4 Data Analysis of Evaluation Study Two Results

The research questions for Evaluation Study Three are as follows:

RQ4: Does Perma-Run motivate users to protect themselves from smartphone security threats?

RQ5: Does the tailored version of Perma-Run improve players' intention to protect themselves?

RQ6: How does Perma-Run perform with respect to the motivational appeal.

RQ7*:* How effective is Perma-Run with respect to promoting a positive user experience?

RQ8: How persuasive is Perma-Run with respect to motivating players to follow secure smartphone behaviour?

RQ9: How does the tailored version of Perma-Run affect the players' play experience?

RQ10: How does the tailored version of Perma-Run affect the players' motivational appeal?

R11: Do the tailored versions of Perma-Run have an effect on the game's perceived persuasiveness?

To answer ***RQ4:*** *Does Perma-Run motivate users to protect themselves from smartphone security threats?*, similar to Evaluation Study One, I leveraged the Protection Motivation Theory (PMT) scale validated by Verkijika et al. [147], to measure users' intention to protect themselves from smartphone security threats. The PMT scale was included both in the pre-study survey and post-study survey, and the user's intention was measured across eight constructs, namely, Self-Efficacy, Response Efficacy, Response Cost, Perceived Severity, Perceived Vulnerability, Anticipated Regret, Security Intention and Security Behaviour. Apart from PMT, I also utilized SSBS [64] and Permission Scenario scales in the pre-study survey and the post-study survey. The following assumptions for ANOVA and t-test were validated before proceeding with the data analysis:

1. The Dependent variables should be measured on a continuous scale.
2. For paired t-tests and RM-ANOVA, the independent variables should be matched pairs. For the one-sample t-test, the data should be independent/ not correlated.
3. No significant outliers should exist in the data.

4. The distribution of the data should be normal. The Shapiro Wilk test is used for this purpose.
5. For ANOVA’s, the independent variables should have two or more categorical independent groups. There needs to be homogeneity of variances which can be checked using Levene’s test. For RM-ANOVA, sphericity should be checked before the analysis, and if violated, the error should be corrected (E.g., greenhouse-geisser correction).

5.4.1 Overall Efficacy at Promoting Secure Smartphone Behaviour

To answer ***RQ4:*** *Does Perma-Run motivate users to protect themselves from smartphone security threats?* I analyzed the overall performance of the game for promoting secure smartphone behaviour by leveraging the paired sample t-test to determine if there was a significant difference between the pre-study survey and post-study survey scores of the PMT scale, SSBS scale and the Permission Scenario scale. For the PMT scale, the results of the paired t-test (Table 5.5), shows that there was a significant increase for *self-efficacy* (t(101) = -3.708, p<0.001)*, response efficacy* (t(101) = -2.472, p=0.015)*, security behaviour* (t(101) = -3.518, p<0.001) and a significant decrease for *response cost* (t(101) = 1.928, p = 0.040). These are positive results for the performance of the game. *Response cost* refers to the effort that needs to be taken by the user to perform a task. A low score on *response cost* shows that users do not feel much effort is needed to perform the task (taking preventive measures). This shows that overall, PermaRun: Version Three performed significantly well across some of the PMT constructs, while the results for other constructs were not significant. Overall, all the values were above the neutral value of 2.5 except for *response cost,* which is significantly less than the neutral point on a 5-point likert scale (Figure 5.8).

Table 5.5 – Paired sample t-test values for PMT constructs

PMT Construct	**Mean**	**SD**	**t_2**	**p**
Self-Efficacy	-0.33	0.92	-3.708	**<0.001**
Response Efficacy	-0.19	0.80	-2.472	**0.015**
Response Cost	0.16	0.88	1.928	**0.040**
Perceived Vulnerability	0.17	0.92	1.955	0.53
Perceived Severity	0.05	0.77	0.724	0.471

Anticipated Regret	-0.7	0.77	-1.130	0.261
Security Intention	0.02	0.77	-0.257	0.798
Security Behaviour	-0.40	1.15	-3.518	**<0.001**

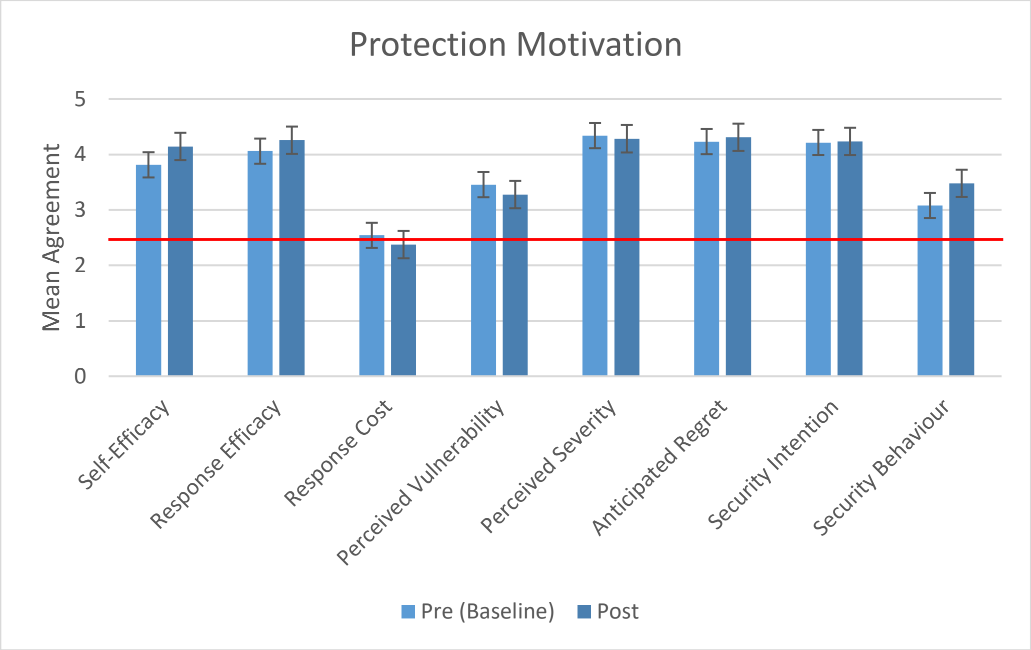


Figure 5.8: Mean values of PMT constructs for Pre-study survey and Post-study survey

The Smartphone Security Behaviour Scale (SSBS) measures security behaviour across two constructs, namely, *Technical* and *Social*. The paired t-test results (Table 5.6), show that there was a significant increase in the mean value of the *Technical* construct (t(101) = -5.692, p<0.001) but the same was not reflected for the *Social* construct (t(101) = -0.748, p=0.456). Both the *Technical* and *Social* constructs values are above the neutral value of 2.5 on a 5-point likert scale (Figure 5.9). The players' self-reported value of social construct is considerably above the neutral value despite the non-significant mean difference across the pre-study and post-study survey. This shows that overall, users were aware of the social aspects of smartphone security and might need training in the technical aspect of smartphone security. Perma-Run covers both the technical aspects and social aspects of smartphone security, and this explains the significant increase in the *Technical* construct scores from the pre-study survey to the post-study survey.

Table 5.6 - Paired sample t-test values for SSBS constructs

SSBS Constructs	**Mean**	**SD**	**t_2**	**p**
Technical Aspect	-0.43	0.76	-5.692	**<0.001**
Social Aspect	-0.57	0.77	-0.748	0.456

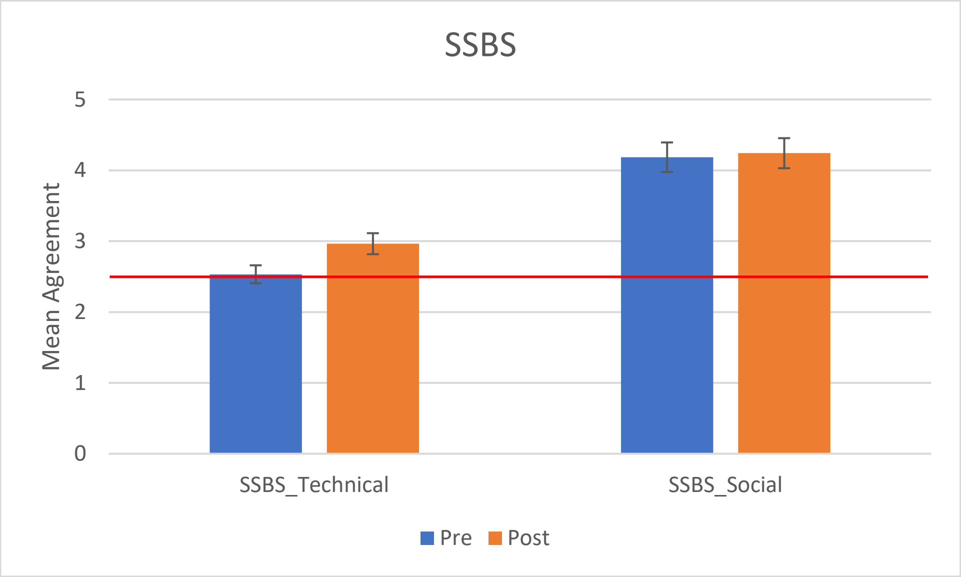


Figure 5.9: Mean values of SSBS constructs for Pre-study survey and Post-study survey

For the permission scenario, the users had to select the necessary permissions for a sample smartphone app (the app features were mentioned to the user) in the pre-study survey and the post-study survey. The result of the paired sample t-test results shows a statistically significant increase in the mean value from the pre-study survey to the post-study survey (t(101) = -2.03, p = 0.045) for the necessary permission (Table 5.7, Figure 5.10). But for the unnecessary permission, there was a decrease in means from the pre-study survey to the post-study survey, although it was not significant.

Table 5.7 - Paired sample t-test values for Permission Scenario constructs

Permission Scenario Constructs	**Mean**	**SD**	**t_2**	**p**
Necessary Permissions	-0.23	1.17	-2.03	0.045
Unnecessary Permissions	0.25	2.07	1.24	0.218

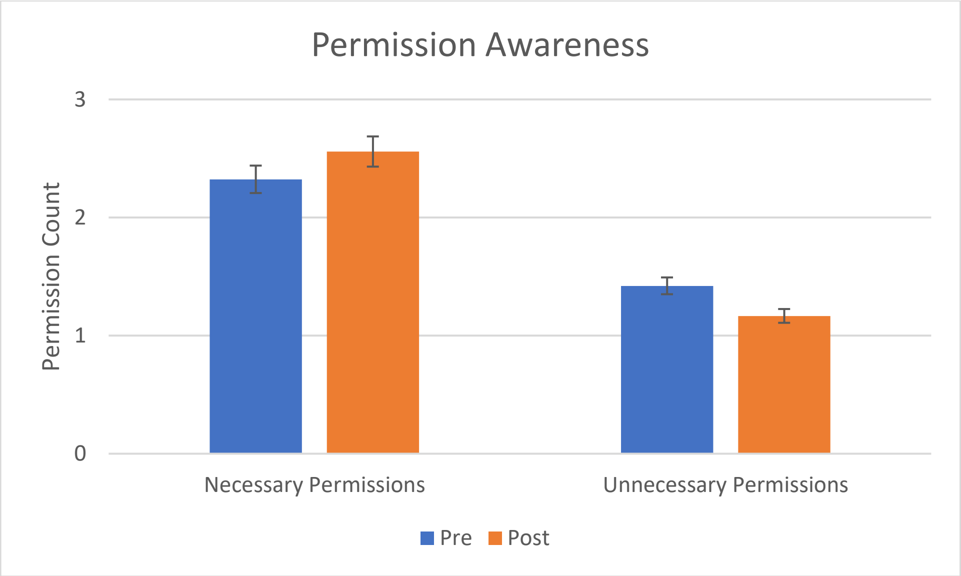


Figure 5.10: Mean values of Permission Scenario constructs for Pre-study survey and Post survey

5.4.2 Effects of Perma-Run across Player's Motivational Orientation, Game Versions and Time for Secure Smartphone Behaviour

Apart from the overall results, to answer ***RQ5***: *Does the tailored version of Perma-Run improve players' intention to protect themselves?* **-** I conducted a repeated measure analysis of variance (RM-ANOVA) with player's motivational orientation (Promotion focused, Prevention focused) and game version (Promotion version (PRF), Prevention Version (PVF)) as between-subjects factors and time (pre-post) as a within-subjects factor with PMT constructs, SSBS constructs and Permission Scenario constructs as the dependant variables. The PMT constructs are self-efficacy, response efficacy, response cost, perceived severity, perceived vulnerability, anticipated regret, security intention and security behaviour. The SSBS constructs are - Technical and Social constructs, and for the Permission Scenario – necessary and unnecessary permissions. The main effects and the interaction effects are discussed in the upcoming sections.

5.4.2.1 Main Effect of Time

The results of the RM-ANOVA show that there was a main effect of time across the constructs: self-efficacy ($F_{1,98}$ = 21.766, p<0.001, η^2 = 0.182), response efficacy ($F_{1,98}$ = 5.781, p = 0.018, η^2 = 0.056) and security behaviour ($F_{1,98}$ = 13.282, p<0.001, η^2 = 0.119) overall. The results show a significant difference between pre-test and post-test scores when a player's motivational orientation and the game version are considered without separating them into groups. From the pairwise comparison, it was evident that there was a significant increase across three constructs: players reported a significant increase in self-efficacy ($p<0.001$), response efficacy ($p = 0.018$) and improved security behaviour ($p<0.001$) after playing the game, compared to the pre-test. Apart from the PMT constructs, there was a main effect of time for SSBS *Technical* construct ($F_{1,98} = 30.932$, $p< 0.001$, $\eta^2 = 0.240$) and *necessary permissions* ($F_{1,98} = 3.992$, $p = 0.048$, $\eta^2 = 0.039$) and from the pairwise comparison, it was evident that there was a significant increase from pre-test to post-test for the SSBS *Technical construct* ($p<0.001$) and *necessary permissions* ($p=0.048$). This shows that after playing Perma-Run, players reported a significant increase in their technical knowledge of smartphone security behaviour along with a significant increase in selecting the necessary permissions in the post-study survey. Apart from this, there was an overall increase in scores of the *Social construct* and a decrease in *Unnecessary permissions* but the change from pre-study survey to the post-study survey was not significant.

5.4.2.2 Interaction between Time and Player's Motivational Orientation

The results of the RM-ANOVA show there was a significant interaction between time and player's motivational orientation for *unnecessary permissions* ($F_{1,98} = 5.642$, $p=0.019$, $\eta^2 = 0.054$) in the Permission Scenario. From the post hoc pairwise comparison, it was evident that over time (pre-test to post-test), there was a significant decrease in unnecessary permissions collected by players' who were promotion focussed ($p=0.013$), but the same was not the case for the prevention focussed players ($p=0.386$). This shows that over time, promotion focused players selected less number of *unnecessary permissions*. It means that the promotion focused players were more impacted by the Perma-Run to reduce their mistakes in collecting unnecessary permissions.

5.4.2.3 3-way Interaction between player's motivational orientation, game versions and time

The results of the 3-way interaction show the effect of tailoring Perma-Run based on players' motivational orientation types. The results of the RM-ANOVA show that there was a 3-way interaction between players' motivational orientation, game versions, and time for the PMT construct *Security Behaviour* ($F_{1,98} = 4.423$, p=0.038, $\eta^2 = 0.043$). From the post-hoc pairwise comparison, it was evident that *promotion focused* players who played the *Promotion Focus version* (tailored version) of the game (p = 0.011), and *prevention focused* players who played the tailored *PVF version* (tailored version) of the game (p=0.002) had a significant increase in *security behaviour* compared to the other two groups (promotion focus non-tailored and prevention focus non-tailored) that played the non-tailored version of the game (p=1.0 and p=0.145) respectively. This shows that the tailored version of the game was beneficial towards improving the player's security behaviour over time compared to the non-tailored version of the game. Table 5.8 outlines some of the participant's sample comments from the interview across the four groups that sheds more light on the results.

Table 5.8 – Sample comments that highlight the benefits of tailoring for security behaviour

Groups	**Sample Comments**
Promotion focus – tailored	*"I was not aware about the banking app and public wifi scenario…that and that was a good one"* – P13 *"For instance, the backup and public Wi-Fi scenario quizzes were direct real time examples that I was able to relate to… "* – P75
Prevention focus – tailored	*"…I liked the overall concept of combining multiple concepts like hiding Bluetooth to not downloading 3rd party apps. I like range of security concepts included in the game."* – P66
Promotion focus – non-tailored	*"I had to read through the choices and it made a big pause in the game … Considering the game play time, it was a bit long"* – P3
Prevention focus – non-tailored	*"…I also saw the recommendation of VPN, but when I was watching youtube videos, they push these things so much that they are being overhyped. Youtubers don't have computer science background but they say all kinds of things to promote products."*- P88

5.4.2.4 Effectiveness of Game Versions on Secure Smartphone Behaviour

To explore if the game versions had an effect on secure smartphone behaviour, I conducted an RM-ANOVA with the game versions as the between-subject factor, time as a within-subject factor, and PMT constructs, SSBS constructs, and Permission scenario constructs as the dependent variables. The results show that there was a main effect of time across both versions of the game for the PMT constructs - *self-efficacy* (F(1,100) = 21.811, p<0.001, $\eta^2 = 0.197$), *response efficacy* (F(1, 100) = 6.175, p = 0.015, $\eta^2 = 0.058$), and *security behaviour* (F(1, 100) = 12.427, p<0.001, $\eta^2 = 0.111$). But, there was no significant interaction between time and game versions for *self-efficacy* (F(1, 100) = 0.017, p = 0.898, $\eta^2 < 0.001$), *response efficacy* (F(1, 100) = 0.348, p = 0.557, $\eta^2 = 0.003$) and *security behaviour* (F(1,100) = 0.214, p = 0.573, $\eta^2 = 0.003$) respectively. This shows that, overall, Perma-Run was significantly effective for some of the PMT constructs irrespective of the game versions. For the other PMT constructs, there was a general increase from the pre-study survey to the post-study survey, but the change was not significant. Similarly, for SSBS, the results show there was a main effect of time across both versions of the game for the *Technical construct* (F(1, 100) = 31.873, p<0.001, $\eta^2 = 0.242$), but there was no significant interaction between time and game versions (F(1,100) = 0.380, p = 0.539, $\eta^2 = 0.004$). This shows that both the versions of Perma-Run were significantly effective in improving the SSBS *Technical construct*. For the *Social construct*, even though there was a general increase from the pre-study survey study to the post-study survey study, the change was not significant (F (1, 100) = 0.042, p = 0.838, $\eta^2<0.001$). Similar to the previous results, there was a main effect of time on the *necessary permissions* construct (F(1,100) = 3.996, p = 0.048, $\eta^2 = 0.038$), but there was no significant interaction between time and game versions (F(1,100) = 0.355, p = 0.553, $\eta^2 = 0.004$). Although there was a decrease in the *unnecessary permissions* construct from the pre-study survey to the post-study survey, the change was not significant (F(1,100) = 0.020, p = 0.888, $\eta^2<0.001$). This shows that, overall, both the game versions were equally effective in improving secure smartphone behaviour without considering users' motivational orientation.

5.4.2.5 Overall Motivational Appeal, Player Experience and Perceived Persuasiveness of Perma-Run

To answer ***RQ6*** (*How does Perma-Run perform overall with respect to the motivational appeal?)*, ***RQ7* (***How effective is Perma-Run with respect to promoting a positive user experience overall?)* ***RQ8*** (*How persuasive is Perma-Run with respect to motivating players to follow secure smartphone behaviour overall?)*, First, I measured the overall motivation appeal using the ARCS motivational appeal questionnaire, player experience (IMI), and perceived persuasiveness scales respectively. I used the one-sample t-test and compared the data against a neutral value of 3.5 for Perceived Persuasiveness and Player Experience (IMI), which were measured on a 7-point likert scale. For the Motivation Appeal (ARCS), the data was measured on a 5-point likert scale, and it was compared against a neutral value of 2.5. The results of the one-sample t-test show that players were highly motivated by the game towards adopting a secure smartphone behaviour (Table 5.9, Figure 5.11). The players also reported a positive play experience (Table 5.11, Figure 5.13) and were motivated to play the game (Table 5.10, Figure 5.12) irrespective of the game version or their motivational orientation. From the results, it was evident that overall, the game performed significantly well across nearly all the constructs.

