Empowering User Security Awareness and Risk Assessment within Gamified Smartphone Environment

Mehrdad Bahrini, Joffrey Weglewski, Karsten Sohr, and Rainer Malaka

Digital Media Lab, TZI, University of Bremen, Bremen, Germany
{mbahrini,joffrey,sohr,malaka}@uni-bremen.de

Abstract. Smartphones facilitate human needs such as communication, entertainment, and knowledge. These instruments simultaneously process and store user data, including email, messages, passwords, financial accounts, and health records. Mobile apps aggregate this data and may transmit it to clouds or third parties. Smartphone operating systems provide security settings and permission mechanisms, empowering users with control over personal data. However, users frequently overlook these, which often leads to data leaks. To prioritize users' attention, we have developed a User Data Access Profile (UDAP) interface to raise awareness and prompt them to evaluate the potential risks of the apps they are considering. We implemented a gamified environment and conducted a between-subjects design study, comparing the UDAP and Android App-Info screens. The findings show that participants were more adept at assessing the privacy risks associated with Android apps when provided with categorized information post-application setup. Additionally, this approach raised user awareness regarding permission grants and configured new apps with personal data.

Keywords: Security Awareness · Risk Assessment · Android Apps · Gamification · Usable Security.

1 Introduction

Smartphone applications (apps) constitute a fundamental aspect of modern digital life, installed by numerous users seemingly without hesitation [9]. Despite this widespread adoption, users exhibit minimal concern regarding the voluntary disclosure of personal data necessary for successful app installations [25]. These unaware decisions increasingly cause the amount of data surrounding users to map their behavior, interests, and thoughts. Ultimately, they are under constant surveillance and provide more targets for attacks and infiltration [29]. Security mechanisms have been implemented and modified for smartphone operating systems to protect the user's privacy. The permission system is an essential component of operating systems such as Android. Each Android app runs in its sandbox with restricted privileges. If an app needs to access resources or information

outside its sandbox, it will ask for the appropriate permission(s) during installation or use. Once an app is installed, a summary of its properties, such as the permissions the app is authorized for, its memory usage, and specific features, including clearing the cache and deleting all data, are available in the "APP-INFO" screen under the Android app settings. Given that the APP-INFO screen does not pop up automatically, users may not constantly review or even be aware of it. Furthermore, studies have revealed that the permission mechanism is often ignored, and users' comprehension is low [23, 15]. Users may make a separate privacy and security assessment when interacting with such highly customized interfaces [30]. They might be comfortable with an app requesting location data for location-based weather forecasting. On the other hand, the same users may find it inappropriate for that same app to access Google account data retrieved for personalized advertising. This ambiguous perception of the app's behavior and lack of knowledge could raise the risk of unintentional resource usage or installation. As a result, users must be informed about such malicious activities, which would reduce the risks of privacy and security breaches [13]. Previous studies have shown that while many smartphone users are aware of information security concepts, their smartphone protection behavior is poor, and they would benefit from education on potential information security risks [12, 35].

Considering the familiarity of Android users with app installation and device configuration, alongside the emerging potential of game-based learning to motivate and enhance knowledge acquisition [24], this study aims to compare the impact of two interfaces within a gamified Android simulator. Specifically, it investigates the effectiveness of the automatic appearance of the APP-INFO page versus providing users with summaries of their data inputs during app configuration on their ability to assess privacy and security risks. To address this inquiry, we devised a gamified Android simulator enabling users to simulate app store browsing, installation, and customization of privacy and security settings. Two representations depict the outcomes of installed and configured apps in the simulator. The initial version, referred to as the *App-Info*, offers a broad overview of the app and its functionalities, akin to the Android APP-INFO page. The second version, known as the User Data Access Profile (*UDAP*), provides a more comprehensive depiction of the personal data provided by the user. Employing a between-subject design, we conducted a comparison of the two presentations. The evaluation results reveal that participants who interacted with the *UDAP* version demonstrated greater accuracy in evaluating the privacy and security risks of targeted apps compared to the other group. These participants expressed enthusiasm for integrating the *UDAP* approach into the Android operating system, indicating a potential for raising security awareness.

2 Related Work

2.1 Empowering Security Knowledge

Individuals acquire two fundamental types of knowledge: conceptual understanding and procedural skills [28]. Conceptual knowledge embodies one's inherent or

articulated grasp of the fundamental principles and interconnections among various elements within a specific domain. This adaptable knowledge transcends specific problem contexts, enabling its application across diverse scenarios [31]. Conversely, procedural knowledge, vital for skill mastery, manifests primarily through performance changes influenced by past experiences rather than explicit recall, often revealing itself in implicit tasks [39]. This knowledge pertains to the ability to execute step sequences for problem-solving but is context-specific and lacks broad applicability [31]. Procedural knowledge finds relevance across numerous disciplines and professions, particularly in managing intricate and potentially risky procedures in fields like healthcare, education, science, and technology [36, 20, 28]. Researchers have explored how conceptual and procedural knowledge impact computer users' self-efficacy in defending against malicious IT threats [4]. Self-efficacy, the belief in one's ability to influence life events through attainable performance levels, plays a crucial role in this context [7]. They have shown that combining conceptual and procedural knowledge affects self-efficacy positively, leading to improved avoidance behavior against online identity theft among computer users [4]. Research indicates that procedural knowledge is also relevant in gamification, as games provide an immersive platform for learning and practicing complex procedures [10]. Gamification techniques such as challenges, stories, and badges have been effectively employed in educational settings to enhance learning experiences [8, 42], even extending to university courses [21]. Game-based approaches significantly enhance the acquisition of procedural knowledge, making learning more efficient and effective [37]. Beyond education, gamification has shown promise in raising cybersecurity awareness and altering behaviors [41, 19, 17]. For instance, implementing gamification in granting Android permissions led to a more captivating and enlightening experience than conventional methods [5]. Similarly, games have been instrumental in educating users about recognizing and avoiding phishing, offering conceptual and procedural knowledge [32]. We apply gaming interventions to enhance users' ability to identify risk assessments and employ privacy management strategies.

