Factors Influencing Smartphone Application Downloads

Wiehan Janse van Rensburg, Kerry-Lynn Thomson, Lynn Futcher

Factors Influencing Smartphone Application Downloads

Wiehan Janse Van Rensburg[1[0000-0002-9142-361X]], Kerry-Lynn Thomson[2[0000-0002-6456-9701]], and Lynn Futcher[3[0000-0003-0406-8718]]

Nelson Mandela University, Port Elizabeth, South Africa
[1]s213461846@mandela.ac.za, [2]kerry-lynn.thomson@mandela.ac.za, [3]lynn.futcher@mandela.ac.za

Abstract. Mobile applications are increasingly being downloaded in modern society. Despite providing many benefits to potential users, many such applications pose security risks to their users including the leaking of personal information. When applications provide features that fulfil the users' needs, smartphone users often neglect to consider security when downloading applications. This paper explores whether students consider relevant Security Factors when selecting an application to download. A Smartphone Simulation Exercise and related questions were used to determine students' reported behaviour regarding smartphone application downloads. The findings suggest that many students do not consider relevant Security Factors important when downloading applications and, therefore, need to be educated in this regard.

Keywords: Mobile Applications, Smartphone Behaviour, Secure Application Downloads, Security Factors

1 Introduction

The number of global smartphone users has grown significantly over the past years, and it is estimated that by the end of 2018, there will be 2.53 billion smartphone users globally [1]. With this demand for smartphones, the need for mobile applications has also increased. The most widely adopted operating system (OS) amongst smartphone users is Android OS having more than 80% of the market share [2]. Smartphone users can choose from millions of applications found in application marketplaces, such as Google Play Store, and it is estimated that smartphone users spend 90% of their time on mobile applications [3]. Smartphone users who download applications are generally aware of the benefits that the applications can provide but are often not aware of the associated risks that these applications can pose [4].

As smartphones become omnipresent in society, increased amounts of private information regarding smartphone users are being collected and shared by the applications they use. Further, due to the distribution models employed, application marketplaces have become targets of cybercrime, making it easy for attackers to upload malicious applications. Smartphone users that download applications but neglect to review the security of the application could find themselves using malicious applications that

could have a negative impact on their privacy and personal information. Therefore, security should be considered by smartphone users when downloading applications.

This paper highlights eight factors that should be considered by smartphone users when downloading an application. The eight factors identified were based on what the Google Play Policy stipulates should be contained within the application listing and on what smartphone users typically see when viewing applications listed within the Google Play Store. The Google Play Developer Policy Center specifies to the developers what they should consider whilst developing an application and this forms the guidelines as to what developers should adhere to [5]. However, only those aspects that are visible to the user when downloading an application were used for this study. The eight factors identified are Application Rating, Application Reviews, Number of Downloads, Detailed Information, Privacy Policy, Permissions Requested, the Developer of the Application, and when the Last Update was released.

The purpose of this paper is to identify whether Information Technology students from a typical higher educational institution in South Africa consider relevant security factors when selecting an application to download. This research focused on the reported behaviour of the students regarding application downloads. A Smartphone Simulation Exercise to determine students' reported behaviour was conducted to identify the most influential factors that students consider when selecting an application to download. The use of simulations allows students to engage within real world situations. This form of teaching also includes group discussions, debates, collaborative projects and internships. This can include any method that asks students to help develop and apply their knowledge [6]. The use of simulations can recreate complex processes in the classroom, allowing students to examine the motivations, behavioural constraints, resources and interactions amongst institutional actors [7]. In this context, students can immerse themselves in real decision-making processes, and thus allowing the course content to become more relevant.

This was followed by related questions regarding their general smartphone usage and general security awareness relating to smartphone application downloads.

The structure of the paper is as follows: Section 2 provides background on smartphone usage and related threats, while Section 3 presents the eight factors which were used in the study. Section 4 discusses the research process followed and the results and findings of the study are presented in Section 5, with a related discussion in Section 6. Section 7 concludes the paper.

