

# The Design and Development of Mobile Game to Promote Secure Smartphone Behaviour

Anirudh Ganesh, Chinenye Ndulue, and Rita Orji

Faculty of Computer Science, Dalhousie University, Canada  
{anirudh.ganesh, cndulue, rita.orji}@dal.ca

**Abstract.** Smartphones have evolved significantly in different ways over the years. Currently, Android and iOS dominate the market, followed by other operating systems. Along with the evolution of smartphones, malware, privacy, and other security issues have evolved along with it. Therefore, there is a need to develop interventions to educate and motivate users towards safe and privacy-sensitive smartphone usage behaviour while engaging with the rapidly changing features of these devices. In this paper, we introduce the design and development of a mobile persuasive game called “*PermaRun*” to improve users’ knowledge, build self-efficacy and create awareness about privacy-sensitive and security-conscious behaviours, especially as it regards to user control and handling of Android permissions and other secure smartphone behaviour. We implement nine persuasive strategies to keep the users motivated and six game design patterns to make the game engaging and more interesting for the player.

**Keywords:** Smartphone Security, Persuasive Game, Game Design Patterns, Self-efficacy, User Awareness.

## 1 Introduction

Humans are the weakest link in the chain of cybersecurity [1] and have been ignored in the initial stages while cybersecurity was being studied. In this age of ubiquitous computing, smartphones have become an integral part of everybody’s life. People take their smartphone wherever they go and use it for various day-to-day tasks, and most of the time, their personal data is involved. Over the years, there have been countless instances where the users’ personal information has been compromised without their knowledge through Android apps [2, 3]. In the recent past, various security flaws were found and patched up [4]. In recent times, Smartphones have evolved in various ways and, uniformity in design (both hardware and software) can be seen in most phones. With uniformity, the common problems were solved, yet the issue of privacy and security seemed to have evolved along with smartphone advancements.

To address these security concerns, smartphone operating systems have employed various techniques to protect user data. For example, the Android Operating System (OS) protects user data through the usage of App Permissions [5], which can be granted or denied by the users. There are two kinds of app permissions: *install-time permissions* and *runtime permissions* [5, 6]. Install-time permissions are granted automatically

Copyright © 2021 for this paper by its authors.

Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

during the installation of an application and further split into two categories, namely normal permissions, and signature permissions. Normal permissions present minimal risk to the users' privacy. Examples of normal permissions include fetching the current date and time, accessing the phone's vibrator. Signature permissions allow apps signed with the same certificate [7] to share permissions to avoid requesting the permission again. Signature permissions are commonly used when the developers declare their own permissions and want to use it in another app developed by them. Examples of signature permissions are fetching the battery status, auto-filling of forms, clearing the app's cache and so on.

Runtime permissions, also called dangerous permissions, require users' decisions since they deal with accessing sensitive data or users' personal data [5, 6]. It is the app developers' responsibility to request a specific permission for a specific functionality of an app, while users decide whether to accept or deny these requests, based on their judgements. To convince users to allow these permissions, developers may show the users why a specific permission is required [8]. Unfortunately, users often make the wrong decisions out of impulse [9], ignorance of what granting the permission entails, and do not always check the permissions and the app's functionality [10, 11]. More recent user studies [1, 12–14] show that user awareness about smartphone security and possible privacy implications are limited, and only a few people follow secure smartphone behaviours. Secure smartphone behaviour refers to the general etiquettes that are to be followed while using a smartphone to stay safe and protect oneself from malware and other kinds of security threats [1, 11–16]. Bitton et al. [10] monitored the users' smartphone behaviour using an Android app and compared it with the data that was monitored over the network and self-reported responses from the users. It was evident that the users' self-reported behaviour was different and inefficient from what was observed over the network and the mobile app. Although the users thought they were aware of what they were doing, from the data collected by the mobile app, it turned out to be the opposite. The users were giving away personal information to spam pop-ups and installed apps that required permissions that were not essential for their functionality. Zhou et al. [17] conducted a longitudinal study among 192 university students in China and found that people use smartphones more securely when their awareness, self-efficacy and social support from others are high.

