# An Educational Intervention Towards Safe Smartphone Usage

W.J. Van Rensburg, K.L. Thomson and L. Futcher

Nelson Mandela University, Port Elizabeth, South Africa
e-mail: s213461846@mandela.ac.za, kerry-lynn.thomson@mandela.ac.za,
lynn.futcher@mandela.ac.za

## Abstract

With the increased popularity of smartphones in modern society, smartphone users often neglect to consider security practices in the use of their devices. This paper explores whether an Educational Intervention could improve students' security knowledge with regard to the usage of their smartphones. With the use of a Pre-Test questionnaire, a customised Educational Intervention was constructed to address gaps in students' security knowledge and reported usage. With the use of a blended learning approach and a Road Trip analogy, the Educational Intervention was constructed and delivered to students through their university's Learning Management System. The results of the study show that the customised Educational Intervention was successful in addressing the identified gaps in students' security knowledge.

## Keywords

Educational Intervention, Smartphone Education, Security Knowledge, Safe Smartphone Usage

## 1 Introduction

There has been a significant increase in the popularity of smartphones since their inception, and it was estimated that the number of global smartphone users will reach 2.5 billion users by the end of 2018 (Statista, 2018). The use of smartphones has seen a major increase due to the vast variety of productivity tools, entertainment, functions and features they offer to their users. These functions and features are provided through mobile applications (Awad & Krishnan, 2006). Smartphone users are aware of the benefits these applications provide them, however, they are generally not aware of the risks that smartphones and their associated applications pose to their privacy and personal information (Allam et al., 2014).

The purpose of this paper is to demonstrate that a customised Educational Intervention, utilising a blended learning approach, can improve students' security knowledge with regards to their smartphone usage. This research focused on the reported behaviour of students regarding their smartphones usage. A Pre-Test, in the form of a questionnaire, was conducted to determine students' general smartphone usage, security knowledge, and concern towards their personal information. The purpose of the Pre-Test was to identify gaps in students' security knowledge in order to develop a customised Educational Intervention for the particular audience. After students completed the Educational Intervention they were presented with a Post-Test questionnaire to determine whether the Educational Intervention did in fact improve their security knowledge and perception towards secure smartphone usage. Figure 1 shows the research process followed to conduct the study.

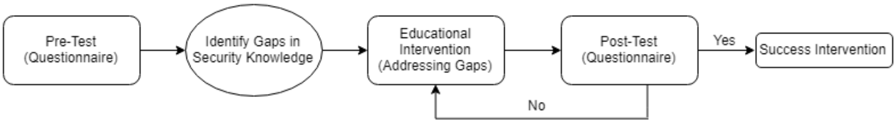
Pre-Test (Questionnaire)
Identify Gaps in Security Knowledge
Educational Intervention (Addressing Gaps)
Post-Test (Questionnaire)
Yes
Success Intervention
No

**Figure 1: Research Process Diagram**

The participants for the study were Information Technology (IT) students from a higher education institution in South Africa. The sample was selected based on convenience as the researcher had access to the students whose curriculum included smartphone behaviour as part of their IT Skills course. The same sample of students was used throughout the study.

The structure of the paper is as follows: Section 2 provides background on smartphone usage and common threats related to smartphone users, while Section 3 presents the results from the Pre-Test that was used to identify gaps in the students' security knowledge. Section 4 presents the design of the Educational Intervention. This is followed by Section 5 which highlights the results and findings from both the Pre-Test and the Post-Test conducted after exposure to the Educational Intervention. Section 6 contains the discussion related to the results from the study, and Section 7 concludes the paper.

## 2 Background

Smartphones have become an integral part of modern society. Smartphones have changed how users conduct themselves in their day to day lives and in online environments. The use of smartphones amongst users has brought new ways of productivity and connectivity in their personal lives. Prominent areas where smartphones have had an impact include business, education, health, and social life (Sarwan & Soomro, 2013). Mobile applications are third party software programs providing smartphones with unique functionality that can be downloaded and accessed directly from a smartphone (Mylonas et al., 2011).

With regards to the process of downloading mobile applications, users often neglect to review what a specific application will request from them in return for its functionality. When users download applications they are generally more focused on the features of the application rather than on the security the application provides (Zhang et al., 2017). Esmaeili (2014) identified that the confidence users might have in the perceived security controls in place of official marketplaces (for example, Google Play Store) has led to users neglecting to take security into consideration when selecting an application to download. This is of great concern with regards to information security when users use smartphones.