2 Smartphone Usage

The adoption of smartphones amongst users has seen a significant increase because of the wide variety of productivity tools, entertainment, functions, and special features offered through their associated applications [8].

Most smartphone users download and install applications, but neglect to review the privacy policies of the applications [9]. These applications, once granted the permissions, have the ability to collect, store, and transmit the personal and private information they collect. Smartphone users often unknowingly surrender personal information for

the expected benefits that smartphone applications might provide, but the release of private information might also come with related risk. Smartphone users that download applications, but do not take security into consideration, could unknowingly authorize access to some protected resources or allow an application to alter users' privacy and security settings due to a lack of awareness regarding the risk posed by applications.

Information security on a smartphone can be seen as the knowledge, attitude, and behaviour that users apply in protecting their personal information [4]. The different types of information that can be found on smartphone devices includes; personal, organizational, financial, authentication, connectivity, or service information [10]. Traditionally, information security was focused on addressing technical solutions to secure users' information assets stored on their devices and little focus was placed on users and their responsibilities. Smartphone users need to take control with regards to information security [11]. The next section presents eight factors, identified through literature that influence smartphone application downloads.

3 Typical Factors within Application Listings

When application developers design and develop applications to upload onto the Google Play Store, they are required to adhere to the relevant policies regarding what should be included within an application listing. Google Play's Developer Policy Center outlines to developers what is required when listing an application on the Play Store to help encourage users to download their application. Within this policy it includes aspects such as App Promotions, Metadata, User Ratings, Reviews, Installs, and Content Ratings [5]. When smartphone users download applications, they would generally look at what information the application listing contains and base their decision to download an application on the information provided. Within an application listing, the following eight factors, as shown in Table 1, can be used to gather more information about an application.

Table 1. Typical factors within an application listing.

Factors	Description of Factors
Application Rating	The application rating can be seen as a measure to define whether the application has value. Google Play uses a five-star rating scale for users to express their experience with the application. Users associate a high rating with a good application and a low rating as bad. This factor is not security related, but more an indication on how the users experienced the application.

Application Reviews	The application review is provided by users of the application. Within the reviews, users express the common problems they are experiencing with the application, as well as highlighting their good experiences. Reading reviews is a good way for potential users to see how others feel about the application. Users depend on reviews to assist them when selecting an application to download. This factor relates to user satisfaction.
Number of Downloads	The number of downloads is typically linked to the popularity of the application. Applications with a high number of downloads are widely used. However, this does not necessarily indicate whether the application is secure.
Detailed Information	This section usually highlights the features of the application as well as providing screenshots of the user interface, but rarely includes security related information. The detailed information typically includes information about the developer and when last the application was updated.
Privacy Policy	If the application is collecting, storing, or sharing personal information, an application generally discloses this within the privacy policy. It is important from a security point of view for users to review the privacy policy of an application, as it can indicate how the application intends to use any information it collects.
Permissions Requested	The permissions requested by the application is what is required to ensure the full functionality of the application once downloaded. However, there are applications that request access to more information than what the application needs to function. This could violate the privacy of smartphone users' information.
Last Update Released	Applications need to be updated to enhance the application functions, performance, stability, and security. Frequently updated applications can be a good indication of whether the application is still being supported by its developer. Outdated applications could potentially contain vulnerabilities which can be exploited.
Developer Information	Typical information that can be found regarding the developer includes their full name, list of their published applications, and contact details. This would indicate whether the application is from the original developer. Downloading an application from a non-reputable developer could result in the download of a malicious application.