As evident from prior research, user awareness about smartphone security is limited and is an essential component to improve secure smartphone behaviour. Therefore, there is a need for interventions to promote smartphone security and privacy awareness among users and persuade them to be more security conscious and privacy-sensitive when using third-party apps on their devices. An interesting intervention for achieving this aim is the use of persuasive games. Persuasive games are interactive and gameful interventions that strategically employ persuasive strategies to motivate and promote changes in human behaviour. In recent times, there have been a lot of persuasive games across various domains [18–20]. Although in the domain of cybersecurity, games that educate about smartphone security practices specifically are very sparse. Most of the existing games focus on other areas of cybersecurity, such as detecting phishing links and spam emails [21–24].

In this paper, we present the design and development of a mobile persuasive game, called *'PermaRun'*, to promote secure smartphone behaviour among users and improve their awareness about Android permissions and other secure smartphone behaviour. We also present the implementation of nine persuasive strategies from the Persuasive System Design model (PSD) as proposed by Oinas-Kukkonen et al. [25] and six game design patterns for 2D games as proposed by Khalifa et al. [26]. We conclude with key takeaways from our game design, and we discuss our future work.

## 2 Background and Related Work

Games for cybersecurity have been around for a considerable amount of time. The most popular one being CyberCIEGE [27], a game that is meant for a classroom environment to educate students in a cybersecurity course. Digital Forensics Interactive (DFI) [28], a Role-Playing Game (RPG) game that aims to educate the player about the field of digital forensics where the player takes the role of a digital forensics expert and solves a case for a company. While playing the game, the user has the opportunity to learn about the various tools used for a particular task in the field of digital forensics. Even the board games category has covered cybersecurity. “[d0x3d!]” and “Control-Alt-Hack” [29] are two such games that received positive feedback from school students and their parents for their role-playing and collaborative playing experience. Scholefield et al. [30] designed a quiz-themed mobile game that taught users about password security. However, the game was missing feedback due to which users had to depend on playing the game repetitively to learn the correct answers. Most of the recent works have been concentrating on phishing and password security [22–24, 31]. Phisher Crush [22] followed the style of a matchmaking game to educate players about identifying phishing links. The author ran a heuristic evaluation for playability and found that the users preferred immediate feedback rather than feedback towards the end of the game. Wen et al. [24] designed a game called “What.Hack” that implemented situated learning to improve the self-efficacy of the users while playing the game. The players take the role of a phishing expert to identify phishing emails for a bank. They have a rule book which they can refer to learn how to identify phishing emails. Hacked time [31] is a role-playing game where the player takes the role of a detective and helps an NPC to solve the case of password theft while learning about keeping passwords safe and secure along with other best practices. We were able to find only a handful of games for smartphone security. This might be because, in recent times, smartphones have undergone considerable evolution and, smartphone and associated security risks is a relatively new topic compared to other areas of cybersecurity.

Zargham et al. [32] designed a humorous, decision-based game to educate users about smartphone security and privacy. The author conducted a study with a between-subject design, where apart from the game, a humorous video and a serious video explaining about smartphone security and privacy issues were used for the study. It was evident from the results that the participants preferred the humorous game followed by the humorous video. However, the users also pointed out that once all the decisions are known, the game would become boring. An Android app called “HappyPermi” [33]

displayed the permissions requested by other apps installed in the users' phone along with examples of what data could be retrieved by the app if a specific permission was granted by the user. In the user study, it was found that the users were surprised to see their data being displayed in the place of example data, and most of them were concerned about their photos being accessible to the apps and also blocked contacts permission after using the "HappyPermi" [33] app. Although the app tries to point out the causes and effects of permissions, it does not educate the users why a specific permission might be necessary for an app or why it might be unnecessary and the potential harms of granting unnecessary permissions. "Make my phone secure" [34], a role-playing game, where the player takes the role of an IT security expert and helps other non-playable game characters (NPC) with their smartphone security problems that revolve around Android permission. The player must turn off appropriate permissions according to the problem statement presented to them in-game. However, the game focuses only on privacy intrusions that are visible in the foreground while using some apps.

While there is plenty of research around games for cybersecurity, very little work has been done for creating persuasive games to raise awareness around secure smartphone behaviour. Also, the games focus on Android permissions for specific apps only and thus, the user misses out on the context of permissions for other apps and is left to decide solely based on their intuition. Therefore, we present a mobile persuasive game, titled '*PermaRun*', to promote secure smartphone user behaviour and improve their awareness about Android permissions in a contextual manner.

### 3 System Design

#### 3.1 Initial Design Phase

To improve the Android permission handling awareness of the users and other secure smartphone behaviour, we designed a persuasive game called *PermaRun*. We followed the eight-step design process for creating a persuasive technology [35] to come up with a design for the initial prototype of our game. We discuss these eight steps that are summarized in five stages below.

1. **Choose a Target Behaviour.** From the background work, it is evident that there is a scarcity of interventions for secure smartphone behaviour. Hence, we selected the target behaviour as secure smartphone behaviour awareness.
2. **Choose a Target Audience.** The audience of our intervention is Android smartphone users.
3. **Find the Barriers Hindering the Target Behaviour.** Users being unaware of secure smartphone behaviour, and dangers of insecure behaviours are barriers that we identified, which we have discussed in the background work section.
4. **Choose a Technology Channel.** Persuasive games have been widely adopted and have been implemented in various domains. Little or no persuasive games exist targeted at promoting secure smartphone behaviour. Thus, we planned to design a persuasive game.

5. **Find Existing Examples of Persuasive Games, Imitate them, and Iterate.** Before starting with our game design, we analyzed various cybersecurity games and persuasive games from other domains, as discussed in our background work section. The game design went through an iterative design process and received informal feedback from potential users to arrive at the final prototype presented in this paper, for which we hope to conduct a formal evaluation in the future.

### 3.2 Game Story

To maintain the context of smartphone security and to introduce this topic to the users, we came up with a story for the game. The story revolves around Android permissions and the need for awareness to teach users about the importance of being aware of secure smartphone behaviour. We call the main game character Dillon, whose main goal is to learn all about Android permissions and associated security and privacy issues to save his friends, who have been captured by a troll. Dillon went on a camping trip with his friends, and their plans are ruined by a troll, that came out of nowhere and started attacking the group. The troll was angry with humans because it was a recent victim of data theft. Dillon found out that the troll had been using an Android Smartphone and downloaded apps from untrusted sources and was careless while granting runtime permissions to the apps and hence became a victim of data theft. Dillon promised to help the troll by selecting appropriate app permissions, but the troll did not trust humans and, hence kidnapped Dillon's friends and promised to release them if Dillon helped the troll choose appropriate permissions.

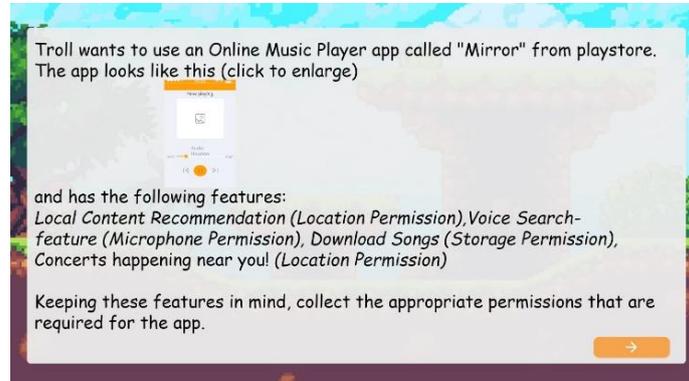
### 3.3 PermaRun Persuasive Game Description

We developed the initial prototype with the Unity Game Engine [36] and Proto.io [37], got informal feedback from the persuasive researchers of the Persuasive Computing Lab at Dalhousie University. We then used the feedback to refine and develop the main game using Unity Game Engine [36]. During the initial prototyping sessions, we decided to have various levels in our game for teaching the players about permissions. Each level simulates a scenario for a specific app for which the player must collect appropriate runtime permissions according to the app's functionality. To give a context of runtime permissions required for a specific app, we include an instruction screen (**Fig. 1**) explaining when it might be necessary for a player to accept runtime permissions and why those permissions are needed for that specific type of app. Apps require only a particular set of runtime permissions from the user to function as expected. This differs from one app to another. However, we try to highlight only the permissions that are essential for the core functionality of each type of app. Hence, we colour coded the permissions in a traffic signal format. The permissions that are green in colour are the ones that are required for an app, whereas the permissions that are red in colour are the ones that are not necessary for an apps' functionality. The main idea is that by playing the game, users learn to decide when a particular type of permission is necessary and when it is unnecessary for the functioning of the app. We plan to include a variety of apps from diverse categories for comprehensive knowledge. For example, an online

music player might need location permission from the user to recommend them with local content. Thus, for each app, we consider the core functionalities and map dangerous permissions according to the required functionality. The description of each runtime permission is available at [38]. Even though there are multiple runtime permissions, the common runtime permissions are grouped by Android [6] into 11 distinct groups. Hence, we only use permission groups [38] to maintain a real-world context. We also designed our game to resemble the old 2D game Super Mario [39], to attract a diverse audience and reduce the learning curve. Recent research suggests that past-memories and satisfaction of competence are directly affected by nostalgia, especially with retro games that are challenging and involve fast gameplay [40].

### 3.4 Game Play

Following our initial high-fidelity prototype and informal feedback from target users, we developed the first level of gameplay and used the “Online Music Streaming App” for which the player must collect the appropriate runtime permissions only. We chose the required permission groups as Microphone, Location and External Storage, which were depicted green in colour (**Fig. 2**). Apart from these, we also had other unnecessary permissions that were red in colour (**Fig. 2**). For every necessary permission that the player collects, they would gain points, and for every unnecessary permission, they would lose points and, their movement speed would be reduced for a short period. Whenever the player picks up a permission, we show them a suggestion related to secure smartphone behaviour, that is displayed in between the in-game controls, over the Heads-Up Display (HUD). The HUD shows the runtime permission symbols that are to be collected for that specific level. When the player finishes picking up a set of runtime permission, that specific permission would disappear from the HUD. When the player reaches the end of the level, they would be able to save Dillon’s friends if they manage to collect all the required runtime permission in that specific level. If the player tries to complete the level without collecting all the app permissions, a dialog box pops up, informing the player to collect all the app permissions to save Dillon’s friends. To make the game more interesting, we have obstacles, hidden areas, enemies, and other in-game items that reward the player with points. We discuss more about these in the upcoming sections.



**Fig. 1.** Instruction Screen



**Fig. 2.** Collectible Permission Symbols

### 3.5 Persuasive Principles

We built a fast-paced 2D side-scrolling game and implemented nine persuasive strategies (*Reduction, Tunnelling, Self-Monitoring, Simulation, Rewards, Suggestion, Liking, Competition, Recognition*) from the Persuasive System Design Framework [25]. We will discuss the implementation of each persuasive principle in this section.

**Self-Monitoring.** A system that helps the user to keep track of their performance to see their progress towards achieving their goals. The player has a HUD in between the in-game controls throughout the game (**Fig. 3**). This HUD shows the permissions that are required for a specific level. When the user has finished collecting a specific set of permissions, then that permission would disappear from the HUD. The HUD serves as a self-monitoring tool for the player to check if there are any other permissions left to collect for that level before completing the level. If the player tries to complete the level

without collecting all the app permissions, a dialog box pops up to inform the user to collect all the app permissions to save Dillon's friends.

**Simulation.** A system that helps the user to observe the link between causes and effects by means of simulation. All the required permissions for a specific app are green in colour, and all the unnecessary permissions are red in colour. When the user picks up a necessary permission, their score increases, but when they pick up an unnecessary permission, their score and health decrease, and the player's movement speed reduces for a short duration.