Table 5.9 - One sample t-test values for Motivational Appeal (ARCS)

Motivational Dimensions	**Mean**	**SD**	**MD**	**t(101)**	**p**
Attention	3.89	0.89	0.89	10.169	<0.001
Relevance	3.99	0.77	0.99	13.024	<0.001
Confidence	4.02	0.80	1.02	12.937	<0.001
Satisfaction	3.81	0.87	0.81	9.374	<0.001

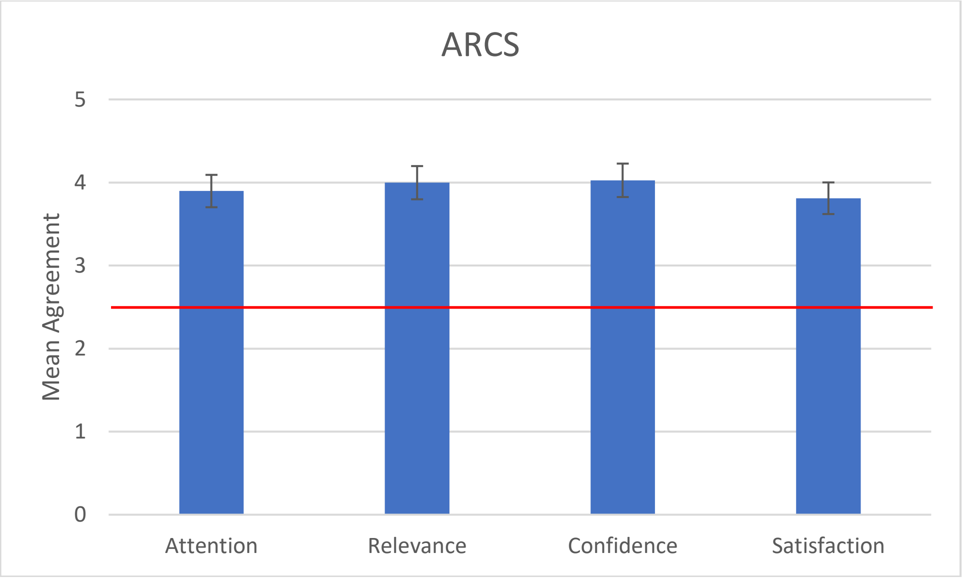


Figure 5.11: Mean values of ARCS

Table 5.10 - One sample t-test values for Perceived Persuasiveness

Persuasive Strategies	**Mean**	**SD**	**MD**	**t(101)**	**p**
Competition	4.88	1.42	0.88	6.218	<0.001
Liking	5.11	1.21	1.11	9.243	<0.001
Praise	5.31	1.21	1.31	10.947	<0.001
Real-World Feel	4.85	1.46	0.85	5.94	<0.001
Recognition	4.91	1.38	0.91	6.685	<0.001
Reduction	5.21	1.19	1.21	10.239	<0.001
Rewards	4.99	1.31	0.99	7.645	<0.001
Self-Monitoring	5.06	1.17	1.06	9.129	<0.001
Simulation	5.08	1.26	1.08	8.656	<0.001
Social Comparison	4.82	1.34	0.82	6.208	<0.001
Suggestion	5.17	1.23	1.17	9.621	<0.001
Surface-Credibility	5.05	1.20	1.05	8.829	<0.001
Trustworthiness	5.27	1.22	1.27	10.502	<0.001
Tunnelling	5.13	1.28	1.13	8.921	<0.001

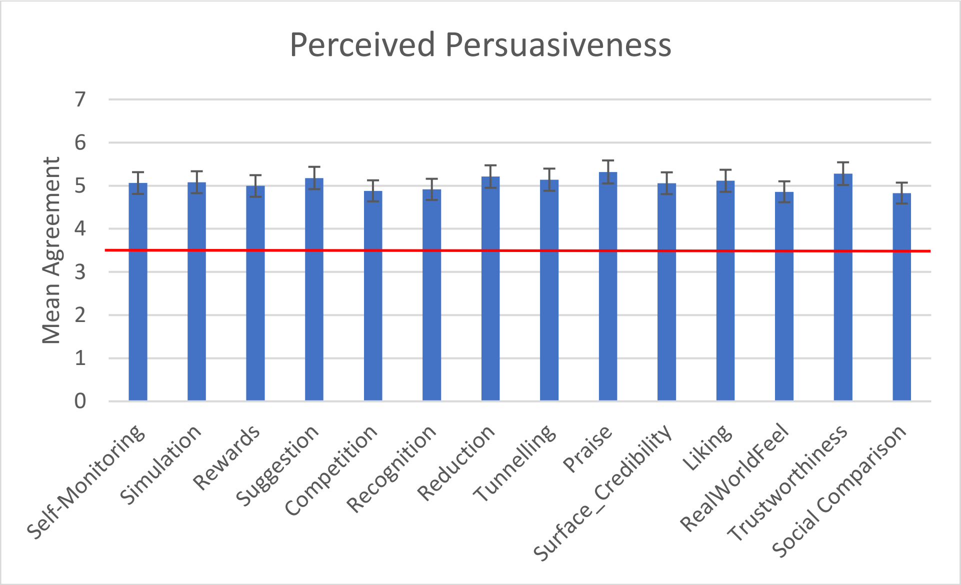


Figure 5.12: Mean values of Persuasive Strategies

Table 5.11 - One sample t-test values for Player Experience (IMI)

Player Experience Constructs	**Mean**	**SD**	**MD**	**t(101)**	**p**
Interest/Enjoyment	5.16	1.29	1.16	9.144	<0.001
Pressure/Tension	2.72	1.28	-1.27	-9.98	<0.001
Value/Usefulness	5.08	1.36	1.08	8.02	<0.001
Perceived Competence	4.52	1.35	0.52	3.95	<0.001
Perceived Choice	5.81	0.25	1.81	72.950	<0.001
Effort/Importance	4.06	1.05	0.06	0.655	0.514

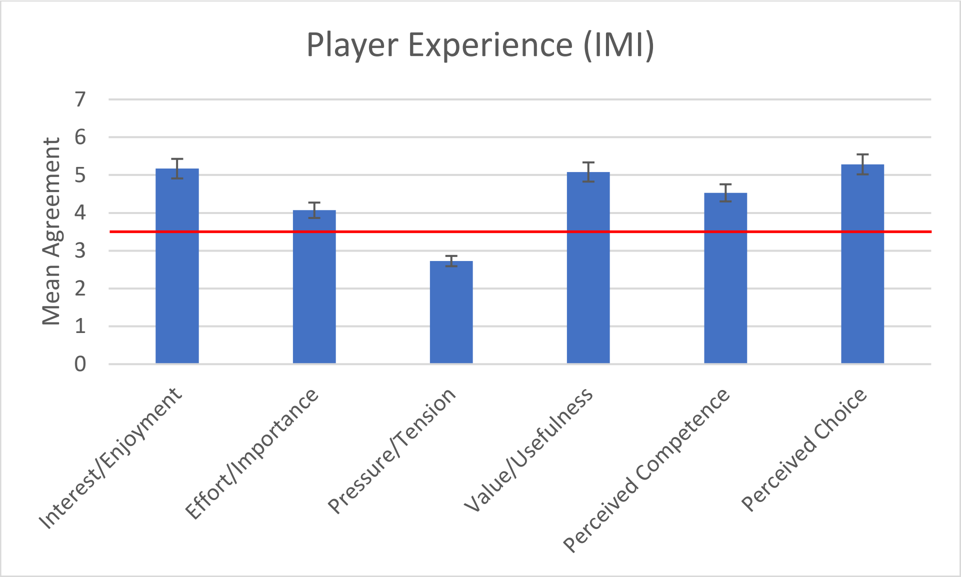


Figure 5.13: Mean values of IMI constructs

Following the one-sample t-test, I conducted an independent sample t-test to know if there were any differences across the two game versions for motivational appeal (ARCS), player experience (IMI), and perceived persuasiveness, across the two game versions. The results of independent sample t-test show that there was no significant differences in players' motivation appeal (t(100) = -0.123, p = 0.902), player experience (t(100) = 0.181, p = 0.857), and perceived persuasiveness (t(100) = 0.112, p=0.911) across the two game versions. This implies that players who played the Promotion focus version of the game rated it equally across the three constructs (ARCS, IMI, and Persuasiveness) compared to those who played the Prevention focus version of the game. These results imply that without considering the players' motivational orientation, both versions of the game are not significantly different in their effectiveness, they are considered equally effective at promoting secure smartphone behaviours.

5.4.2.6 Effects of Tailoring on Player Experience and Motivational Appeal

To compare the effectiveness of the tailored versus non-tailored version of the game with respect to players' motivational orientation, the players were randomly assigned into four sub-groups (promotion focus tailored, promotion focus non-tailored, prevention focus tailored, prevention focus non-tailored). To answer ***RQ9:*** *How does the tailored version of Perma-Run affect the players' play experience? and* ***RQ10****: How does the tailored version of Perma-Run affect the players' motivational appeal?* **-** I conducted a One-Way

ANOVA with these four sub-groups as between-subject factors and with Motivational Appeal and players' experience as the dependent measures. From the results of the One-Way ANOVA, it was evident that there was a significant difference between the group means ($F_{1,98} = 3.905$, $p=0.011$) for the *Perceived Choice* construct. From the post hoc pairwise comparison, it was evident that for the *Perceived Choice* construct of Player Experience (IMI), the tailored versions of the game performed better ($p = 0.019$, $p = 0.032$) than the non-tailored versions ($p>0.05$). For motivational appeal, there were no significant differences across the four groups, and this might be because of measuring the overall motivational appeal (ARCS) for the game. Some group-level differences might be uncovered if the motivational appeal is measured for each persuasive strategy.

5.4.2.7 Effects of Tailoring on Player's Perceived Persuasiveness

To answer ***RQ11*** *Do the tailored versions of Perma-Run have an effect on the game's perceived persuasiveness?* - I conducted a 2-way ANOVA with the game versions and players' motivational orientation as the between-subject factors and perceived persuasiveness as the dependent variable. From the results, it was evident that there was an interaction between the game versions and the players' motivational orientations for *competition* ($F(1,98) = 5.418$, $p = 0.022$, $\eta^2 = 0.052$), *recognition* ($F(1, 98) = 5.668$, $p = 0.019$, $\eta^2 = 0.055$), and *social comparison* ($F(1,98) = 4.878$, $p = 0.030$, $\eta^2 = 0.047$) strategies. Surprisingly, from the pairwise comparison, it was evident that the non-tailored groups ($p = 0.003$, $p = 0.005$, $p = 0.012$) performed better compared to the tailored groups ($p = 0.747$, $p = 0.575$, $p = 0.546$) respectively. This shows that players who played the non-tailored version of the game preferred *competition, recognition, and social comparison* strategies compared to the players who played the tailored version of the game. Recent research has shown that non-competitive groups tend to perform significantly better with game-based learning tasks, compared to the competitive groups which might lead to better engagement in-game [33]. These results also support the reason why the participants who played the tailored version reported a significant increase in their security behaviour compared to those who played the non-tailored version. This shows that implementing *competition, recognition, or social comparison* strategies in a one-fit-for-all manner might not always be the best for game-based learning. These results are discussed further in the upcoming Discussion Chapter. Table 5.12 outlines some of the sample comments of participants across the four groups from which it was evident that the players who played the non-tailored version preferred *competition, recognition,* and *social comparison* persuasive strategies. A key point to note here is that the persuasive strategies were the same across the two versions of the games, but the implementation of two of the strategies (*Simulation and Suggestions*) were tailored according to Regulatory Focus Theory. These results might be valuable for future work and are further discussed in the upcoming discussion section.

Table 5.12 – Sample comments that highlight non-tailored participant's motivation towards *competition, recognition, and Social-Comparison*

Groups	**Sample Comments**
Promotion focus – tailored	*"I couldn't finish some levels at first…I wanted to complete those levels and see how the game was constructed. The graphics was really good and I'm a picky person, so that was something that I liked about this game."* – P98
Prevention focus – tailored	*"People get much connected easily via internet and whatever it is about privacy and security, it gets my attention. When a game is trying to teach about security, that is what I was interested about"* – P43
Promotion focus – non-tailored	*"When I checked the score board, my name was not there and that actually bothered me. Then I played to climb on the scoreboard. I wanted to collect the badges only for the hidden places.,So I played the game again to collect the badges and to find the hidden places."* – P1
Prevention focus – non-tailored	*"I tried at first but couldn't make it to the leaderboard. But then I made it to the 3rd place the second time I played."* – P86

5.5 Thematic Analysis of Qualitative Data

I interviewed a total of 25 participants across the four intervention groups (*promotion focused tailored (N = 5), promotion focused non-tailored (N = 7), prevention focused* *tailored (N = 6), prevention focused non-tailored (N = 7)*) after the post-study survey to learn more about their gameplay experience and their opinions about smartphone security. The interview was optional and was audio recorded with the participant's consent. I transcribed the interview data and conducted a thematic analysis using an affinity diagram (Figure 5.14). Ten main themes emerged from the thematic analysis (Table 5.13) with a few other sub-themes. The ten main themes were – *Liking – Game Aesthetics and Nostalgia, Positive and Negative Aspects of Game Controls, Security and Privacy Factors, Motivation to Play, That's Enough For Today!, Finding Hidden Areas, In-game Quizzes, Minor Usability Issues, Nit Pick by Players, Ouch..that hurts! (Game Difficulty)*.

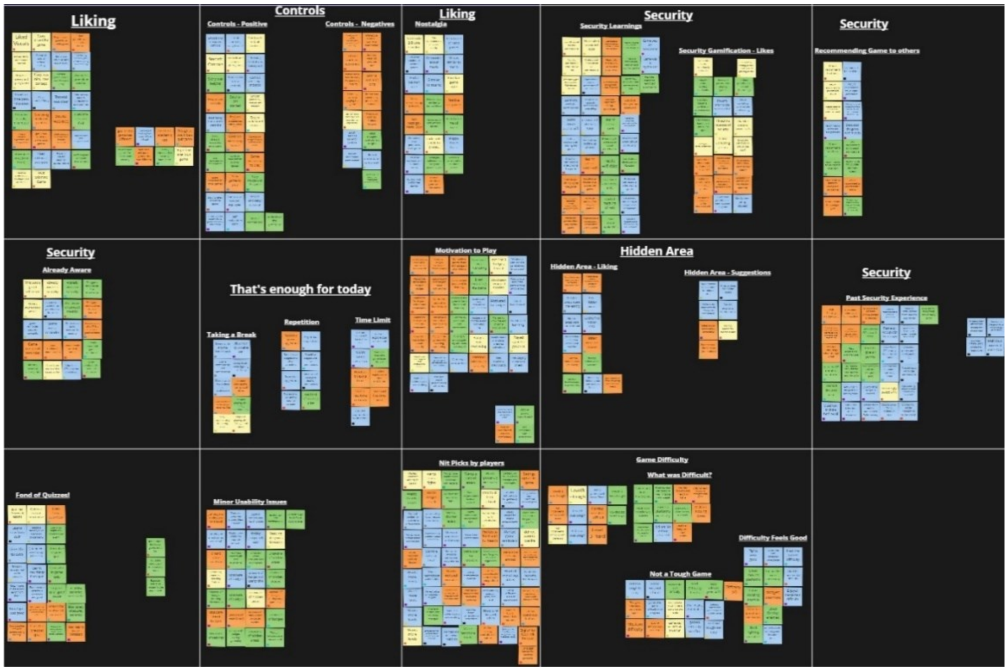


Figure 5.14: Affinity diagram for Evaluation Study Two Qualitative Data

Table 5.13 – Themes for Evaluation Study Two Thematic Analysis

Themes for Evaluation Study Two
Liking – Game Aesthetics and Nostalgia
Positive and Negative Aspects of Game Controls
Security and Privacy Factors
Motivation to Play
That's Enough for Today
Finding Hidden Areas

In-Game Quizzes
Minor Usability Issues
Nit Pick by Players
Ouch..that hurts! (Game Difficulty)

5.5.1 Liking – Game Aesthetics and Nostalgia

When asked about their first impression of the game, nearly all the players mentioned the game's aesthetics and how it reminded them of the games that they played during their childhood. This reinforces our design decision of building a retro-style 2-D game that is familiar to the users. A familiar game might reduce the learning for the players, and this would make it easy for them to concentrate on the game content rather than figuring out what to do in the game. As mentioned before, previous research has shown that nostalgia is directly impacted by past memories, and satisfaction of competence, especially with retro games that focus on challenging and fast gameplay [156]. Table 5.14 shows some of the sample comments from the participants.

Table 5.14 – Sample comments for the theme Liking (Nostalgia, aesthetics)

Sample Comments
"… I liked the way the story was laid out… the graphics were really good, and it was a smooth experience. There were no crashes in the game, and it was a pleasant experience going through the game. I am picky about what I play, and this game was up to the mark." – P98 *"When I started playing the game, it looked very familiar, like contra, which you might have played, and super mario."* – P74 *"When I opened the game, I liked the graphics and the aesthetics of it, and I remember appreciating the background music. I found it to be cool even before starting to play the game."* – P7 *"I liked the UI, it was similar to Mario and the controls were simple. It was very easy to use… the best part is you get to learn about security features also."* – P84

5.5.2 Positive and Negative Aspects of Game Controls

When players were asked about their opinions regarding the game controls and the tutorial, both positive and negative comments emerged as a prominent theme, with the number of positive comments being more than the negative comments. Designing and assigning game controls, and designing tutorials for a mobile game can be tricky. Hence, following the industry best practices might be helpful to keep the usability issues at bay, and the players would also be familiar with the commonly used controls. This was evident from the player's comments shown in Table 5.15. Perma-Run provides two movement control options for users namely, movement buttons and a draggable virtual joystick to move the player in the game. The buttons for attack, jump and pause were also included (Figure 5.15). The game tutorial is shown to the players before the start of the game. A key positive aspect of the controls includes the players being comfortable and familiar with the controls. Some of the negative feedback included blaming the users' device and the in-game character friction. This could be solved by introducing a practice level for the users to familiarize themselves with the controls.

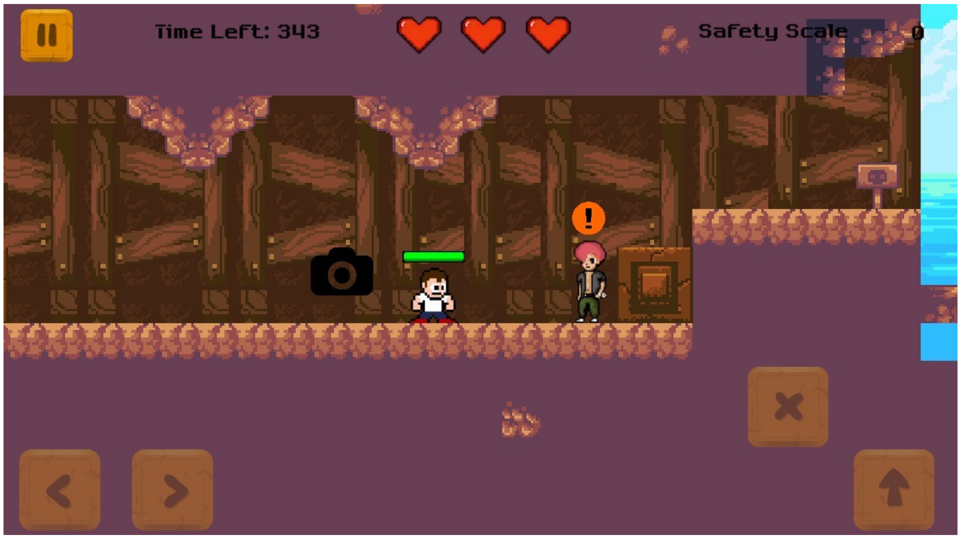


Figure 5.15: Perma-Run:Version3 Button Layout

Table 5.15 – Sample comments for the theme Controls (positives, negatives)

Sample Comments
Positives *"The controls are nice…I'm not a big fan of mobile gaming altogether and I could play it well…You can accurately jump or move just like using a keyboard...Everything was smooth."* – P15 *"I took a bit of time to get used to it with the controls being on the left and right. After a few days, I was able to navigate properly."* – P66 *"There was a bit of a learning curve for the controls but I was able to adapt to it quickly since I was familiar with these kinds of games."*- P69 *"The controls were fine… I tried both options and preferred the buttons because of the punch hole camera of my phone. I had to turn it around and play."*- P99 *"If I had to complain... then I'd say I had to mash the attack button for taking down enemies."* – P15
Negatives *"For my device, they were not up to the mark, because sometimes, I'd misplace the placement of my fingers on the left and right arrows. Even when I tried to jump, the character might slide off and fall"* – P59 *"It was slippery and difficult to make a precise jump. A lot of times, the permissions I mustn't be touching are there, but I couldn't avoid them. There were some instances where the character would slide off after landing… Sometimes I couldn't jump while running, and the character fell."*- P88

5.5.3 Security and Privacy Factors

When the participants were asked about smartphone security and how the game educates about smartphone security, five sub-themes emerged for security, namely, *learning about security & privacy, likes security & privacy, recommending to others, existing awareness about security & privacy, and users' past experiences*. Some of the players learnt new information and tried out a few of the suggestions that they learned from the game in the real world while some of them had experience with malware or were already aware of security and found this game to be a good reinforcement or a reminder. Past experience might motivate them to take precautionary measures prudently, and research has shown that individuals who try to averse regret are more likely to make secure decisions to avoid negative consequences [147]. Participants also mentioned that they would recommend this game to other people realizing the importance of smartphone security. Table 5.16 outlines some of the sample player comments.