From the eight factors identified in Table 1, four factors can be seen as General Factors to consider when selecting an application. The General Factors include Application Rating, Application Reviews, Number of Downloads and Detailed Information. The remaining four factors relate directly to security and are therefore referred to as Security Factors in this paper. As security should be a concern when smartphone users download

applications, the four Security Factors of Privacy Policy, Permissions Requested, Last Update Released of the application, and the Developer Information of the application should be key considerations when selecting an application to download. This paper details how important the Information Technology students considered Security Factors throughout the process of downloading an application. The next section presents the research process of the study.

4 Research Process

This research focused on the reported behaviour of first year IT students. The study was conducted by firstly performing a Smartphone Simulation Exercise, followed by related questions. The sample of students was selected based on convenience as the researcher had access to the sample of students whose curriculum included smartphone behaviour as part of their IT skills course.

The Smartphone Simulation Exercise was conducted in controlled computer labs and students were given two scenarios and asked to download one application per scenario. In the first scenario seen in Figure 1, the students were given a list of six Photo Editing Applications, while in the second scenario seen in Figure 2, students were given a list of five Alarm Clock applications from which to choose.

Figure 1: First Scenario Applications

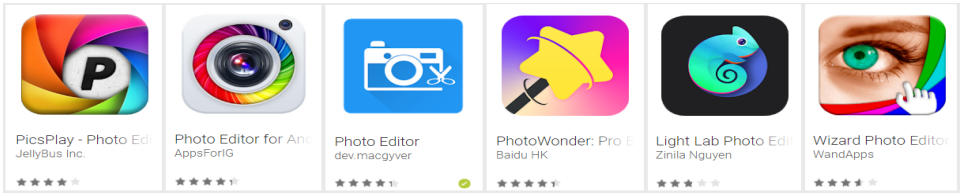
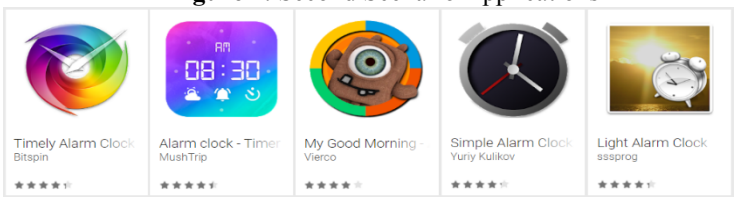


Figure 2: Second Scenario Applications



Once the students completed the Smartphone Simulation Exercise, related questions were presented to the students.

The students were given eight questions directly linked to the eight factors discussed in Table 1. Each question asked, 'Did you consider the (*factor)* when selecting the application to download?'. For each of the questions, four options were given:

- Yes, but only for the application I downloaded.
- Yes, but only for a few of the applications listed.
- Yes, I considered the (*factor*) for all the applications listed.
- No, I did not consider the (*factor*).

Further questions were used to identify students' smartphone awareness related to smartphone application downloads, and their smartphone adoption, usage, knowledge, perceptions and privacy concerns. This paper, however, primarily reports back on factors related to the decision-making processes during the application download in the Smartphone Simulation Exercises.

Participating students were from various demographic backgrounds and all Smartphone Simulation Exercises and related questions that were successfully completed were taken into consideration. The following section presents the results and findings from the study.

5 Results and Findings

Although 228 students participated in the Smartphone Simulation Exercise, only 224 responses were considered valid due to incomplete questions. These questions covered the consideration of students with regards to the General Factors and Security Factors when selecting an application to download. When asked how long it took them to decide which application to download, 64% of students took less than 5 minutes to select an application in each scenario.

After the students completed the Smartphone Simulation Exercise and its accompanying questions, the students were presented with a further question which related to their general awareness with regards to security considerations when downloading an application. The results from the study conducted indicated that the students spend, on average, more than 4 hours a day on their smartphones. The students download applications and spend most of their time on the internet, listening to music and being actively involved on social media. The most popular social media platforms amongst these students were WhatsApp, YouTube, Facebook, and Instagram. Smartphones are used for various purposes and personal information is stored on the devices. Over 75% of students stated that they would be extremely concerned if their personal information stored on their smartphone was lost or stolen.