**Rewards.** A system that rewards the user for performing a specific task or target behaviour. The game currently has three rewards. When the players pick up the correct permissions or if they destroy an enemy, their score increases. Apart from this, the game has fruits that increase the player's health by a small amount. There are also extra lives in hidden areas for the player to collect. The player is transported to these hidden areas (**Fig. 4**) when they pick up a gem in the game.

**Suggestion.** A system that provides appropriate suggestions while the user is using the system. We give the users immediate feedback and tips regarding secure smartphone behaviour. Whenever the player picks up a permission, we show them tips and suggestions about secure smartphone behaviour. These suggestions are displayed in-between the in-game controller, over the HUD for a short period (**Fig. 5**).

**Liking.** A system that is visually attractive and appealing will be more persuasive. To improve the attractiveness of the game, we added sound effects for the game character and background music apart from other in-game features and animations.

**Competition.** A system that leverages the human tendency of competition will be more persuasive. We have a leaderboard (**Fig. 6**) where we rank the players according to their in-game score. This score increases as the player proceeds to successive levels. 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 destroyed.

**Recognition.** A system that offers public recognition for a user will motivate the user to adopt the target behaviour. The users get badges if they reach a specific level/score or find a hidden item. The badges that the players earn show up on the leaderboard and are visible to other players too (**Fig. 6**), and this might also serve as a normative influence.

**Reduction.** A system that reduces the number of steps for achieving a target will motivate the users. During the initial phase of the prototype design, we decided to have various in-game checkpoints (**Fig. 7**). Whenever the player loses health in the game,

they start again from the last checkpoint. This process repeats until they lose all of their three lives, and a game-over dialog box would appear if they lose all of their lives, and the player would have options to either start over or quit the game. We consider this as a reduction since the player need not repeat the whole level if they make a mistake and lose a life in the middle of the game.

**Tunnelling.** A system that guides the user in a step-by-step manner to achieve their target behaviour. There are two instances of tunnelling, one before the start of the game where the player encounters the storyline followed by an instruction screen that explains how to play the game and shows other instructions like collecting appropriate permissions and destroying enemies would increase the player's score (**Fig. 3**). Apart from the instruction screen, we placed the collectible permissions to guide the player to the end of the level.

### 3.6 Game Design Patterns

To ensure that the game is engaging and enjoyable for the players, we followed the six game design patterns (*Guidance, Foreshadowing, Safe Zone, Layering, Branching, Pace Breaking*) as specified by Khalifa et al. [26].

**Guidance.** A non-verbal game element that guides the player towards the goal or in the right direction comes under guidance. Guidance can either be the in-game path or can be in-game collectible items or an enemy that attracts the players' attention to a particular location or an environmental cue that grabs the players' attention. We used the pathways to guide the player, and we used permissions as collectibles. Enemies and items were also placed in a manner to increase the players' curiosity and guide them towards a specific path. This game design pattern can be correlated with the tunnelling persuasive principle but in a gamified manner.

**Foreshadowing.** Teasing the player with an in-game element with which they might not be able to interact or can be a game element that changes over the course of the game comes under foreshadowing. We introduced foreshadowing in two ways. We tease players with hidden areas or inaccessible game items which would be accessible to them as they proceed to play through the levels (**Fig. 4**). This design pattern increases the player's curiosity and keeps them hooked to the game. Initially, enemies are introduced in a stationary way, and later the player is introduced to patrolling enemies. This makes the game more interesting to play and might increase the players' curiosity.



**Fig. 3.** In-game Instructions



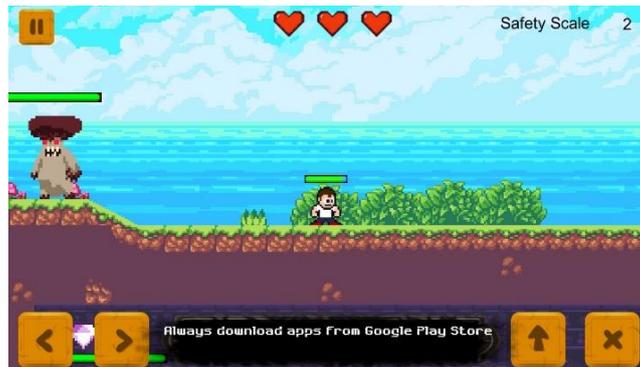
**Fig. 4.** Hidden Area underneath the player that is accessible when the player picks up a gem

**Safe Zone.** The areas in-game, where the player is not in danger and can think about their next actions or where they can take a break from all the tension that was built in-game. We treat the checkpoints in our game as safe zones, where the player is not in danger and would feel safe. We have three checkpoints in our game (**Fig. 7**) placed in such a way that the player would feel safe after exiting combat or can plan a strategy before going into combat. This pattern can be correlated with the *reduction* persuasive principle but in a gamified manner.

**Layering.** Combining multiple game elements or reusing the same game elements to introduce challenges is classified as layering. We placed enemies in-front of collectibles, positioned app permissions near enemies, and players can reach some areas only through a moving platform or platforms that are suspended in mid-air.

**Branching.** Giving the player multiple paths to explore in-game is classified as branching. If we apply constraints, where the player needs to meet specific conditions to choose another pathway, then it is called conditional branching. In our game, 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.



**Fig. 5.** In-game Suggestions



LEADERBOARD		
Martin	1350	🏆
Jessel	1200	🏆
Bauxi	1103	
Siva	1000	
Lizzy	430	

**Fig. 6.** Leaderboard



**Fig. 7.** In-game Checkpoint

**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 a long period of combat. We implement pace breaking by introducing enemies and then by giving the player a brief break from combat. We mix the layering pattern with this by adding obstacles to the paths to keep the game interesting and to keep the players engaged.

## 4 Conclusion and Future Work

Due to the lack of interventions for smartphone security and privacy awareness, we designed a persuasive game for improving users' awareness and self-efficacy about secure smartphone behaviour. The key takeaways from our design are: (a) Our game gives instant feedback or tips about secure smartphone behaviour when the player picks up a permission symbol in-game. (b) We built the game according to six game design patterns [26] to make it more enjoyable for the player and implemented nine persuasive principles to motivate the players. (c) We impart skills for secure smartphone behaviour and expose the dangers of unnecessary permissions to an individual's privacy and security using an interesting game narrative while maintaining the context of smartphone security. For our future work, we are looking forward to evaluating the game to examine both its usability and effectiveness with respect to promoting safe smartphone security behaviour and privacy knowledge. We are also planning to tailor the game [41–43] and consider the players' emotions because most times when a security incident occurs, it is because the user is either desperate, careless [14], or impulsive [9].

**Acknowledgement.** This research was undertaken, in part, thanks to funding from the Canada Research Chairs Program. We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) through the Discovery Grant.

## References

1. Popova, F.C. and I.: Smartphone Cyber Security Awareness in Developing Countries: A Case of Thailand. *Dep. Comput. Syst. Sci. Stock. Univ. Sweden*. 58–68 (2019). <https://doi.org/10.1007/978-3-030-05198-3>.
2. Bosu, A., Liu, F., Yao, D.D., Wang, G.: 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*. pp. 71–85 (2017). <https://doi.org/10.1145/3052973.3053004>.
3. Reardon, J., Feal, Á., Elazari, A., On, B., Vallina-Rodriguez, N., Egelman, S.: Open access to the Proceedings of the 28th USENIX Security Symposium is sponsored by USENIX. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System.

4. Flynn, L., Klieber, W.: Smartphone Security. *IEEE Pervasive Comput.* 14, 16–21 (2015). <https://doi.org/10.1109/MPRV.2015.67>.
5. Google: App permissions overview | Android Developers, <https://developer.android.com/training/basics/permissions>, last accessed 2020/12/03.
6. Google: Permissions on Android | Android Developers, <https://developer.android.com/guide/topics/permissions/overview>, last accessed 2020/11/29.
7. Application Signing | Android Open Source Project, <https://source.android.com/security/apksigning>, last accessed 2020/12/04.
8. Google: App permissions best practices | Android Developers, <https://developer.android.com/training/permissions/usage-notes>, last accessed 2020/11/29.
9. Butavicius, M., Parsons, K., Pattinson, M., McCormac, A.: Breaching the human firewall: Social engineering in phishing and spear-phishing emails. In: *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*. pp. 1–10 (2015).
10. Bitton, R., Boyngold, K., Puzis, R., Shabtai, A.: Evaluating the Information Security Awareness of Smartphone Users. In: *Conference on Human Factors in Computing Systems - Proceedings (2020)*. pp. 1–13 (2020). <https://doi.org/10.1145/3313831.3376385>.
11. Zhang, X.J., Li, Z., Deng, H.: Information security behaviors of smartphone users in China: An empirical analysis. *Electron. Libr.* 35, 1177–1190 (2017). <https://doi.org/10.1108/EL-09-2016-0183>.
12. Breitingner, F., Tully-Doyle, R., Hassenfeldt, C.: A survey on smartphone user’s security choices, awareness and education. *Comput. Secur.* 88, (2020). <https://doi.org/10.1016/j.cose.2019.101647>.
13. Koyuncu, M., Pusatli, T.: Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Mob. Inf. Syst.* 2019, (2019). <https://doi.org/10.1155/2019/2786913>.
14. Renaud, K.: 60 . Smartphone Owners Need Security Advice . How Can We Ensure They Get It ? In: *CONF-IRM 2016 Proceedings (2016)*.
15. Bitton, R., Finkelshtein, A., Sidi, L., Puzis, R., Rokach, L., Shabtai, A.: Taxonomy of mobile users’ security awareness. *Comput. Secur.* 73, 266–293 (2018). <https://doi.org/10.1016/j.cose.2017.10.015>.
16. Shah, P., Agarwal, A.: Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Inf. Comput. Secur.* 28, 293–318 (2020). <https://doi.org/10.1108/ICS-04-2019-0041>.
17. Zhou, G., Gou, M., Gan, Y., Schwarzer, R.: Risk Awareness, Self-Efficacy, and Social Support Predict Secure Smartphone Usage. *Front. Psychol.* 11, 1–8 (2020). <https://doi.org/10.3389/fpsyg.2020.01066>.
18. Orji, R., Vassileva, J., Mandryk, R.L.: LunchTime: A slow-casual game for long-term dietary behavior change. *Pers. Ubiquitous Comput.* 17, 1211–1221 (2013). <https://doi.org/10.1007/s00779-012-0590-6>.
19. Ndulue, C., Orji, R.: STD PONG: Changing Risky Sexual Behaviour in Africa

- 86 Ninth International Workshop on Behavior Change Support Systems (BCSS 2021): *The Design and Development of Mobile Game to Promote Secure Smartphone Behaviour* through Persuasive Games. In: Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities. ACM, New York, NY, USA (2018).
20. Oyebode, O., Maurya, D., Orji, R.: Nourish Your Tree! Developing a Persuasive Exergame for Promoting Physical Activity among Adults. In: 2020 IEEE 8th International Conference on Serious Games and Applications for Health, SeGAH 2020 (2020). <https://doi.org/10.1109/SeGAH49190.2020.9201637>.
21. Gokul, C.J., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., Lodha, S.: 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. pp. 169–181 (2018). <https://doi.org/10.1145/3270316.3273042>.
22. Ndulue, C., Oyebode, O., Orji, R.: 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). pp. 223–233. Springer International Publishing (2020). <https://doi.org/10.1007/978-3-030-45712-9>.
23. Weanquoi, P., Johnson, J., Zhang, J.: Using a game to teach about phishing. SIGITE 2017 - Proc. 18th Annu. Conf. Inf. Technol. Educ. 75 (2017). <https://doi.org/10.1145/3125659.3125669>.
24. Wen, Z.A., Lin, Z., Chen, R., Andersen, E.: What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. Conf. Hum. Factors Comput. Syst. - Proc. 1–12 (2019). <https://doi.org/10.1145/3290605.3300338>.
25. Oinas-Kukkonen, H., Harjumaa, M.: Persuasive systems design: Key issues, process model, and system features. Commun. Assoc. Inf. Syst. 24, 485–500 (2009). <https://doi.org/10.17705/1cais.02428>.
26. Khalifa, A., De Mesentier Silva, F., Togelius, J.: Level design patterns in 2D games. IEEE Conf. Comput. Intell. Games, CIG. 2019-Augus, (2019). <https://doi.org/10.1109/CIG.2019.8847953>.
27. Thomps, M., Irvine, C.: Active learning with the CyberCIEGE video game. In: 4th Workshop on Cyber Security Experimentation and Test, CSET 2011. pp. 1–8 (2011).
28. Yerby, J.: Development Of Serious Games For Teaching Digital Forensics. Issues Inf. Syst. 13, 112–122 (2014).
29. Gondree, M., Peterson, Z.N.J., Denning, T.: Security through play. IEEE Secur. Priv. 11, 64–67 (2013). <https://doi.org/10.1109/MSP.2013.69>.
30. Scholefield, S., Shepherd, L.A.: 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 (2019).
31. Chen, T., Dabbish, L., Hammer, J.: Self-efficacy-based game design to encourage security behavior online. In: Conference on Human Factors in Computing Systems - Proceedings. pp. 1–6. Association for Computing