Table 5.16 – Sample comments for the theme Security

Sample Comments
"I am a computer science student, and I am aware of what to do. The risks I take are intentional and not using a VPN is more of a technical decision than security…I'd say this game helped in reinforcing what I already know." – P15 *"…I liked the overall concept of combining multiple concepts like hiding Bluetooth to not downloading* 3^{rd} *party apps. I like a range of security concepts included in the game."* – P66
"Personally, I am a bit techy, but the thing I learnt new is being cautious of my Bluetooth…I don't pay much attention to it… that game scenario made me aware of Bluetooth" – P46 *"I was not aware of the banking app and public wifi scenario…that and that was a good one"* – P13 *"I'd recommend this to my parents because when I look at their phone, it's full of bloatware and lots of unnecessary apps on their home screen. I think they might be a perfect audience for this game"*– P7

5.5.4 Motivation to Play

When players were asked about their likes and dislikes about the game, the reasons that motivated them to play emerged from this qualitative data. From the data, the reasons for players who played the non-tailored version support the quantitative results of the perceived persuasiveness interaction between the game versions and the player's motivational orientation type. The players who played the non-tailored version of the game liked the rewards and the competitiveness of the game. On the contrary, people who played the tailored version of the game played it for exploring the game and its aesthetics in general. Some of the sample comments for this theme are shown in Table 5.16.

Table 5.16 – Sample comments for the theme Motivation to Play

Sample Comments
Tailored Version *"I couldn't finish those levels at first…I wanted to complete those levels and see how the game was constructed… the graphics were really good, and I'm a picky person, so that was something that I liked about this."* – P98 *"Security in general… people get much more connected easily via the internet…whatever it is about privacy and security, it gets my attention. When a game is trying to teach about security, that is what I am interested in"* – P43
Non-Tailored Version *"…the scoreboard, which was there in the game, when I checked the scoreboard, my name was not there, and that bothered me. then I played to be there…I wanted to collect the badges only for the hidden places, I played the game again to collect the badges and to find the hidden places."* – P1 *"The leaderboard stats, who scored the highest, I tried at first but couldn't make it but made it to the 3rd place the second time I played."* – P86

5.5.5 That's enough for today!

Players also commented about what made them stop playing the game at first before picking it up later again. These were related to continuously losing in-game, repetitive suggestions and the game's time limit. A player quitting a persuasive game after some time might not be a bad thing as long as they can learn and apply what they learned in their behaviour in the real world instead of playing it for the gamified content alone. This way, the game might be balanced in a good way. The sample comments for this theme are outlined in Table 5.17.

Table 5.17 – Sample comments for the theme That's enough for today!

Sample Comments
"Failing after a couple of tries, and maybe reaching towards the end and dying and replaying again, that stopped me from playing…then I take a break and come back to it later" – P15 *"I have been busy with my work lately, so I couldn't play, and I try to play when I am free"* – P98 *"…those jumps, I had to jump, but there were also spikes. I lost my lives again and again because I was impatient."* – P44 *"I had to read through the choices, and it made a big pause in the game … Considering the gameplay time, it was a bit long"* – P3 *"I stopped playing when I felt I was not making much progress."* – P87 *"I was not able to complete level 3 because of frustration, and the war with Ukraine distracted me completely. I saw the game reminder, but with the war, it was off my mind"* – P88

5.5.6 Finding Hidden Areas

All the players who uncovered hidden areas liked finding them and some of the players had their own suggestions. Hidden areas can be classified under the *foreshadowing* 2D level design pattern [70]. As mentioned before, these visual cues create a sense of uncertainty called perpetual curiosity [143] that leads to increased attention to the game. This design pattern has been used across various popular games for a long time. The sample comments for this theme are outlined in Table 5.18.

Table 5.18 – Sample comments for the Hidden Area theme

Sample Comments
"As I was playing, I saw something like a diamond hidden behind another object. You really had to pay attention to note these things. The badges also made me aware that there were hidden areas." – P13 *"There were some hidden areas which I found interesting. Sometimes I find a way to reach them but most of the time, I can see an area above me but I didn't know how to reach it"* – P28 *"In level 2, it goes to the underground, and I got lost, something like a sign board would be helpful. That was a hidden area…"* – P37 *"I liked the small things in this game… hidden areas and stuff...it would have been nice if it was a secret level like mario…"* – P35 *"I saw a place first and I wanted to go there, when I tried to access it, it popped me to another place …"* – P59 *"I discovered 2 to 3 hidden areas and for one of them, I did not even realize that was a hidden area when I took a different route… It was a fun aspect in the game"* -P87

5.5.7 In-Game Quizzes

Nearly all the participants who were interviewed liked the in-game quizzes and thought that they were good for breaking the flow of the game. These in-game quizzes covered other smartphone security scenarios/issues, and appropriate feedback was given to the players for each option. The in-game quizzes were shown to the players when they encounter an NPC who needs help with their smartphone issue. The sample comments for this theme are outlined in Table 5.19.

Table 5.19 – Sample comments for the theme In-Game Quizzes

Sample Comments
"The questions that popped up scenarios (explains about the public Wi-Fi scenario)… those scenarios were good in the game…I am a beginner to security and learning how the security decisions influenced was quite good" – P62 *"The quizzes directly relate to real-world scenarios…(explains backup scenarios and public Wi-Fi scenario)… those real-time examples were nice. I also liked the badges."*- P57 *"I love the quizzes, honestly, it's the part I love about the game. After playing the game you kind of have this pause that helps you…this was a contrasting activity that intriguing for me"* – P46 *"…they added a different level of depth to the game. Having this switch from the game engaged me differently."*- P7 *"The game characters ask me simple security questions and this way the game lets me know how to behave in certain situations. These questions sort of covered real-life scenarios and teaches us how to react to these situations."* – P15 *"I liked the quizzes, and I was learning about privacy …It doesn't dump everything on me at the same time, and that was very nice"* – P36 *"The frog and other small characters ask for help… those were cool…whether it is to take regular backup or using VPN, the quizzes were very informative"* – P99

5.5.8 Minor Usability Issues

When players were asked about their dislikes for the game, and what changes they would make to the game, some minor usability issues surfaced. Things like players' inability to go back using the back button on a specific screen of the game and being unaware of badges and hidden areas were some of the issues faced by some of the players. The sample comments are outlined in Table 5.20.

Table 5.20 – Sample Comments for the theme Minor Usability Issue

Sample Comments
"No, I was not aware of hidden areas in the game" – P98 *"If I had to complain... then I'd say I had to mash the attack button for taking down enemies."* – P15 *"Once I click on play, I was not able to go back to the main menu from the permission legends screen. There was no back button or quit. I discovered this when I clicked on Level2 by mistake."* – P74 *"I learned about badges much later in the game. It would've been better if I had known earlier"* – P7 *"I was not aware of the badges. As soon as I meet the requirements, there should be an announcement on the screen. I had to check the leaderboard instead."* – P88

5.5.9 Nit Picks by Players

For any game, players will have their own suggestions, and they might be picky about certain features. This theme is a combination of participants' comments that were either feature requests or suggestions for the game. Among these suggestions, one of the most requested things was the need for more levels. Table 5.21 outlines the participant's comments on this theme.

Table 5.21 – Sample comments for the theme Nit Picks by Players

Sample Comments
"Dark souls…it's tough to play, but you can still take down enemies without taking damage. There's a blocking and dodging mechanism. Generally, games have stealth kill option, and if you could have things like this, that would be fine." – P15 *"I might add more levels to play more. Although three levels might be ideal, I would like to add more levels to keep playing."* – P57 *"Even the background could have been shifted to day or night for each level. This would have made the game more interesting"* – P37

"I would have preferred a voice-over for the game story and for performing actions. Something like try and navigate or something like that." – P46
"Maybe reduce the number of monsters, that's one change that I'd make" – P44
"If I can adjust the control panel inside the game, that'd be great" – P59
"Maybe a super beginner level that doesn't have any obstacles and if you can offer a level Zero where it would be easy to practice and get through..." – P36

5.5.10 Ouch.. That hurts! (Game Difficulty)

The game's difficulty was mentioned at various moments during the interview. Users' perceived difficulty might be helpful for a designer to balance the game or confirm their game design. From the participant's feedback, two major themes for difficulty emerged - *what was difficult?* And *Difficulty feels good*. It was evident that the players felt that level 3 was harder than the other two levels, and most of them enjoyed various aspects of the game's difficulty. Table 5.22 outlines the sample comments of the participants for this theme.

Table 5.22 – Sample comments for the Game Difficulty Theme

Sample Comments
"I liked the game's difficulty. I think the levels had incremental difficulty and I improved playing as I progressed in the game." – P98
"…There were those flying bricks that you had to jump on… that was a scary part for me… there were spikes or skulls on the floor and when you walk on them, you die… I had to start from the last checkpoint" – P66
"If I have to rate it on a scale of 5, I will rate it 3… 5 being very difficult and 1 being easy." – P87
"It is challenging yet the right amount of difficulty. The first 2 levels were fine, the third level was a bit difficult, but I did enjoy it." – P69

Chapter 6 - Discussion

In recent times, video games have been used for various purposes across various research domains. Persuasive games are designed to motivate the players towards a positive behaviour change. For a naïve person, designing a game might sound like an easy and enjoyable task, irrespective of the purpose of the game. Designing a game takes thought and time, a series of informed decisions before the final version. While designing a persuasive game, one needs to consider the research domain and purpose of the persuasive game. There are a variety of design frameworks to guide designers toward success, and each step in the design process is informed by research. Following the research results, appropriate changes were made to the design before moving to the next version. The target audiences are also involved at some point in the iterative process to test the design, and changes are made to the game accordingly. Even though persuasive games motivate players overall, past research has shown some mixed results where games motivate only certain people, and some people might not feel motivated. For example, a competitive game might attract only certain groups of users, while some players might rather prefer to explore an open world.

In the recent past, tailored persuasive games have been successful in bringing about a positive behaviour change in players. Various theories are used for tailoring digital applications for the population. While tailoring a persuasive game or any persuasive digital application, the underlying theory chosen for tailoring the application should be chosen according to the domain. For example, according to the transtheoretical model [87,88,116], a person might be at their early stage of behaviour change or later stage of behaviour change. Another example is the BrainHex player satisfaction model [92,106], which outlines seven types of player's playstyle, namely, seeker, survivor, daredevil, mastermind, conqueror, socializer and achiever. Another example is the Self-Determination Theory, which is a popular macro theory that is often used to study the effects of video games. The macro theory states that *autonomy, competence* and *relatedness* lead to an improvement in intrinsic motivation and is often used to study motivation and personality and to break down the games and learn about the various motivational aspects of a game [56,127]. Choosing a behaviour theory for tailoring is an important step in the process of tailoring digital applications, and past works often serve as a helpful guide for this process.

For Perma-Run, I chose to tailor the game according to the Regulatory Focus Theory [27,59], which is a goal pursuit theory that emphasizes the motivational orientation of the users and how they pursue their goals. The theory states that people try to reach their goals according to their predominant motivational orientation, which could be either *Promotion Focus* or *Prevention Focus*. Over a period of one's lifetime, people are either predominantly promotion focused or prevention focused, and hence adapt to one of the focuses while trying to reach a goal [27,59]. When a person tries to reach a goal because of the advancement or accomplishment that they might get out of performing the task, they are considered to be *promotion focused*. *Promotion focused* people might often take an eager means (proactively trying to achieve positive outcomes) to achieve their goal whereas, a *Prevention focused* individual might take a vigilant means (proactively trying to avoid negative outcomes) to achieve their goal.

6.1 User's Intention to Protect Themselves from Smartphone Threats

I measured the players' intention to protect themselves from smartphone security threats, both in the pre-study survey and the post-study survey. This was measured using the Protection Motivation Theory (PMT) scale [147], Smartphone Security Behaviour Scale [64] and a Permission Scenario where the users must select the required permissions for an app. Overall, there was a significant improvement and a significant Main effect of time on some of the constructs. Starting with PMT, Figure 6.1 shows the overall means against the median value of 2.5.

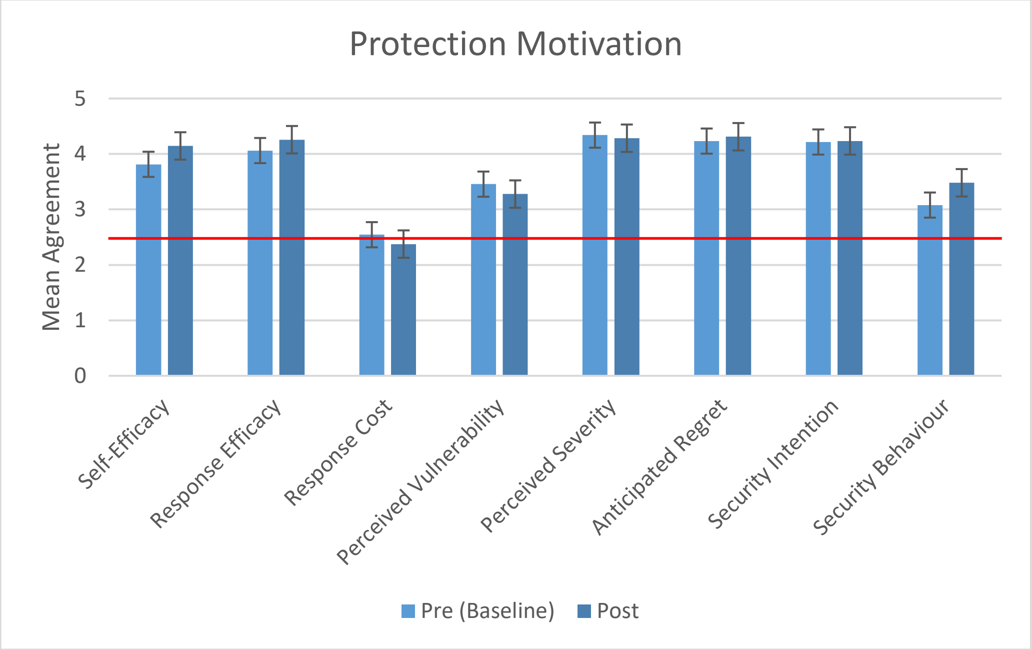


Figure 6.1: Overall Means of PMT Constructs for Pre-study Survey and Post-study Survey

There was a significant main effect of time on *self-efficacy* ($F_{1,98}$ = 21.766, p<0.001, η^2 = 0.182), *response efficacy* ($F_{1,98}$ = 5.781, p = 0.018, η^2 = 0.056) and *security behaviour* ($F_{1,98}$ = 13.282, p<0.001, η^2 = 0.119). From the above figure, it is evident that nearly all the constructs are on or above the median value of 3 except *response cost*. *Response cost* refers to the amount of effort needed to perform a task, and a low value signifies that it is relatively easy to perform that task. The results show that there was a significant reduction in *Response Cost* (*t* = 1.928, p = 0.040) after playing the game. For the constructs that did not have a significant change over time, it should be noted that nearly all the constructs are well above the median value in the pre-study survey. This shows that the users might already have the intention of protecting themselves from smartphone security threats, but the low score on security behaviour shows that users might not be following secure smartphone behaviour. The gap between intention and behaviour may probably be due to the lack of knowledge on how to protect themselves from security threats. Although intentions to adopt a behaviour are postulated as a good predictor of behaviour, this is always not the case in the real world. It depends on whether the behaviour is a single action or a multi-action behaviour [147] and a user's intention might be to only achieve the end goal (securing their smartphone). They might or might not be aware of the necessary steps to adopt the specific behaviour. Hence, it is necessary to measure the users' security behaviour (which might be a single action or multi-action behaviour) in a study to gauge the user's self-reported actions [147]. From the results, it was evident that *security behaviour,* which was a little higher than the median value, significantly increased after playing the game along with *self-efficacy* and *response efficacy*.

The benefits of tailoring were evident for *security behaviour* from a 3-way interaction between time, game versions and user's motivational orientation. From the results, it was evident that players who played the game tailored according to their motivational orientation had a significant improvement in security behaviour over time compared to those who played the non-tailored version of the game. These results are similar to previous studies (both in the domain of games for change and health interventions) that employed Regulatory Focus Theory and found that tailoring the intervention according to users' motivational orientation persuaded them toward their goals [43,58,75,76]. This is also supported by sample feedback comments from the players:

"I was not aware of the banking app and public wifi scenario… and that was a good one" – P13.
"The questions that popped up scenarios (explains about the public Wi-Fi scenario)… those scenarios were good in the game…I am a beginner to security and learning how the security decisions influenced was quite good" – P62

The results of Evaluation Study Two show that tailoring the game according to the player's motivational orientation was indeed beneficial for improving the users' security behaviour. It was also evident that users who played the counter-tailored version were motivated by competition, rewards, and social comparison persuasive strategies. There are only a handful number of games that leverage Regulatory Focus Theory [43,58,62,76], and this work is a step toward adding valuable results to the literature.

6.2 Player Experience and the Effects of Tailoring

The results show that the overall player experience, measured by the Intrinsic Motivation Inventory (IMI) scale [126], was above the median value of 3.5 (Figure 6.2) except for Pressure/Tension. This is a positive aspect of player experience because the players rated that they were not tensed, nor did they feel pressured while playing the game. Ideally, games should pose some level of challenge to sustain players' interest; if it is too easy, players may quickly get bored with the game in the long run. However, if persuasive games are too challenging, players may drop off before they are exposed to all the persuasive content that would lead to behaviour change. For persuasive games to be effective at impacting the desired changes, players need to be able to play and finish them. This was also evident from the player's feedback – "*…It's down to the difficulty of the game. I'd compare this to GTA Vice City's helicopter mission where you try, stop for a while and try again later. At least some level of difficulty is needed in a game else what is the point. If it is difficult, you get a **sense of achievement***" (Evaluation Study One, Player-8). *"It is challenging yet the right amount of difficulty, first two levels were fine, but the third level was a bit difficult, but I did enjoy it."* (Evaluation Study Two, P69).

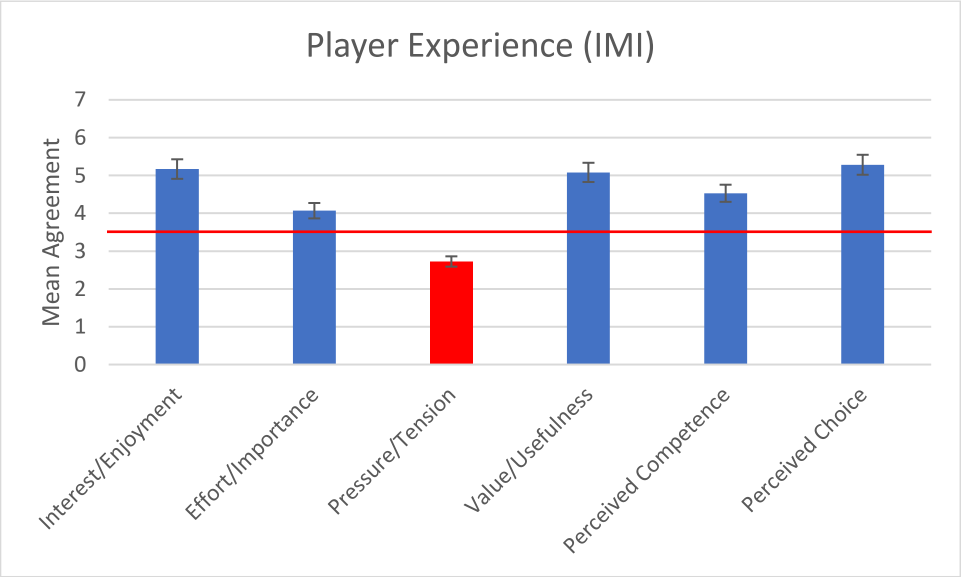


Figure 6.2: Mean Levels of IMI constructs

All other values of other constructs were on or above the median value of 3.5 on a 7-point likert scale. A high score on *Interest/Enjoyment* shows that players enjoyed the game. This is one of the basic requirements for any game. A persuasive game should be enjoyable to the players so that they would continue playing the game in the long run, and this is an important factor for a positive behaviour change. The results of *Perceived Competence* also support the factor that the players enjoyed the game and felt competent at playing the game. This also shows that the design decision of designing a retro game paid off [156].

The high score of *Value/Usefulness* shows that the players valued the game, and the *Importance* score shows that the players considered it important with respect to smartphone security issues. This shows that overall, the players consider the importance of playing the game for improving their smartphone security behaviour. *Perceived Choice* scored the highest among all, which shows that the players chose to play the game out of their own interest and felt they had a choice to play the game. All these factors show that the players played the game out of their own interest, and they enjoyed it while feeling competent at playing the game and considered the importance of playing the game for learning about smartphone security and privacy. This also means that players might play the game repeatedly, which was also evident from the game logs.

From the results, it was also evident that tailoring the game increases the *Perceived Choice* of players. Players preferred the tailored version over the non-tailored version of the game. This result was seen only for *Perceived Choice* and not other constructs. This might be because, overall, players enjoyed the game in the same manner and found it to be useful and important, irrespective of the game versions. This shows that tailoring the game impacted the players' preferences even though players enjoyed both game versions. Existing research shows that players tend to put more effort into their preferred games [101] compared to the games that do not appeal to them. This might increase the number of times the player plays the game, which might lead to better in-game performance for problem-solving and improve the player's understanding of the game [33]. Given the number of games in the market and the plethora of choices available for players, players might be used to playing games of different genres, and everyone might have their own nitpicks with each game. Tailoring games with a behaviour theory allows the designers to adjust the game design according to the various user types, which might lead to a considerable increase in the perceived choice of players and their overall player experience.

6.3 Perceived Persuasiveness and the Effects of Tailoring

Measuring the perceived persuasiveness of a persuasive game is imperative. For measuring perceived persuasiveness, I adapted the widely used perceived persuasiveness scale [42,141]. The results show that all the persuasive strategies scored well above the median value of 3.5 (Figure 6.3) on a 7-point likert scale. This shows that overall, players perceived the game as persuasive irrespective of the game versions. Persuasive strategies in a persuasive game motivate players to continue playing the game, and the game motivates the user towards a positive behaviour change.

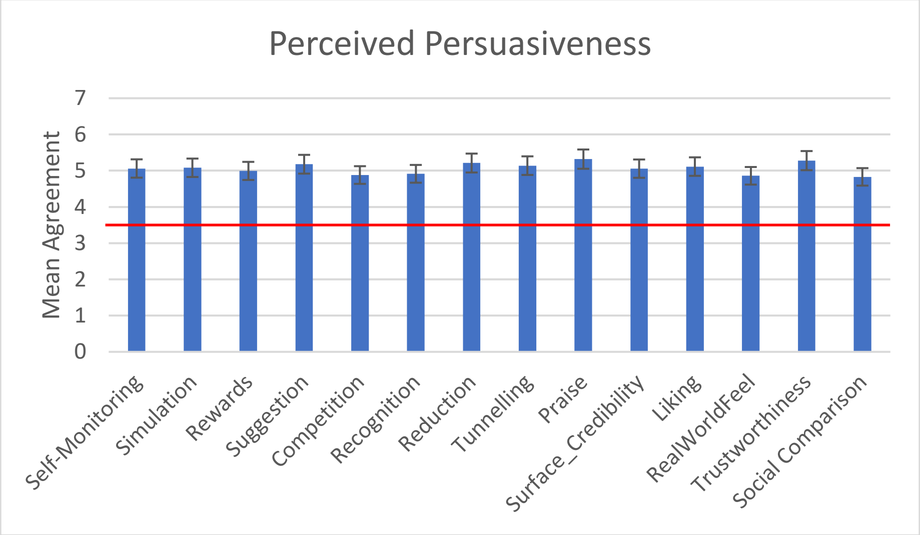


Figure 6.3: Overall means of Persuasive Strategies

Surprisingly, players preferred the non-tailored version of the game for *competition*, *recognition*, and *social comparison* persuasive strategies and the persuasive strategies were the same across both versions. This shows that people who played the non-tailored version, preferred competition, unlike those who played the tailored version. Recent research shows that non-competitive groups might tend to perform significantly better with game-based learning tasks compared to the competitive groups, which might only lead to better engagement in-game [33]. This also explains the significant interaction of the Security Behaviour result, which shows that the tailored groups had a significant increase in Security Behaviour compared to the non-tailored groups. Recent research shows that grouping users according to their performance or personality might improve the individual's performance and the group's performance in a collaborative gamified setting [30,31,101,117]. Hence, designers need to think accordingly before including *Competition*, *Rewards* or *Social Comparison* strategies. From the results of persuasive strategies for Evaluation Study Two, it is clear that tailoring the game according to the users' motivational orientation (using Regulatory Focus Theory) is beneficial for imparting knowledge to the players.

6.4 Implications for Persuasive Game Designers

In this section, I discuss some of the implications of the evaluation studies conducted as part of this research work.

Some of the key implications of the evaluation studies are as follows:

1. Designing a retro-themed game puts the players at ease, and this reduces the overhead required to learn about a new gameplay style. In our evaluation studies, players were able to relate the retro-style game design with their past game experiences and felt nostalgic.
2. Pausing the game while displaying suggestions or tips and providing the player with the autonomy to close/dismiss the suggestions will help the player to read suggestions at their own pace.
3. Collecting background in-game player data for adjusting game difficulty or for similar design goals helps to balance the game and improve the player experience.
4. Introducing hidden areas in a game will increase the players' curiosity and might motivate them to explore the game. Following level design patterns is helpful for designing interesting levels and for keeping the players motivated.
5. Tailoring the game according to the players' motivational orientation leads to increased security behaviour levels and improved perceived choice of the players.

Some of the key implications like players relating to the retro game and being motivated by hidden areas were evident across the Heuristic Evaluation and Evaluation Study One. This also shows the advantages of conducting iterative user-centred evaluation studies to inform design changes accordingly. The limitations of this study and future works are discussed in the upcoming chapter.

Chapter 7 - Conclusion

In this chapter, I summarize the study details and then discuss the limitations of the work and possible future works.

7.1 Study Summary

This research focuses on designing a persuasive game to motivate users to adopt secure smartphone practices. With each study, the design was iterated accordingly. Initially, the persuasive game was designed according to BJ Fogg's eight-step methodology [47]. Following this, the game design was presented to subject matter experts for initial feedback, and then I conducted Heuristic Evaluation for Playability (Perma-Run: Version One) using six researchers. According to the results of the heuristic evaluation, the game design was iterated, and other security scenarios were added to the game in the form of in-game quizzes. This version was called Perma-Run: Version Two, and I compared this version with an existing educational document, published by the NSA [199] and this study was called Evaluation Study One. From the results of Evaluation Study One, it was evident that overall, the game performed better than the security document.

Following this, I iterated the design according to the study results and tailored the game according to Regulatory Focus Theory. This design iteration is Perma-Run: Version Three with two versions of the game: the Promotion Focus Version and Prevention Focus Version tailored to people with different motivational orientation types. Following this, I conducted a 2x2 between-subject study with 102 participants and randomly assigned them into four groups, namely – Promotion focus tailored, Prevention focus tailored, Promotion focus non-tailored and Prevention focus non-tailored. The results show that overall, tailoring was beneficial for improving the users' security behaviour and the user's preferred playing the tailored version of the game over the non-tailored version of the game. It was also evident that the players who played the non-tailored version of the game preferred the *competition*, *rewards*, and *social comparison* persuasive strategies. Overall, there are various advantages of tailoring the game with Regulatory Focus Theory for players of different motivational orientations.

7.2 Limitations

Surveys are widely used across various research domains, and it is one of the common methods in HCI research. I conducted the experiments as remote in-the-wild studies, and hence, the surveys were self-administered by the users and all the survey data were self-reported by the users. A limitation here is the possibility of participants' bias while answering the survey irrespective of the instructions provided to them and keeping track, if the user who answered the survey played the game indeed. Considering the length of the survey, survey fatigue is another factor that might affect participants' responses despite the care taken to reduce the fatigue by minimizing the number of questions on each page. Game images were included wherever possible in the lieu of a detailed explanation of the game. For the heuristic evaluation of playability (HEP), the evaluators were from the Persuasive Computing and HCI Lab, Dalhousie University, and there is a chance for personal bias from each evaluator. For the choice of platform, we focused on the Android phone. Although Android is regarded as less secure compared to the iOS, with an overall higher market share [1,5,86], creating another game for both operating systems in a similar way might be a plausible solution as part of future work (only the permissions would change between iOS and Android). From the survey demographics, it was evident that apart from smartphones, players also frequently played PC games and consoled games. Considering the ubiquitous nature of games, it might be wise to roll out Perma-Run for various devices like PC and Consoles apart from just smartphones to educate a wider range of audiences.

7.3 Future Work

As part of our future work, we plan to run a longitudinal study with a larger sample size, and the duration of the study would be 3+ months. There would be at least three points of data collection during the study. This way, one can monitor the participant's secure smartphone behaviour over a long time. To reduce survey fatigue, the number of questions shown on a screen would be less, and the average time to complete the survey and the survey progress would be shown to the participant. Apart from this, there are various other research directions for future work that emerged from this research. It was evident from the background research that people from various countries followed different kinds of secure smartphone practices. This shows that there might be cultural implications for smartphone security, and this could be another interesting research direction. Research has shown that people from the west are more individualistic compared to those from the east where a collectivist culture is followed. Due to this, people might approach smartphone security in different ways. For example, someone from North America might be willing to protect their phones to avoid leakage of their private data, whereas someone from Africa or India might be motivated to protect their closer community of friends and family [8]. Therefore, the persuasive game can further be tailored based on culture. The persuasive messages could be further tailored by writing them in a persuasive and culturally tailored manner to study various impacts of suggestions on people of various motivational orientations [8]. This work can also be extended to other domains like physical activity, healthy eating, and mental wellness. Recent research [64] has shown that people who were not addicted to the internet were aware of the secure smartphone behaviour in a social aspect, and people who showed moderate to severe depression symptoms performed better on the technical aspects of smartphone security. This might be a new avenue for tailoring gamified interventions according to specific mental health issues. Perma-Run could also be tailored to reflect more on technical or social aspects of smartphone security according to the needs of the player for improving their secure smartphone behaviour.

7.4 Conclusion

This thesis is an important and fruitful contribution to the field of Persuasive Technology for Security & Privacy. This work shows how to tailor a persuasive game according to the user's motivational orientation (using Regulatory Focus Theory) to motivate them to follow secure smartphone behaviour. The game underwent several iterations for smoothening the gameplay and fixing usability issues before tailoring the game. After comparing the game with an existing educational document published by NSA, it was evident that overall, the game performed better than the document for improving users' secure smartphone behaviour and their intention to protect themselves from smartphone security threats. The tailored versions of the game significantly improved the player's security behaviour compared to the non-tailored version of the game. Looking at the IMI - perceived choice construct, it was evident that players preferred the game that was tailored to their motivational orientation type. Players who played the non-tailored version preferred to compete on the leaderboard and wanted rewards but did not show a significant improvement for secure smartphone behaviour. The overall persuasiveness scores and the player experience scores show that the game is highly persuasive, and this is also supported by users' feedback.

7.5 Publications

Given below is the list of published conference papers from this thesis and my other published works as a co-author. Perma-Run has been published on Google Playstore [198].

1. **Anirudh Ganesh**, Chinenye Ndulue, and Rita Orji. 2021. The design and development of mobile game to promote secure smartphone behaviour. In *CEUR Workshop Proceedings*, 73–87
2. **Anirudh Ganesh**, Chinenye Ndulue, and Rita Orji. 2021. PERMARUN- A Persuasive Game to Improve User Awareness and Self-Efficacy towards Secure Smartphone Behaviour. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411763.3451781
3. **Anirudh Ganesh**, Chinenye Ndulue, and Rita Orji. 2022. Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory. In *International Conference on Persuasive Technology*, 89–100. https://doi.org/10.1007/978-3-030-98438-0_7
4. Oladapo Oyebode, **Anirudh Ganesh**, and Rita Orji. 2021. TreeCare: Development and Evaluation of a Persuasive Mobile Game for Promoting Physical Activity. In *IEEE Conference on Games*.
5. Chinenye Ndulue, Oladapo Oyebode, Ravishankar Subramani Iyer, **Anirudh Ganesh**, Syed Ishtiaque Ahmed and Rita Orji. 2022. Personality-targeted Persuasive Gamified Systems : Exploring the Impact of Application Domain on the Effectiveness of Behavior Change Strategies Personality-targeted Persuasive Gamified Systems : Exploring the Impact of Application Domain on the Effective. *User Modeling and User-Adapted Interaction*, January: 0–45. https://doi.org/10.1007/s11257-022-09319-w

BIBLIOGRAPHY

1. Mohd Shahdi Ahmad, Nur Emyra Musa, Rathidevi Nadarajah, Rosilah Hassan, and Nor Effendy Othman. 2013. Comparison between android and iOS Operating System in terms of security. In *2013 8th International Conference on Information Technology in Asia - Smart Devices Trend: Technologising Future Lifestyle, Proceedings of CITA 2013*. https://doi.org/10.1109/CITA.2013.6637558
2. Junho Ahn, James Williamson, Mike Gartrell, Richard Han, Qin Lv, and Shivakant Mishra. 2015. Supporting healthy grocery shopping via mobile augmented reality. *ACM Transactions on Multimedia Computing, Communications and Applications* 12. https://doi.org/10.1145/2808207
3. Milad Taleby Ahvanooey, Prof Qianmu Li, Mahdi Rabbani, and Ahmed Raza Rajput. 2017. A Survey on Smartphones Security : Software Vulnerabilities , Malware , and Attacks. *International Journal of Advanced Computer Science and Applications* 8, 10: 30–45.
4. Icek Ajzen. 2011. The theory of planned behaviour: Reactions and reflections. *Psychology and Health* 26, 9: 1113–1127. https://doi.org/10.1080/08870446.2011.613995
5. Fattoh Al-Qershi, Muhammad Al-Qurishi, Sk Md Mizanur Rahman, and Atif Al-Amri. 2014. Android vs. iOS: The security battle. In *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*. https://doi.org/10.1109/WCCAIS.2014.6916629
6. Jaffar A. Al-Tawfiq and Didier Pittet. 2013. Improving hand hygiene compliance in healthcare settings using behavior change theories: reflections. *Teaching and learning in medicine* 25, 4: 374–382. https://doi.org/10.1080/10401334.2013.827575
7. Majed Abdullah Alrowaily and Manolya Kavakli. 2017. The use of augmented reality for encouraging pro-environmental behaviors: The case of Australia. In *ACM International Conference Proceeding Series*, 21–25. https://doi.org/10.1145/3057039.3057082

8. Maria Bada, Angela M. Sasse, and Jason R.C. Nurse. 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In *International Conference on Cyber Security for Sustainable Society, 2015*. Retrieved March 6, 2021 from http://arxiv.org/abs/1901.02672

9. Mehrdad Bahrini, Marcel Meissner, Rainer Malaka, Nina Wenig, and Karsten Sohr. 2019. HappyPerMi: Presenting critical data flows in mobile application to raise user security awareness. *Conference on Human Factors in Computing Systems - Proceedings*, April. https://doi.org/10.1145/3290607.3312914

10. Mehrdad Bahrini, Georg Volkmar, Jonas Schmutte, Nina Wenig, Karsten Sohr, and Rainer Malaka. 2019. Make my phone secure! Using gamification for mobile security settings. *ACM International Conference Proceeding Series*: 299–308. https://doi.org/10.1145/3340764.3340775

11. Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. October. https://doi.org/10.14722/usec.2014.23006

12. Albert Bandura. 1978. Reflections on self-efficacy. *Advances in Behaviour Research and Therapy* 1, 4: 237–269. https://doi.org/10.1016/0146-6402(78)90012-7

13. René van Bavel, Nuria Rodríguez-Priego, José Vila, and Pam Briggs. 2019. Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies* 123: 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

14. Elke Beck, Kai Von Holdt, Jochen Meyer, and Susanne Boll. 2019. Sneaking physical exercise into sedentary work life: Design explorations of ambient reminders in opportune moments. *2019 IEEE International Conference on Healthcare Informatics, ICHI 2019*: 1–7. https://doi.org/10.1109/ICHI.2019.8904662

15. Ron Bitton, Kobi Boymgold, Rami Puzis, and Asaf Shabtai. 2020. Evaluating the Information Security Awareness of Smartphone Users. In *Conference on Human Factors in Computing Systems - Proceedings (2020)*, 1–13. https://doi.org/10.1145/3313831.3376385

16. Ron Bitton, Andrey Finkelshtein, Lior Sidi, Rami Puzis, Lior Rokach, and Asaf Shabtai. 2018. Taxonomy of mobile users' security awareness. *Computers and Security* 73: 266–293. https://doi.org/10.1016/j.cose.2017.10.015

17. Marcela C.C. Bomfim, Sharon I. Kirkpatrick, Lennart E Nacke, and James R. Wallace. 2020. Food Literacy while Shopping: Motivating Informed Food Purchasing Behaviour with a Situated Gameful App. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376801

18. Marcela C.C. Bomfim and James R. Wallace. 2018. Pirate bri's grocery adventure: Teaching food literacy through shopping. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April: 1–6. https://doi.org/10.1145/3170427.3188496

19. Amiangshu Bosu, Fang Liu, Danfeng Daphne Yao, and Gang Wang. 2017. Collusive data leak and more: Large-scale threat analysis of inter-app communications. In *ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security*, 71–85. https://doi.org/10.1145/3052973.3053004

20. Frank Breitinger, Ryan Tully-Doyle, and Courtney Hassenfeldt. 2020. A survey on smartphone user's security choices, awareness and education. *Computers and Security* 88. https://doi.org/10.1016/j.cose.2019.101647

21. Tim Buckers, Boning Gong, Elmar Eisemann, and Stephan Lukosch. 2018. VRabl: Stimulating physical activities through a multiplayer augmented reality sports game. In *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3210299.3210300

22. Marcus Butavicius, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. 2015. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*, 1–10.

23. Feren Calderwood and Iskra Popova. 2019. Smartphone cyber security awareness in developing countries: A case of Thailand. In *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, 79–86. https://doi.org/10.1007/978-3-030-05198-3_7

24. Ufuk Celikcan, Ahmed Şamil Bülbül, Cem Aslan, Zehra Buyuktuncer, Kübra Işgın, Gözde Ede, and Nuray Kanbur. 2018. The virtual cafeteria: An immersive environment for interactive food portion-size education. In *MHFI 2018 - 3rd Workshop on Multisensory Approaches to Human-Food Interaction*. https://doi.org/10.1145/3279954.3279960

25. Joseph Cesario, Heidi Grant, and E Tory Higgins. 2004. Regulatory Fit and Persuasion : Transfer From " Feeling Right ." *Journal of Personality and Social Psychology* 86, 3: 388–404. https://doi.org/10.1037/0022-3514.86.3.388

26. Joseph Cesario and E. Tory Higgins. 2008. Making message recipients "feel right": How nonverbal cues can increase persuasion. *Psychological Science* 19, 5: 415–420. https://doi.org/10.1111/j.1467-9280.2008.02102.x

27. Joseph Cesario, E. Tory Higgins, and Abigail A. Scholer. 2008. Regulatory Fit and Persuasion: Basic Principles and Remaining Questions. *Social and Personality Psychology Compass* 2, 1: 444–463. https://doi.org/10.1111/j.1751-9004.2007.00055.x

28. Shelly Chaiken, Wendy Wood, and Alice H Eagly. 1996. Principles of persuasion. *Social psychology: Handbook of basic principles.*, 702–742.