2.2 Enhancing Privacy Management

The proliferation of privacy-invasive malware and low-quality apps poses significant challenges, evidenced by numerous instances of sensitive data exposure within the Google Play Store [38]. Moreover, different limitations of smartphone privacy and security mechanisms make it difficult for users and developers to comprehend and handle them [33]. Despite Google's efforts to remove policy-violating apps, privacy-violating ones persistently find their way onto users' devices, complicating the accurate assessment of associated privacy risks, particularly when assuming equal user concern for each risk. Frik et al. underscored the importance of user familiarity with smartphone security settings and associated risks, revealing users' lack of knowledge and the need for comprehensive education [16]. Their study highlighted that many users avoid configuring settings due to usability issues, opting for avoidance strategies rather than adopting effective protection measures. To mitigate the risks associated with private data handling,

Harbach et al. explored the visualization of such risks within the context of Android app permissions [18]. They extended Android's permission dialogues to visually depict accessible private data, leading users to make informed decisions and pay more attention to permission settings. Similarly, Lin et al. proposed privacy profiles to assist users in managing privacy settings, emphasizing the importance of understanding the purpose behind app permissions [26]. Additionally, Liu et al. developed a personalized privacy assistant based on user profiles, offering tailored recommendations for privacy settings [27]. These studies found that user education and personalized recommendations significantly contribute to improved privacy management. Meanwhile, researchers developed "ProtectMyPrivacy" for Android, which detects and controls data access by third-party libraries, offering enhanced privacy management [11]. Bahrini et al. introduced a user-friendly Android analyzer to increase user awareness of Android permissions, emphasizing the importance of understanding data accessibility through permissions [6]. These efforts collectively empower users to make informed decisions and protect their privacy. Our study highlights the importance of providing summaries of data inputs and advice after app installation and initial use.

3 Simulator Description

We developed a gamified simulator app for Android, offering two versions named *UDAP* and *App-Info*. In this simulator, players assist Simon, a tax consultant new to Android, in learning how to install and configure apps. The task involves installing four specified apps and entering the necessary information, with Simon's personal data provided beforehand. The simulator focuses on installing and launching apps from four common categories: tools, games, health & fitness, and social media, commonly used by Android users [3]. Player actions and choices during installation and setup are evaluated within the simulator. The development of the simulator followed an iterative and user-centric design approach [1]. An initial prototype was devised and assessed by potential smartphone users on the university campus. Feedback was collected through various means, including user interactions, observations, and discussions, covering interface clarity and navigation ease. This input guided refinements in design, leading to the simulator's development via Android Studio. The prototype prioritizes augmenting users' procedural knowledge by integrating gamification features such as storytelling, challenges, and feedback.

3.1 Walkthrough

The simulator features an interactive avatar, Simon, who guides players textually and verbally. Simon introduces himself and presents his problem upon app launch. Players progress through dialogue by tapping the screen. Simon disappears after his explanation, allowing players to access the App Store icon. Throughout the simulation, Simon prompts players to install an app from the store, which, once installed, appears on the home screen. The simulated App

Store mirrors the Google Play Store, enabling horizontal and vertical scrolling to explore various app categories (Figure 1 shows this setup).

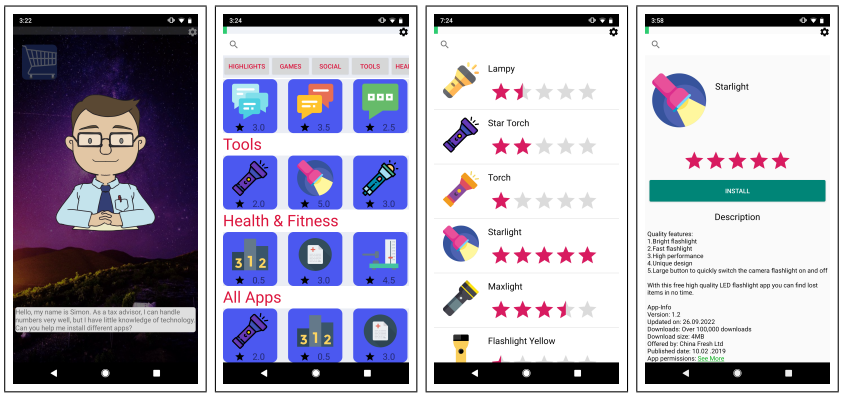

Fig. 1. On the left side, Simon introduces himself; the App Store and the list of flashlight apps are in the middle, while information about the flashlight app is on the right.

Players view detailed information on a dedicated screen after selecting an app in the App Store. They can scroll down to read the full description and tap "See More" to view all required permissions. If a player decides to install the app and matches Simon's desired category, it proceeds with installation; otherwise, Simon intervenes. After successful installation, Simon provides further instructions, including launching the app from the home screen and configuring it according to preferences. The setup process remains consistent for all four apps, granting players control over required data. Users are prompted to create an account or skip this step upon app launch. Subsequent screens prompt for demographic details, which players can skip. The app permissions screen follows, allowing players to review and modify permissions if desired. Additional screens may request information on financial status, health, and religious affiliation, prompting players to decide if this data is necessary (Refer to Figure 3 and Figure 4 in the appendix). Although users can decide what information and permissions the app categories require to run, we have considered certain requirements for each category. Therefore, after the last settings screen and before launching the app, the requirements are prompted depending on the app category. These requirements also play a crucial role in defining the risk level associated with each app. The flashlight app necessitates camera permission, which is considered high-risk due to privacy concerns. Seemingly innocuous apps seeking such permissions can still pose risks. For instance, the flashlight app could misuse camera access to capture media without consent. Additionally, when coupled with apparently harmless permissions like Internet access, the app could exploit data to compromise user privacy [22]. The game app's risk level is considered to be medium. Besides the normal permissions, such as Internet access, it requests permission

to access the user's location, which introduces a moderate level of risk, as the app may share the user's location data within the app, potentially compromising privacy. While location data could enhance gameplay experiences, users should be cautious about sharing it. Conversely, the health & fitness app aims to be safe and low-risk. It requests health information, body sensor permission, and demographic data to function optimally and provides personalized health insights and guidance. The app's risk level is intentionally kept low, as its query data primarily revolve around improving the user's well-being and overall experience. Lastly, the social media app falls under the neutral risk category. Users must create an account, which involves sharing personal details like name, email, and password. Additionally, the app requests camera permission to facilitate photo and video sharing. While the risk here is relatively balanced, users need to be mindful of the information they share on social media platforms, considering potential implications on privacy and security.

3.2 Simulator Versions

After the players successfully install and set up the fourth app, they will encounter one of two screens based on their assigned group. In *App-Info* screen version, Simon pops up again and informs the player what kind of data and to what extent these four apps access his information. For this purpose, each installed app has an *App-Info* page, which mimics the foundational elements of the Info-Page of the latest Android. The player can navigate through the four *App-Info* pages with the left and right arrow keys and view the granted permissions. The app details are also accessible when the player scrolls down. This shortcut directs the player to the app store, providing more details about the app that the player may not have checked before installing. Alternatively, in the *UDAP* screen version, Simon explains how the *UDAP* functions and the information it offers. Similar to the previous one, the player can navigate between the *UDAP*s of the four installed apps. The *UDAP* representation consists of different sections. At the top, the name of the installed app, its corresponding category, and the app's icon are displayed. The Info button in the bottom left corner provides the player details about the colors used in the *UDAP*. Green indicates no issues with the category's settings, yellow signifies that some unnecessary data or permissions were granted, and red implies that the category has been incorrectly configured, potentially leading to personal information exposure. For instance, in the case of the flashlight app, when both camera permissions and internet access are combined, it opens up the possibility of data misuse. Consequently, in Figure 2, the standard permission category is shaded in red to denote this issue.

The *UDAP* incorporates eight sections that align with the information categories set up by the player within the app. Each *UDAP* category offers the player detailed insights into how their actions and the app's features may result in data leakage. The player can review all the entered data by tapping on a category. For each one, privacy and security statements are presented to the player. The privacy recommendations primarily center on protecting personal information and the right to control its dissemination. These guidelines advise users on how

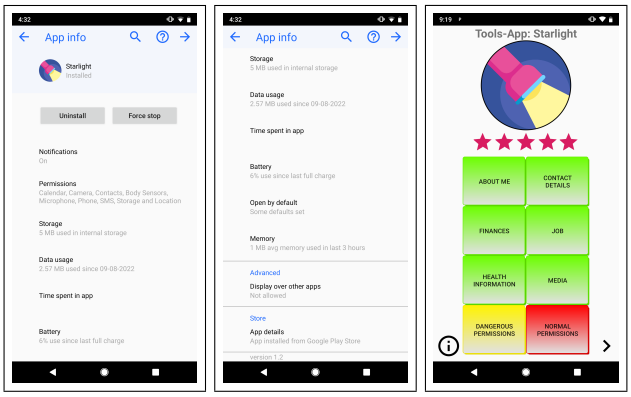

Fig. 2. The left and middle depict the *App-Info*, while the right shows the *UDAP*

to limit the collection, usage, and sharing of their data. At the same time, the security recommendations revolve around safeguarding Android operating systems, networks, and devices from unauthorized access, cyberattacks, and data breaches. The explanations encompass both normal permissions, necessary for the app's regular functionality, and runtime permissions, also known as dangerous permissions, which provide the app with additional access to specified data or the ability to perform restricted actions (Refer to Figure 5 in the appendix).

After completing the simulator, the player is awarded a star ranking based on the entered data. The player's granted permissions and entered data are compared against the recommendations for each app. When the player's decisions align with the advice, points are awarded. A maximum of 25 points can be earned per category, totaling 100 points across the four installed apps. Depending on the player's accumulated points, Simon expresses gratitude with three facial expressions: happy, neutral, or sad.

4 Evaluation

We conducted a user study employing a between-subjects design. Once participants provided informed consent, the study director instructed them to complete pre-exposure questionnaires. Following that, the study instructor explained the simulator's functionality and provided instructions for the experiment. Participants then began playing the simulator according to the assigned version. After completing the simulator, participants were asked to fill out post-exposure questionnaires. Experiments were conducted in the laboratory, each session lasting about 50 minutes per participant. We utilized a Google Pixel 2 XL running Android 9.0 as the device platform, while the simulator mirrored the latest Android version and behavior from the Google Play Store as of March 2022.

Two questionnaires were developed for the data collection. One questionnaire refers to the App-Info variant, and the other to the *UDAP* variant. Consequently, the results for the two variants were collected separately to be evalu-

ated afterward. Both questionnaire sections were identically structured to allow a comparison between the two variants. The pre-exposure questionnaires deal with the participant's demographic information, including gender and age. They also include questions about installing an Android app to obtain the participants' awareness and attitude toward this topic. The post-exposure questionnaires have three sections. In the first one, we requested participants to deliver an overall risk assessment concerning the four installed apps, utilizing a 5-point Likert scale that measures individuals' risk perceptions from "Not Risky at All" to "Very Risky". Participants then had to assess the privacy risk associated with each app requirement, including account creation, personal data, bank account information, health data, and claimed permissions. Similar to the initial section, 5-point Likert scales were employed for each inquiry, maintaining the same scope. Finally, the post-exposure questionnaires comprised specific questions about the respective simulator variants. The aim was to collect participant feedback regarding their experiences with the specified simulator. They were asked to express their general opinion and address the potential and challenges of simulators. All questions are included in the paper appendix.