The following sub-sections present the results from the Smartphone Simulation Exercise and the related questions.

5.1.1 General Factors

As can be seen in Table 2, when selecting an application to download, the students consider the General Factors of Application Reviews, Application Rating, Number of Downloads, and Detailed Information as important in their decision-making process. As can be seen in Table 2, 89.7% of students considered the Application Reviews for one or more applications listed in the scenarios, 93.3% considered the Application Rating for one or more applications listed in the scenarios, 74% took the Number of Downloads of the application into consideration when selecting an application for download, and 79.7% read the Detailed Information of the application for one or more applications listed in the scenarios.

Table 2: General Factors When Downloading

Options	App Reviews	App Rating	Number of Downloads	Detailed Info
Yes, I considered the *factor* for one or more applications	**89.7%**	**93.3%**	**74.0%**	**79.7%**
– Yes, but only for the one I downloaded.	22.3%	16.5%	21.0%	33.2%
– Yes, but only for a few of the applications listed.	29.9%	17.0%	20.0%	25.7%
– Yes, I considered the *factor* for all applications listed.	37.5%	59.8%	33.0%	20.8%
No, I did not consider the *Factor*	**10.3%**	**6.7%**	**26.0%**	**20.3%**

5.1.2 Security Factors

As can be seen in Table, 3, when selecting an application to download, the students do not consider the Security Factors of Privacy Policy, Last Update, Permissions Requested, and Developer Information as important as the General Factors. The majority of students stated that they did not consider the Security Factors during the process of selecting an application to download. As can be seen in Table 3, 58.5% of students did not review the Privacy Policy of the application when deciding which application to download, 56% indicated that they did not consider the Last Update released for the application, 38.6% did not review the Permissions Requested when selecting an application to download, and 63.4% indicated that they did not consider the Developer Information.

Table 3: Security Factors When Downloading

Options	Privacy Policy	Last Update	Permissions Requested	Developer Info
Yes, I considered the *factor* for one or more applications	**41.5%**	**44.0%**	**61.4%**	**36.6%**
– Yes, but only for the one I downloaded	19.6%	22.8%	36.4%	19.5%
– Yes, but only for a few of the applications listed	9.4%	11.4%	12.5%	10.0%
– Yes, I considered the *factor* for all applications listed	12.5%	9.8%	12.5%	7.1%
No, I did not consider the *Factor*	**58.5%**	**56.0%**	**38.6%**	**63.4%**

Based on these results, the General Factors and Security Factors were ranked to indicate what students considered important when downloading an application. Table 4

ranks the factors based on the percentage of students that considered these factors important. In the table it is clearly shown that a lot more consideration was given to the General Factors and less consideration was placed on the Security Factors.

Table 4: Student Consideration Ranking

	Students consideration when selecting an application	**% of students that considered the factor**
General Factors	1. Application Rating	93.3%
	2. Application Reviews	89.7%
	3. Detailed Information	79.7%
	4. Number of Downloads	74.0%
Security Factors	5. Permissions Requested	61.4%
	6. Last Update	44.0%
	7. Privacy Policy	41.5%
	8. Developer Information	36.6%

The factors identified in Table 4 relate to the eight factors in Table 1 and were based on students' reported behaviour on how they selected the applications they downloaded. A further question determined students' general security awareness regarding the secure downloading of applications.

This question was not related to the Smartphone Simulation Exercise, but asked which General Factors and Security Factors students considered important from a security point of view when selecting an application to download. This question was a general perception question that related to security and asked students to rank the importance of given factors from highest to lowest. The factors given to students were App Rating, App Reviews, Privacy Policy, App Permissions, and Developer Information. General Factors were added to the list of factors to determine if students could make a distinction between General Factors and Security Factors. The results from this question were used to determine whether students consider relevant Security Factors as important when selecting an application.

Table 5 shows an example of how the Cumulative Importance Value is calculated for Privacy Policy. The values in the table are calculated based on the importance ranking (X) multiplied by the number of students who ranked that specific factor (Y). The importance ranking consisted of six levels of importance, ranging from Most Important (6), Very Important (5), Fairly Important (4), Important (3), Less Important (2), and Least Important (1). Each student could only assign an importance ranking once to a factor. All Calculated Importance Values for each factor were added together to provide the final Cumulative Importance Value.

Table 5: Example of Cumulative Importance Value Calculation for Privacy Policy

	Importance Ranking ***(X)***	**Number of times (** ***factor*** **) ranked** ***(Y)***	**Calculation (** ***X*** x ***Y*** **)**	**Calculated Importance Value**
Factor ***(Privacy Policy)***	**6**	67	6 x 67	402
	5	43	5 x 43	215
	4	38	4 x 38	152
	3	35	3 x 35	105
	2	16	2 x 16	32
	1	10	1 x 10	10
Cumulative Importance Value				**916**

Table 6 ranks the importance value of each factor from highest to lowest according to how students indicated the importance of each factor from a security point of view.

Table 6: Importance Value

Factors	**Cumulative Importance Value**
Privacy Policy	916
App Rating	768
App Reviews	736
App Permission	718
Developer Information	695

From the factors provided in this question, two related to the General Factors of Application Rating and Application Reviews, while three related to the Security Factors of Privacy Policy, Permissions Requested and Developer Information. The results in Table 6 show that Privacy Policy is the most important factor students would consider when selecting an application. Further, students incorrectly perceived General Factors as security related as two from the top three factors were General Factors. These two factors, however, do not have any impact on the security of an application. As Privacy Policy was identified as the top security related factor followed by General Factors it is apparent that students cannot make a clear distinction between General Factors and Security Factors.

6 Towards an Educational Intervention

The Smartphone Simulation Exercise was set up to determine students' reported behaviour when selecting an application to download and students were asked to complete the Smartphone Simulation Exercise followed by related questions. These questions identify students' decision-making process throughout the process of selecting an application by determining what General Factors and Security Factors they considered when downloading an application. The results of the study show that students tend to consider General Factors in the application listing as more important than Security Factors when downloading an application.

Thereafter, an additional question not related to the Smartphone Simulation Exercise was asked to identify students' general perception related to security when downloading an application. The additional question asked which factors are perceived important when considering security during the selection of an application. The results of this question shows that students perceive factors such as Application Rating and Application Reviews as security related while they are, in fact, are General factors. Furthermore students stated that considering the Privacy Policy of an application is the most important factor related to security, and more than 75% of students stated that they would be extremely concerned if their privacy was compromised when downloading an application. However, this was not reflected in their reported behaviour in the Smartphone Simulation Exercise, as only 41.5% of the students considered the Privacy Policy when selecting an application to download.

Security Factors should be important considerations when downloading a smartphone application. However, the majority of students participating in the study (58.5%) did not deem the Security Factors important in the Smartphone Simulation Exercise. Therefore, it can be argued that an educational intervention is needed to make students aware of the potential risks associated with not considering Security Factors.

Table 7 below shows the Security Factors that should be addressed through an educational intervention.

Table 7: Security Factors to be addressed through an Educational Intervention

Security Factor	What Must Be Addressed
Permissions Requested	It is important that users read the Permissions Requested carefully to ensure the application is not requesting access to unnecessary information. If Permissions Requested are not considered, it could have a negative impact on their privacy and personal information. For example, an Alarm Clock Application should not need access to user contact details, e-mails, and photos.
Last Update	It is important that users check when last the application was updated to ensure it is still supported by its developers. If the Last Update is not considered, the application could be outdated and unsupported, and may not have the necessary security patches and updates. An unsupported application could be vulnerable to malicious attacks and an easy target for cybercriminals to exploit.
Privacy Policy	It is important that users read the Privacy Policy of an application before downloading to determine if the application will be collecting, storing or sharing personal information collected. If the Privacy Policy is not considered, personal information could unknowingly be disclosed to third-parties. For example, WhatsApp has been certified to the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework regarding the collection and processing of personal data of business partners [12].
Developer Information	It is important that users review the Developer Information to ensure that the application is from the original developer and not a cloned version of the application, which may include malware. Popular applications are often cloned and made freely available to entice users to download the application. For example, Rovio Entertainment Corporation is the original developer of the popular 'Angry Birds' application. However, a fake version of 'Angry Birds Space' contained malware which downloads additional malware to the smartphone and enlists the smartphone as part of a botnet [13].

Future research will develop an educational intervention that will address each of these Security Factors, the related risks and how they could be mitigated in order to increase students' security awareness when downloading an application. This educa-

tional intervention will be presented to the same sample of students, followed by a further set of questions to determine any changes in their level of security awareness when downloading smartphone applications.

7 Conclusion

Being aware of Security Factors when downloading a smartphone application can help reduce the risk of potentially downloading a malicious application. The study determined the students' reported behaviour with regards to their process of selecting an application to download. Over 75% of students indicated that they were concerned about the privacy of their personal information, however this was not reflected in their reported behaviour. An educational intervention could create awareness amongst students and educate them on the factors that should be considered when selecting an application to download.

8 Acknowledgements

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed, and conclusions arrived at, are those of the authors, and cannot necessarily be attributed to the NRF.

References

[1] Statista, "Smartphone users worldwide 2014-2020" [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. [Accessed: 15-Apr-2018].

[2] Statista, "Share of global population that uses a smartphone 2014-2021" [Online]. Available: https://www.statista.com/statistics/203734/global-smartphone-penetration-per-capita-since-2005/. [Accessed: 15-Apr-2018].

[3] Chaffey, D. (2016) Percent time spent on mobile apps 2016. Retrieved 8 August 2017 from http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/attachment/percent-time-spent-on-mobile-apps-2016/

[4] Allam, S., Flowerday, S. V., Flowerday, E. (2014) Smartphone information security awareness: A victim of operational pressures. Computers and Security, 42. https://doi.org/10.1016/j.cose.2014.01.005

[5] Google Play, "Developer Policy Center" [Online]. Available: https://play.google.com/about/developer-content-policy-print/. [Accessed: 18-Apr-2018].

[6] Shaw, C. M. (2010) "Designing and Using Simulations and Role-Play Exercises." The International Studies Encyclopedia (Denemark, Robert A. Blackwell Publishing)

[7] Smith, E. T. & Boyer, M.A. (1997) 'Designing In-Class Simulations' Political Science and Politics Vol. 29, No.6, pp. 690–694.

[8] Awad, N., & Krishnan, M. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly, 30(1), 13-28. doi:10.2307/25148715

[9] Negash, S., & Shahriar, H. (2015) Mobile app permissions awareness. In Information & Communication Technology and Accessibility (ICTA), 2015 5th International Conference on (pp. 1-4). IEEE.

[10] Theoharidou, M., Mylonas, A., Gritzalis, D. (2012) A risk assessment method for smartphones. In: 27th IFIP international information security and privacy conference. Crete, Greece: Springer (AICT267); pp. 428-40.

[11] Furnell, S. & Clarke, N. (2012) "Power to the people? the evolving recognition of human aspects of security," Computers & Security, vol. 31, no. 8, pp. 983–988.

[12] Privacy Shield Framework, WhatsApp Inc. [Online]. Available: https://www.privacyshield.gov/participant?id=a2zt0000000TSnwAAG [Accessed: 30-Jun-2018].

[13] Cluley, G. (2012) Android malware poses as Angry Bird Space game. Retrieved 30 June 2018 from https://nakedsecurity.sophos.com/2012/04/12/android-malware-angry-birds-space-game/