Smartphone users often become the target of cyberattacks due to their lack of security considerations (Dawson et al., 2015). Smartphones can be seen as a vault of private information which attackers often try and exploit by uploading malicious applications to various application marketplaces. In this context, the number of cybercrimes committed through malicious mobile applications has also seen an increase (Felt et al, 2011). RSA Quarterly Fraud Report stated that in Q1 of 2018 they discovered over 8,000 rogue mobile applications and since 2015 there has been a 680% increase in mobile app fraud (RSA, 2018). Sensitive information that can be found on smartphones include contact details, communication records, location information, e-mails and banking details (Jeon et al., 2011). As a result of this, a great amount of personal information is available on smartphones. This makes the protection of such information a critical issue that needs to be addressed. Information security relating to smartphones can be described as the knowledge, attitude, and behaviour that users apply in protecting their personal information (Allam et al, 2014), and creating awareness could be used as a means of reducing security risk (Kruger & Kearney, 2006). Allam et al (2014) also state that increasing awareness influences behaviour, which could ultimately reduce risk by focussing on smartphone users and not just on the smartphone as a device.

Adopting appropriate security controls alone is not enough to protect information assets on smartphones. This is because the behaviour of the smartphone user plays a critical role in the security of information in the use of smartphones (Esmaeili, 2014). Information security is seen as a means of reducing security risk across numerous threat areas. Educational interventions are often used to address a lack of awareness that users might have in a specific risk area.

Identifying the gaps in security knowledge that smartphone users might have could assist in the creation of an appropriate Educational Intervention. With the use of such an Educational Intervention, gaps in security knowledge could be addressed which ultimately could lead to a change in the behaviour of smartphone users. The next section discusses the Pre-Test used to identify where students might lack adequate knowledge to protect themselves against risks introduced through the use of smartphones.

## 3 Pre-Test to identify gaps in smartphone users' behaviour and knowledge

A Pre-Test consisting of a questionnaire was used to identify concepts surrounding smartphone adoption, usage, knowledge and privacy concerns smartphone users might have whilst using their smartphones. The questionnaire was set up in four sections, each addressing one of these criteria. The use of the questionnaire assisted the researcher in identifying gaps in the students' security knowledge on which the customised Educational Intervention could be structured. With the results of the questionnaire the following gaps in students' smartphone security knowledge were identified:

1. Knowledge of where applications should be downloaded (for example, official marketplaces, third-Party marketplaces or developer website).
2. The importance of updating applications, updating operating systems, and uninstalling applications that are no longer in use.
3. Awareness of threats to smartphones.
4. Awareness of the risk that applications might pose to users' privacy and personal information.
5. Physical access controls and the encryption of information stored on smartphones.
6. What to consider in the application listing when selecting an application to download.

These gaps identified were addressed in the Educational Intervention. The following section discusses the design of the Educational Intervention, and Section 5 provides a discussion comparing the results of the Pre-Test and Post-Test.

## 4 Educational Intervention

Based on the results from the Pre-Test, it was apparent that a need for an Educational Intervention existed. Smartphone users need to have an adequate understanding as to why it is important to approach the use of their smartphones in a secure manner. The Educational Intervention was created using a blended learning approach. Blended learning is an approach using online and face-to-face instruction activities (Boelens et al., 2015) to provide a more flexible approach of delivering educational content to students in higher educational institutions. With the use of a blended learning approach, students could work through the educational material provided to them as frequently as required and from wherever they wanted to access it.

Based on the gaps identified during the Pre-Test, the researcher designed PowerPoint slides to assist in the reflection on the results from the Pre-Test. The results were presented to the students in a theory lecture, where a discussion on the various gaps in knowledge took place. Here students were introduced to various topics identified as gaps in their personal security knowledge relating to their smartphone usage. The reflection was used to assist in the initial creation of awareness amongst the students about certain risk areas related to their smartphones. Reflection learning is seen as an active and awareness related process that can occur anytime and anywhere. Reflection assists students in re-evaluating and learning from decisions and choices they made, how they made them and what they should do in the future (The University of Sheffield, n.d.). In this reflection lecture, students were presented with the results of their study and were made aware of the areas in which they show a lack of security awareness relating to their smartphone usage.

After the reflection lesson, the students were informed that they would be given a week to work through the educational material made available to them on their Moodle Site and that they would be tested again a week later. The Moodle site is an example of a Learning Management System (LMS) where students can find their course material. With the use of an LMS, students were able to access the educational content from remote locations and work through the material outside of a typical class environment.

The Educational Intervention was designed using questionnaire software called QuestionPro. This software allowed the researcher to develop a custom lesson plan where, based on the answers given in the Educational Intervention, relevant educational material would be presented to the students. As a whole, all gaps in knowledge were addressed, but if incorrect answers were given, additional material was provided to increase their knowledge. The educational material was presented through various media that included videos and slides.

The researcher's approach to designing the Educational Intervention was by using the analogy that '*Downloading smartphone applications is like taking a road trip*'. With this analogy, the researcher developed the educational content around numerous aspects that should be considered when setting off on a road trip. With the use of analogies, concepts that are similar can be used to build a conceptual bridge to connect what is known to what is new. Analogies can be used to form an understanding of complex concepts and allow students to construct their own knowledge surrounding topics addressed (Glynn, 2004).

Each step in taking a road trip was used to assist in the development of the Educational Intervention. Tables 1 to 7 address each stage of taking a road trip, how it relates to the analogy, and what content was covered in the Educational Intervention to address the gaps in knowledge identified.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| You should know how you are getting to your destination (what route are you taking). | You should know where you are going to download your application from (reputable application marketplace). |

**Table 1: Plan Your Destination**

The Educational Intervention addressed this topic by delivering relevant information on why it is important to download applications from an official application marketplace. The information was presented with the use of slides explaining that the safest route to take when downloading applications is by going through official marketplaces, as applications on these marketplaces are screened for malicious software.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| Before leaving on your road trip you need to ensure that your vehicle is well maintained and ready to go on the road. | Performing regular maintenance on your smartphone strengthens the device against any threats it might encounter. |

**Table 2: Perform Maintenance**

The Educational Intervention addressed this topic by delivering relevant information on how smartphone users can do maintenance on their devices to strengthen it. The topics that were covered during the Intervention were 1) why it is important to update applications when new updates are released; 2) why keeping the Operating System of the smartphone up to date is important; and 3) why it is important to uninstall applications that are no longer being used.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| Know about the threats to your vehicle and ensure you have protection when threats occur (vehicle insurance). | Know the threats that smartphones might encounter and how to mitigate these threats (security software). |

**Table 3: Be Aware of Threats**

The Educational Intervention made use of videos that discussed the various threats to smartphones and how users can mitigate these threats. The videos, accompanied by slides, discussed the various threats and what smartphone users can do to mitigate them, as well as what solutions or preventative measures they can deploy to prevent threats from happening. Topics included, for example, why it is important to turn off Wi-Fi when it is not in use.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| Whilst you are on your road trip you may discover obstacles along your way e.g. a section of road that is closed due to road works (taking a detour). | Setting out to download a new application and discovering that the application you are about to download is requesting too much information. |

**Table 4: Potential Obstacles**

The Educational Intervention addressed this topic by discussing that when downloading an application and discovering that the potential application might request access to unnecessary information, or is not going to provide the required features, it is recommended that you start looking at some alternative applications.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| The valuable property you are taking with you will be packed in your vehicle's trunk that can be locked to ensure no one has access to it | Valuable information stored on smartphones also needs to be protected by ensuring that physical access controls are in place and information stored on smartphones is encrypted |

**Table 5: Protecting Valuables**

The Educational Intervention addressed this gap in knowledge by displaying solutions that users can employ to encrypt personal information stored on their device so that only they can access their information. The material included the importance of having screen lock protection on one's smartphones to ensure no unauthorised user can access resources and information on their smartphones.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| When going on your road trip you will stop to visit various places on route (e.g. fuel stops, food stops). | When you set out to download applications you need to stop and view certain features in the application listing before making your selection |

**Table 6: Taking the Journey**

The Educational Intervention highlights eight 'stops' users should consider before installing an application. The eight stops can be found in the listing of the application and can give users a good overall indication of the application. The Educational Intervention discussed each of the eight stops in detail. The eight stops included were App Rating, App Review, Number of Downloads, Privacy Policy, Detailed Information, Last Update Released, Permissions Requested and Developer.

| Road Trip Analogy | Gap in Knowledge Addressed |
|---|---|
| Planning your journey from start to end and knowing what to expect and how to mitigate any threats along your way will ensure your safe arrival at your destination. | Taking a pro-active approach in the use of your smartphone. Knowing what to expect and being able to mitigate against any threats along the way |

**Table 7: Arriving at your destination**

The final topic covered in the Educational Intervention gave an overall discussion on the previously mentioned topics that users should know to ensure that they can be confident in the secure usage of their smartphones. This provided users with a checklist that they could go through to ensure their smartphone is ready for its road trip. This checklist included:

- Ensure that your smartphone Operating System and mobile applications are frequently updated.
- Only download mobile applications from official application marketplaces (e.g. Google Play Store).
- Verify the permissions requested by the developer, and reputability of the mobile application developer.
- Avoid unknown and unsecured Wi-Fi networks.
- Ensure that your device is protected from unauthorised access.
- Install good security software onto your smartphone.

Once students completed the Educational Intervention they were given a Post-Test. The next section compares the results from the Pre-Test to the results of the Post-Test. This was done in order to determine whether the Educational Intervention assisted in addressing the gaps in students' smartphone security knowledge and their reported behaviour.

# 5 Discussion of Pre-Test and Post-Test results

The majority of students (98%) that completed the Post-Test were smartphone owners. The smartphone operating systems amongst students ranged from Android, iOS, Blackberry to Windows. The majority of students (88%) own smartphones running Google's Android operating system. These students use their smartphones for various tasks including downloading of applications. The researcher asked the students where they download their applications from as downloading applications from sources other than official marketplaces could result in malicious software being installed on smartphones. The Educational Intervention addressed this topic and why it is important to download applications from official marketplaces. The results from the Post-Test showed a 10% decrease in students reported behaviour when downloading applications from third-party marketplaces after completing the Intervention.

Students primarily use smartphones to connect to their social media sites. The most popular social media platforms amongst students were WhatsApp (97.3%), YouTube (92.1%), Facebook (81.5%) and Instagram (68.4%). Although the students primarily use smartphones for social media, they also use several different applications on their smartphones. The researcher wanted to determine whether students uninstall applications they are no longer using. From the results of the Post-Test the percentage of students that always uninstall unused applications went from 60% to 70% after the Educational Intervention. The reasons students say they uninstall applications were (1) to free up space, (2) replacing it with a better application, and (3) for security reasons. A positive result with regards to the security knowledge of students is that the percentage of students that uninstall applications for security reasons increased from 25.4% to 44.5%.

In the Pre-Test, students stated that they base their decision to install applications on the (1) application rating, the (2) application reviews, (3) popularity, (4) ease of use, (5) look of the application, and, lastly, on the (6) permissions requested by the application. It can be seen that security features were not seriously considered during the Pre-Test. After the Educational Intervention, the results changed and although students stated they select applications based on the (1) application reviews and (2) application ratings, they also stated (3) permissions requested has a greater influence on their decision when selecting an application. Therefore, the security feature of Permissions Requested was of greater importance to the students in the Post-Test.

Topics covering smartphone security in the Educational Intervention focussing on Encryption, Updating Applications, Screen Lock protection, and the use of public Wi-Fi networks also improved after the Intervention. Table 8 below shows the improvement in students' knowledge regarding what features they relate to smartphone security.

| Topic | Pre-Test | Post-Test |
|---|---|---|
| Encryption | 76% | 81% |
| Updating Applications | 41% | 66% |
| Screen-Lock Protection | 66% | 76% |
| Use of Wi-Fi network | 39% | 61% |

**Table 8: What Students Relate to Smartphone Security**

The Pre-Test identified what threats, related to smartphones, students are currently aware of. This assisted in educating students about threats that they currently are not aware of. In the Educational Intervention, less emphasis was placed on a topic such as Viruses as the majority of students (92.8%) were already aware of it. Threats such as Malware, Ransomware, Rootkits, and Trojans were identified as threats that fewer students were aware of. The Intervention addressed these threats by giving relevant information about each specific threat and how to mitigate against these threats. The results in Table 9 show the increase in awareness of threats after the Educational Intervention.

| Topic | Pre-Test | Post-Test |
|---|---|---|
| