An Empirical Study on Secure Usage of Mobile Health Apps: The Attack Simulation Approach

Bakheet Aljedaani[a], Aakash Ahmad[b], Mansooreh Zahedi[c], M. Ali Babar[d,e]
[a]Computer Science Department, Aljumum University College, Umm Alqura University, Makkah, Saudi Arabia
[b]School of Computing and Communications, Lancaster University Leipzig, Germany
[c]School of Computing and Information Systems, University of Melbourne, Australia
[d]CREST – the Centre for Research on Engineering Software Technologies, University of Adelaide, Australia
[e]Cyber Security Cooperative Research Centre (CSCRC), Australia
[a]bhjedaani@uqu.edu.sa, [b]a.ahmad13@lancaster.ac.uk, [c]mansooreh.zahedi@unimelb.edu.au,
[d]ali.babar@adelaide.edu.au

Abstract
Context: Mobile applications (apps) have proven their usefulness in enhancing service provisioning across a multitude of domains that range from smart healthcare, to mobile commerce, and areas of context-sensitive computing. In smart healthcare context, mobile health (mHealth) apps - representing a specific genre of mobile apps that manage health information - face some critical challenges relating to security and privacy of device and user data. In recent years, a number of empirically grounded, survey-based studies have been conducted to investigate secure usage of mHealth apps. However, such studies rely on self-reported behaviors documented via interviews or survey questions that lack practical approaches that can simulate attack scenario for monitoring users' actions and behaviors while using mHealth apps.
Objective: Our objective was to conduct an empirical study - engaging participants with attack simulation scenarios and analyze their actions - for investigating the security awareness of mHealth app users.
Method: We simulated some common security attack scenarios in mHealth context and engaged a total of 105 app users to monitor their actions and analyze their behavior. We analyzed users' data with statistical analysis including correlations test, descriptive analysis, and qualitative data analysis (i.e., thematic analysis method).
Results: Our results indicate that whilst the minority of our participants perceived access permissions positively, the majority had negative views. Users provide their consent, granting permissions, without a careful review of privacy policies that leads to undesired or malicious access to health data. Findings also indicated that 73.3% of our participants had denied at least one access permission, and 36% of our participants preferred no authentication method.
Conclusion: The study complements existing research on secure usage of mHealth apps, simulates security threats to monitor users' actions, and provides empirically grounded guidelines for secure development and usage of mobile health systems.

Keywords: Mobile Computing, Software Engineering, Mobile Healthcare (mHealth), Empirical Study.

1. Introduction
Mobile and pervasive technologies offer users with a multitude of context-aware services that include but are not limited to social networking, mobile commerce, along with smart and connected health care [1, 2]. Mobile health (mHealth) apps, and their enabling infrastructures such as context-sensitive mobile devices and wireless networking have empowered users and transformed the healthcare sector to provide a wide range of healthcare services. This has resulted in a significant improvement in the mHealth adoption by users (e.g., patients, medics, public health stakeholders), increased effectiveness, and reduced costs for healthcare services [1]. Public and private healthcare providers can leverage mHealth apps to offer digitize healthcare practices such as health and fitness monitoring [3], dermatologic care [4], chronic management [5, 6], and clinical practices [7]. A recent report by Allied Market Research revealed that the global digital health market size was valued at $145,884.3 million in 2020, and is projected to reach $767,718.9 million by 2030 [8].

Despite the potential benefits and strategic importance of mobile technologies and mHealth initiatives in smart systems context, a number issues such as resource poverty, security of device resources, and privacy of context-sensitive data represent critical challenges to mobile computing solutions [9, 5, 2]. Specifically, the security of mHealth apps is considered a challenge due to the pervasive environment that continuously ingests health-critical data from embedded sensors (hardware), processes and persists data inside the device (via mobile apps), and transmits it across ad-hoc networks [2, 10]. According to a report by cybercrime magazine in 2020, ransomware has become the fastest growing and one of the most damaging types of cybercrime. The global cost for ransomware damage, including mobile devices, could reach $20 billion by 2021, which is 57 times more than it

was in 2015 [11]. As a typical example, some of the installed apps can be granted (undue/excessive) access unintentionally by the users to all of a device's resources to gain, use, and share users' data. Data in mobile devices and apps, specifically health-critical data in the context of this study, can be leaked to an external host or a third party through excessive app permissions [9, 12], phishing attacks [13], or when installing other mobile apps from unknown resources [14]. Recent studies (e.g., [15, 16]) highlight that users have limited security awareness of what they should do to protect their private and health-critical information. Besides, social engineering methods can be used by hackers to deceive users into leaking their private information [17, 12]. Molyneaux et al. in [18] indicated that it is difficult for users to make security-related decisions when facing security threats. Indeed, most users are unaware of such a threat to their data, or are unable to understand the technical mechanisms behind data leakage, which can lead them to ignore the associated security risks. Furthermore, employing suitable technical solutions including, privacy preserving mechanisms and two-factor-authentication, cannot address security issues alone; instead, the role of users and their understanding of how they should react to different security threats and attacks is an important factor in ensuring the secure usage of mobile apps [19].

In mobile systems - enhanced interactivity and context sensitivity are considered as ultimate criterion of success - technical measures alone may not be sufficient to ensure security, unless they are complemented with required human-centric knowledge and practices to protect data [20]. Human-centric knowledge and awareness in terms of necessary actions and behaviors, e.g., granting only the appropriate access permissions or opting-in for multi-factor authentication can significantly influence mHealth security [19]. According to a Proofpoint cybersecurity report, 95% of observed attacks exploited the "human factor" rather than relying on software and hardware vulnerabilities (such as phishing emails, or granting unnecessary permissions) [21]. Users could become a self-threat to their private data and can be easily deceived into revealing or leaking classified information if they are not fully aware of the security features they are utilizing [17, 12]. This issue can be seen with technology-based solutions that involve using security features in such a way that users find them difficult to understand [22]. mHealth app developers often undermine the user's security knowledge and behavior with a belief of having already delivered a secure app by following the principle and practices of secure software development [23]. However, users find these security features as hard to understand and use [17], confirmed with a recently conducted empirical study that investigated the security knowledge, attitude and behavior of mHealth app users [24]. The study highlights knowledge as the level of security understanding by the users, an attitude refers to how the users feel about their knowledge, and behavior refers to their actions that users perform to ensure security. The results of the study revealed that users had the knowledge, attitude about the security measures of the investigated apps. However, users' knowledge did not significantly influence their behaviors, indicating that users are aware of the risks but are reluctant, or unaware, of appropriate actions that mitigate such security risks (e.g., setting privacy preferences to restrict undesired data access).

To this end, state-of-the-art on secure usage of mHealth apps mainly relies on surveys and interviews to collect and analyze users' responses based on their security knowledge and behavior [24-29]. However, the results of such studies could be affected by social desirability (i.e., self-reported behavior not supporting the respondents' claims), and/or the sampling method (i.e., relying on a particular group of users). The above-mentioned limitations demand for an attack simulation mechanism, taking users in the loop to monitor and analyze their actions in a real context, simulated as security threats scenarios to their health critical data. This study aims to investigate the behavior(s) of users (i.e., users' actions in a specific security scenario based on their knowledge) when dealing with mHealth apps. Users' actions and behaviors such as clicking on suspicious links or granting unnecessary permissions could lead to compromised security of data. Contrary to asking the users via interview(s) or survey(s) to report their behaviors that surfer measurement bias [30-32], we engage users to demonstrate their behavior that can be monitored and analyzed using an attack simulation approach. We use the term attack to refer to the social engineering attacks that aim to exploit human vulnerabilities, as conducted in [14, 33]. The term also include the threats, and the actions that lead to a potential compromise of resources of mobile devices. The findings provide an indication for participants' ability to mitigate the investigated attacks. Whilst several studies (e.g., [34-36]) used phishing simulation attacks (i.e., a type of experiments that aim to investigate and assess users' security awareness and their ability to understand the associated risks), we used this term to monitor and assess users security behavior when they face a certain simulated attacks (e.g., requesting unnecessary permissions). Our aim is to find answers for the two Research Questions (RQ) that aim to investigate (1) the actions of users, and (2) mistakes made by them while using mHealth apps in a security critical scenario. Thus, we outlined the following (RQs):

RQ1: *How do end-users react while facing potential security threats during the usage of mHealth apps?*

RQ2: *What security-related mistakes do end-users make while using mHealth apps?*

To find the answers, we adopted an attack simulation research approach [14, 33] to develop an attack simulation solution and engaged 105 (Android device) users to monitor their actions for analyzing their security knowledge. mHealth apps can be classified into different genres such as general health advisory to fitness monitoring and nutritional data apps, our study uses fitness monitoring app as such class of apps are considered as most common and widely used apps in mHealth systems. This study complements our previous works [20, 24] that aimed to understanding the security awareness of users while using clinical mHealth apps. This study involves participants from 14 countries (across 5 continents), with different age groups, various educational backgrounds, and different IT knowledge. Our decision to select the Android platform for security attack simulation solution is influenced by two reasons (a) it is the most widely used mobile platform for mHealth apps, and (b) it is considered as comparatively more vulnerable than other mobile platforms such as iOS. Study participants were monitored based on their actions and behaviors under simulated attacks on security of mHealth app. In addition, we sought users' input via an exit survey collecting user's demographic and other auxiliary information that compliments study results. Data analysis consisted of two steps. The first step involved statistical analysis to measure the correlations of study items, and a descriptive analysis to report the demographic data and our participants' (re-) actions corresponding to security threats. The second step included qualitative analysis to present the findings for the open-ended question. This study makes the following contributions:

- Simulates the most frequently encountered security threats to monitor and investigate the actions and behaviors of mHealth apps users – at attempt to overcoming the issues and bias in self-reported behaviors.
- Identify and classify the main reasons considered by users while facing access permissions' requests in mHealth context.
- Empirically grounded guidelines for secure usage of mHealth app driven by user's actions in security threat scenarios.

Section 2 presents the related work. Section 3 details the adopted research methodology. Sections 4 and 5 reports the study findings. Section 6 discusses the findings of the study. Section 7 describes validity threats for this study. Section 8 concludes the paper.

2. Related Work

We now review the most relevant existing research generally classified as (i) self-reported survey studies on secure mHealth apps (Section 2.1) and (ii) measuring the momentary behavior of subjects during specific events to understand secure usage of mobile computing (Section 2.2), detailed below.

2.1 Self-Reported Surveys to Investigate Security Awareness of mHealth Users

In the extent literature on mHealth security, one of the most common approaches to assess the security awareness of users is to conduct survey-based studies (i.e., survey, interviews, focus groups, etc.). Such approaches for survey-based studies [24-29], engage mHealth app users to self-report their security-related actions and behaviors in the past and the consequences of such actions [37] via pre-defined questionnaire. From an empiricism perspective, such self-reported studies may suffer some inherent bias including but not limited to exaggerated answers, or a sense of scepticism (often shyness or embarrassment) in sharing private information that may relates to someone health critical data [38], resulting in unreliable findings [14].

Security actions and habits: A recently published work [24] surveyed 101 participants to measure the security awareness of users about using clinical mHealth apps. The study utilized the Human Aspects of Information Security (HAIS) model to measure users' security knowledge, attitude, and behavior. Besides the potential bias in data collection (i.e., self-reported behavior), the study participants were from only two health providers in one region that impacts participants diversity, and ultimately impacting the generalisation of the results. The study by Zeybek et al. [29] surveyed 120 participants in a public institution to investigate mobile apps users' security habits (i.e., installation and rejection for app's permissions, the usage of antivirus app, locking screen, frequent updates for the apps, and installation for the apps from official store). The study concluded that awareness training and malware analysis through internal experts or external institutions are required. The results can be biased due to the fact that employees might report their best behavior as they have been informed that the study outcomes might be view by their senior managers.

Cyber Security awareness: Watson et al. [28] surveyed 94 participants and Mylonas et al. [27] surveyed 458 participants to investigate the security awareness of mobile devices users about critical security options (e.g., device settings, user behaviors, etc.). While the findings of Watson et al. revealed that participants, especially

those without strong IT knowledge, tend to ignore or are unaware of many critical security options, Mylonas et al. found that users were not adequately prepared to make appropriate security decisions. Furthermore, users had poor adoption of 'pre-installed' security controls, such as encryption, remote data wipe, and remote device locator. The limitations that could affect the results can be relying solely on the self-reported behavior, and focusing on specific group of participants (age 15 – 30). A study by Alotaibi et al. in 2016 [25] surveyed 629 Saudi Arabia based participants to investigate the cyber security awareness of computer and mobile users by focusing on three contexts, namely, cyber security practices, cybercrime awareness, and incident reporting. The study found that, although the participants had a good knowledge of IT, their awareness of the threats associated with cybercrime, cyber security practices, and the role of government and organizations in ensuring information safety across the internet, is very limited.

2.2 Experimental Research on Secure Mobile Usage

The second approach is measuring the security awareness of subjects during specific events (other studies call it objective data sources) such as [39, 14, 33, 40-42]. This approach tends to measure the actual behavior through installing an agent and allows the researcher to monitor the participants' reactions of a specific security phenomenon. Producing inaccurate results is one of the limitations for survey-based research due to the self-reported behavior. Thus, studies developed more effective mechanism to measure the security awareness through measuring the actual behavior of users, namely simulation-based approach [14, 33].

Simulation-based Understanding of App Access and Permission Reactions: In addition to the simulation-based analysis, studies such as [40, 42] were found involving other methods, (e.g., interviews, think aloud, exit survey) to allow participants to share their thoughts instead of relying on simulation-based approach only. Specifically, the researchers in [42] conducted an experiment with 36 participants to examine users' ability to deny applications access to protected resources. Felt et al. [40] evaluated whether or not Android users pay attention to, understand, and act on permission information during installation. The study conducted through two usability studies: an Internet survey of 308 Android users, and a laboratory study wherein 25 participants interviewed and observed.

Experimental Studies to Understand Secure Usage of Mobile Apps: Bitton et al. [14] measured the security awareness of smartphone users (i.e., 162 participants) for specific attack classes. The actual behavior was measured using a developed mobile agent and network traffic monitor and compared the findings with self-reported behavior, which have been collected through a survey. Barth et al. [39] examined the privacy paradox by focusing on the actual behavior and eliminating the effects of a lack of technical knowledge, privacy awareness, and financial resources. The study conducted as an experiment (including a questionnaire) on the downloading and usage of a mobile phone app among 66 Computer science students by giving them sufficient money to buy a paid-for app. Egelman et al. [33] measured the computer and mobile device security attitudes of users by utilizing the Security Behavior Intentions Scale (SeBIS). Four security sub-scales were mainly investigated including awareness towards phishing attacks, passwords, frequent updates, and locking the devices. The study was conducted through two surveys (555 participants) and a field study to monitor the security activities of 71 participants. The study found that: (i) testing high on the awareness sub-scale correlated with correctly identifying a phishing website, (ii) testing high on the passwords sub-scale correlated with creating passwords that could not be quickly cracked, (iii) testing high on the updating sub-scale correlated with applying software updates, and (v) testing high on the securement sub-scale correlated with smartphone lock screen usage (e.g., PINs).

Conclusive Summary: We now present a conclusive summary and comparative analysis of the most relevant existing research, as in Table 1. Comparative analysis is based on four-point criteria including *(i) research challenge(s), (ii) focus and contributions, (iii) evaluation context,* and *(iv) research limitations*. The study reference points to an individual research work under discussion and its year of publication. Existing studies including [24-29] measured the security awareness of users about using mHealth apps. However, all the indicated studies were measuring security behavior through a questionnaire, which is not sufficient to report accurate measurement. Alternatively, studies including [39, 14, 33, 40-42] tend to measure the security awareness using simulation-based research that can provide better results. However, none of the simulation-based research studies were focused on mHealth apps. To the best of our knowledge, there has been no experimental research study to measure users' security awareness about using mHealth apps. We investigated the security awareness for users of mHealth apps via an attack simulation approach. We measured users' reactions through posing a few security threats, and monitor their spontaneous reactions. Furthermore, our study followed by an exit survey to collect demographic data from the participants and capture their security views.

Table 1. Comparative Analysis of most Relevant Existing Studies Compared to our Study

Study Reference	Research Challenges	Focus and Contributions	Evaluation Context	Research Limitations	Pub. Year
Survey-based Studies					
[4]	To exploit the Human Aspects of the Information Security (HAIS) model to investigate the security awareness of users regarding the usage of mHealth apps.	- Analyse users' *security knowledge, attitude, and behavior* towards mHealth apps - Investigate prominent security issues for users such as privacy and usability.	- Survey of mHealth app users (*101 participants*) Quantitative data	- Bias in data collection (diversity and types of participants) - *Self-reported behavior* by users	2020
[60]	To investigate, through empirical study, the *security awareness of public institution personnel* towards using mobile devices.	- Investigate Security habits of users (*apps' permissions, usage of antivirus and protection mechanisms, lock screen, etc.*)	- Survey of workspace users (*120 participants*) - Quantitative data	- *Bias in data collection* - *Self-reported intentions of users*	2019
[57]	To analyse the usage of security settings and control by mobile device users.	- Analyse security recommendations to users (e.g., *device settings, user behaviors, and applications)*	- Survey of mobile app users (*94 participants*) - Survey-based qualitative data. - Quantitative data	- Bias in data collection (self-reported behavior of users) - Diversity of users (i.e., students, faculty, and staff of one institute)	2017
[5]	To conduct an empirical Investigation into the cyber security awareness of users	- Analyse challenges of cyber security. - Investigate cyber security awareness (*cyber security practices*, *cybercrime awareness*, and *incident reporting.)*	- User survey questionnaire (*629 users*) - Quantitative and qualitative data	- Data collected from users of mobile and PCs. - Bias in data collection (self-reported intention)	2016
Controlled Experiments					
[8]	To investigate the privacy and security paradox of mobile users by focusing on the actual behavior.	The study eliminated the effects (i.e., *lack of technical knowledge, privacy awareness, and financial resources).*	Experiment and survey (*66 participants*)	- Bias in recruiting users (High knowledge in IT). - App selection might affect participants' consideration of security and privacy.	2019
[11]	To classify types of security threats and investigate information security awareness of mobile users for different classes of threats.	- Measuring security awareness of users - Measuring users' behavior by mobile agent and network traffic monitor	- Survey of the mobile user (*162 participants*) - Monitoring of mobile agents and mobile network traffic	- No specific type of apps to be investigated	2020
[15]	To exploit the Security Behavior Intentions Scale (SeBIS) to analyse the security attitudes of users	- Analyse the security attitude of users - Supporting users' security knowledge (e.g., awareness *of phishing attacks, frequent updates, passwords*, and *device locking*).	- User survey questionnaire (*555 participants*) - Experimental monitoring of users (71 participants).	- No specific type of apps to be investigated - Bias in data collection (creating passwords for low-risk accounts)	2016
Proposed Study	To monitor the security awareness of users of mHealth apps via a security attack simulation.	- Understanding users' security behavior when they are facing certain security threats/attacks.	- Utilising a simulation system and a survey to collect data. - Quantitative and qualitative data	- Focusing on mHealth apps. - Multiple data sources (i.e., simulation-based, survey) - Engaging users with diverse backgrounds (e.g., age, education level, etc.).	NA

3. Research Method

In this section, we discuss the research methodology that we followed to investigate the security awareness of users of mHealth apps through a simulation-based attack. The adopted method comprises of three phases, each detailed below, as per the illustrations in Figure 1.

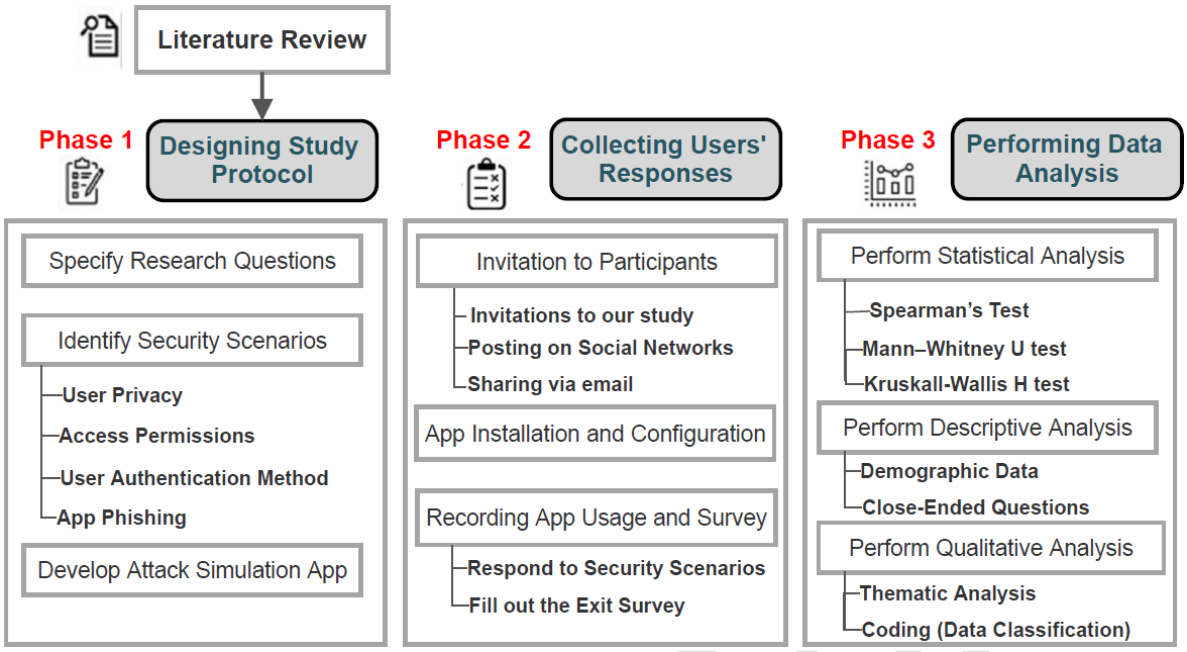


Figure 1. Overview of Research Method for Simulation-based Attack

3.1 Phase 1 – Designing the Study Protocol

Our literature review in Section 3.2 helped us understand state-of-the-art on users security issues, concerns, and preferences when using mHealth apps. In addition, we reviewed the literature to identify the existing methods to measure users' security awareness when using mobile apps (Section 3.3). Consequently, we understand and analyze the impact of the current research, highlighting proposed solutions and their limitations, specifying the research questions, and designing our study as in Figure 1. In the study protocol, we (i) specified the research questions (**RQ1**, and **RQ2** outlined in Section 1) (ii) identified the security scenarios that we plan to investigate, as in Table 2, and (iii) developed the simulation app. We investigated three major security threats, including user privacy and app permissions, authentication, and application phishing. It should be noted that each major security threat has a few potential security threats and at least one attack scenario, as highlighted in Table 2. We also gave the participants the option of reporting any security threats that they found and their interest in receiving security advice or training. Furthermore, we concluded our experiment with an open-ended question to capture users' thoughts in regards to the reasons behind paying attention to app permissions and the impact of giving an app more access permissions.

Table 2. The Investigated Security Threats and Scenarios in the Simulation-based Attack Study

Major security threats	Minor sub-security threats (Potential Security Threat)	Example (Scenarios/use-cases)
A. User Privacy and Permissions	1. Reading privacy policy	• Show privacy policy to users to investigate the time that spent to read it.
	2. Request access permission to device resources (e.g., user location, contacts, photos, microphone, camera, data of other apps)	• Request access permissions that are not mandatory for the app. The given permission for users can be either accept, or deny.
B. Authentication	3. Selecting secure authentication methods (e.g., none, PIN, 2FA, etc.).	• Provide a few options for authentication to investigate users' preferences.
C. Application Phishing	4. Pop-up window that requests users to share their private information.	• Show a pop-up window to request information from users given them the options to allow pop-up, or discard pop-up.
D. Feedback and reporting	5. Reporting security issues to developers.	• Ask participants if they want to contact developers to report any security issues.
	6. Understanding users interest in security education and training.	• Provide a signup option to receive frequent emails on secure mobile app usage.

Identification of Security Scenarios: Studies such as [20, 24, 15, 43, 44] examined users' views about the security of mHealth apps. The surveyed participants agreed that mHealth apps need to implement the security countermeasures that ensure confidentiality, availability, and integrity of health-critical data. However, there is a lack of evidence based on what participants' reactions are in a real scenarios. Studies such as [39, 14, 33, 40-42] conducted experimental research to measure the security behaviors for users of mobile apps when they face certain security challenges (e.g., phishing attacks, app permissions). These studies have inspired our research and significantly helped us to identify four security threats and eight security scenarios to be examined as illustrated in Table 2. To further understand the participants' reaction about these security threats, we included an option to report the security issues that they may notice. In addition, we asked our participants in case they want to learn about security which can help us to plan further research. This study is approved by the Human Research Ethics Committee at the *University of Adelaide (H-2021-106)*.

Simulation Mobile App: We developed a health and fitness app called "Workout" to convince participants to be a part of the study. Due to time limit that we had to complete this research, we made the app (.APK file) downloadable directly from a designed webpage instead of uploading it to apps stores. In fact, some participants were in doubt about installing the simulation app on their devices, which can be considered as a study limitation. The .APK file is available in [45]. Thus, we assured them in the study preamble that this is a part of a research study and we received ethical approval from concerned authorities and institutes to conduct this research and that the collected data will be anonymous and will be used solely for research purposes. Figure 2 presents the flowchart of our study procedure.

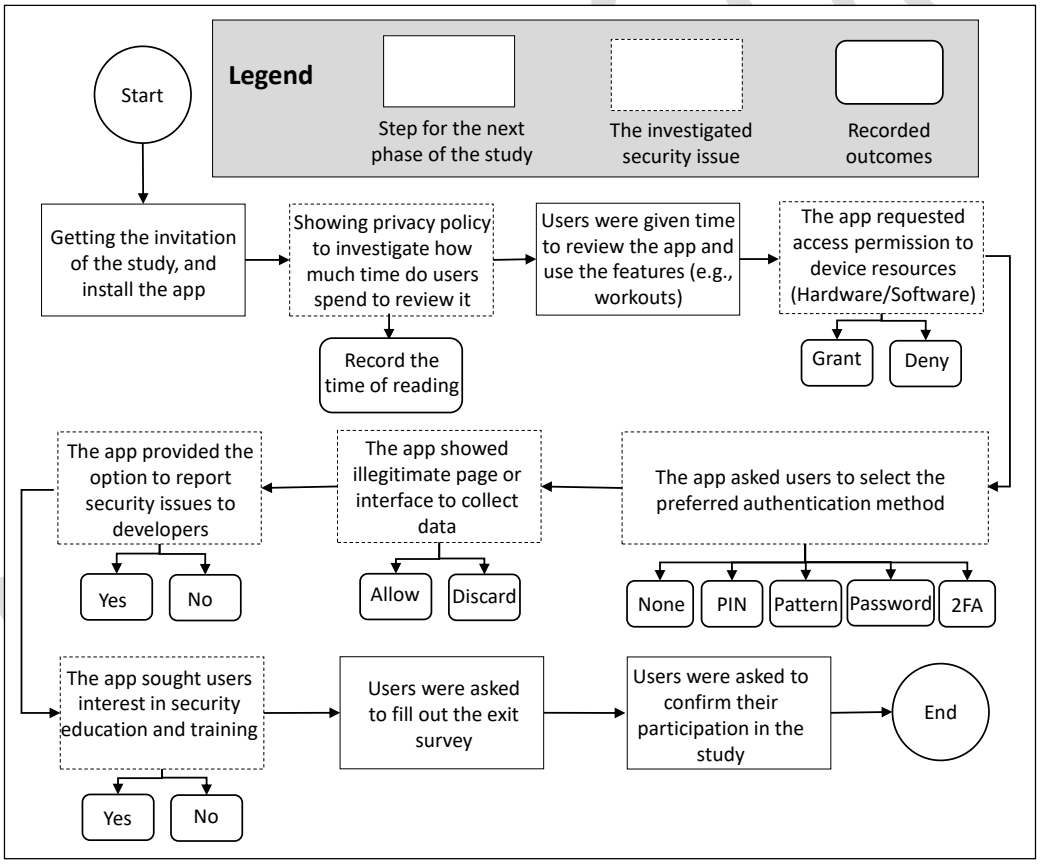
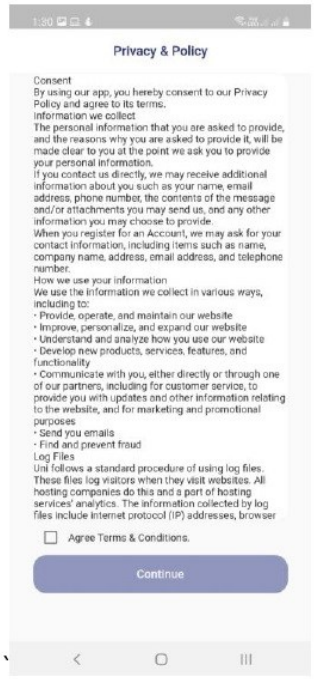


Figure 2. Flowchart of our Study Procedure

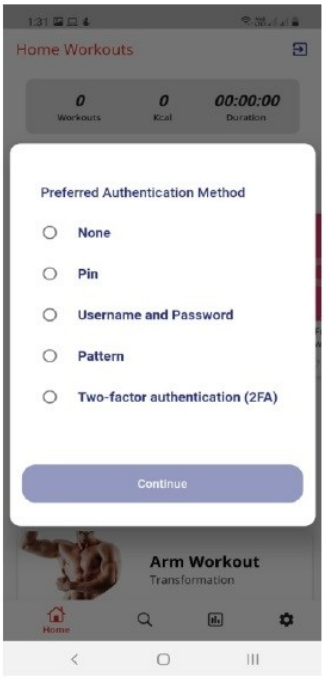
3.2 Phase 2 – Collect Users' Responses

Recruitment for Participants: We targeted anyone who uses Android device since our simulation app is only compatible with Android OS. We advertised for our study by posting our study invitation on social network (e.g., Twitter, Reddit, WhatsApp groups, etc.) to recruit participants. Our app was available to download by visiting a designed webpage that also include instructions to involve in the study. Participant has to be at least 18 year-old to engage in the study. We were able to monitor participants' reactions from the moment they install the app and we recorded their security reactions. Participants faced many challenges related to the security aspects of mobile

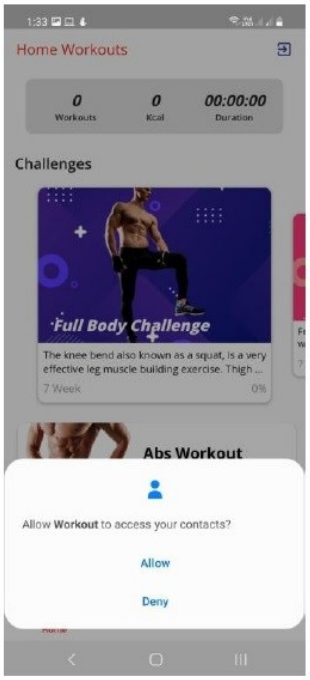
health apps, as illustrated in Table 2. Figure 3 shows six examples (screenshots) of the research activities that our participants faced. Additional screenshots for our simulation app are available in [45]. At the end, we provided an exit survey to collect demographic data and an open-ended question to allow them to share their thoughts. We carried out a pilot testing for our study with at least 10% of the participants to ensure the reliability and validity. Participants were given the option to withdraw their data during the study by simply deleting the app. As a result, their responses would be considered as incomplete and hence excluded from further analysis. After removing incomplete responses, we were able to collect data from 105 participants (referred to as **P1** to **P105**). Collected data along with the exit survey questions are available in [45].



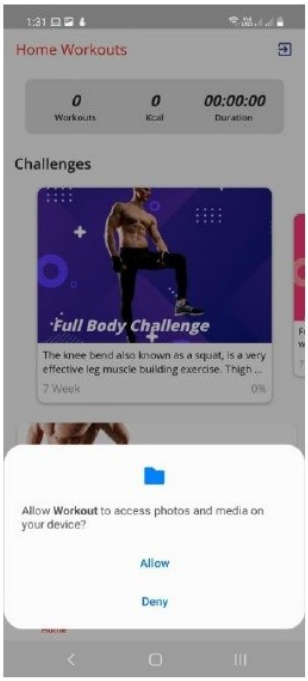
(a) Privacy Policy for our simulation app



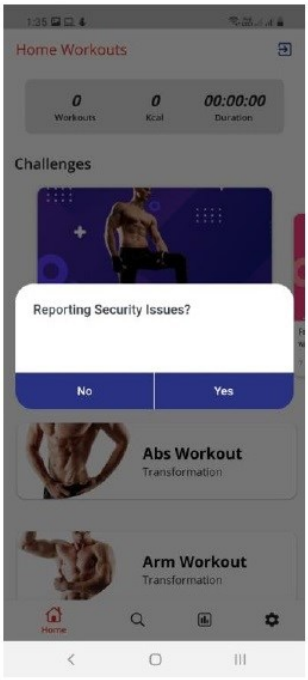
(b) Selecting the preferred authentication method



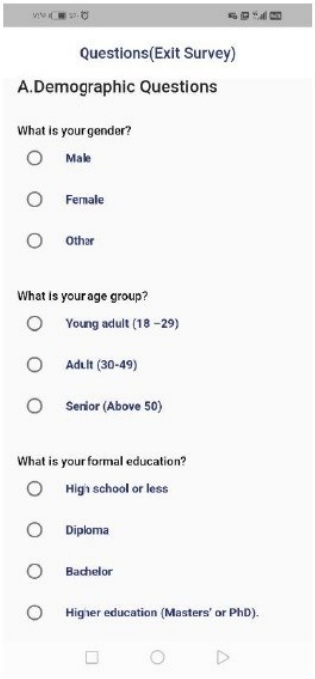
(c) Example of requesting access permission from participants



(d) Example of requesting access permission from participants



(e) Reporting security issue about the simulation app



(e) Exit survey for the simulation app

Figure 3. Examples of Research Activities for Simulation-based Attack Study

Participants' characteristics: As depicted in Figure 4, our study engaged 105 Android devices users from various countries (i.e., 14 countries, five continents), and with different age groups. Our participants were having various educational backgrounds and different IT knowledge. The demography analysis presented in Figure 4 complements the exit survey responses (Q1-Q6), available in [45], helps us with fine-grained analysis of the study results. For example, the analysis helped us to understand the difference in male and female reactions about access permissions.

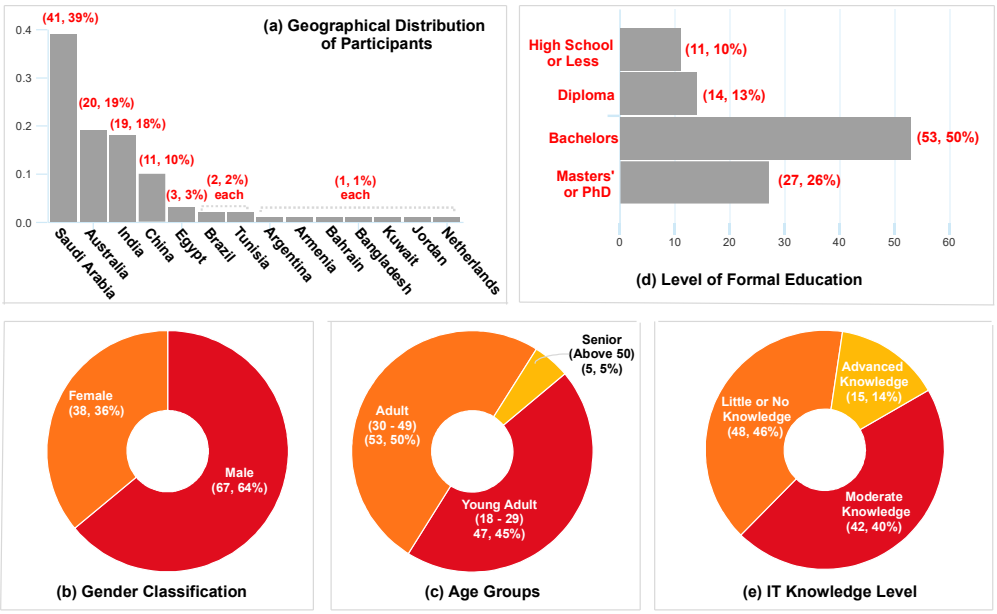


Figure 4. Demographic Details of the Participants of Attack-Simulation Study (Sample Size =105)

3.3 Phase 3 – Perform Data Analysis

We collected quantitative and qualitative data that help us to answer the outlined RQs. Based on the nature of data and the purpose of the analysis, we performed three techniques. Each technique is detailed below as per the illustrations in Figure 1.

Descriptive analysis: We reported the participants' demographic data by using **descriptive analysis** as presented in Figure 4. We also used this technique to report the participants' reactions when we asked them to make certain security decisions during using the simulation app.

Statistical analysis: SPSS version 28 (a popular data analysis software) was used to perform all statistical analysis. We also evaluated the correlation between the permission requests responses using **Spearman's statistical test** [46]. This test helped us to understand the correlation (i.e., strength and direction of association) between the permission requests items. Furthermore, we used statistical significance to compare our participants' reactions to the requested access permissions among multiple groups of users. **Mann–Whitney U test** was performed to compare the gender group since we have two independent samples (i.e., male and female) [47]. The **Kruskall-Wallis H test** [48, 49] was performed to compare the participants' reactions for more than two independent samples (e.g., IT knowledge level, age group). We followed our statistical analysis by performing a post hoc test once required [50] (e.g., Bonferroni correction) to examine the significance of differences using the adjusted alpha value (alpha level divided by the number of tests). For each demographic data, we tested the null hypothesis (i.e., *H_0: there is no significant difference*) against the alternative hypothesis (i.e., *H_1: there is a significant difference*), whereas $\mu 1$, μ_2, …, μk refers to population means.

Qualitative analysis: For the open-ended question, we used **thematic analysis** method [51-53] to identify the reasons that users reported about paying attention to the requested access permissions. Thematic analysis supports

extracting the data and synthesizing the results. We used NVivo[1] software, a popular computer-based tool, to organize and analyze data. Coding was initially done by one of authors in the team that was reviewed and revised (wherever required) by the second author to avoid potential bias. It should be noted that we considered the five steps of the conceptualized thematic analysis method: (1) reviewing and examining the provided responses to determine the parts that were relevant to each other; (2) generating initial codes, which involved extracting the initial lists themes; (3) searching for themes, which involved trying to combine different initial codes generated from the second step into potential themes; (4) reviewing and refining themes, which involved checking the identified themes from step 3 against each other to understand what themes had to be merged with others or dropped; and (5) defining and naming themes, which involved defining a name for each theme.

Findings of the study: We now present the findings to answer **RQ1**, and **RQ2** as outlined in Section 1. We divided our results section into two main sections: (i) Section 4 that reports the statistical and the descriptive analysis, and (ii) Section 5 that provides a thematic analysis for the open-ended question to investigate the rationale for paying attention to the app permissions based on our participants' perspectives.

4. Statistical and Descriptive Analysis

In this section, we enhance our results by including a few statistical analyses, as indicated in Figure 1. Such analyses would help to investigate the relationships by relying on the obtained quantitative data. It also helps to determine the significant results within the different demographic data.

4.1 Measuring the correlations of the study items

To further assess the relationship between the permissions request items (i.e., strength and direction of the linear relationship), we conducted Spearman's statistical test to whether there is a statistical significant correlation or not among the obtained data. It also helps to understand the direction of the relationship [54]. Such an investigation can help us to understand when one access permission type changes in value, the other access permission type tends to change in a specific direction. As illustrated in Table 3, we found that all the investigated permissions have a positive and statistical significant correlations at 0.01 level. For example, there is a statistically significant correlation between access to device storage and device camera and the chances of observing the obtained correlation (0.792) through random error are less than 0.01. The correlation results ranged from a strong (e.g., 79%: permission to storage and permission to access device camera) to a moderate (e.g., 53%: respond to permission to storage and permission to access device location) relationship [55]. To further elaborate on one example, the correlation indicates that when the score of permission to access storage increases, we expect (i.e., more likely) the score of accessing device camera to increase positively (it is not a causality relationship). Additionally, our analysis revealed that all the tested items were significantly correlated at 0.01 level.

Table 3. Correlation for the Permissions Requests

Permission type		Permission to storage	Permission to Camera	Permission to contacts	Permission to audio recording	Permission to location
Permission to storage	Correlation coefficient	1.000				
	95% Confidence Interval: Lower	1.000				
	Upper	1.000				
Permission to Camera	Correlation coefficient	.792**	1.000			
	95% Confidence Interval: Lower	.668	1.000			
	Upper	.892	1.000			
Permission to contacts	Correlation coefficient	.602**	.770**	1.000		
	95% Confidence Interval: Lower	.438	.641	1.000		
	Upper	.747	.886	1.000		
Permission to audio microphone	Correlation coefficient	.526**	.694**	.730**	1.000	
	95% Confidence Interval: Lower	.347	.545	.591	1.000	
	Upper	.680	.831	.848	1.000	
Permission to location	Correlation coefficient	.581**	.639**	.641**	.717**	1.000
	95% Confidence Interval: Lower	.399	.477	.489	.581	1.000
	Upper	.734	.774	.772	.848	1.000

**. Correlation is significant at the 0.01 level (2-tailed).

[1] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home/

4.2 Participants reaction about permissions requests and pop-up window

The security awareness for users towards using smartphones, in general, can be measured by understanding how users deal with four technological aspects, namely applications, communication and browsing, channels, and device [56]. Each aspect has a few attack scenarios that can be further investigated [56]. For example, access permissions and users reaction towards fake links were classified as examples of applications security. In our study, we explicitly attempted to exploit the human vulnerability (i.e., lack of security awareness) to exploit specific targets (e.g., device contacts) to gain an understanding of how the users' reacted (i.e., denied or granted access). Based on the type of the app that we developed for our simulation, no access permissions were mandatory for the app to be functioning. Denying these permissions would create no issue for app usage, and granting access could put users data at risks (e.g., allow third-party to access sensitive data). Overall, we requested 630 permissions (i.e., six per participants) in simulation app and we recorded their reactions without reaching the requested resources (including the pop-up window). We found that 296 access permissions (i.e., 47%) were granted to our simulation app, and 334 access permissions (i.e., 53%) were denied. Whilst 33 participants out of 105 (31.4%) had denied all the requested permissions, 77 participants out of 105 (73.3%) had prevented at least one permission, 28 participants out of 105 (26.7%) had responded to grant all the requested permissions for our simulation app. To be specific, we examined our participants' behaviors when they face a phishing link. We presented a pop-up window that offer them with free exercises which were not available in the app. We found that 47% have granted our request and 53% denied it. Additionally, we requested our participants to grant our simulation app unreasonable permissions to their device software, and hardware, namely, access to the device storage, contacts, camera, microphone, and location. Surprisingly, our findings indicated that 47.5% (± 2.5) of our participants have granted our simulation app access to the requested permissions. Figure 5 presents our participants reactions towards the requested permissions. Our findings also indicated that granting the app to access the device storage and location were the highest among other permissions (i.e., 50% each).

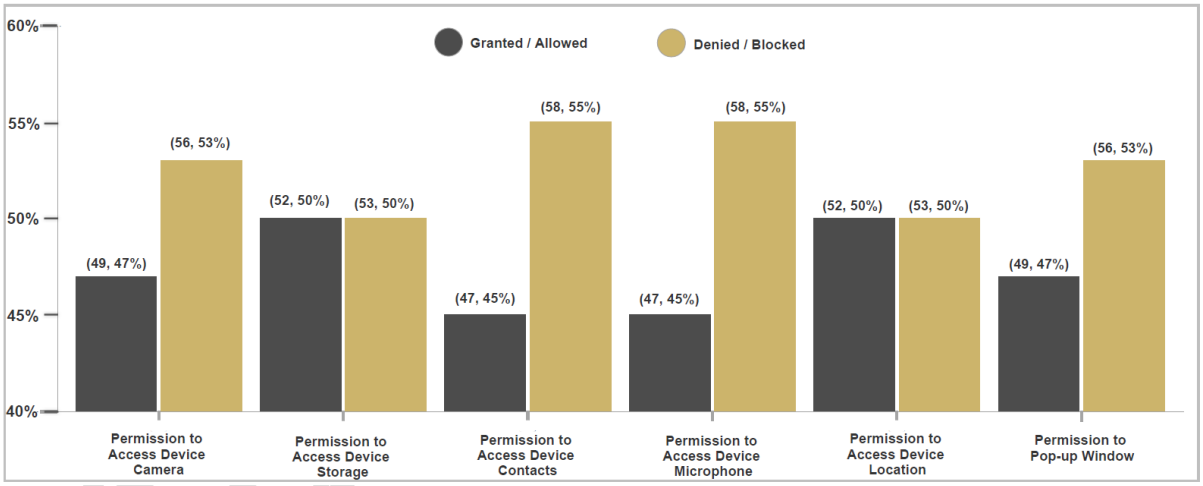


Figure 5. Participants' Reactions for the Requested Access Permissions

4.3 Relationship between demographic characteristics and participants reactions to access permissions

As indicated in (Section 3.3 Phase 3 – Perform Data Analysis), we performed Mann–Whitney U test for gender since we were comparing two independent samples (i.e., male and female), and Kruskall-Wallis H test for more than two independent samples (e.g., IT knowledge level, age group, etc.). These statistical tests helped us to determine whether there were statistically significant differences in regards to our participants' reactions to the requested access permissions (pop-up window request were excluded from these tests) among the defined groups of users (i.e., male vs. female, little or no IT knowledge vs. moderate IT knowledge vs. advanced IT knowledge, etc.). We performed Kolmogorov-Smirnov normality test for the obtained responses to check the assumptions of the statistical tests used in this study. The result ($p < 0.05$) suggested that the data were skewed (i.e., violated the normality assumption). As a result, we supported the usage of the statistical tests with the concept of central limit theorem [57], indicating that a sufficiently large (i.e., 105 in our case), has an approximate normal distribution. In addition, we considered the argument, has been verified by simulation results, that nonparametric tests (i.e., Spearman's test, Mann–Whitney U test, Kruskall-Wallis H test) are not sensitive to the non-normality assumption

[49, 58, 54]. The findings provides fine-grained analysis of the security reactions to access permissions for each specific group. For example, which access permissions received the highest allowance by female participants, which group of users are more likely to click on a phishing link, etc. We further investigated the significant differences for the groups whenever applicable (i.e., whenever p-value < .05). We used the Mann Whitney U test to compare the median differences between the overall extents [47, 48]. For each demographic data, we tested the null hypothesis (i.e., H_0: *there is no significant difference*) against the alternative hypothesis (i.e., H_1: *there is a significant difference*), whereas $\mu_1, \mu_2, \ldots, \mu k$ refers to population means. Due to the multiple hypotheses testing we carried out, our results can be inflated by family-wise error rate. Hence, the p-values were corrected through applying Bonferroni correction whenever applicable.

A. Access Permissions Based on Gender

To understand and compare how male (n=67) and female (n=38) participants reacted with the requested access permissions, we performed a statistical test (i.e., **Mann–Whitney U test**) to show if there is any significant difference. It should be noted that since we had unequal sample size for male and female, this could reduce the power of using Mann-Whitney U Test. The overall result indicated that there was no significant difference between male and female, as in Table 4, (u = 1061.500, z= -1.468, p-value= 0.142, effect size: Cohen's d =2.957, 95% confidence interval: Lower bound= .135, Upper bound= .149). However, we ran the same test to determine differences in each access permission between male and female. We found that access permission to device storage is statistically significant (u = 915.00, z= -2.757, p-value= .006). The mean rank for female = 62.42 which is higher than the mean rank for male = 47.66 indicating that female have a higher attention to granting our simulation app access to the device storage. Thus, we concluded that both male and female in our sample have reacted equally to the requested access permissions excluding accessing device storage.

Table 4. Differences towards Permissions Requests Based on the Characteristics of Study Respondents

Demography Data Category	Identified groups	N (%)	p-value
Gender	*Male*	67 (64%)	0.142
	Female	38 (36%)	
IT Knowledge Level	*Little or no knowledge*	48 (46%)	0.001
	Moderate knowledge	42 (40%)	
	Advanced knowledge	15 (14%)	
Age Group	*18 – 29 young adult*	47 (45%)	0.001
	30 – 49 adult	53 (50%)	
	Above 50 senior	5 (5%)	
Formal Education	*High school or less*	11 (10%)	0.053
	Diploma	14 (13%)	
	Bachelor degree	53 (50%)	
	Master's or PhD	27 (26%)	

B. Access Permissions Based on IT Knowledge Level

We conducted the Kruskall-Wallis H test to investigate the significance of granting or denying access permissions based on the participants' IT knowledge (i.e., Little or no knowledge, Moderate knowledge, and Advanced knowledge), as in Table 4. Our findings revealed that reacting to access permissions is differed significantly (p = 0.001, effect size: Cohen's d = 0.283, 95% Confidence interval: Lower bound= 0.000, Upper bound= 0.001). For the Moderate IT knowledge mean rank = 63.14 which is less than Advanced IT knowledge mean rank = 60.43 and less than Little or no knowledge mean rank = 41.80. Specifically, significant differences were found (using post-hoc Mann-Whitney U Test) between Little or no knowledge group compared with Moderate knowledge group (adjusted p =.002). Whilst we found that there is no statistically significant difference on the security awareness between Moderate knowledge group, and Advanced knowledge group (adjusted p=1.000), and there is no statistically significant difference on the security awareness between Little or no knowledge group, and Advanced knowledge group (adjusted p=.094). Therefore, we reject H_0 and concluded that IT knowledge level had an impact on their decisions to grant or deny access permissions for our participants.

C. Access Permissions Based on Age Group

We conducted Kruskall-Wallis H test to determine any significant difference among the three age groups (i.e., n=47; young adult, n=53; adult, n=5; senior) regarding to how they reacted to the requested access permissions. Our simulation app was developed to help the participants to do exercises as we were advertising for our study. We believe that we were not attracting as many seniors as we should. This could be the main reason that we had a very low number of Senior group (5 out of 105). As in Table 4, our findings suggested that there is a statistically significant (p=0.001, effect size: Cohen's d = 0.283) when reacting to the requested access permission for the three age groups. (95% Confidence interval: Lower bound= 0.000, Upper bound= 0.001). Adult group (mean rank = 62.36) were less than Young Adult group (mean rank = 45.86), were less than Senior group (mean rank = 24.20). Bonferroni Correction was performed to understand the significant differences among the three groups. Whilst we found that there is no statistically significant difference between Senior group and Young Adult group (adjusted p= .345), our results revealed that there is a statistically significant difference between Senior group and Adult group (adjusted p= .016). We also found that there is a statistically significant difference between Young Adult group and Adult group (adjusted p= .015). Therefore, we reject H_0: $\mu_1 = \mu_2 = \mu_3$ and conclude that age did have an impact on the participants when reacting with the requested access permissions.

D. Access Permissions Based on Level of Formal Education

We also wanted to investigate respondents' differences by considering the impact of the level of formal education on our participants. We conducted Kruskall-Wallis H test on the four groups, which we identified in Table 4. Our results indicated that there is no statistically significant difference among the four groups (p=0.053, effect size: Cohen's d = 0.347, 95% confidence interval: Lower bound= 0.047, Upper bound 0.056). We found that reacting to requested permissions of those with a postgraduate qualification (n= 27, mean rank= 59.57) was lower, than those with an education level of Bachelor (n=53, mean rank= 56.06), less than those who are having Diploma (n=14, mean rank= 42.43), and less than those with High School or less (n=11, mean rank= 35.59). Since there was no statistical significant difference based on the education level, we did not perform multiple comparisons (i.e., Bonferroni Correction). Our conclusion based on the obtained results suggested to accept H_0: $\mu_1 = \mu_2 = \mu_3 = \mu_4$. Thus, the level of formal education did not have an impact on the participants when dealing with access permissions.

4.5 Time spent of reviewing privacy policy by our participants

App privacy policy is a legal statement that regulates the engagement with users. It presents to the users how and when their personal data would be collected, retained, or shared with a third party. It also explains what resources the app is requesting, and for what purpose including access permissions, and the financial obligations for the app usage [59]. Some installed app can do an activity that is risky for user without they being realized [16]. App developers may share users' data with third parties for advertising purposes, or data can be leaked without developers having any thought about how that occurred [60]. Hence, the privacy policy should be carefully read by users before agreeing. In our simulation app and as most mobile apps do, we presented the privacy policy before the installation for our participants, as in Figure 3 (a). Our aim was to investigate how the participants would react and how much time they spent on reading it. To calculate the time, we recorded the time once the privacy policy was presented and the time the participants clicked on the "Continue" button. The average time spent on reviewing the privacy policy for all participants was 8.02 ms to review about 500 words, which requires at least a minute. Only nine participants (8%) spent more than 20 seconds reviewing the privacy policy, presented in Figure 3 (a). Interestingly, three participants spent rational time reviewing it (i.e., a minute and 55 seconds, a minute and 13 seconds, a minute and 3 seconds, respectively).

Due to the fact that IT knowledge can make a difference in regards to dealing with mobile apps, we further investigated reviewing the privacy policy behavior by our participants by looking into their IT knowledge level. We found that participants with advanced IT knowledge (n=15) spent an average time 19.61 ms. While participants with moderate IT knowledge (n=42) spent an average time 7.26 ms, and the participants with little or no knowledge on IT (n=48) spent an average time 5.06 ms. The participant identified as **P96** who spent 5 seconds in reviewing privacy policy wrote "*I don't pay attention to the privacy policy except when the duties and financial responsibility towards the app are mentioned. For example, the policy of cancelling the subscription if the app requires payment or financial fees*".

4.6 Preferred authentication method for our participants

User authentication in our context refers to how the participant wants to log into the simulation app and what method can be used to prove that s/he the legitimate app user. In our previous study [20], we surveyed 101 mHealth

apps users to investigate the desired security features they want to be employed. We found that users were having different opinions about the authentication method (e.g., employing biometric authentication, interactive authentication, direct access, etc.). Hence, in our simulation app, we provided a variety of options for authentication (ranging from weak, moderate or robust security) to investigate users selection. We asked our participants to customize the simulation app by selecting their preferred authentication method. We presented five common authentication methods, namely, none (i.e., without authentication), pattern, Personal Identification Number (PIN), username and password, and Two-factor authentication (2FA). 38 (36%) of our participants preferred no authentication method. Using Personal Identification Number (PIN) to access the app was selected by 20 participants (i.e., 19%). Using pattern was the preferred option for 13 participants (12%). 23 participants (22%) preferred to have a username and password to log in to the app, and only 11 participants (10%) preferred 2FA.

4.7 Participants interest in reporting security issue and receiving security advice

In our simulation app, we wanted to investigate the participants' behaviors towards reporting security issues within the simulation app in case they noticed. Our findings indicate that only 36 (34%) participants wanted to report security issue and 69 (66%) participants did not want to report any security issue. However, we are unsure whether these participants actually noticed an issue or not. One possible reason is that participants ignored what they have seen and did not want to bother about these issues. In fact, **P97** wrote "*When I see a security issue with the app, I just uninstall it*". For further analysis, we looked into the level of IT knowledge for the participants who wanted to report security issue(s) within the simulation app. We found that 9 participants with advanced IT knowledge (n=15), 12 participants with moderate IT knowledge (n=42), and 15 participants with little or no IT knowledge (n=48).

We also asked our participants whether they want to receive frequent security advices or not. Our results indicated that 76 (72%) participants accepted getting security advices and 29 (28%) participants refused this idea. For further analysis, we looked into the level of IT knowledge for the participants who decided on not to receive any security advice. Interestingly, the participants were from different levels of IT knowledge. 4 participants with advanced IT knowledge (n=15), 13 participants with moderate IT knowledge (n=42), and 12 participants with little or no IT knowledge (n=48).

5. Reasons for paying attention to the app permissions

In this section, we provide our analysis for the open-ended question that we included in the exit survey, as detailed in Section 3.3. We aimed to identify the reasons that make our participants pay attention to the requested app permissions based on their views. Based on the obtained responses, we used the qualitative descriptive analysis (Section 3.3 – Phase 3 – Perform Data Analysis) to create the conceptualization, as in Figure 6. Whilst a few participants perceived the requested permissions positively (Section 5.1), the majority had a negative views about the requested permissions as in (Section 5.2 – Section 5.5). Violating/losing privacy were explicitly mentioned by some participants, e.g., **P46**, **P47**, **P51**, **P54**, **P68**, **P82**, **P83**, **P88**, **P89, P92,** and **P98**. Four participants **P42**, **P47**, **P66**, and **P71** indicated that the requestion permissions were unnecessary. **P71** stated, *"[the app] should not access my contacts, photos, or location because the app does not need access to my information*". We provided cherry-picked examples for each theme to support our findings in Figure 6. Each theme is discussed in the following sections.

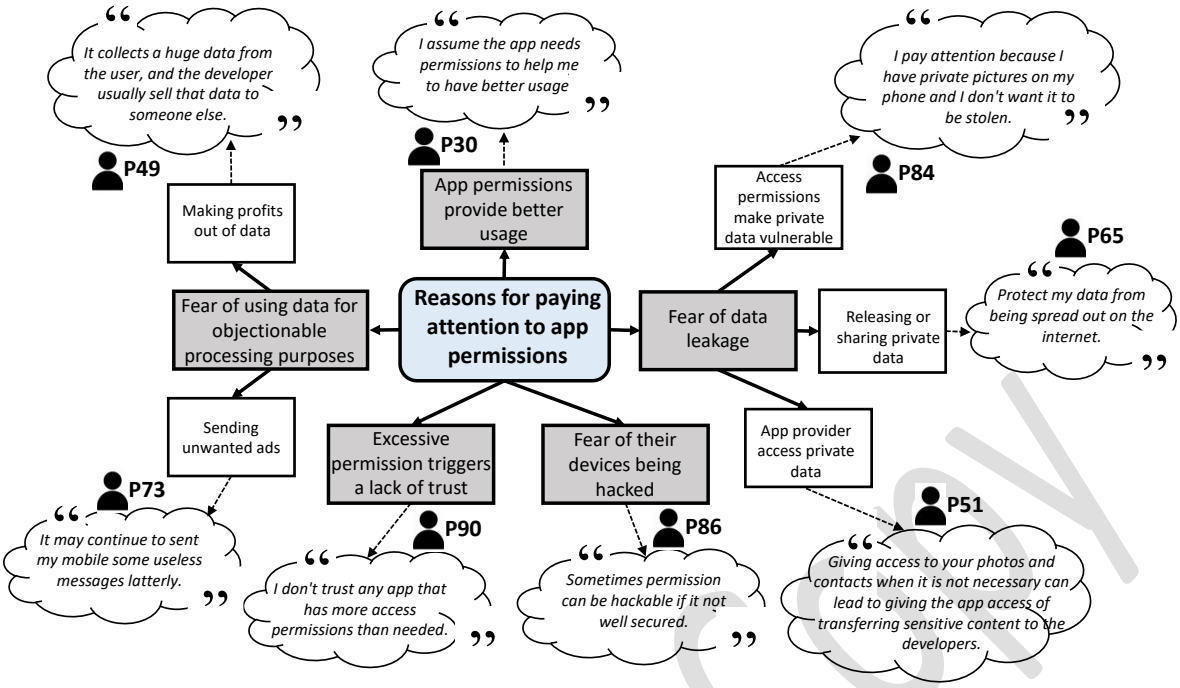


Figure 6. Participants' Views on the Reasons for Paying Attention to Access Permissions with Some Cherry-Picked Example for Each Theme.

5.1 App permissions provide a better usage

The ideal permission for our simulation apps which would make sense to request is accessing fitness data such as Health app in iOS. This permission would help to retrieve the data (e.g., steps count, burnt calories, etc.) into our app and perform the required analysis for users. However, we did not request this permission purposefully. Instead, we requested permissions to camera, contacts, microphone, location, photos that would make no logic to be granted. Five participants **P30**, **P45**, **P65**, **P82**, **P87** considered the requested permissions were necessary for the app functionality. The participants assumed that the simulation app was requesting permissions to perform relevant tasks. **P30** mentioned, "*I assume the app needs permissions to help me to have better usage*", and **P87** wrote, "*It is ok to grant the app to access my location because it is already the case with all other apps".*

5.2 Fear of data leakage

Data leakage can be defined as the unauthorized distribution for any confidential or sensitive users data [61]. Whilst app permissions is not the only method for data leakage, providing personal information when registering for the app could potentially leaked without app's provider/developer awareness [62]. We are reporting the participants' feedback regarding the reasons for granting or denying app permissions. Our findings revealed that 16 participants **P34**, **P36**, **P46**, **P51**, **P53, P54, P65, P68, P71 - P74, P84**, **P89**, **P92, P98** were having fear of data leakage for either their personal information (e.g., contact number, email address) or device data (e.g., contacts, photos, location). Four participants **P34**, **P51**, **P53,** and **P89** specified that app permissions would permit the app's provider/developer to access their private data. **P89** wrote, *"App permission, based on my knowledge, allow the developer to access my data in the device*", **P51** stated, *"Giving access to your photos and contacts when it is not necessary can lead to giving the app access of transferring sensitive content to the developers"*, and **P53** indicated "*when I have sensitive data on my phone, [access permissions] my take sms, contacts, or mails to do some things I don't like.* " Four participants, **P51**, **P68, P72, P92** indicated that they want to protect and maintain their private data. **P51** added, *"...I value my privacy and everything that is on my phone"*, and **P68** wrote, *"To maintain the privacy of my data",* and **P92** wrote, *"Protecting my personal information and data".* Three participants **P54**, **P65**, and **P71** mentioned that access permissions would lead to intentionally releasing or making the information publicly available to others. **P71** stated, *"The impact can be sharing data publicly such as the app that store the contacts and make it available to others",* and **P65** wrote, *"Protect my data from being spread out on the internet"*. Five participants indicated giving access permissions can make their private data vulnerable to data leakage. **P84**

wrote, *"I pay attention because I have private pictures on my phone and I don't want it to be stolen"*, **P73** wrote, "*It may be leaked my location information and mobile number*", and **P74** wrote, *"may lose my personal information"*.

5.3 Fear of their devices being hacked

Access permissions can be the role of attack surface that could be exploited. A compromised app would allow attackers to exploit whatever the app is already connected with including camera, microphone [63]. Six participants **P42**, **P46**, **P49, P86, P95, P102** expressed their fears of giving more permissions to our simulation app may lead to make their devices insecure. The participants indicated that doing so may make their devices vulnerable for malicious activities such as spying (**P42**, **P46**), or their devices may become hackable (**P49**, **P86**, **P95**, **P102**). Specifically **R42** stated **"***It will be a back door that will open vulnerabilities to be used to harm the device and its data"*, and **R46** wrote, *"Spy on my data and activity".* Furthermore, **P86** indicated "*Sometimes permission can be hackable if it not well secured*", and **P49** mentioned "*To protect myself from hacks*".

5.4 Excessive permission triggers a lack of trust

As indicated in Section 2.4.1, we developed our simulation app and we hosted it on our storage. Since participants had to download from unknown source, most likely this process gave an impression that our app was suspicious (no reviews or rating available to view). When we asked our participants the reasons of granting or denying the requested permissions, four participants **P66**, **P73**, **P90,** and **P105** indicated that the simulation app is not trusted to be granted the requested permissions. For example, **P73** stated, *"I will be unhappy about the more permission than needs and don't trust this app using, so that I will stop the app from accessing my information"***. R66** found that app permissions should not be requested. **R66** wrote, *"I don't let it go easily. I denied the requested permissions because the app does not need them. Only malicious app would ask for these access privileges."*

5.5 Fear of using data for objectionable processing purposes

Gathering users' data (e.g., contacts, location, etc.) through app permissions can be done easily. However, it becomes a problematic in case the app providers share that data without declaration or consent from users. This data processing would be objected by users if they were asked in advance. Four participants pointed out this concern and indicated that app permissions would gather data to make profits (**P46, P47, P49, R68**). For instance, **P68** stated *"Saving the data and distribute it to private parties. Some companies enable some apps to sell their clients' data*", **P47** wrote *"Transforming users into products, by selling their information"*, and **P49** indicated "*It collects a huge data from the user, and the developer usually sell that data to someone else"*. In addition, two participants reported that the purpose of requesting more permissions is sending advertisements (**P30, P73**). **P73** wrote, "*It may continue to sent my mobile some useless messages latterly*", and **P30** stated "*Sending ads to me*".

6. Discussion

We now discuss the results that highlight the core findings of this study, based on methodological details in Figure 1, and outline the potential future work. Table 5 guides the discussion and presents a summary of the key findings. The discussion highlights reviewing privacy policy (Section 6.1). We then discuss the results of participants' reactions about requesting access permissions (Section 6.2), and finally the reasons for paying attention to the requested permissions is discussed in Section 6.3.

6.1Time Spent on Privacy Policy

As we presented in (Section 4.5), most of participants skipped reading through the privacy policy and look for required action (ticking the box) to install the app. Our finding of this is consistent with previous research such as [64, 65, 60]. It should be noted that the entire time which our participants spent on the privacy policy page does not mean that participants were reviewing it. The time was calculated from the time that privacy policy page loaded until the participants clicked on continue button. Therefore, future research could consider employing accurate mechanisms such as eye-tracking (requires accessing the device camera) to record the time which participants are actually spending. Whilst there are several studies that indicated that there is a lack of clarity and transparency in presenting such policies for mHealth apps [2, 64, 65], and recommendations to improve the privacy policy for users [66, 9, 67, 68], further work can be done to examine users reactions when presenting the privacy policy through using innovative methods including summarizing the main points, using visualization, or a displaying it in video. This approach would be effective to encourage users, especially those who have little or no IT knowledge, to spend more time to understand what data the app requires, and how their data are being

handled. Such a study would help to understand how users review privacy policy and their understanding of the associated risks of using the apps.

Overall, users claimed to be worried and concerned about securing their data; however, our study showed that only a few have reviewed the presented privacy policy. Users need to pay attention to the presented privacy policy as it would increase their privacy awareness. At the same time, app providers should encourage and support their users for better understanding through using innovative methods.

Table 5. Summary of the Core Findings for Attack Simulation Approach Study

<table>
<tr><th colspan="6">Measuring the Security Awareness of Users about Using mHealth Apps: Attack Simulation Approach</th></tr>
<tr><th>Gender Classification</th><th>Age Group</th><th>Formal Education</th><th colspan="2">IT Knowledge Level</th><th>Country</th></tr>
<tr><td>• 64% Male
• 36% Female</td><td>• 45% 18 – 29
• 50% 30 – 49
• 5% above 50</td><td>• 10% High school or less
• 13% Diploma
• 50% Bachelor's
• 26% Postgraduate level</td><td colspan="2">• 46% little/no knowledge
• 40% moderate knowledge
• 14% advanced knowledge</td><td>• 39% Saudi Arabia
• 19% Australia
• 18% India
• 10% China
• 14% Others</td></tr>
<tr><th colspan="6">Users security reactions when facing potential security threats</th></tr>
<tr><th>Reviewing Privacy Policy</th><th>Selecting authentication method for the app</th><th colspan="3">Reactions about requesting access permissions and phishing</th><th>Reporting security issue</th><th>Interest in receiving security learning and advice</th></tr>
<tr><td rowspan="7">• All participants (n=105) spent 14 minutes and 03 seconds.
• Average of 8.02 ms per participant</td><td rowspan="7">• 36% None
• 19% PIN
• 12% Pattern
• 22% Username/ password
• 10% 2FA</td><td>Permission Type</td><td>Granted</td><td>Denied</td><td rowspan="7">• 34% Yes
• 66% No</td><td rowspan="7">• 72% Yes
• 28% No</td></tr>
<tr><td>Pop-up window</td><td>47%</td><td>53%</td></tr>
<tr><td>Device storage</td><td>50%</td><td>50%</td></tr>
<tr><td>Contacts</td><td>47%</td><td>53%</td></tr>
<tr><td>Camera</td><td>45%</td><td>55%</td></tr>
<tr><td>Microphone</td><td>45%</td><td>55%</td></tr>
<tr><td>Location</td><td>50%</td><td>50%</td></tr>
<tr><th colspan="6">Reasons for paying attention to the requested access permissions</th></tr>
<tr><td colspan="6">• App permissions provide a better usage
• Fear of data leakage
- Access permissions make private data vulnerable
- Releasing or sharing private data
- App provider access private data
• Fear of their devices being hacked
• Excessive permission triggers a lack of trust
• Fear of using data for objectionable processing purposes
- Making profit out of data
- Sending unwanted advertisements</td></tr>
</table>

6.2 Access Permissions for the Simulation App

Interestingly, 52 participants (50%) granted the simulation app access to their location. Table 6 presents further details about the participants who granted or denied accessing to their location based on the IT knowledge. **R87** (FBL[2]) wrote *"It is ok to grant the app to access my location because it is already the case with all other apps*". Most likely that users have trust in giving some permissions, such as location or specific hardware (e.g., microphone). This could lead to further work to investigate what other access permissions that users trust, and the reasons that make them trust.

The findings in Section 4.4 (a) indicated that there was no statistical significant difference for access permissions request based on the gender, as in Table 4. However, we further found that 53 participants (50%) denied the

[2] FBL refers to a **F**emale with a **B**achelor degree, and **L**ittle or no knowledge

simulation app access to the storage of their device. To provide further analysis, we looked into the denied permissions based on gender, as in Table 7. We found that females have a higher concern about granting access to their devices. Due to the fact that device storage store their private photos which cannot be shared, accessing device storage received the highest denial by 26 females (68%). This point confirms our results in Table 5 which indicates a statistical significant difference between female and male participants in regards to accessing device storage. Accessing to the device location had the lowest denial by 21 females (55%). **R71** (FBM[3]) wrote, *"[The app] should not access my contacts, photos, or location because the app does not need access to my information*". On the other hand, we found that out of 67 males, 27 (40%) denied access to device storage which is the lowest denial. The highest denial from males were contact and microphone (i.e., 36 males (54%) for each permission request). Table 7 presents the numbers of male and female who granted/denied the access permissions. **R51** (MBM[4]) wrote, *"giving access to your photos and contacts when it is not necessary can lead to giving the app access of transferring sensitive content to the developers"*. In our study conclusion, females have a higher concern about requesting access to the device storage. Device storage store their private photos that cannot be shared others.

We presented an empirical investigation that aimed to understand users' reactions when requesting access permissions. Despite the fact that some apps would not be functioning without accessing the required resources in the device, some apps (including our simulation app) may request unnecessary permissions that can be questionable. Hence, users are encouraged to pay attention to the requested permissions within the apps. App developers, on the other hand, need to request what would be required to make the running. Furthermore, a detailed explanation should be provided for the users to justify such a request.

Table 6. Participants Responses to Requesting Access Permission to their Devices' Locations and Storage based on IT Knowledge Level

Access Permission Type	Options	Little or no IT knowledge (n=48)	Moderate IT knowledge (n=42)	Advanced IT knowledge (n=15)
Access to Location	Granted, 52 (50%)	31 (64%)	16 (38%)	5 (33%)
	Denied, 53 (50%)	17 (36%)	26 (62%)	10 (67%)
Access to Device Storage	Granted, 52 (50%)	29 (60%)	16 (38%)	7 (47%)
	Denied, 53 (50%)	19 (40%)	26 (62%)	8 (53%)

Table 7. Participants Responses to deny the Requested Access Permission based on Gender

Denied access permissions requests based on gender	Device storage	Camera	Contacts	Microphone	Location	pop-up Window
Female (n=38)	26 (68%)	24 (63%)	22 (58%)	22 (58%)	21 (55%)	22 (58%)
Male (n=67)	27 (40%)	32 (48%)	36 (54%)	36 (54%)	32 (48%)	34 (51%)

6.3 Paying attention to the requested permissions

Almost 50% of our participants granted the simulation app permissions. Interestingly, a few participants claimed that they paid attention to app permissions because they were worried about their privacy. However, we found contradiction with their responses in the exit survey. For example, **R34 (**MBM[4]**)**, and **R73** (MHM[5]) fully granted our simulation app the requested permissions. **R34** wrote, "*To not get permissions to private images*", and **R73** wrote, "*I will be unhappy about the more permission than needs and don't trust this app using, so that I will stop the app from accessing my information*". The results also indicated that users can be easily fall into the ambush of sharing their data and devices. This triggers the alarm that users need to pay careful attention when installing

[3] FBM refers to a **F**emale with a **B**achelor degree, and **M**oderate IT knowledge

[4] MBM refers to **M**ale with a **B**achelor degree, and **M**oderate IT knowledge

[5] MHM refers to **M**ale with a **H**igher education, and **M**oderate IT knowledge

and using mobile apps. Further work can be done using similar approach with allowing the participants to share their views about granting or denying permissions after every single request. In addition, a summary report can be shared with each participants as soon as s/he completes the study. Such a summary should explain what mistakes the participant has done with their potential impacts, and what could have been done better when facing these access permissions. Consequently, this would help to increase the security awareness of the users before thinking to grant any app a permission.

We reported the different reasons that our participants considered for granting/denying the requested access permission. Overall, users are required to understand what, why permissions such as app needs by reviewing the privacy policy. App providers needs to minimize the requested permissions as possible and justify the needed permissions for users.

Despite the fact that we had limited security scenarios (Table 2) that we investigated, we believe our study contributed to the existing knowledge through presenting real-life security scenarios that end-users may face every day. We applied an attack simulation approach which helped us to measure users' reactions through posing a few security threats, and monitor their reactions. Our study helped to understand the common weaknesses that end-users fall into when using mobile apps. Our results are expected to make significant contributions to the growing body of evidential knowledge about end-users' reactions when reviewing privacy policy, access permissions and what reasons to grant/deny such permissions.

7. Threats to Validity

We now discuss some threats to the validity that represent potential limitations that might impact the finding of the study.

Internal validity: We collected data through a simulation app, and presented some real-life security scenarios that any users face during mobile apps usage. Findings might get affected since we had to explicitly indicate to the participants that we were investigating their security awareness. Initially our plan was to hide the aim of the study by mentioning that we are going to investigate participants' habits and behaviors towards mHealth apps. Yet, due to the limited-disclosure of the study aim, we were not able to get the ethical approval. Indeed, the application of our study was elevated to a high-risk review, and it took so many reviews until we addressed the concerns of the ethics committee (i.e., explaining the aim of the study for participants in advance). Additionally, our simulation app was not downloadable from the official app stores (i.e., Google Play store). Thus, our participants were skeptical to involve in our study. Even those who have participated, we are unsure whether the participants provide truthful reactions towards the requested access permissions. They might have reacted in a way that is different than they would have otherwise reacted.

Construct validity: Our study could be also impacted by the limited security scenarios that we already measured. Some security scenarios (e.g., password strength, password changing habits) were questionable by the ethics committee; hence, we had to drop them during the study design phase to ensure carrying out the study. In addition, we have limited number of some categories (e.g., only English version, a few participants above the age of 50).

External validity: Our simulation app is only compatible with Android devices. The given time to finish the research has limited us to configure the app with iOS devices of the study. The findings of our study cannot be generalizable.

Conclusion validity: To ensure the credibility of the study conclusions, the first three authors were continuously involved in the survey instrument development and data analysis process. However, all other authors occasionally (consent meetings) reviewed the data and provided their feedback to tackle the conflicts that appeared during the data collection and analysis process. Finally, brainstorming sessions were conducted, and all the authors participated in discussing the study findings and drawing conclusions.

8. Conclusions and Future Work

Mobile computing as the backbone of context-sensitive digital servicing is revolutionizing the smart and mobile health across various domains of medical practices that range from clinical apps, to fitness trackers to diet and nutrition decision support [2]. Despite the offered benefits such as autonomy, efficiency, and pervasiveness of healthcare services, mHealth apps face some challenges pertaining to security and privacy of health critical data.

In addition to developing secure mHealth apps and optimizing the methods and techniques for secure storage, processing, and transmission of data, there is a need to understand and enhance the security awareness of the users. Security understanding of mHealth app users relates to their knowledge and behavior (often translating into actions) to ensure secure usage. In addition to the technical measures that ensure security of mHealth apps, enhancing the security awareness of mobile users is critical due to the high number of security threats and the numerous malicious activities. Such an awareness would help to secure confidential data stored within the devices. We conducted an empirical study to monitor and analyze the actions and behaviors of mHealth app users – relying on an attack simulation approach – to overcome the inherent bias and limitations of the self-reported surveys. The key findings of our study are:

- mHealth users most often overlook the privacy policies while installing or updating the apps, resulting in issues of apps accessing classified data with user granted permissions. We noted that the average time spent on reviewing privacy policies was 8.02 ms, that is 67% less than bare minimum time to go through the policies (at least a minute to review).
- Users (i.e., 36% of our participants) selected no security method for the simulation app as their favourable method to access the app and 47.5% (± 2.5) of our participants have granted our simulation app access to the unnecessary permissions (e.g., accessing contacts, camera, location, etc.).
- The majority of participants had negative views about the requested access permissions (fear of data leakage, fear of their devices being hacked, excessive permission triggers a lack of trust, fear of using data for objectionable processing purposes).

Dimensions for potential future work: This study examined users' security awareness through an attack simulation approach, and it has uncovered some possible directions for future work. It could be further extended to include a larger number of participants with different demographic information. Future studies could also include other security threats which have not been covered in this study (such as strength of passwords, changing passwords, data security at rest and data in transit, etc.). It could be further extended by using the same approach but by also providing a summary report to be shared with each participants as soon as s/he completes the study. Such a summary could explain what mistakes the participant has made and potential impacts of those mistakes, and what could have been done better when facing these access permissions.

Implications of research: The study can have the following implications for research and development of secure and usable mobile health solutions.

- Researchers who are interesting in exploring security awareness of users or specific group of users (e.g., male vs. female). We suggest formulating new hypothesis to be tested for secure mHealth apps (e.g., evaluating how users' perceive reviewing privacy policy as well as employing eye-tracking feature, evaluating users' reactions in regards to granting the common requested permission such as location). Interested researchers on secure mobile computing could utilize an attack simulation research to measure user' reactions as it helps to avoid biased data collection.
- Developers and stakeholders to understand security specific knowledge and behaviors of user, monitored by our proof of the concept attack simulator to develop and provide emerging and futuristic class of mHealth apps that are secure and usable.

Acknowledgments

We thank Abdulrahman Gharwi for sharing his experience that helped to develop the simulation app. We also thank Leonardo Iwaya for his input during the different phases of the study.

References

[1] L. H. Iwaya, A. Ahmad, and M. Ali Babar, "Security and Privacy for mHealth and uHealth Systems: A Systematic Mapping Study," IEEE Access, vol. 8, pp. 150081-150112, 2020.

[2] A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice," IEEE Access, vol. 6, pp. 9390-9403, 2018.

[3] K. Knorr and D. Aspinall, "Security testing for Android mHealth apps," in 2015 IEEE 8th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2015 - Proceedings, 2015.