We conducted the study in German, with exclusively German-speaking participants selected through a quota sampling strategy based on predetermined criteria. This recruitment approach aimed to obtain a sample of Android users who were unique to each condition. The participation was entirely voluntary and without remuneration. Participants were recruited through mailing lists, social networks, and word-of-mouth. A total of 32 people partook in the study. In the *App-Info* group, 16 participants (8 female and 8 males) were between 18 and 31 years aged ($M = 25.1$, $SD = 3.7$). Within the *UDAP* group, 16 participants (7 females and 9 males) were between 19 and 32 years old ($M = 25.7$, $SD = 3.16$). All participants used the Google Play store to search for and install new apps. Regarding the information they look for before installing a new app, all respondents indicated that they pay attention to the name of the app they seek and whether it is cost-free. In the *App-Info* group, seven respondents said they check for ratings and reviews of the apps, as do 11 respondents in the *UDAP* group. Two participants in each group also pay attention to the app description. We asked participants if they pay attention to app permissions and decide whether or not to use an app based on those permissions and if they can identify whether the requested permissions are essential. In the *App-Info* group, only one user sometimes attends to permissions. 2 participants rarely, and 13 of them never. Fifteen stated that permissions do not influence their decision to use an app. Only one person specified rarely. 2 participants in this group stated that they could sometimes understand why an app requests permissions. Twelve participants were not able to, and 2 participants rarely. Among the *UDAP* group, four users rarely pay attention to permissions, and 12 never do. Fifteen of them stated that permissions do not influence their decision to use an app or not, and only one person rarely. 2 participants in this group said they rarely know why an app requests permissions and 14 participants cannot understand. Following these questions, we further asked participants how concerned they are about

their privacy when installing a new app and whether they can quickly determine whether an app violates their privacy. In the *App-Info* group, 5 participants indicated concern about their privacy, and six were somewhat concerned. Two participants are neutral, one is relatively unconcerned, and one is unconcerned. Eleven participants stated that they could never tell if an app violates their privacy, four users rarely, and only one person frequently. Within the *UDAP* group, 5 participants reported concern about their privacy when installing a new app; nine users are somewhat concerned, and two are neutral. Regarding whether an app violates their privacy, 9 participants can never determine this, and seven users can rarely find out.

5 Results

5.1 Overall Risk Assessment

Participants were asked to assess the overall risk of the four installed apps. We applied statistical analysis to determine possible differences between the two groups. An alpha level of 0.05 was used for all statistical tests. The independent t-test [34] demonstrated that participants in the *UDAP* group ($M = 3.31$, $SD = 1.35$) considered the flashlight app significantly riskier ($t(30) = -4.25$, $p < .001$, $Cohen'sd = -1.5$) than participants in the *App-Info* group ($M = 4.81$, $SD = 0.4$). The independent t-tests for the other three app categories revealed no significant differences between the two conditions ($p > .05$) (see Table 1).

Table 1. Overall Risk Assessment of Game, Health & Fitness, and Social Media

	Game		Health & Fitness		Social Media	
	App-Info	UDAP	App-Info	UDAP	App-Info	UDAP
Mean	3.44	4.06	3.13	2.44	3.44	3.69
Std. Deviation	1.26	0.77	1.41	1.09	1.41	1.35

5.2 Categories Risk Assessment

We asked players in both groups to evaluate the risks of 5 categories of requested data, including account creation, personal data, bank account information, health data, and requested permissions in each app category.

Tools Regarding the flashlight app, the independent t-test showed that participants in the *UDAP* group ($M = 4.88$, $SD = 0.45$) found creating an account significantly riskier ($t(30) = -5.53$, $p < .001$, $Cohen'sd = -1.95$) than participants in the *App-Info* group ($M = 3.25$, $SD = 1.13$). The players in the *UDAP* group ($M = 4.94$, $SD = 0.25$) perceived entering personal data to be riskier

($t(30) = -3.08$, $p = 0.004$, $Cohen'sd = -1.09$) than players in the App-Info group ($M = 4.13$, $SD = 1.03$). The statistical test confirmed that asking for bank account data was riskier ($t(30) = -3.17$, $p = 0.003$, $Cohen'sd = -1.12$) for the *UDAP* players ($M = 4.94$, $SD = 0.25$) than for the players in the *App-Info* group ($M = 4$, $SD = 1.16$). Similarly, giving camera permission was riskier ($t(30) = -2.27$, $p = 0.03$, $Cohen'sd = -0.8$) for participants in the *UDAP* group ($M = 3.94$, $SD = 0.77$) than for the *App-Info* group ($M = 3.38$, $SD = 0.62$). We did not find significant changes in giving health information ($p > .05$).

Games Concerning the game app, the independent t-test revealed that participants in the *App-Info* group ($M = 3.56$, $SD = 1.03$) found creating an account significantly riskier ($t(30) = 3.96$, $p < .001$, $Cohen'sd = 1.4$) than participants in the *UDAP* group ($M = 2.13$, $SD = 1.03$). The statistical test indicated that asking for bank account data was riskier ($t(30) = -3.05$, $p = 0.005$, $Cohen'sd = -1.08$) for the *UDAP* players ($M = 4.88$, $SD = 0.34$) than for the players in the *App-Info* group ($M = 3.75$, $SD = 1.44$). The players in the *UDAP* group ($M = 4.88$, $SD = 0.34$) perceived entering health data to be riskier ($t(30) = -2.51$, $p = 0.018$, $Cohen'sd = -0.87$) than players in the *App-Info* group ($M = 4.15$, $SD = 1.15$). Granting location permission was also riskier ($t(30) = 2.18$, $p = 0.037$, $Cohen'sd = 0.77$) for participants in the *App-Info* group ($M = 4$, $SD = 0.82$) than for the *UDAP* group ($M = 3.44$, $SD = 0.63$). We did not find significant changes in giving personal data ($p > .05$).

Health & Fitness The independent t-test indicated that asking for bank account data was riskier ($t(30) = -3.07$, $p = 0.005$, $Cohen'sd = -1.08$) for the *UDAP* players ($M = 4.63$, $SD = 0.72$) than for the players in the *App-Info* group ($M = 3.13$, $SD = 1.82$). The participants in the *App-Info* group ($M = 3.5$, $SD = 1.55$) perceived entering health data to be riskier ($t(30) = -2.15$, $p = 0.040$, $Cohen'sd = -0.76$) than participants in the *UDAP* group ($M = 2.63$, $SD = 0.5$). Granting body sensor permission was also riskier ($t(30) = 3.51$, $p = 0.001$, $Cohen'sd = 1.24$) for players in the *App-Info* group ($M = 3.25$, $SD = 1.39$) than for the *UDAP* group ($M = 1.88$, $SD = 0.72$). We did not notice significant changes in setting up accounts and entering personal data ($p > .05$).

Social Media Regarding the social media app, the statistical test indicated that participants in the *App-Info* group ($M = 3.63$, $SD = 1.2$) found creating an account significantly riskier ($t(30) = 4.44$, $p < .001$, $Cohen'sd = -1.57$) than participants in the *UDAP* group ($M = 1.94$, $SD = 0.93$). There were no significant changes in the entry of personal data, bank account information, health data, and granting camera permission ($p > .05$).

5.3 Participants Feedback

Within the *App-Info* group, 14 participants stated that they were unaware of the *App-Info* page on Android, and only two used it sometimes. One player was very

dissatisfied with the *App-Info* page providing enough security and privacy information about the particular app. Seven participants were dissatisfied, and eight users were neutral. Fifteen participants stated that Android needs a mechanism to display security and privacy concerns regarding an app. Only one respondent indicated that this might be the case. All respondents indicated that a mechanism is required to provide more information on the privacy and security of apps. Three respondents specified that the goal of permissions should be more precise. Two respondents specified that this mechanism needs to be able to be turned on or off by users. In contrast, all participants in the *UDAP* group indicated that they use the *UDAP* mechanism every time they install new apps if it is available on their smartphone. Fourteen users were delighted with the *UDAP* providing enough privacy and security information about the particular app, and only two were satisfied. All respondents mentioned that Android requires the *UDAP* mechanism to indicate privacy concerns regarding an app. Similarly, all users reported wanting to see this mechanism on Android rather than in the Google Play Store. Twelve participants claimed that the *UDAP* mechanism informed them very well, and they could quickly find out the privacy and security statements. 2 participants thought there should be a way for the *UDAP* mechanism to automatically set the apps according to the recommendations if requested by the user. One pointed out that this mechanism could also be displayed before the app is launched so that users can get information beforehand.

6 Discussion

The analysis of the study's results provides an insightful discussion of how the two study groups perceived and evaluated the risks associated with various app categories. It is evident from the findings that the *UDAP* group tends to have a more conservative and cautious approach, likely due to a heightened awareness of privacy and security issues, which is reflected in their accurate high-risk assessment of the flashlight app. This group's sensitivity to privacy infringements may derive from a more robust understanding or prior negative experiences with app permissions. On the other hand, the *App-Info* group's assessments of the game and social media apps indicate a slight understanding of risk that aligns well with real-world app usage scenarios, recognizing the trade-offs between functionality and potential privacy concerns [40]. Their evaluations suggest that while they may not always perceive higher risks, they are attuned to the specific risks that are more prevalent or impactful. This divergence in risk perception highlights the critical need for developing effective educational tools and clearer privacy information mechanisms [16]. Such initiatives should aim to bridge the procedural knowledge and risk awareness gap, ensuring that all users, regardless of their initial awareness level, can make informed decisions about app installations and data sharing. The qualitative feedback from participants provided further insights into their perceptions and preferences. In the *App-Info* group, many participants expressed a lack of awareness about the *App-Info* page on Android. Several participants expressed dissatisfaction with the level of privacy and secu-

rity information provided on the *App-Info* page. They emphasized the need for Android to display more comprehensive privacy and security concerns regarding an app. Conversely, players in the *UDAP* group conveyed their readiness to incorporate the *UDAP* interface into their routine for installing new apps, expressing satisfaction with its capability to furnish privacy and security details. They emphasized the need for Android to integrate the *UDAP* mechanism rather than relying solely on the Google Play Store. Some participants suggested additional features or improvements, such as automatic app configuration based on recommendations and displaying the *UDAP* before launching an app. These suggestions reflect users' desire for a more seamless and integrated experience supporting their decision-making while prioritizing privacy and security concerns. Overall, the study's findings demonstrate the potential of the *App-Info* and *UDAP* approaches to improve users' ability to assess privacy and security risks associated with app usage. By providing users with transparent and comprehensive information, these approaches can enhance users' procedural knowledge and contribute to a more privacy-conscious app installation process [14]. Further research and development could help refine these approaches and address users' needs and preferences, ultimately fostering a safer and more user-centric app ecosystem [2]. While the study provides valuable insights, it is essential to consider its limitations for a comprehensive interpretation of the findings. The sample size was relatively small, and the study focused on German-speaking participants, limiting the generalizability of the results. Our comprehension of the impact of the feedback mechanism (facial expressions: happy, neutral, or sad) on participants' post-exposure responses remains limited, leaving a gap in our knowledge of how this mechanism shapes individuals' answers following their exposure to certain stimuli or experiences. Moreover, the reliance on self-reported data introduces the possibility of biases and subjective interpretations. A simulated environment may not fully capture real-world app usage scenarios, potentially affecting participants' behavior and risk assessments. Additionally, the study focused on specific app categories, potentially overlooking risks associated with other types of apps and comparing only two interfaces, which might cover only a portion of the complete range of possibilities.

7 Conclusion and Future Work

This study compared smartphone users' risk perceptions across different app categories in a gamified setting. The *UDAP* group adopts a conservative approach driven by a heightened awareness of privacy and security, while the *App-Info* group demonstrates an understanding of the trade-offs between functionality and privacy concerns. Future research could extend to other platforms and demographics with longitudinal studies. Additionally, testing advanced privacy features and integrating privacy assessments into app development are crucial steps to improve app protection and boost user privacy awareness.

Acknowledgments. This work was funded by the Klaus Tschira Foundation.

Appendix A Questionnaires

A.1 Android Awareness Questions

- How do you usually install an app on your smartphone?
- What information do you look for before installing an app?
- Based on the previous question, how do you find this information?
- Do you pay attention to the permissions of a new app?
- Are you comfortable determining whether or not requested permissions are required?
- Do permissions affect your decision to download or use an app?
- How concerned are you about your privacy when installing a new app?
- Can you comfortably determine if an app violates your privacy?

A.2 Post-Exposure Questions: Overall Risk Assessment

- How do you assess the risk of the installed Flashlight app violating your privacy?
- How do you assess the risk of the installed Game app violating your privacy?
- How do you assess the risk of the installed Health & Fitness app violating your privacy?
- How do you assess the risk of the installed Social Media app violating your privacy?

A.3 Post-Exposure Questions: Categories Risk Assessment

- Which of the queries in the Flashlight app pose a risk to your privacy, and to what extent?
- Which of the queries in the Game app pose a risk to your privacy, and to what extent?
- Which of the queries in the Health & Fitness app pose a risk to your privacy, and to what extent?
- Which of the queries in the Social Media app pose a risk to your privacy, and to what extent?

A.4 Post-Exposure Questions: Feedback (App-Info group)

- The App-Info page displays information about installed apps in the Android settings. Do you use this page on your smartphone?
- How satisfied are you that the App-Info page contains enough security and privacy information about the specific app?
- On Android, you can manage permissions through settings. However, some settings in the apps can affect your privacy. Do you think Android needs a mechanism to indicate security and privacy concerns about an app?
- If you have an idea about such a mechanism based on the last question, please share how the Android settings or the Google Play Store should inform users about app privacy and security.

A.5 Post-Exposure Questions: Feedback (UDAP group)

- The UDAP page displays information about installed apps in the Android settings. Do you want to see and use it on your smartphone?
- How satisfied are you that the UDAP page contains enough security and privacy information about the specific app?
- On Android, you can manage permissions through settings. However, some settings in the apps can affect your privacy. Do you think Android needs the UDAP mechanism to indicate security and privacy concerns about an app?
- The UDAP mechanism can be implemented either in the Google Play Store or in the Android operating system. In which environment would you prefer this mechanism?
- Based on the last question, please indicate to what extent the UDAP should inform users about app privacy and security in Android settings or the Google Play Store.

Appendix B The Screenshots of the Simulator

The following screenshots show the flashlight app's configuration post-installation and initial use. Players are tasked with identifying the essential information needed for this app.

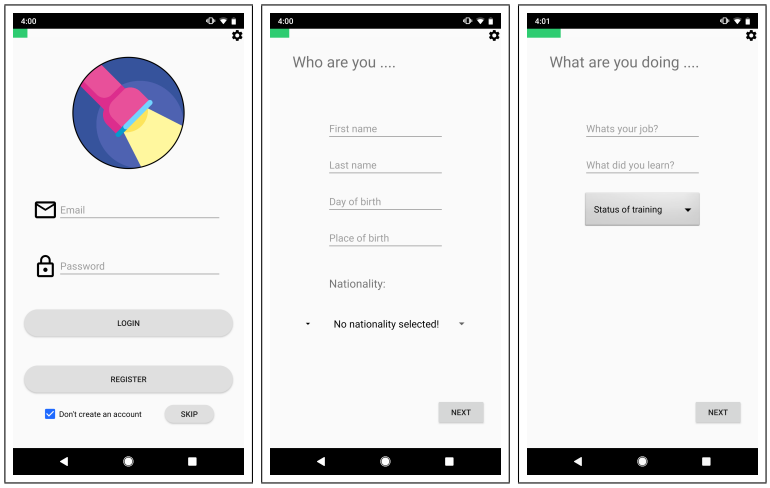

Fig. 3. During this step, a player installs the desired app, in this case, a flashlight, and launches it for the first time. To utilize the app, the player needs to configure its settings. On the left, the player can create an account; in the middle, provide demographic information; and on the right, specify Simon's job occupation. The player must decide for each step whether this information is required when using this app.

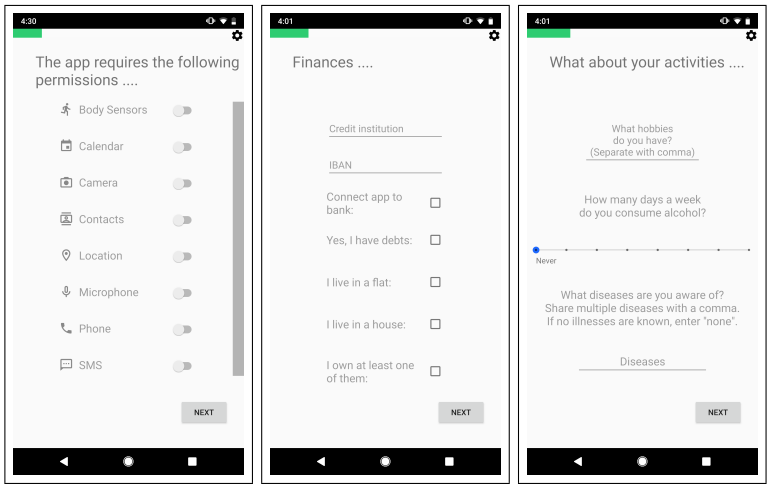

Fig. 4. The three screenshots offer the player various choices: granting permissions on the left, inputting financial information in the middle, and providing health information on the right. The player has the option to either configure or skip each of these choices.

Appendix C The Screenshots of the UDAP Interface

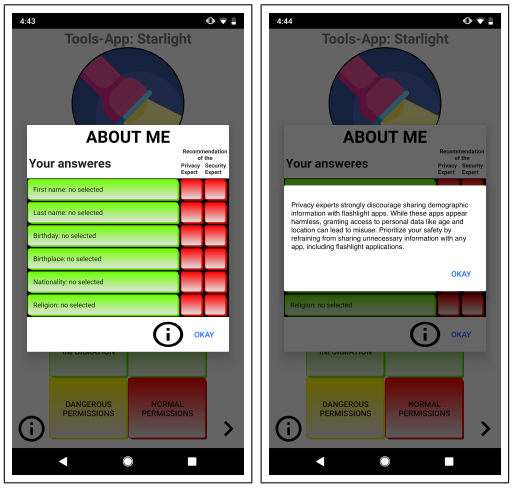

Fig. 5. The two screenshots guide the player regarding the "About Me" category in *UDAP*, showing insights into possible data leakage from actions and app features. These insights are accessible through tapping and accompanying privacy and security statements.

References

1. Abras, C., Maloney-Krichmar, D., Preece, J., et al.: User-centered design. Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications **37**(4), 445–456 (2004)
2. Alsoubai, A., Ghaiumy Anaraky, R., Li, Y., Page, X., Knijnenburg, B., Wisniewski, P.J.: Permission vs. app limiters: Profiling smartphone users to understand differing strategies for mobile privacy management. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA (2022), https://doi.org/10.1145/3491102.3517652
3. Appfigures, Statista: Google play most popular app categories 2022. https://www.statista.com/statistics/279286/google-play-android-app-categories/ (Oct 2022), accessed: 2024-3-27
4. Arachchilage, N.A.G., Love, S.: Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior **38**, 304–312 (2014). https://doi.org/https://doi.org/10.1016/j.chb.2014.05.046
5. Bahrini, M., Volkmar, G., Schmutte, J., Wenig, N., Sohr, K., Malaka, R.: Make my phone secure! using gamification for mobile security settings. In: Proceedings of Mensch Und Computer 2019. p. 299–308. MuC'19, Association for Computing Machinery, New York, NY, USA (2019), https://doi.org/10.1145/3340764.3340775
6. Bahrini, M., Wenig, N., Meissner, M., Sohr, K., Malaka, R.: Happypermi: Presenting critical data flows in mobile application to raise user security awareness. In: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems. p. 1–6. CHI EA '19, Association for Computing Machinery, New York, NY, USA (2019), https://doi.org/10.1145/3290607.3312914
7. Bandura, A.: Self-efficacy: toward a unifying theory of behavioral change. Psychological review **84**(2), 191 (1977)
8. Barata, G., Gama, S., Jorge, J., Gonçalves, D.: Studying student differentiation in gamified education: A long-term study. Computers in Human Behavior **71**, 550–585 (2017). https://doi.org/https://doi.org/10.1016/j.chb.2016.08.049
9. Barth, S., de Jong, M.D., Junger, M., Hartel, P.H., Roppelt, J.C.: 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 **41**, 55–69 (2019). https://doi.org/https://doi.org/10.1016/j.tele.2019.03.003
10. Boyle, E.A., Connolly, T.M., Hainey, T., Boyle, J.M.: Engagement in digital entertainment games: A systematic review. Computers in Human Behavior **28**(3), 771–780 (2012). https://doi.org/https://doi.org/10.1016/j.chb.2011.11.020
11. Chitkara, S., Gothoskar, N., Harish, S., Hong, J.I., Agarwal, Y.: Does this app really need my location? context-aware privacy management for smartphones. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **1**(3) (sep 2017), https://doi.org/10.1145/3132029
12. Das, A., Khan, H.U.: Security behaviors of smartphone users. Information & Computer Security **24**(1), 116–134 (2016)
13. Di Geronimo, L., Braz, L., Fregnan, E., Palomba, F., Bacchelli, A.: UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception, p. 1–14. Association for Computing Machinery, New York, NY, USA (2020), https://doi.org/10.1145/3313831.3376600

14. Ebert, N., Alexander Ackermann, K., Scheppler, B.: Bolder is better: Raising user awareness through salient and concise privacy notices. In: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. CHI '21, Association for Computing Machinery, New York, NY, USA (2021), https://doi.org/10.1145/3411764.3445516
15. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: User attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security. SOUPS '12, Association for Computing Machinery, New York, NY, USA (2012), https://doi.org/10.1145/2335356.2335360
16. Frik, A., Kim, J., Sanchez, J.R., Ma, J.: Users' expectations about and use of smartphone privacy and security settings. In: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. CHI '22, Association for Computing Machinery, New York, NY, USA (2022), https://doi.org/10.1145/3491102.3517504
17. Hamari, J., Koivisto, J.: Social motivations to use gamification: An empirical study of gamifying exercise. In: ECIS 2013 - Proceedings of the 21st European Conference on Information Systems. Association for Information Systems, United States (2013), european Conference on Information Systems, ECIS ; Conference date: 06-06-2013 Through 08-06-2013
18. Harbach, M., Hettig, M., Weber, S., Smith, M.: Using personal examples to improve risk communication for security & privacy decisions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. p. 2647–2656. CHI '14, Association for Computing Machinery, New York, NY, USA (2014), https://doi.org/10.1145/2556288.2556978
19. Hendrix, M., Al-Sherbaz, A., Victoria, B.: Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games **3**(1), 53–61 (Mar 2016). https://doi.org/10.17083/ijsg.v3i1.107
20. Hiebert, J., Lefevre, P.: Conceptual and procedural knowledge in mathematics: An introductory analysis. Conceptual and procedural knowledge: The case of mathematics **2**, 1–27 (1986)
21. Iosup, A., Epema, D.: An experience report on using gamification in technical higher education. In: Proceedings of the 45th ACM Technical Symposium on Computer Science Education. p. 27–32. SIGCSE '14, Association for Computing Machinery, New York, NY, USA (2014), https://doi.org/10.1145/2538862.2538899
22. Karthick, S., Binu, S.: Android security issues and solutions. In: 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA). pp. 686–689 (2017). https://doi.org/10.1109/ICIMIA.2017.7975551
23. Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D.: A conundrum of permissions: installing applications on an android smartphone. In: International conference on financial cryptography and data security. pp. 68–79. Springer (2012)
24. Krath, J., Schürmann, L., von Korflesch, H.F.: Revealing the theoretical basis of gamification: A systematic review and analysis of theory in research on gamification, serious games and game-based learning. Computers in Human Behavior **125**, 106963 (2021). https://doi.org/https://doi.org/10.1016/j.chb.2021.106963
25. Li, K., Cheng, L., Teng, C.I.: Voluntary sharing and mandatory provision: Private information disclosure on social networking sites. Information Processing & Management **57**(1), 102128 (2020). https://doi.org/https://doi.org/10.1016/j.ipm.2019.102128

26. Lin, J., Liu, B., Sadeh, N., Hong, J.I.: Modeling Users' mobile app privacy preferences: Restoring usability in a sea of permission settings. In: 10th Symposium On Usable Privacy and Security (SOUPS 2014). pp. 199–212. USENIX Association, Menlo Park, CA (Jul 2014), https://www.usenix.org/conference/soups2014/proceedings/presentation/lin
27. Liu, B., Andersen, M.S., Schaub, F., Almuhimedi, H., Zhang, S.A., Sadeh, N., Agarwal, Y., Acquisti, A.: Follow my recommendations: A personalized privacy assistant for mobile app permissions. In: Twelfth Symposium on Usable Privacy and Security (SOUPS 2016). pp. 27–41. USENIX Association, Denver, CO (Jun 2016), https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu
28. McCormick, R.: Conceptual and procedural knowledge. International journal of technology and design education **7**, 141–159 (1997)
29. Michel, M.C.K., King, M.C.: Cyber influence of human behavior: Personal and national security, privacy, and fraud awareness to prevent harm. In: 2019 IEEE International Symposium on Technology and Society (ISTAS). pp. 1–7 (2019). https://doi.org/10.1109/ISTAS48451.2019.8938009
30. Peruma, A., Palmerino, J., Krutz, D.E.: Investigating user perception and comprehension of android permission models. In: Proceedings of the 5th International Conference on Mobile Software Engineering and Systems. p. 56–66. MOBILESoft '18, Association for Computing Machinery, New York, NY, USA (2018), https://doi.org/10.1145/3197231.3197246
31. Rittle-Johnson, B., Siegler, R.S., Alibali, M.W.: Developing conceptual understanding and procedural skill in mathematics: An iterative process. Journal of educational psychology **93**(2), 346 (2001)
32. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd symposium on Usable privacy and security. p. 88–99. SOUPS '07, Association for Computing Machinery, New York, NY, USA (2007). https://doi.org/10.1145/1280680.1280692, https://doi.org/10.1145/1280680.1280692
33. Stevens, R., Ganz, J., Filkov, V., Devanbu, P., Chen, H.: Asking for (and about) permissions used by android apps. In: 2013 10th Working Conference on Mining Software Repositories (MSR). pp. 31–40. IEEE (2013)
34. Student: The probable error of a mean. Biometrika pp. 1–25 (1908)
35. Taha, N., Dahabiyeh, L.: College students information security awareness: A comparison between smartphones and computers. Education and Information Technologies **26**(2), 1721–1736 (mar 2021), https://doi.org/10.1007/s10639-020-10330-0
36. Tsai, Y.L., Tsai, C.C.: A meta-analysis of research on digital game-based science learning. Journal of Computer Assisted Learning **36**(3), 280–294 (2020). https://doi.org/https://doi.org/10.1111/jcal.12430
37. Turner, A.P., Martinek, T.J.: An investigation into teaching games for understanding: Effects on skill, knowledge, and game play. Research Quarterly for Exercise and Sport **70**(3), 286–296 (1999). https://doi.org/10.1080/02701367.1999.10608047, pMID: 10522286
38. Wang, H., Li, H., Li, L., Guo, Y., Xu, G.: Why are android apps removed from google play? a large-scale empirical study. In: Proceedings of the 15th International Conference on Mining Software Repositories. p. 231–242. MSR '18, Association for Computing Machinery, New York, NY, USA (2018), https://doi.org/10.1145/3196398.3196412

39. Willingham, D.B., Nissen, M.J., Bullemer, P.: On the development of procedural knowledge. Journal of experimental psychology: learning, memory, and cognition **15**(6), 1047 (1989)
40. Wottrich, V.M., van Reijmersdal, E.A., Smit, E.G.: The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. Decision Support Systems **106**, 44–52 (2018). https://doi.org/https://doi.org/10.1016/j.dss.2017.12.003
41. Zhang-Kennedy, L., Chiasson, S.: A systematic review of multimedia tools for cybersecurity awareness and education. ACM Comput. Surv. **54**(1) (jan 2021), https://doi.org/10.1145/3427920
42. Zichermann, G., Cunningham, C.: Gamification by design: Implementing game mechanics in web and mobile apps. " O'Reilly Media, Inc." (2011)