29. Rachel Chambers, Lauren Tingey, Britta Mullany, Sean Parker, Angelita Lee, and Allison Barlow. 2016. Exploring sexual risk taking among American Indian adolescents through protection motivation theory. *AIDS Care - Psychological and Socio-Medical Aspects of AIDS/HIV* 28, 9: 1089–1096. https://doi.org/10.1080/09540121.2016.1164289

30. Gerry Chan, Ali Arya, Rita Orji, and Zhao Zhao. 2019. Motivational strategies and approaches for single and multi-player exergames: A social perspective. *PeerJ Computer Science* 5: 1–34. https://doi.org/10.7717/PEERJ-CS.230

31. Gerry Chan, Ali Arya, and Anthony Whitehead. 2018. Keeping players engaged in exergames: A personality matchmaking approach. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3170427.3188455

32. Aditya Chand, Monica Gonzalez, Julian Missig, Purin Phanichphant, and Pen Fan Sun. 2006. Balance pass: Service design for a healthy college lifestyle. *Conference on Human Factors in Computing Systems - Proceedings*: 1813–1818. https://doi.org/10.1145/1125451.1125795

33. Ching Huei Chen, Victor Law, and Kun Huang. 2019. The roles of engagement and competition on learner's performance and motivation in game-based science learning. *Educational Technology Research and Development* 67, 4: 1003–1024. https://doi.org/10.1007/s11423-019-09670-7

34. Tianying Chen, Laura Dabbish, and Jessica Hammer. 2019. Self-efficacy-based game design to encourage security behavior online. In *Conference on Human Factors in Computing Systems - Proceedings*, 1–6. https://doi.org/10.1145/3290607.3312935

35. Zhi-Hong Chen, Howard Hao, Jan Chen, and Wan-Jhen Dai. 2018. Using Narrative-based Contextual Games to Enhance Language Learning: A Case Study. *Source: Journal of Educational Technology & Society* 21, 3: 186–198.

36. Luca Chittaro and Riccardo Sioni. 2015. Serious games for emergency preparedness: Evaluation of an interactive vs. a non-interactive simulation of a terror attack. *Computers in Human Behavior* 50: 508–519. https://doi.org/10.1016/j.chb.2015.03.074

37. Amit Das and Habib Ullah Khan. 2016. Security behaviors of smartphone users. *Information and Computer Security* 24, 1: 116–134. https://doi.org/10.1108/ICS-04-2015-0018

38. Scott M. Debb and Marnee K. Mcclellan. 2021. Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking* 24, 9: 605–611. https://doi.org/10.1089/cyber.2021.0043

39. Lotfi Derbali and Claude Frasson. 2010. Players' motivation and EEG waves patterns in a serious game environment. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 297–299. https://doi.org/10.1007/978-3-642-13437-1_50

40. Heather Desurvire, Martin Caplan, and Jozsef A. Toth. 2004. Using Heuristics to Evaluate the Playability of games. In *Conference on Human Factors in Computing Systems - Proceedings*, 1509–1512. https://doi.org/10.1145/985921.986102

41. Leyla Dogruel and Sven Jöckel. 2019. Risk perception and privacy regulation preferences from a cross-cultural perspective. A qualitative study among German and U.S. smartphone users. *International Journal of Communication* 13: 1764–1783.

42. Filip Drozd, Tuomas Lehto, and Harri Oinas-Kukkonen. 2012. Exploring perceived persuasiveness of a behavior change support system: A structural model. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 157–168. https://doi.org/10.1007/978-3-642-31037-9_14

43. Maha Elgarf, Natalia Calvo-Barajas, and Ana Paiva. 2021. Reward seeking or loss aversion? impact of regulatory focus theory on emotional induction in children and their behavior towards a. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445486

44. William Enck, Machigar Ongtang, and Patrick Mcdaniel. 2009. On Lightweight Mobile Phone Application Certification. In *Proceedings of the 16th ACM conference on Computer and communications security (CCS '09).*, 235–245.

45. Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, and Muttukrishnan Rajarajan. 2015. Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys and Tutorials* 17, 2: 998–1022. https://doi.org/10.1109/COMST.2014.2386139

46. Lori Flynn and Will Klieber. 2015. Smartphone Security. *IEEE Pervasive Computing* 14, 4: 16–21. https://doi.org/10.1109/MPRV.2015.67

47. B. J. Fogg. 2009. Creating persuasive technologies: An eight-step design process. *ACM International Conference Proceeding Series* 350. https://doi.org/10.1145/1541948.1542005

48. Luciano Gamberini, Nicola Corradi, Luca Zamboni, Michela Perotti, Camilla Cadenazzi, Stefano Mandressi, Giulio Jacucci, Giovanni Tusa, Anna Spagnolli, Christoffer Björkskog, Marja Salo, and Pirkka Aman. 2011. Saving is Fun: Designing a Persuasive Game for Power Conservation. Retrieved December 23, 2021 from www.energyawareness.eu

49. Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2021. The design and development of mobile game to promote secure smartphone behaviour. In *CEUR Workshop Proceedings*, 73–87.

50. Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2021. PERMARUN- A Persuasive Game to Improve User Awareness and Self-Efficacy towards Secure Smartphone Behaviour. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411763.3451781

51. Anirudh Ganesh, Chinenye Ndulue, and Rita Orji. 2022. Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory. In *International Conference on Persuasive Technology*, 89–100. https://doi.org/10.1007/978-3-030-98438-0_7

52. C. J. Gokul, Sankalp Pandit, Sukanya Vaddepalli, Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha. 2018. Phishy - A serious game to train enterprise users on phishing awareness. In *CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169–181. https://doi.org/10.1145/3270316.3273042

53. Mark Gondree, Zachary N.J. Peterson, and Tamara Denning. 2013. Security through play. *IEEE Security and Privacy* 11, 3: 64–67. https://doi.org/10.1109/MSP.2013.69

54. Google. 2021. Permissions on Android | Android Developers. Retrieved November 5, 2021 from https://developer.android.com/guide/topics/permissions/overview

55. Michael Grace, Wu Zhou, Xuxian Jiang, and Ahmad Reza Sadeghi. 2012. Unsafe exposure analysis of mobile in-app advertisements. *WiSec'12 - Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks* 067, Section 2: 101–112. https://doi.org/10.1145/2185448.2185464

56. Stuart Hallifax, Elise Lavoué, and Audrey Serna. 2020. To tailor or not to tailor gamification? An analysis of the impact of tailored game elements on learners' behaviours and motivation. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12163 LNAI: 216–227. https://doi.org/10.1007/978-3-030-52237-7_18/TABLES/3

57. Emmi Harjuniemi, Ashley Colley, Emmi Harjuniemi, and Ashley Colley. 2018. Idle Stripes Shirt - Ambient Wearable Display for Activity Tracking. October. https://doi.org/10.1145/3267242.3267303

58. Carrie Heeter, Yu-Hao Lee, Brian Magerko, Carrie Cole, and Ben Medler. 2012. Regulatory Focus and Serious Games: A Quasi-Experimental Study. Retrieved March 3, 2022 from http://gel.msu.edu/playertypes

59. E. Tory Higgins. 1998. Promotion and Prevention: Regulatory Focus as A Motivational Principle. *Advances in Experimental Social Psychology* 30, C: 1–46. https://doi.org/10.1016/S0065-2601(08)60381-0

60. E. Tory Higgins, Ronald S. Friedman, Robert E. Harlow, Lorraine Chen Idson, Ozlem N. Ayduk, and Amy Taylor. 2001. Achievement orientations from subjective histories of success: Promotion pride versus prevention pride. *European Journal of Social Psychology* 31, 1: 3–23. https://doi.org/10.1002/ejsp.27

61. E. Tory Higgins, Emily Nakkawita, and James F. M. Cornwell. 2020. Beyond outcomes: How regulatory focus motivates consumer goal pursuit processes. *Consumer Psychology Review* 3, 1: 76–90. https://doi.org/10.1002/arcp.1052

62. Shu-Hsun Ho, Chutinon Putthiwanit, and Chia-Ying Lin. 2011. May I continue or should I stop? The effects of regulatory focus and message framings on video game players' self control. *International Journal of Business and Social Science* 2, 12: 194–200. Retrieved March 3, 2022 from www.ijbssnet.com

63. Corine Horsch, Willem-Paul Brinkman, Rogier van Eijk, and Mark Neerincx. 2012. Towards the usage of persuasive strategies in a virtual sleep coach. 1–4. https://doi.org/10.14236/ewic/hci2012.77

64. Hsiao Ying Huang, Güliz Seray Tuncay, Soteris Demetriou, Carl A Gunter, Rini Banerjee, and Masooda Bashir. 2020. Smartphone Security Behavioral Scale: A New Psychometric Measurement for Smartphone Security. *arXiv*.

65. Kenneth Hullett and Jim Whitehead. 2010. Design patterns in FPS levels. In *FDG 2010 - Proceedings of the 5th International Conference on the Foundations of Digital Games*, 78–85. https://doi.org/10.1145/1822348.1822359

66. J.M. Keller. 1983. Motivational Design of Instruction. In *Instructional-design theories and models : an overview of their current status*. Hillsdale, N.J. : Lawrence Erlbaum Associates, Hillsdale, N.J., 383–484.

67. John Keller. *How to integrate learner motivation planning into lesson planning: The ARCS model approach*.

68. John M Keller. 1987. Development and use of the ARCS model of instructional design. *Journal of Instructional Development* 10, 3: 2–10. https://doi.org/10.1007/BF02905780

69. Christine Keung, Alexa Lee, Shirley Lu, and Megan O'Keefe. 2013. BunnyBolt: A mobile fitness app for youth. *ACM International Conference Proceeding Series*: 585–588. https://doi.org/10.1145/2485760.2485871

70. Ahmed Khalifa, Fernando De Mesentier Silva, and Julian Togelius. 2019. Level design patterns in 2D games. *IEEE Conference on Computatonal Intelligence and Games, CIG* 2019-Augus. https://doi.org/10.1109/CIG.2019.8847953

71. Lenka Knapova, Agata Kruzikova, Lenka Dedkova, and David Smahel. 2021. Who Is Smart with Their Smartphones? Determinants of Smartphone Security Behavior. *Cyberpsychology, Behavior, and Social Networking* 24, 9: 584–592. https://doi.org/10.1089/CYBER.2020.0599/FORMAT/EPUB

72. Murat Koyuncu and Tolga Pusatli. 2019. Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mobile Information Systems* 2019. https://doi.org/10.1155/2019/2786913

73. Hanna Krasnova and Annika Baumann. 2014. Gender Differences in Online Gaming: A Literature Review The Internet-Topology and Vulnerability View project. In *Gender Differences in Online Gaming: A Literature Review*. Retrieved June 7, 2022 from https://www.researchgate.net/publication/277597582

74. Ari Kusyanti and Harin Puspa Ayu Catherina. 2018. An empirical study of app permissions: A user protection motivation behaviour. *International Journal of Advanced Computer Science and Applications* 9, 11: 106–111. https://doi.org/10.14569/IJACSA.2018.091116

75. Angela Y Lee and Jennifer L Aaker. 2004. Bringing the Frame into Focus: The Influence of Regulatory Fit on Processing Fluency and Persuasion. *Journal of Personality and Social Psychology* 86, 2: 205–218. https://doi.org/10.1037/0022-3514.86.2.205

76. Yu Hao Lee, Carrie Heeter, Brian Magerko, and Ben Medler. 2013. Feeling right about how you play: The effects of regulatory fit in games for learning. *Games and Culture* 8, 4: 238–258. https://doi.org/10.1177/1555412013498818

77. James C. Lester, Jonathan P. Rowe, and Bradford W. Mott. 2013. Narrative-centered learning environments: A story-centric approach to educational games. In *Emerging Technologies for the Classroom: A Learning Sciences Perspective*. Springer New York, 223–237. https://doi.org/10.1007/978-1-4614-4696-5_15

78. Kun Li and John M. Keller. 2018. Use of the ARCS model in education: A literature review. *Computers and Education* 122: 54–62. https://doi.org/10.1016/j.compedu.2018.03.019

79. Huigang Liang and Yajiong Xue. 2009. Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly: Management Information Systems* 33, 1: 71–90. https://doi.org/10.2307/20650279

80. Alexander De Luca and Emanuel Von Zezschwitz. 2016. Usable privacy and security. *IT - Information Technology* 58, 5: 215–216. https://doi.org/10.1515/itit-2016-0034

81. Karen MacDonell. 2013. A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth. *Journal of Addiction Research & Therapy* 04, 03. https://doi.org/10.4172/2155-6105.1000154

82. James E Maddux and Ronald W. Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* 19, 5: 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

83. Florian Mathis, Kami Vaniea, and Mohamed Khamis. 2022. Prototyping Usable Privacy and Security Systems: Insights from Experts. *International Journal of Human-Computer Interaction* 38, 5: 468–490. https://doi.org/10.1080/10447318.2021.1949134

84. Yannic Meier, Johanna Schäwel, Elias Kyewski, and Nicole C Krämer. 2020. Applying Protection Motivation Theory to Predict Facebook Users' Withdrawal and Disclosure Intentions. In *ACM International Conference Proceeding Series*, 21–29. https://doi.org/10.1145/3400806.3400810

85. Gaurav Misra, Nalin Asanka Gamagedara Arachchilage, and Shlomo Berkovsky. 2017. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. Retrieved December 12, 2021 from http://arxiv.org/abs/1710.06064

86. Ibtisam Mohamed and Dhiren Patel. 2015. Android vs iOS security: A comparative study. In *Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015*, 725–730. https://doi.org/10.1109/ITNG.2015.123

87. Dinesh Mulchandani. 2021. Design and Evaluation of COVID Pacman–A Persuasive Game to Promote the Awareness and Adoption of COVID-19 Precautionary Measures Tailored to the Stages of Change. Dalhousie University. Retrieved March 4, 2022 from https://dalspace.library.dal.ca/handle/10222/80525

88. Dinesh Mulchandani, Alaa Alslaity, and Rita Orji. 2022. Exploring the effectiveness of persuasive games for disease prevention and awareness and the impact of tailoring to the stages of change. *Human–Computer Interaction* 37, 4: 1–35. https://doi.org/10.1080/07370024.2022.2057858

89. Dinesh Mulchandani and Rita Orji. 2021. Persuasiveness of a Game to Promote the Adoption of COVID-19 Precautionary Measures and the Moderating Effect of Gender. *UMAP 2021 - Adjunct Publication of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, June: 303–308. https://doi.org/10.1145/3450614.3464623

90. Dinesh Mulchandani and Rita Orji. 2021. A Persuasive Game to Promote Awareness and Adoption of COVID-19 Precautionary Measures. In *UMAP 2021 - Adjunct Publication of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, 83–85. https://doi.org/10.1145/3450614.3461678

91. Florence Mwaka Mwagwabi. 2015. A Protection Motivation Theory Approach to Improving Compliance with Password Guidelines.

92. Lennart E Nacke, Chris Bateman, and Regan L Mandryk. 2014. BrainHex: A neurobiological gamer typology survey. *Entertainment Computing* 5, 1: 55–62. https://doi.org/10.1016/j.entcom.2013.06.002

93. Annamalai Narayanan, Lihui Chen, and Chee Keong Chan. 2014. AdDetect: Automated detection of Android ad libraries using semantic analysis. *IEEE ISSNIP 2014 - 2014 IEEE 9th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Conference Proceedings*, April: 21–24. https://doi.org/10.1109/ISSNIP.2014.6827639

94. Emily Naul and Min Liu. 2020. Why Story Matters: A Review of Narrative in Serious Games. *Journal of Educational Computing Research* 58, 3: 687–707. https://doi.org/10.1177/0735633119859904

95. Chinenye Ndulue and Rita Orji. 2018. STD PONG: Changing risky sexual behaviour in Africa through persuasive games. In *ACM International Conference Proceeding Series*, 134–138. https://doi.org/10.1145/3283458.3283463

96. Chinenye Ndulue and Rita Orji. 2021. Heuristic Evaluation of an African-centric Mobile Persuasive Game for Promoting Safety Measures against COVID-19. In *ACM International Conference Proceeding Series*, 43–51. https://doi.org/10.1145/3448696.3448706

97. Chinenye Ndulue, Oladapo Oyebode, and Rita Orji. 2020. PHISHER CRUSH: A Mobile Persuasive Game for Promoting Online Security. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 223–233. https://doi.org/10.1007/978-3-030-45712-9

98. Chinenye Ndulue, Oladapo Oyebode, and Rita Orji. 2020. PHISHER CRUSH: A Mobile Persuasive Game for Promoting Online Security. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 223–233. https://doi.org/10.1007/978-3-030-45712-9_17

99. Jakob Nielsen and Rolf Molich. 1990. Heuristic evaluation of user interfaces. In *Conference on Human Factors in Computing Systems - Proceedings*, 249–256. https://doi.org/10.1145/97243.97281

100. Jakob Nielsen, Rolf Molich, and Jn@neuvml Bitnet Denmark. 1990. *CHI 90 Procee&qs HEURISTIC EVALUATION OF USER INTERFACES*.

101. Domen Novak, Aniket Nagle, Urs Keller, and Robert Riener. 2014. Increasing motivation in robot-aided arm rehabilitation with competitive and cooperative gameplay. *Journal of NeuroEngineering and Rehabilitation* 11, 1: 1–15. https://doi.org/10.1186/1743-0003-11-64

102. Shohana Nowrin and David Bawden. 2018. Information security behaviour of smartphone users: An empirical study on the students of university of Dhaka, Bangladesh. *Information and Learning Science* 119, 7–8: 444–455. https://doi.org/10.1108/ILS-04-2018-0029

103. Dimitris Ntalaperas, Efthimios Bothos, Konstantinos Perakis, Babis Magoutas, and Gregoris Mentzas. 2015. DISYS: An intelligent system for personalized nutritional recommendations in restaurants. *ACM International Conference Proceeding Series* 01-03-Octo: 382–387. https://doi.org/10.1145/2801948.2801997

104. Harri Oinas-Kukkonen and Marja Harjumaa. 2009. Persuasive systems design: Key issues, process model, and system features. *Communications of the Association for Information Systems* 24, 1: 485–500. https://doi.org/10.17705/1cais.02428

105. Rita Orji, Regan L. Mandryk, and Julita Vassileva. 2017. Improving the efficacy of games for change using personalization models. *ACM Transactions on Computer-Human Interaction* 24, 5. https://doi.org/10.1145/3119929

106. Rita Orji, Regan L. Mandryk, Julita Vassileva, and Kathrin M. Gerling. 2013. Tailoring persuasive health games to gamer type. *Conference on Human Factors in Computing Systems - Proceedings*: 2467–2476. https://doi.org/10.1145/2470654.2481341

107. Rita Orji and Karyn Moffatt. 2018. Persuasive technology for health and wellness: State-of-the-art and emerging trends. *Health Informatics Journal* 24, 1: 66–91. https://doi.org/10.1177/1460458216650979

108. Rita O Orji. DESIGN FOR BEHAVIOUR CHANGE: A MODEL-DRIVEN APPROACH FOR TAILORING PERSUASIVE TECHNOLOGIES.

109. Rita Orji, Derek Reilly, Kiemute Oyibo, and Fidelia A. Orji. 2019. Deconstructing persuasiveness of strategies in behaviour change systems using the ARCS model of motivation. *Behaviour and Information Technology* 38, 4: 319–335. https://doi.org/10.1080/0144929X.2018.1520302

110. Rita Orji, Gustavo F. Tondello, and Lennart E. Nacke. 2018. Personalizing persuasive strategies in gameful systems to gamification user types. *Conference on Human Factors in Computing Systems - Proceedings* 2018-April, January. https://doi.org/10.1145/3173574.3174009

111. Rita Orji, Julita Vassileva, and Regan L. Mandryk. 2013. LunchTime: A slow-casual game for long-term dietary behavior change. *Personal and Ubiquitous Computing* 17, 6: 1211–1221. https://doi.org/10.1007/s00779-012-0590-6

112. Rita Orji, Julita Vassileva, and Regan L. Mandryk. 2014. Modeling the efficacy of persuasive strategies for different gamer types in serious games for health. *User Modeling and User-Adapted Interaction* 24, 5: 453–498. https://doi.org/10.1007/s11257-014-9149-8

113. Brian Orland, Nilam Ram, Dean Lang, Kevin Houser, Nate Kling, and Michael Coccia. 2014. Saving energy in an office environment: A serious game intervention. *Energy and Buildings* 74: 43–52. https://doi.org/10.1016/j.enbuild.2014.01.036

114. Oladapo Oyebode, Mona Alhasani, Dinesh Mulchandani, Tolulope Olagunju, and Rita Orji. 2021. SleepFit: A Persuasive Mobile App for Improving Sleep Habits in Young Adults. In *SeGAH 2021 - 2021 IEEE 9th International Conference on Serious Games and Applications for Health*. https://doi.org/10.1109/SEGAH52098.2021.9551907

115. Oladapo Oyebode, Anirudh Ganesh, and Rita Orji. 2021. TreeCare: Development and Evaluation of a Persuasive Mobile Game for Promoting Physical Activity. In *IEEE Conference on Games*.