[4] H. K. Flaten, C. St Claire, E. Schlager, C. A. Dunnick, and R. P. Dellavalle, "Growth of mobile applications in dermatology-2017 update," Dermatology online journal, vol. 24, 2018.

[5] T. Mabo, B. Swar, and S. Aghili, "A vulnerability study of Mhealth chronic disease management (CDM) applications (apps)," in Advances in Intelligent Systems and Computing vol. 745, ed, 2018, pp. 587-598.
[6] F. Zahra, A. Hussain, and H. Mohd, "Factor Affecting Mobile Health Application for Chronic Diseases," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, pp. 77-81, 2018.
[7] L. Ramey, C. Osborne, D. Kasitinon, and S. Juengst, "Apps and Mobile Health Technology in Rehabilitation: The Good, the Bad, and the Unknown," Physical Medicine and Rehabilitation Clinics, vol. 30, pp. 485-497, 2019.
[8] A. M. Research, "Digital Health Market available at https://www.alliedmarketresearch.com/digital-health-market-A10934," 2021.
[9] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, et al., "Conceptual framework for the security of mobile health applications on Android platform," Telematics and Informatics, 2018.
[10] G. Thamilarasu and C. Lakin, "A security framework for mobile health applications," in Proceedings - 2017 5th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2017, 2017, pp. 221-226.
[11] S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025 available at "https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/" [Last accessed: 06/11/2021]," 2020.
[12] F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, "Security of mobile health (mHealth) systems," in 2015 IEEE 15th International Conference on Bioinformatics and Bioengineering, BIBE 2015, 2015.
[13] Y. Cifuentes, L. Beltrán, and L. Ramírez, "Analysis of Security Vulnerabilities for Mobile Health Applications," in 2015 Seventh International Conference on Mobile Computing and Networking (ICMCN 2015), 2015.
[14] R. Bitton, K. Boymgold, R. Puzis, and A. Shabtai, "Evaluating the Information Security Awareness of Smartphone Users," in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1-13.
[15] A. A. Atienza, C. Zarcadoolas, W. Vaughon, P. Hughes, V. Patel, W.-Y. S. Chou, et al., "Consumer attitudes and perceptions on mHealth privacy and security: findings from a mixed-methods study," Journal of health communication, vol. 20, pp. 673-679, 2015.
[16] M. Koyuncu and T. Pusatli, "Security Awareness Level of Smartphone Users: An Exploratory Case Study," Mobile Information Systems, vol. 2019, 2019.
[17] S. Furnell, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user," Computers & Security, vol. 75, pp. 1-9, 2018.
[18] H. Molyneaux, E. Stobert, I. Kondratova, and M. Gaudet, "Security Matters… Until Something Else Matters More: Security Notifications on Different Form Factors," in International Conference on Human-Computer Interaction, 2020, pp. 189-205.
[19] S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," Computers & Security, vol. 25, pp. 27-35, 2006.
[20] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "End-Users' Knowledge and Perception about Security of Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers," arXiv preprint arXiv:2101.10412, 2021.
[21] I. Technologies, "Hackers increasingly exploit human factor avaliable at https://www.ipctech.com/hackers-increasingly-exploit-human-factor/," 2021.
[22] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (HAIS-Q): two further validation studies," Computers & Security, vol. 66, pp. 40-51, 2017.
[23] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "An Empirical Study on Developing Secure Mobile Health Apps: The Developers' Perspective," 27th Asia-Pacific Software Engineering Conference (APSEC), Singapore, Singapore, pp. 208-217, 2020.
[24] B. Aljedaani, A. Ahmad, M. Zahedi, and M. A. Babar, "Security Awareness of End-Users of Mobile Health Applications: An Empirical Study," presented at the MobiQuitous 2020 - 17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, Darmstadt, Germany, 2020.
[25] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A survey of cyber-security awareness in Saudi Arabia," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 154-158.
[26] V. Gkioulos, G. Wangen, S. K. Katsikas, G. Kavallieratos, and P. Kotzanikolaou, "Security awareness of the digital natives," Information, vol. 8, p. 42, 2017.
[27] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," Computers & Security, vol. 34, pp. 47-66, 2013.
[28] B. Watson and J. Zheng, "On the user awareness of mobile security recommendations," in Proceedings of the SouthEast Conference, 2017, pp. 120-127.
[29] M. Zeybek, E. N. Yılmaz, and İ. A. Doğru, "A Study on Security Awareness in Mobile Devices," in 2019 1st International Informatics and Software Engineering Conference (UBMYK), 2019, pp. 1-6.
[30] E. M. Redmiles, Y. Acar, S. Fahl, and M. L. Mazurek, "A summary of survey methodology best practices for security and privacy researchers," 2017.
[31] R. Tourangeau and T. W. Smith, "Asking sensitive questions: The impact of data collection mode, question format, and question context," Public opinion quarterly, vol. 60, pp. 275-304, 1996.
[32] R. Tourangeau and T. Yan, "Sensitive questions in surveys," Psychological bulletin, vol. 133, p. 859, 2007.

[33] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS)," in Proceedings of the 2016 CHI conference on human factors in computing systems, 2016, pp. 5257-5261.
[34] D. Aljeaid, A. Alzhrani, M. Alrougi, and O. Almalki, "Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks," Information, vol. 11, p. 547, 2020.
[35] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks," Education and Information Technologies, pp. 1-24, 2021.
[36] P. Rajivan and C. Gonzalez, "Creative persuasion: a study on adversarial behaviors and strategies in phishing attacks," Frontiers in psychology, vol. 9, p. 135, 2018.
[37] R. Wash, E. Rader, and C. Fennell, "Can people self-report security accurately? Agreement between self-report and behavioral measures," in Proceedings of the 2017 CHI conference on human factors in computing systems, 2017, pp. 2228-2232.
[38] J. S. Molléri, K. Petersen, and E. Mendes, "Survey guidelines in software engineering: An annotated review," in Proceedings of the 10th ACM/IEEE international symposium on empirical software engineering and measurement, 2016, pp. 1-6.
[39] S. Barth, M. D. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," Telematics and informatics, vol. 41, pp. 55-69, 2019.
[40] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in Proceedings of the eighth symposium on usable privacy and security, 2012, pp. 1-14.
[41] E. Struse, J. Seifert, S. Üllenbeck, E. Rukzio, and C. Wolf, "PermissionWatcher: Creating User Awareness of Application Permissions in Mobile Systems," in International Joint Conference on Ambient Intelligence, 2012, pp. 65-80.
[42] P. Wijesekera, A. Baokar, A. Hosseini, S. Egelman, D. Wagner, and K. Beznosov, "Android permissions remystified: A field study on contextual integrity," in 24th {USENIX} Security Symposium ({USENIX} Security 15), 2015, pp. 499-514.
[43] W. Peng, S. Kanthawala, S. Yuan, and S. A. Hussain, "A qualitative study of user perceptions of mobile health apps," BMC Public Health, vol. 16, p. 1158, 2016.
[44] L. Zhou, J. Bao, V. Watzlaf, and B. Parmanto, "Barriers to and facilitators of the use of mobile health apps from a security perspective: Mixed-methods study," JMIR mHealth and uHealth, vol. 7, 2019.
[45] B. Aljedaani, "Measuring the Security Awareness of End-Users towards Using Mobile Health Apps: An Attack Simulation Approach [Supplementary Data]. [Online:] https://sites.google.com/view/attack-simulation-approach/home" 2021.
[46] L. Statistics, "Chi-Square Test for Association using SPSS Statistics [online] available at https://statistics.laerd.com/spss-tutorials/chi-square-test-for-association-using-spss-statistics.php," 2018.
[47] R. G. v. d. Berg, "SPSS Mann-Whitney Test – Simple Example available at https://www.spss-tutorials.com/spss-mann-whitney-test-simple-example/," November 2020.
[48] S. Glen, "Kruskal Wallis H Test: Definition, Examples & Assumptions available at https://www.statisticshowto.com/kruskal-wallis/," May 2021.
[49] L. Statistics, "Kruskal-Wallis H Test using SPSS Statistics [online] available at https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php," 2018.
[50] S. H. To, "Post Hoc Definition and Types of Tests [online] available at https://www.statisticshowto.com/probability-and-statistics/statistics-definitions/post-hoc/."
[51] V. Braun and V. Clarke, "Using thematic analysis in psychology," Qualitative research in psychology, vol. 3, pp. 77-101, 2006.
[52] D. S. Cruzes and T. Dyba, "Recommended steps for thematic synthesis in software engineering," in Empirical Software Engineering and Measurement (ESEM), 2011 International Symposium on, 2011, pp. 275-284.
[53] M. B. Miles and A. M. Huberman, Qualitative data analysis: An expanded sourcebook: sage, 1994.
[54] L. statistics, "Spearman's Rank-Order Correlation [online] available at https://statistics.laerd.com/statistical-guides/spearmans-rank-order-correlation-statistical-guide.php," 2018.
[55] ""Spearman's correlation" available at https://www.statstutor.ac.uk/resources/uploaded/spearmans.pdf."
[56] R. Bitton, A. Finkelshtein, L. Sidi, R. Puzis, L. Rokach, and A. Shabtai, "Taxonomy of mobile users' security awareness," Computers & Security, vol. 73, pp. 266-293, 2018.
[57] M. Rosenblatt, "A central limit theorem and a strong mixing condition," Proceedings of the national Academy of Sciences, vol. 42, pp. 43-47, 1956.
[58] L. Statistics, "Mann-Whitney U Test using SPSS Statistics [online] available at https://statistics.laerd.com/spss-tutorials/mann-whitney-u-test-using-spss-statistics.php," 2018.
[59] T. L. Team, "Mobile App Privacy Policy Template available at "https://termly.io/resources/templates/app-privacy-policy/#what-is-an-app-privacy-policy"," 2017.

[60] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, et al., "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," in The 25th Annual Network and Distributed System Security Symposium (NDSS 2018), 2018.
[61] Y. Bertrand, K. Boudaoud, and M. Riveill, "What do you think about your company's leaks? A survey on end-users perception towards data leakage mechanisms," Frontiers in big Data, vol. 3, p. 38, 2020.
[62] B. Hainzinger, "How to avoid mobile phone apps from leaking your personal data available at https://appdevelopermagazine.com/how-to-avoid-mobile-phone-apps-from-leaking-your-personal-data/," 2020.
[63] T. Germain, "How to Protect Yourself From Camera and Microphone Hacking available at https://www.consumerreports.org/privacy/how-to-protect-yourself-from-camera-and-microphone-hacking-a1010757171/," 2019.
[64] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? An empirical study of mental health app privacy policies and practices," International Journal of Law and Psychiatry, vol. 64, pp. 198-204, 2019.
[65] M. Plachkinova, S. Andres, and S. Chatterjee, "A Taxonomy of mHealth apps - Security and privacy concerns," in Proceedings of the Annual Hawaii International Conference on System Sciences, 2015, pp. 3187-3196.
[66] R. Adhikari, D. Richards, and K. Scott, "Security and privacy issues related to the use of mobile health apps," in Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014, 2014.
[67] B. Martínez-Pérez, I. de la Torre-Díez, and M. López-Coronado, "Privacy and Security in Mobile Health Apps: A Review and Recommendations," Journal of Medical Systems, vol. 39, 2015.
[68] E. P. Morera, I. de la Torre Díez, B. Garcia-Zapirain, M. López-Coronado, and J. Arambarri, "Security Recommendations for mHealth Apps: Elaboration of a Developer's Guide," Journal of Medical Systems, vol. 40, 2016.