- Machinery, New York, NY, USA (2019).  
<https://doi.org/10.1145/3290607.3312935>.
32. Zargham, N., Bahrini, M., Volkmar, G., Sohr, K., Wenig, D., Malaka, R.: What could go wrong? Raising mobile privacy and security awareness through a decision-making game. *CHI Play 2019 - Ext. Abstr. Annu. Symp. Comput. Interact. Play.* 805–812 (2019). <https://doi.org/10.1145/3341215.3356273>.
  33. Bahrini, M., Meissner, M., Malaka, R., Wenig, N., Sohr, K.: HappyPerMi: Presenting critical data flows in mobile application to raise user security awareness. *Conf. Hum. Factors Comput. Syst. - Proc.* (2019). <https://doi.org/10.1145/3290607.3312914>.
  34. Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., Malaka, R.: Make my phone secure! Using gamification for mobile security settings. *ACM Int. Conf. Proceeding Ser.* 299–308 (2019). <https://doi.org/10.1145/3340764.3340775>.
  35. Fogg, B.J.: Creating persuasive technologies: An eight-step design process. *ACM Int. Conf. Proceeding Ser.* 350, (2009). <https://doi.org/10.1145/1541948.1542005>.
  36. Unity: Unity Real-Time Development Platform | 3D, 2D VR & AR Engine, <https://unity.com/>, last accessed 2020/12/04.
  37. Proto.IO: Proto.io - Prototypes that feel real, <https://proto.io/>, last accessed 2020/12/04.
  38. Manifest.permission\_group | Android Developers, [https://developer.android.com/reference/android/Manifest.permission\\_group](https://developer.android.com/reference/android/Manifest.permission_group), last accessed 2020/12/03.
  39. The official home of Super Mario™ – Home, <https://mario.nintendo.com/>, last accessed 2021/01/11.
  40. Wulf, T., Bowman, N.D., Velez, J.A., Breuer, J.: Once Upon a Game: Exploring Video Game Nostalgia and Its Impact on Well-Being. *Psychol. Pop. Media Cult.* (2018). <https://doi.org/10.1037/ppm0000208>.
  41. Orji, R., Oyibo, K., Lomotey, R.K., Orji, F.A.: Socially-driven persuasive health intervention design: Competition, social comparison, and cooperation. *Health Informatics J.* 25, 1451–1484 (2019). <https://doi.org/10.1177/1460458218766570>.
  42. Orji, R., Mandryk, R.L., Vassileva, J.: Improving the efficacy of games for change using personalization models. *ACM Trans. Comput. Interact.* 24, (2017). <https://doi.org/10.1145/3119929>.
  43. Fortes Tondello, G., Valtchanov, D., Reetz, A., Wehbe, R.R., Orji, R., Nacke, L.E.: Towards a Trait Model of Video Game Preferences. *Int. J. Human-Computer Interact.* 34, 732–748 (2018). <https://doi.org/10.1080/10447318.2018.1461765>.