116. Oladapo Oyebode, Chinenye Ndulue, and Dinesh Mulchandani. 2021. Tailoring persuasive and behaviour change systems based on stages of change and motivation. In *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3411764.3445619

117. Oladapo Oyebode and Rita Orji. 2022. Player Matching in a Persuasive Mobile Exergame: Towards Performance-Driven Collaboration and Adaptivity. . 164–173. https://doi.org/10.1007/978-3-030-98438-0_13

118. Carlo Perrotta, Gill Featherstone, Helen Aston, and Emily Houghton. 2013. *Game-based learning: Latest evidence and future directions*.

119. Y. S. Poong, S. Yamaguchi, and J. Takada. 2015. Impact of learning content on World Heritage Site preservation awareness in town of Luang Prabang, Lao PDR: Application of protection motivation theory. In *ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 251–256. https://doi.org/10.5194/isprsannals-II-5-W3-251-2015

120. Yew Siang Poong, Shinobu Yamaguchi, and Jun Ichi Takada. 2014. Persuasive content development: Application of protection motivation theory in promoting heritage site preservation awareness. In *Conference on Human Factors in Computing Systems - Proceedings*, 2437–2442. https://doi.org/10.1145/2559206.2581259

121. Feren CalderWood and Iskra Popova. 2019. Smartphone Cyber Security Awareness in Developing Countries: A Case of Thailand. *Department of Computer and System Sciences, Stockholm University, Sweden*: 58–68. https://doi.org/10.1007/978-3-030-05198-3

122. Raghu Raman, Athira Lal, and Krishnashree Achuthan. Serious Games based approach to cyber security concept learning : Indian context. 3–7.

123. George E Raptis and Christina Katsini. 2021. Beter, funner, stronger: A gameful approach to nudge people into making less predictable graphical password choices. In *Conference on Human Factors in Computing Systems - Proceedings*, 17. https://doi.org/10.1145/3411764.3445658

124. Joel Reardon, Álvaro Feal, Amit Elazari, Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *Proceedings of the 28th USENIX Security Symposium*, 603–620. Retrieved January 19, 2021 from https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

125. Karen Renaud. 2016. 60 . Smartphone Owners Need Security Advice . How Can We Ensure They Get It ? In *CONF-IRM 2016 Proceedings*.

126. J. Lynn Reynolds. 2006. Measuring intrinsic motivations. *Handbook of Research on Electronic Surveys and Measurements*, Imi: 170–173. https://doi.org/10.4018/978-1-59140-792-8.ch018

127. Ryan Rogers. 2017. The motivational pull of video game feedback, rules, and social interaction: Another self-determination theory approach. *Computers in Human Behavior* 73: 446–450. https://doi.org/10.1016/J.CHB.2017.03.048

128. R Rogers W. 1983. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. *Social Psychophysiology: A Sourcebook*, October 2014: 153–177.

129. Irwin M. Rosenstock. 1977. The Health Belief Model and Preventive Health Behavior. *Health Education & Behavior* 2, 4: 354–386. https://doi.org/10.1177/109019817400200405

130. Borja Sanz, Igor Santos, Carlos Laorden, Xabier Ugarte-Pedrero, Pablo Garcia Bringas, and Gonzalo Álvarez. 2013. PUMA: Permission usage to detect malware in android. *Advances in Intelligent Systems and Computing* 189 AISC: 289–298. https://doi.org/10.1007/978-3-642-33018-6_30

131. Sam Scholefield and Lynsay A Shepherd. 2019. Gamification Techniques for Raising Cyber Security Awareness. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (2019) 11594 LNCS 191-203*.

132. Anna Noakes Schulze. 2001. A User-Centered Design for Information Professionals. *Journal of Education for Library and Information Science* 42, 2: 116–122.

133. Pintu Shah and Anuja Agarwal. 2020. Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information and Computer Security* 28, 2: 293–318. https://doi.org/10.1108/ICS-04-2019-0041

134. Mudassar Sharif, Adeel Zafar, and Uzair Muhammad. 2017. Design Patterns and General Video Game Level Generation. *International Journal of Advanced Computer Science and Applications* 8, 9. https://doi.org/10.14569/ijacsa.2017.080952

135. Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Conference on Human Factors in Computing Systems - Proceedings*, 2347–2356. https://doi.org/10.1145/2556288.2557421

136. Ruth V. Small. 1997. Motivation in Motivation in Instructional Design. ERIC Digest. *ERIC Digest*: 1–7. Retrieved March 4, 2022 from www.eric.ed.gov

137. Gillian Smith, Ryan Anderson, Brian Kopleck, Zach Lindblad, Lauren Scott, Adam Wardell, Jim Whitehead, and Michael Mateas. 2011. Situating quests: Design patterns for quest and level design in role-playing games. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 326–329. https://doi.org/10.1007/978-3-642-25289-1_40

138. Aleksandra Solinska-nowak, Piotr Magnuszewski, Margot Curl, and Adam French. 2018. An overview of serious games for disaster risk management – Prospects and limitations for informing actions to arrest increasing risk International Journal of Disaster Risk Reduction An overview of serious games for disaster risk management – Prospects an. *International Journal of Disaster Risk Reduction* 31, September: 1013–1029. https://doi.org/10.1016/j.ijdrr.2018.09.001

139. Ekta Srivastava, Satish Sasalu Maheswarappa, and Bharadhwaj Sivakumaran. 2017. Nostalgic advertising in India: a content analysis of Indian TV advertisements. *Asia Pacific Journal of Marketing and Logistics* 29, 1: 47–69. https://doi.org/10.1108/APJML-10-2015-0152

140. Janine Stockdale, Marlene Sinclair, and W. George Kernohan. 2014. Applying the ARCS design model to breastfeeding advice by midwives in order to motivate mothers to personalise their experience. *Evidence Based Midwifery (EVID BASED MIDWIFERY)* 12, 1: 4–10.

141. Rosemary J. Thomas, Judith Masthoff, and Nir Oren. 2019. Can I Influence You? Development of a Scale to Measure Perceived Persuasiveness and Two Studies Showing the Use of the Scale. *Frontiers in Artificial Intelligence* 2: 24. https://doi.org/10.3389/FRAI.2019.00024

142. Michael Thomps and Cynthia Irvine. 2011. Active learning with the CyberCIEGE video game. In *4th Workshop on Cyber Security Experimentation and Test, CSET 2011*, 1–8.

143. Alexandra To, Safinah Ali, Geoff Kaufman, and Jessica Hammer. 2016. Integrating Curiosity and Uncertainty in Game Design. *Proceedings of 1st International Joint Conference of DiGRA and FDG*: 1–16.

144. Xin Tong, Ankit Gupta, Henry Lo, Amber Choo, Diane Gromala, and Christopher D Shaw. 2017. Chasing lovely monsters in the wild, exploring players' motivation and play patterns of pokémon go: Go, gone or go away? In *CSCW 2017 - Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 327–330. https://doi.org/10.1145/3022198.3026331

145. Chau Kien Tsong, Zarina Samsudin, Wan Ahmad Jaafar, and Wan Yahaya. 2017. Designing a Motivated Tangible Multimedia System for Preschoolers Emotional Design in Multimedia Learning View project Persuasive Multimedia Learning Environment View project. *Researchgate.Net* 11, 2: 451–459. Retrieved from https://www.researchgate.net/publication/313903320

146. Unity. Unity Real-Time Development Platform | 3D, 2D VR & AR Engine. Retrieved December 4, 2020 from https://unity.com/

147. Silas Formunyuy Verkijika. 2018. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers and Security* 77: 860–870. https://doi.org/10.1016/j.cose.2018.03.008

148. María Vanessa Villasana, Ivan Miguel Pires, Juliana Sá, Nuno M. Garcia, Nuno Pombo, Eftim Zdravevski, and Ivan Chorbev. 2019. CoviHealth: Novel approach of a mobile application for nutrition and physical activity management for teenagers. *ACM International Conference Proceeding Series*: 261–266. https://doi.org/10.1145/3342428.3342657

149. Patrickson Weanquoi, Jaris Johnson, and Jinghua Zhang. 2017. Using a game to teach about phishing. *SIGITE 2017 - Proceedings of the 18th Annual Conference on Information Technology Education*: 75. https://doi.org/10.1145/3125659.3125669

150. Rina R Wehbe, Elisa D Mekler, Mike Schaekermann, Edward Lank, and Lennart E. Nacke. 2017. Testing incremental difficulty design in platformer games. In *Conference on Human Factors in Computing Systems - Proceedings*, 5109–5113. https://doi.org/10.1145/3025453.3025697

151. Devon Wemyss, Roberta Castri, Vanessa De Luca, Francesca Cellina, Evelyn Lobsiger-kägi, Pamela Galbani Bianchi, and Christian Hertach. 2016. Keeping up with the Joneses : examining community-level collaborative and competitive game mecha .... *BEHAVE 2016 - 4th European Conference on Behaviour and Energy Efficiency*, September: 8–9. Retrieved from http://www.zhaw.chhttp//www.supsi.ch

152. Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. *Conference on Human Factors in Computing Systems - Proceedings*: 1–12. https://doi.org/10.1145/3290605.3300338

153. Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android permissions remystified: A field study on contextual integrity. In *Proceedings of the 24th USENIX Security Symposium*, 499–514. https://doi.org/10.5281/zenodo.3264702

154. Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences. *Proceedings - IEEE Symposium on Security and Privacy*: 1077–1093. https://doi.org/10.1109/SP.2017.51

155. Meredydd Williams, Jason R.C. Nurse, and Sadie Creese. 2019. (Smart)Watch Out! encouraging privacy-protective behavior through interactive games. *International Journal of Human Computer Studies* 132: 121–137. https://doi.org/10.1016/j.ijhcs.2019.07.012

156. Tim Wulf, Nicholas David Bowman, John A. Velez, and Johannes Breuer. 2018. Once Upon a Game: Exploring Video Game Nostalgia and Its Impact on Well-Being. *Psychology of Popular Media Culture*, October. https://doi.org/10.1037/ppm0000208

157. Affan Yasin, Lin Liu, Tong Li, Rubia Fatima, and Wang Jianmin. 2019. Improving software security awareness using a serious game. *IET Software* 13, 2: 159–169. https://doi.org/10.1049/iet-sen.2018.5095

158. Johnathan Yerby. 2014. Development Of Serious Games For Teaching Digital Forensics. *Issues in Information Systems* 13, 2: 112–122.

159. Ming-Hsiung Ying and Kai-Ting Yang. 2013. A Game-based Learning System using the ARCS Model and Fuzzy Logic. https://doi.org/10.4304/jsw.8.9.2155-2162

160. Nima Zargham, Mehrdad Bahrini, Georg Volkmar, Karsten Sohr, Dirk Wenig, and Rainer Malaka. 2019. What could go wrong? Raising mobile privacy and security awareness through a decision-making game. *CHI PLAY 2019 - Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play*: 805–812. https://doi.org/10.1145/3341215.3356273

161. Xiao Juan Zhang, Zhen Li, and Hepu Deng. 2017. Information security behaviors of smartphone users in China: An empirical analysis. *Electronic Library* 35, 6: 1177–1190. https://doi.org/10.1108/EL-09-2016-0183

162. Man Zhou, Qian Wang, Jingxiao Yang, Qi Li, Feng Xiao, Zhibo Wang, and Xiaofeng Chen. 2018. PatternListener: Cracking android pattern lock using acoustic signals. In *Proceedings of the ACM Conference on Computer and Communications Security*, 1775–1787. https://doi.org/10.1145/3243734.3243777

163. Yajin Zhou and Xuxian Jiang. 2012. Dissecting Android malware: Characterization and evolution. *Proceedings - IEEE Symposium on Security and Privacy*, 4: 95–109. https://doi.org/10.1109/SP.2012.16

164. What even is a “retro game” anymore? Retrieved July 1, 2022 from https://www.inputmag.com/gaming/what-even-is-a-retro-game-anymore

165. Indie game - Wikipedia. Retrieved July 1, 2022 from https://en.wikipedia.org/wiki/Indie_game

166. The official home of Super Mario^{TM} – Home. Retrieved January 11, 2021 from https://mario.nintendo.com/

167. Dangerous Dave - Wikipedia. Retrieved November 6, 2021 from https://en.wikipedia.org/wiki/Dangerous_Dave

168. Mega Man - Wikipedia. Retrieved November 6, 2021 from https://en.wikipedia.org/wiki/Mega_Man

169. Claw (video game) - Wikipedia. Retrieved November 6, 2021 from https://en.wikipedia.org/wiki/Claw_(video_game)

170. ACM Digital Library. Retrieved February 15, 2022 from https://dl.acm.org/

171. Google Scholar. Retrieved February 15, 2022 from https://scholar.google.ca/

172. Google. Retrieved February 15, 2022 from https://www.google.ca/

173. The Visual Collaboration Platform for Every Team | Miro. Retrieved July 2, 2022 from https://miro.com/index/

174. Android | The platform pushing what's possible. Retrieved May 19, 2021 from https://www.android.com/intl/en_ca/

175. Manifest.permission_group | Android Developers. Retrieved December 3, 2020 from https://developer.android.com/reference/android/Manifest.permission_group

176. Request app permissions | Android Developers. Retrieved January 2, 2021 from https://developer.android.com/training/permissions/requesting

177. Android 12 Privacy & Security. Retrieved November 5, 2021 from https://www.android.com/android-12/#a12-safe

178. (No Title). Retrieved May 21, 2021 from https://www.cyberswachhtakendra.gov.in/documents/Mobile_phone_Security.pdf

179. What is User Centered Design? | Interaction Design Foundation (IxDF). Retrieved December 19, 2021 from https://www.interaction-design.org/literature/topics/user-centered-design

180. How Many People Have Smartphones Worldwide (Feb 2022). Retrieved February 3, 2022 from https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

181. • Smartphone users 2026 | Statista. Retrieved February 3, 2022 from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

182. • Android versions market share 2019 | Statista. Retrieved January 3, 2021 from https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

183. • Mobile OS market share 2021 | Statista. Retrieved February 3, 2022 from https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

184. • Top devices for gaming 2021 | Statista. Retrieved February 3, 2022 from https://www.statista.com/statistics/533047/leading-devices-play-games/

185. Luang Prabang - Wikipedia. Retrieved February 7, 2022 from https://en.wikipedia.org/wiki/Luang_Prabang

186. English for kids at home | EMYS Robot. Retrieved March 2, 2022 from https://www.emys.co/

187. Draw Freely | Inkscape. Retrieved November 6, 2021 from https://inkscape.org/

188. Proto.io - Prototyping for all. Retrieved February 20, 2021 from https://proto.io/

189. Pokémon FireRed and LeafGreen - Wikipedia. Retrieved March 9, 2022 from https://en.wikipedia.org/wiki/Pokémon_FireRed_and_LeafGreen

190. Diablo (video game) - Wikipedia. Retrieved March 9, 2022 from https://en.wikipedia.org/wiki/Diablo_(video_game)

191. Unity Asset Store - The Best Assets for Game Making. Retrieved March 11, 2022 from https://assetstore.unity.com/

192. Download the latest indie games - itch.io. Retrieved March 11, 2022 from https://itch.io/

193. 2.5 million+ Stunning Free Images to Use Anywhere. Retrieved March 11, 2022 from https://pixabay.com/

194. Purple Planet Royalty Free Music. Retrieved February 19, 2021 from https://www.purple-planet.com/

195. Quantitative Research for new user researchers - How to be a Games User Researcher. Retrieved November 28, 2021 from https://gamesuserresearch.com/2021/07/19/quantitative-research-for-new-user-researchers/

196. Snowball sampling - Wikipedia. Retrieved July 1, 2022 from https://en.wikipedia.org/wiki/Snowball_sampling

197. • U.S. video gamer gender statistics 2021 | Statista. Retrieved June 7, 2022 from https://www.statista.com/statistics/232383/gender-split-of-us-computer-and-video-gamers/

198. Perma-Run – Apps on Google Play. Retrieved June 5, 2022 from https://play.google.com/store/apps/details?id=com.PCLab.PermaRun

199. 2020. *NSA Mobile Device Best Practices*. https://doi.org/10.4324/9780429269110-11

Appendix A. Permission To Use

In presenting this thesis in partial fulfilment of the requirements for master's in computer science degree from the Dalhousie University, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the Dalhousie University in any scholarly use which may be made of any material in my thesis.

Requests for permission to copy or to make other use of the material in this thesis in whole or part should be addressed to:

Head of the Faculty of Computer Science
6050 University Ave,
Dalhousie University,
Halifax, Nova Scotia, Canada B3H 1W5

Appendix B. Pre-Study Survey Questions

Section1: Demographics (age, gender, education, frequently played genre of games, preferred gaming platform)

Section2: PMT Questionnaire

Scale for each item: 1(Strongly Disagree) 2(Disagree) 3(Neutral) 4(Agree) 5(Strongly Agree)

Self-efficacy

- I feel comfortable taking measures to secure my smartphone
- I have the resources and the knowledge to take the necessary security measures on my smartphone
- Taking the necessary security measures on my smartphone is easy
- I can enable security measures on my smartphone by myself

Response Efficacy

- Enabling security measures on my smartphone will prevent security breaches
- Implementing security measures on my smartphone is an effective way to prevent hackers
- Enabling security measures on my smartphone will prevent hackers from stealing my identity
- The preventative measures available to stop people from getting confidential personal or financial information on my smartphone are effective

Response cost

- Taking smartphone security measures inconveniences me
- Taking security measures on my smartphone would require considerable investment of effort
- Implementing security measures on my smartphone would be time-consuming
- The cost of implementing recommended security measures on my smartphone exceeds the benefits

Perceived vulnerability

- I could be vulnerable to a serious information security threat on my smartphone
- I am facing more and more information security threats on my smartphone
- I feel that my smartphone could be vulnerable to a security threat

- I could fall victim to a malicious attack if I fail to follow good smartphone security practices

Perceived Severity

- A security breach on my smartphone would be a serious problem for me
- Loss of information resulting from hacking would be a serious problem for me
- Having my confidential information on my smartphone accessed by someone without my consent or knowledge would be a serious problem for me

Anticipated Regret

- There is a high probability that I would regret it, if I failed to secure my smartphone
- I would feel very worried if my smartphone is not secured
- If I left my phone somewhere, without it being secure (e.g., password protected) I would regret it.

SecurityIntentions

- I am likely to take security measures on my smartphone
- It is possible that I will take security measures to protect my smartphone
- I am certain that I will take security measures to protect my smartphone

Security behavior

I have installed security software on my smartphone

[ ]Yes [ ] No

I have recent backups of my smartphone

[ ]Yes [ ] No

I have enabled automatic updates for my smartphone software

[ ]Yes [ ] No

I regularly use security software (anti-virus/anti malware/VPN)

[ ]Yes [ ] No

My smartphone is secured by a password or another authentication method (e.g., fingerprint)

[ ]Yes [ ] No

Section3: SSBS Questionnaire

Note: T- Technical S- Social, measured on a scale of 1(Never) to 5(Always)

T1 I reset my Advertising ID on my smartphone.

[ ]1 (Never) [ ]2 (Rarely) [ ]3 (Sometimes) [ ]4 (Mostly) [ ]5 (Always)

T2 I hide device in my smartphone's Bluetooth settings.

T3 I change my passcode/PIN for my smartphone's screen lock at a regular basis.

T4 I manually cover my smartphone's screen when using it in the public area (e.g., bus or subway).

T5 I use an adblocker on my smartphone.

T6 I use an anti-virus app.

T7 I use a Virtual Private Network (VPN) app while connected to a public network.

T8 I turn off WiFi on my smartphone when not actively using it.

S1 I care about the source of the app when performing financial and/or shopping tasks on that app.

S2 When downloading an app, I check that the app is from the official/expected source.

S3 Before downloading a smartphone app I ensure the download is from official application stores.

S4 I verify the recipient/sender before sharing text messages or other information using smartphone apps.

S5 I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.

Section4: Permission Scenario

Imagine you are about to install an online music player app. These are the features the app: ***Local Music Recommendation (recommends popular music from your region), Voice Search (Use your voice to search for songs), Download Songs(Download music for offline experience), Concerts Happening Near you (Get notified about concerts happening near you)***.

Select the permissions that would be required for these features:

☐ Activity Recognition (Allows app to recognize physical activity)

☐ Calendar (Allows to read and write in your calendar)

☐ Camera (Allows access to Camera)

☐ Contacts (Allows the app to read contacts in your phone)

☐ Location (Allows location access)

☐ Mic (Allows microphone access to the app)

☐ Phone (Allows the app to make calls)

☐ Sensors (Eg: Heartrate Sensor)

☐ SMS (Read & Write SMS)

☐ Storage (Read & Write to Storage)

Section5: Regulatory Focus Questionnaire

This set of questions asks you HOW FREQUENTLY specific events actually occur or have occurred in your life. Please indicate your answer on a scale of 1(never or seldom) to 5 (very often)

1. Compared to most people, are you typically unable to get what you want in life?
(1) [ ] Never or Seldom (2)[ ] (3)[ ] Sometimes (4)[ ] (5)[ ] very often

2. Growing up, would you ever "cross the line" by doing things that your parents would not tolerate?

3. How often have you accomplished things that got you "psyched" to work even harder?

4. Did you get on your parents' nerves often when you were growing up?

5. How often did you obey rules and regulations that were established by your parents?

6. Growing up, did you ever act in ways that your parents' thought were objectionable?

7. Do you often do well at different things that you try?

8. Not being careful enough has gotten me into trouble at times

9. When it comes to achieving things that are important to me, I find that I don't perform as well as I ideally would like to do.

10. I feel like I have made progress towards being successful in my life

11. I have found very few hobbies or activities in my life that capture my interest or motivate me to put effort into them.

The RFQ yields independent scores for Promotion and Prevention, both ranging from 1-5. There are 3 reverse-scored questions for the promotion subscale and 4 reverse-scored questions for the prevention subscale.

Six questions quantify Promotion and five questions quantify Prevention Therefore, the promotion sums must be divided by 6, and the prevention sums must be divided by 5 in order to place scores for both orientations on the same 1-5 scale:

$\textit{Promotion} = [\,(6 - Q1) + Q3 + Q7 + (6 - Q9) + Q10 + (6 - Q11)\,] / 6$

$\textit{Prevention} = [\,(6 - Q2) + (6 - Q4) + Q5 + (6 - Q6) + (6 - Q8)\,] / 5$

The mean score of prevention focus items are subtracted from the mean score of promotion focus items. The RFQ results in a single continuous measure, with positive numbers indicating predominant promotion focus and negative numbers indicating predominant prevention focus.

Section6: Participant's email-id for forwarding the game, Participant-Id (auto-generated)

Appendix C. Post Survey Questions

Section1: Email-Id and Participant Id
Section2: Player Experience (IMI) measure on a scale of 1(Not at all True) to 7(Very True)

Interest/Enjoyment
I enjoyed playing this game very much
This game was fun to play
I thought this was a boring game
This game did not hold my attention at all
I would describe this game as very interesting
I thought this game was quite enjoyable
While I was playing this game, I was thinking about how much I enjoyed it

Effort/Importance
I put a lot of effort into this game
I didn't try very hard to do well in this game
I tried very hard to play this game
It was important to me to do well at this game
I didn't put much energy into this game

Pressure/Tension
I did not feel nervous at all while playing this game
I felt very tense while playing this game
I was very relaxed while playing this game
I was anxious while playing this game
I felt pressured while playing this game

Value/Usefulness
I believe this activity could be of some value to me
I think that doing this activity is useful for improving my awareness about secure smartphone behaviour
I think this is important to do because I can learn to protect myself from smartphone related threats
I would be willing to do this again because it has some value to me
I think playing this game could help me to change my current secure smartphone behaviour
I believe playing this game could be beneficial to me
I think this is an important game

Perceived Competence
I think I am pretty good at this game
After playing this game for a while, I felt pretty competent
I am satisfied with my performance at this game
I was pretty skilled at this game
This was a game that I couldn't play very well

Perceived Choice
I believe I had some choice about playing this game
I felt like it was not my own choice to play this game
I didn't really have a choice about playing this game

I felt like I had to play this game
I played this game because I had no choice
I played this game because I wanted to
I played this game because I had to

Section3: ARCS, measured on a scale of 1 (Strongly Disagree) to 5 (Strongly Agree)

Attention

This game captures and holds my attention
This game has some contents that stimulate my curiosity

Relevance

This game is relevant to me
I am able to relate with the contents of this game
The contents of this game make sense to me
The contents of this game are useful to me

Confidence

It was easy to understand and use this system
The game would help me improve my smartphone security awareness
This game built my confidence in my ability to improve my secure smartphone behaviour and protect myself from threats related to smartphones

Satisfaction

I really enjoyed using this game
It was a pleasure to use a game like this
This game would help me accomplish my behaviour goal (improved awareness about smartphone security practices)

Section4: PMT

Scale for each item: 1(Strongly Disagree) 2(Disagree) 3(Neutral) 4(Agree) 5(Strongly Agree)

Self-efficacy

- I feel comfortable taking measures to secure my smartphone
- I have the resources and the knowledge to take the necessary security measures on my smartphone
- Taking the necessary security measures on my smartphone is easy
- I can enable security measures on my smartphone by myself

Response Efficacy

- Enabling security measures on my smartphone will prevent security breaches
- Implementing security measures on my smartphone is an effective way to prevent hackers
- Enabling security measures on my smartphone will prevent hackers from stealing my identity

- The preventative measures available to stop people from getting confidential personal or financial information on my smartphone are effective

Response cost

- Taking smartphone security measures inconveniences me
- Taking security measures on my smartphone would require considerable investment of effort
- Implementing security measures on my smartphone would be time-consuming
- The cost of implementing recommended security measures on my smartphone exceeds the benefits

Perceived vulnerability

- I could be vulnerable to a serious information security threat on my smartphone
- I am facing more and more information security threats on my smartphone
- I feel that my smartphone could be vulnerable to a security threat
- I could fall victim to a malicious attack if I fail to follow good smartphone security practices

Perceived Severity

- A security breach on my smartphone would be a serious problem for me
- Loss of information resulting from hacking would be a serious problem for me
- Having my confidential information on my smartphone accessed by someone without my consent or knowledge would be a serious problem for me

Anticipated Regret

- There is a high probability that I would regret it, if I failed to secure my smartphone
- I would feel very worried if my smartphone is not secured
- If I left my phone somewhere, without it being secure (e.g., password protected) I would regret it.

Security Intentions

- I am likely to take security measures on my smartphone
- It is possible that I will take security measures to protect my smartphone

I am certain that I will take security measures to protect my smartphone

Section5: SSBS
Note: T- Technical S- Social, measured on a scale of 1(Never) to 5(Always)

T1 I reset my Advertising ID on my smartphone.

[ ]1 (Never) [ ]2 (Rarely) [ ]3 (Sometimes) [ ]4 (Mostly) [ ]5 (Always)

T2 I hide device in my smartphone’s Bluetooth settings.

T3 I change my passcode/PIN for my smartphone’s screen lock at a regular basis.

T4 I manually cover my smartphone’s screen when using it in the public area (e.g., bus or subway).

T5 I use an adblocker on my smartphone.

T6 I use an anti-virus app.

T7 I use a Virtual Private Network (VPN) app while connected to a public network.

T8 I turn off WiFi on my smartphone when not actively using it.

S1 I care about the source of the app when performing financial and/or shopping tasks on that app.

S2 When downloading an app, I check that the app is from the official/expected source.

S3 Before downloading a smartphone app I ensure the download is from official application stores.

S4 I verify the recipient/sender before sharing text messages or other information using smartphone apps.

S5 I delete any online communications (i.e., texts, emails, social media posts) that look suspicious.

Section6: Permission Scenario
Imagine you are about to install an online music player app. These are the features the app: ***Local Music Recommendation (recommends popular music from your region), Voice Search (Use your voice to search for songs), Download Songs(Download music for offline experience), Concerts Happening Near you (Get notified about concerts happening near you)***.

Select the permissions that would be required for these features:

☐ Activity Recognition (Allows app to recognize physical activity)

☐ Calendar (Allows to read and write in your calendar)

☐ Camera (Allows access to Camera)

☐ Contacts (Allows the app to read contacts in your phone)

☐ Location (Allows location access)

☐ Mic (Allows microphone access to the app)

☐ Phone (Allows the app to make calls)

☐ Sensors (Eg: Heartrate Sensor)

☐ SMS (Read & Write SMS)

☐ Storage (Read & Write to Storage)

Section7: Perceived Persuasiveness, measured on a scale of 1 (Strongly Disagree) to 7 (Strongly Agree)

1. This strategy influences me to follow secure smartphone behaviour to protect myself from smartphone security and privacy threats
2. This strategy convinces me to improve my current secure smartphone behaviour
3. This strategy is personally relevant to me
4. This strategy makes me reconsider my current secure smartphone behaviour
5. This strategy motivates me to keep playing the game

Appendix D. Interview Questions

1. What was your first impression when you opened the game?
2. How were the game controls?
3. What was your favourite part of the game?
4. Is there something that you did not like in the game? Why?
5. How did you feel when you first encountered the story?
6. Were there any places in the game that you were not able to reach?/ Did you find any hidden areas in-game? (how did you feel when you discovered them?)
7. what motivated you to play the game again?
8. what stopped you from playing the game?/ What made you to exit the game?
9. How do you feel about playing a game for improving awareness about smartphone security?
10. Can you tell me about how the game tries to teach about smartphone security?
11. How was the in-game quiz?
12. Which specific security or privacy concept stood out for you in the game?
13. Did you learn any new thing about smartphone security from playing the game and what did you learn?
14. What do you think about learning smartphone permissions through a game?
15. Did you try out any of the security recommendations that you read in the game?
16. How was the game tutorial?
17. What are your thoughts on the leaderboard feature?
18. How was the User profile page on the main menu?
19. What do you think about the game's difficulty?
20. If you had the chance to make changes to the game, what would you do?
21. Do you have any recommendation for improving the game in terms of its content and functionality/presentation?
22. Do you have any other feedback?

Appendix E. Sample Game Screenshots

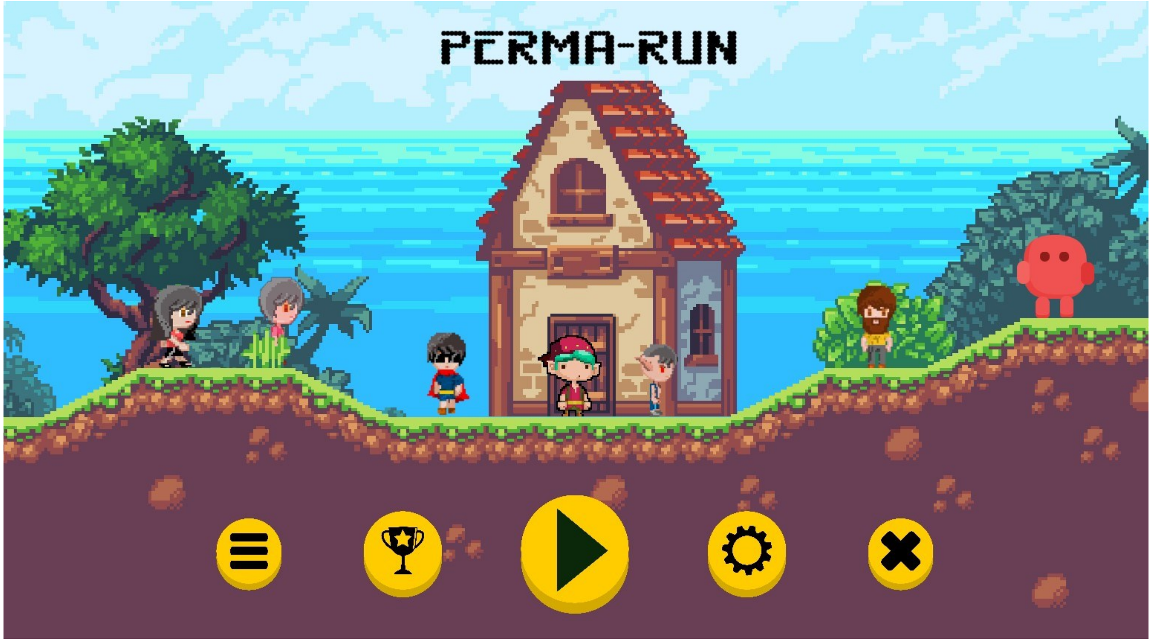
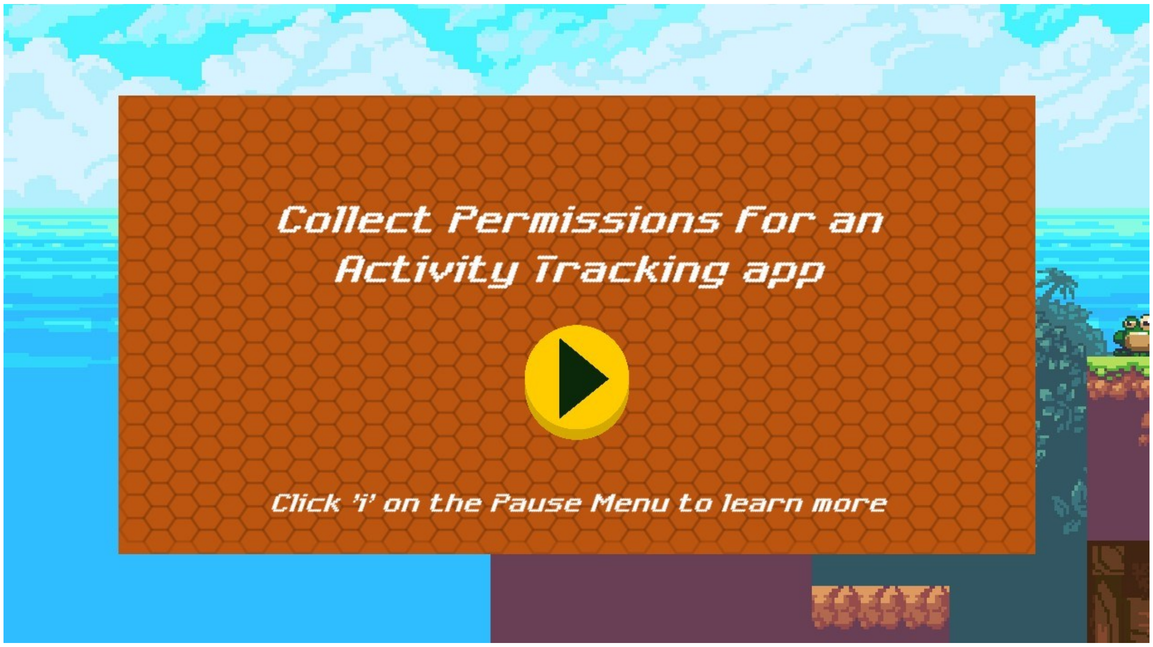


Figure E.1: Game Main Menu Screen


Collect Permissions for an Activity Tracking app

Click 'i' on the Pause Menu to learn more

Figure E.2: Beginning of a Level

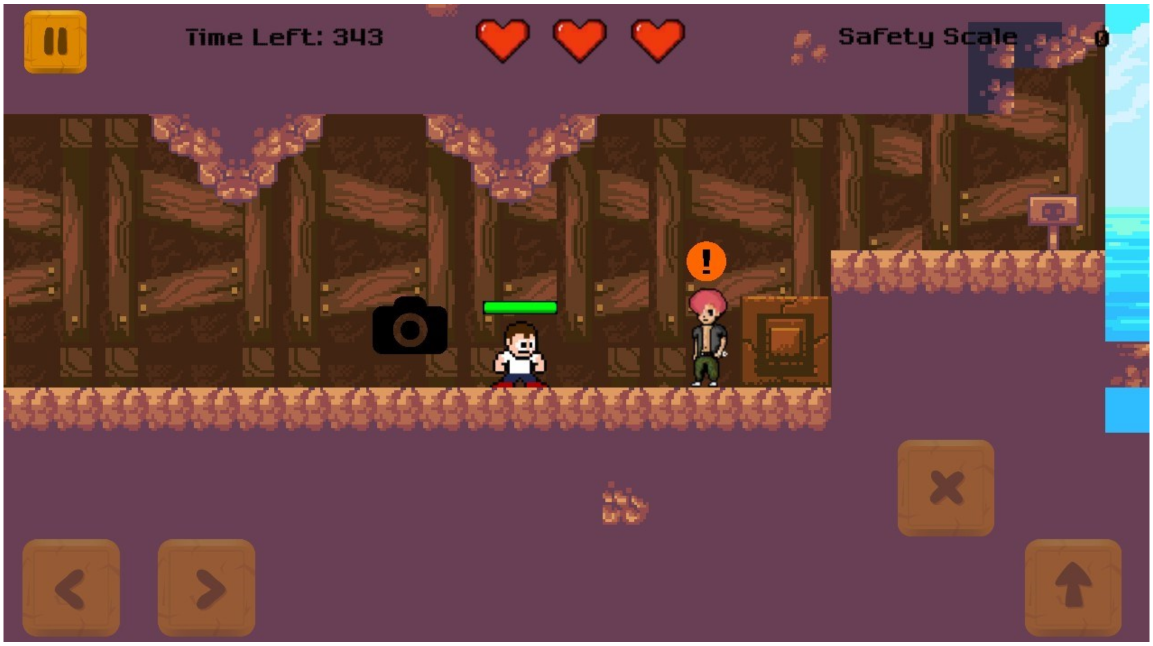


Figure E.3: In-game Screenshot of an NPC waiting for help

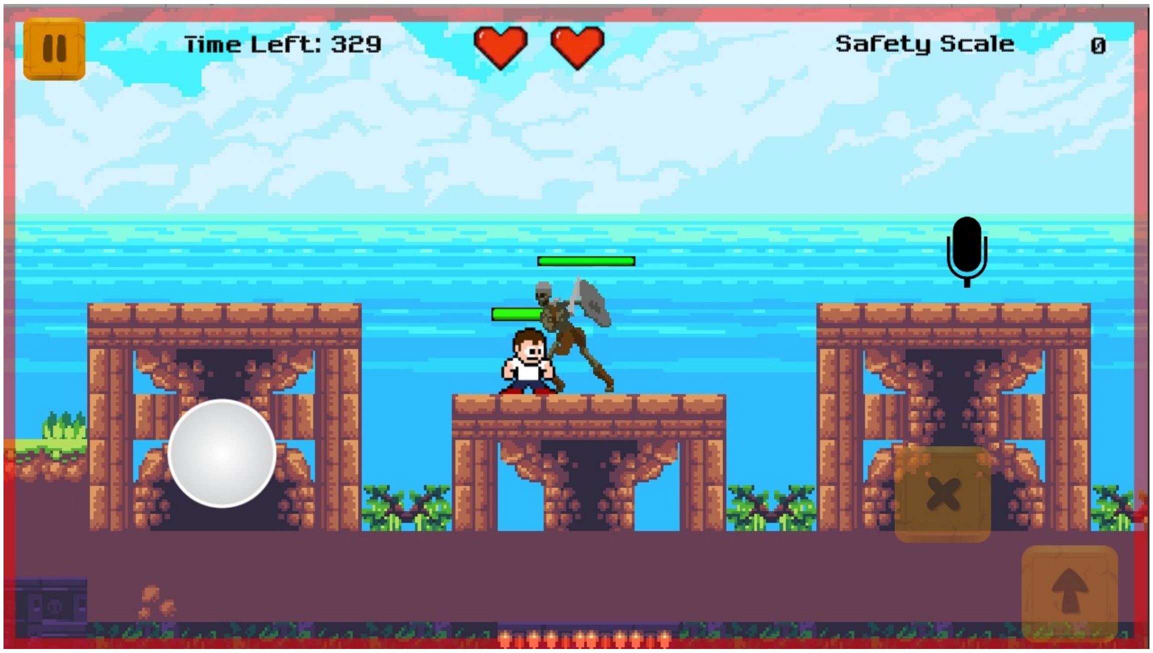


Figure E.4: Player getting hit by an Enemy (Red border is a hit indicator)

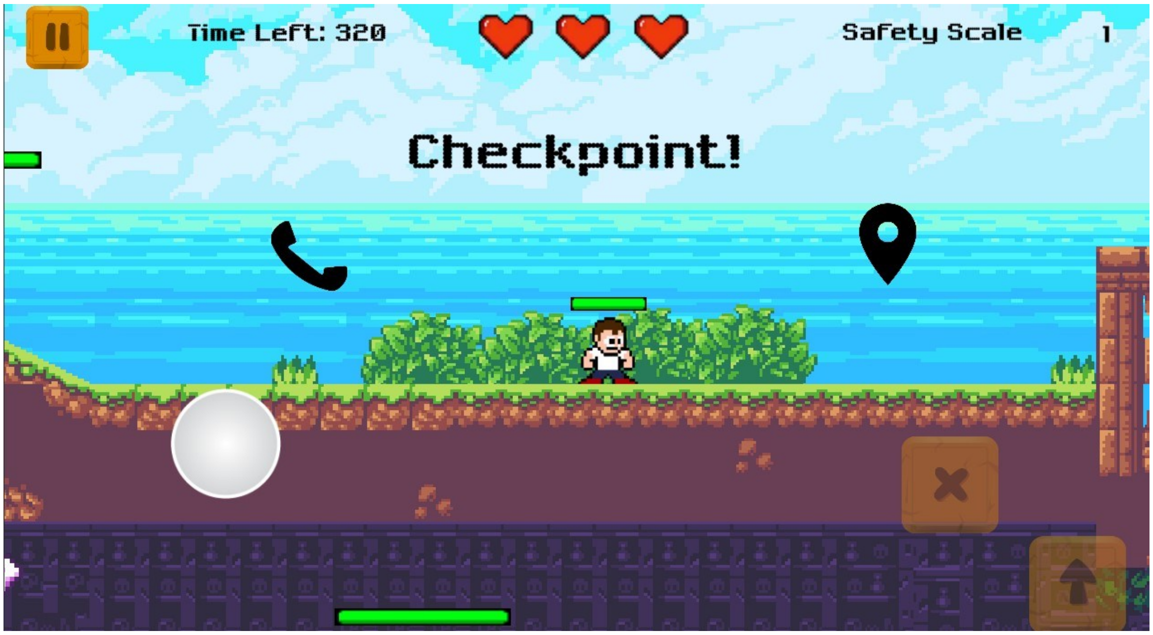
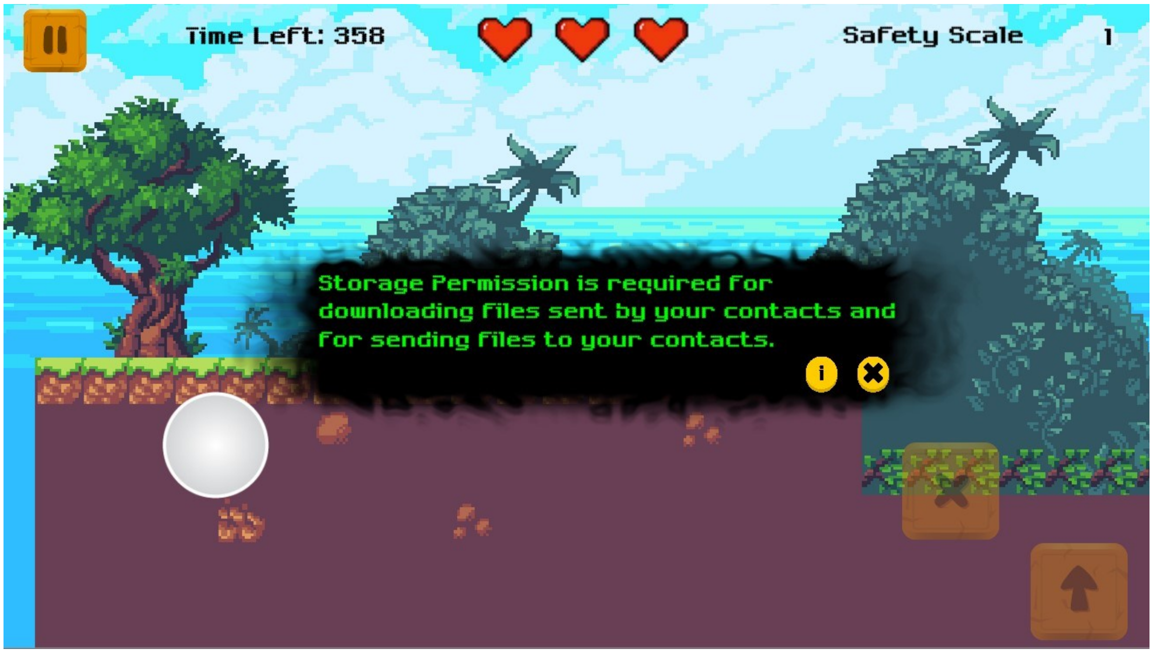
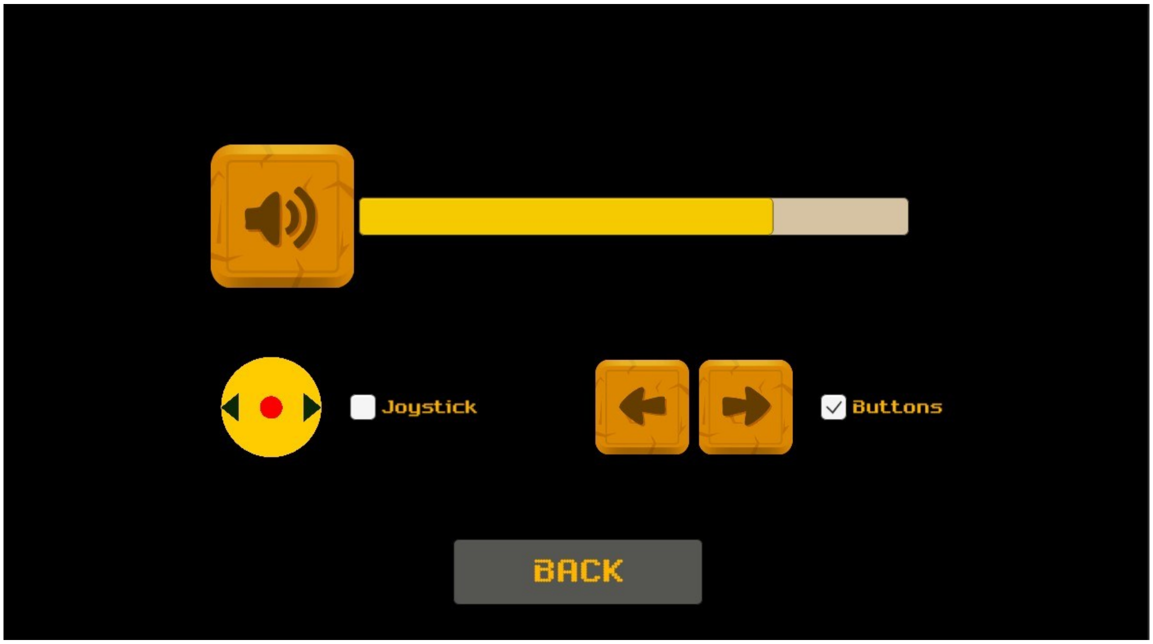


Figure E.5: In-game Checkpoint



Storage Permission is required for downloading files sent by your contacts and for sending files to your contacts.

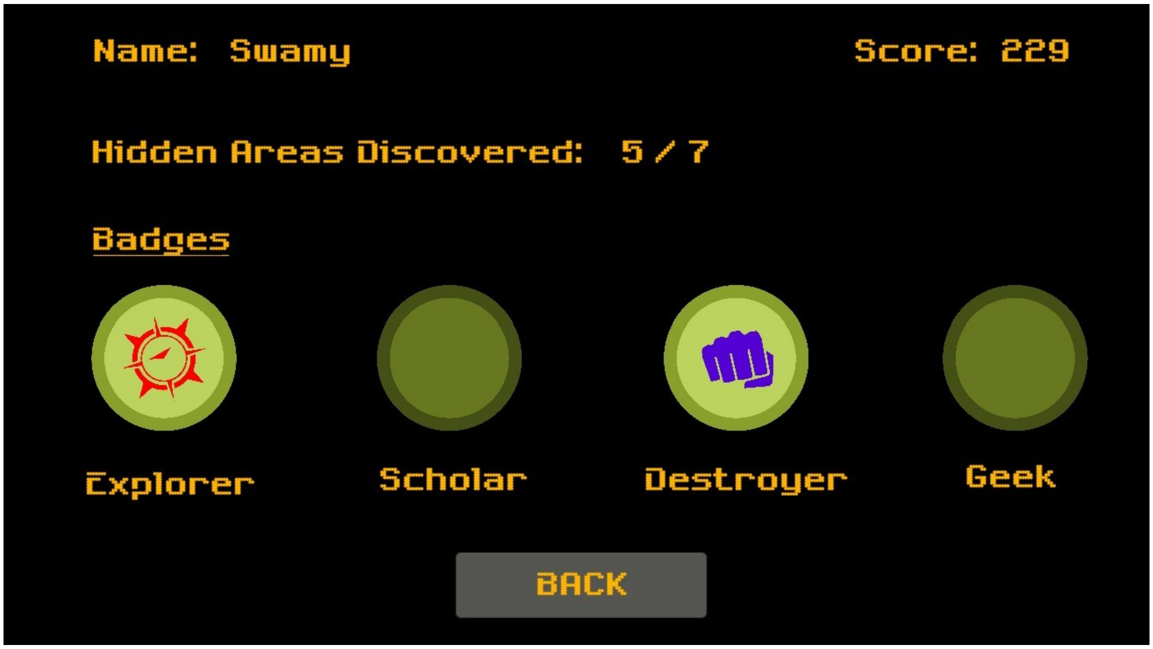
Figure E.6: In-game Suggestion for picking up a Permission



□ Joystick

☑ Buttons

Figure E.7: Settings Menu

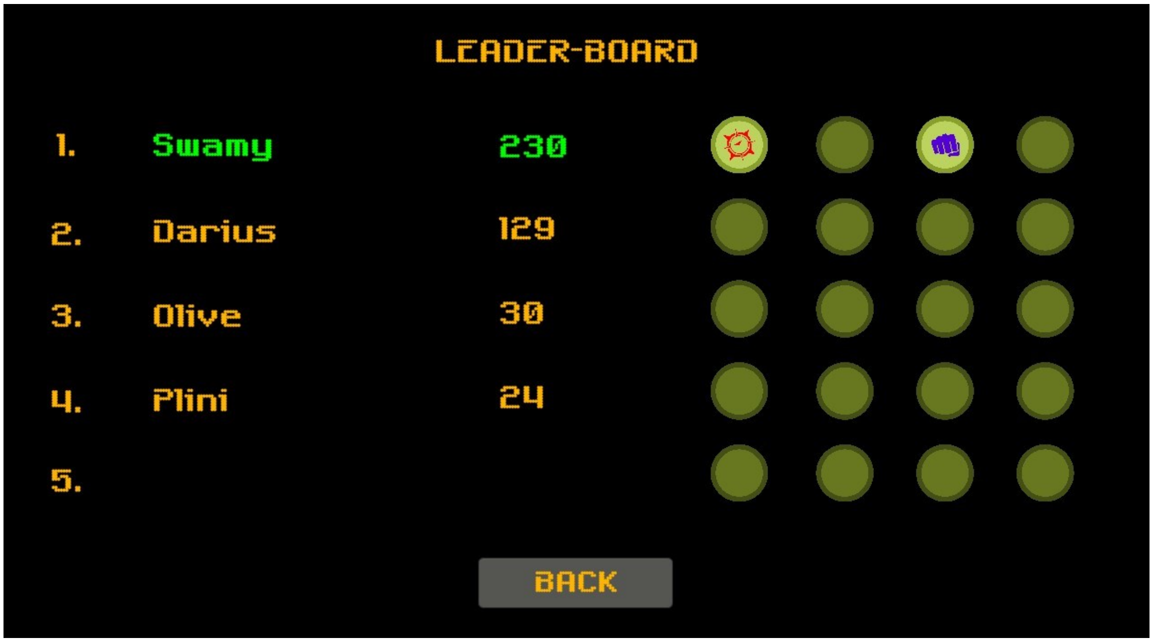


Name: Swamy

Score: 229

Hidden Areas Discovered: 5 / 7

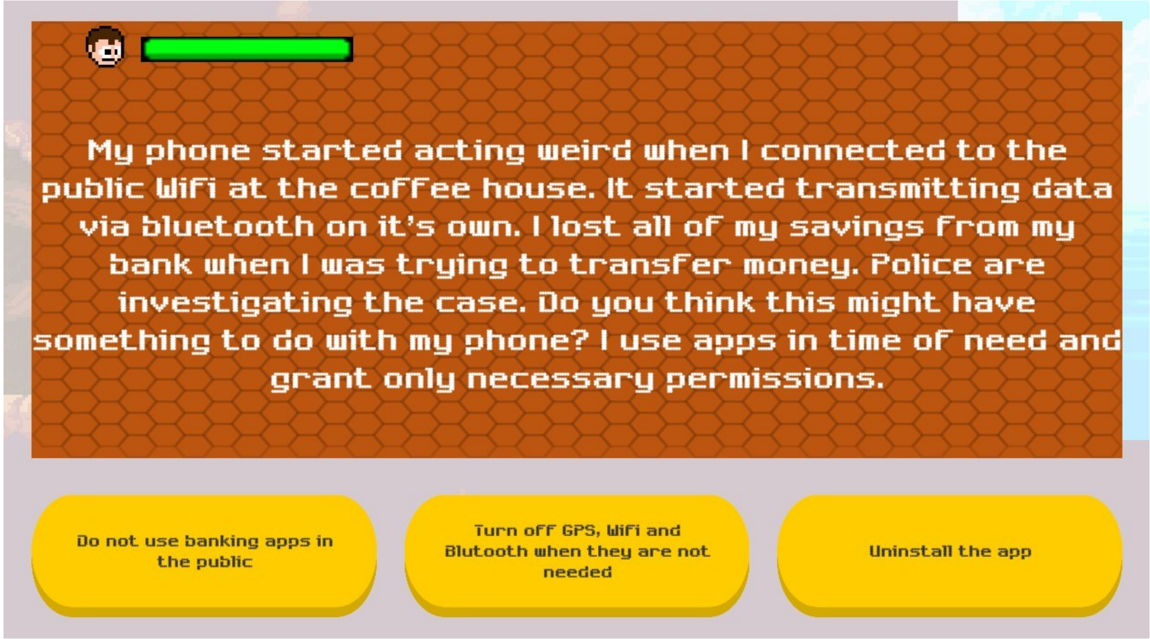
Figure E.8: User Profile



LEADER-BOARD

1.	Swamy	230
2.	Darius	129
3.	Olive	30
4.	Plini	24
5.		

Figure E.9: Leaderboard Screen



My phone started acting weird when I connected to the public Wifi at the coffee house. It started transmitting data via bluetooth on it's own. I lost all of my savings from my bank when I was trying to transfer money. Police are investigating the case. Do you think this might have something to do with my phone? I use apps in time of need and grant only necessary permissions.

- Do not use banking apps in the public
- Turn off GPS, Wifi and Blutooth when they are not needed
- Uninstall the app

Figure E.10: In-game Quiz

Appendix F. In-game Quiz Scenarios

Table F.1 – In-game Quiz Scenarios

Security Scenario (Game Character)	**Promotion Focus Suggestion**	**Prevention Focus Suggestion**
Allowing only necessary Permission for an App (Level1, Honey-Bee)	By granting only necessary permissions, you would be safe from misuse of personal data.	If you grant unnecessary permissions, your personal data might be misused.
Setting up a Lockscreen to avoid unauthorized physical access to phone (Level1, Rabbit)	If you setup a lock screen, you would be safe from unauthorised access and data theft.	If you do not setup a lock screen, you would be vulnerable to unauthorised access and data theft.
Downloading apps from 3rd party app store/marketplace (Level1, Grasshopper)	If you avoid installing apps from 3rd party app stores, you would be safe from malware, data theft and misuse of data.	If you install apps from 3rd party app stores, you might be prone to malware, data theft and misuse of data.
Background app process (Level1, Fairy)	If you install only apps that you need, you can avoid malware intrusion. Close the apps when not in use to avoid background tracking of data.	If you Install unnecessary apps, malware might infiltrate your phone. If you don't Close apps when not in use, your data might be tracked in background.
Turning off WiFi, GPS, Bluetooth when not in use (Level2, Hunter)	If you turn off Bluetooth, Wifi, GPS when they aren't required, you would be safe from location tracking, data theft and eavesdropping.	If you do not turn off Bluetooth, GPS, Wifi when they are not required, then you would be vulnerable to location tracking, data theft and eavesdropping.

Using a VPN (Level2, Fox)	If you use VPN while connecting to unknown networks, you would be safe from eavesdropping and data theft.	If you connect to unknown wireless networks without a VPN, you might be vulnerable to eavesdropping and data theft.
Clicking on unknown links from unknown senders. (Level2, Squirrel)	If you avoid clicking on unknown links from unknown sources, you would be safe from malware and phishing links.	If you click on unknown links from unknown sources, you might be vulnerable to malware and phishing links.
Antivirus (Level2, Ant)	If you install an anti-virus on your phone, you would be safe from malware and harmful files.	If you do not install an anti-virus on your phone, you would be vulnerable to malware and harmful files.
OS Update (Level3, Pink)	If you update your phone's OS regularly, you would be much safer from malware attacks due to security holes in the OS.	If you do not update your Phone's OS regularly, you might be vulnerable to malware attacks due to security pitfalls in the OS.
Regular Data Backup (Level3, Totem)	If you backup your phone's data regularly, you need not worry about losing access to your data even if you lose your phone.	If you do not backup your phone's data regularly, you might be vulnerable to losing your data when you lose your phone.
Factory Reset while disposing Phone (Level3, Astronaut)	If you wipe your phone's data before disposing it, chances of data misuse by perpetrators will be less.	If you don't wipe your phone's data before disposing it, it might be misused by perpetrators.

Remote Lock & Wipe (Level3, Frog)	If you activate remote lock and wipe, you can prevent data theft and misuse when you lose your phone	If you don't activate remote lock and wipe, you might be vulnerable to data theft and misuse when you lose your phone

Appendix G. Research Ethics Board Approval Letter

Social Sciences & Humanities Research Ethics Board
Letter of Approval

July 28, 2021
Anirudh Ganesh
Computer Science\Computer Science

Dear Anirudh,

REB #: 2021-5672
Project Title: PERMARUN - A Persuasive Game to Improve User Awareness and Self-Efficacy Towards Secure Smartphone Behaviour

Effective Date: July 28, 2021
Expiry Date: July 28, 2022
The Social Sciences & Humanities Research Ethics Board has reviewed your application for research involving humans and found the proposed research to be in accordance with the Tri-Council Policy Statement on *Ethical Conduct for Research Involving Humans.* This approval will be in effect for 12 months as indicated above. This approval is subject to the conditions listed below which constitute your on-going responsibilities with respect to the ethical conduct of this research.

Effective March 16, 2020: Notwithstanding this approval, any research conducted during the COVID-19 public health emergency must comply with federal and provincial public health advice as well as directives from Dalhousie University (and/or other facilities or jurisdictions where the research will occur) regarding preventing the spread of COVID-19.
Sincerely,

Dr. Karen Foster, Chair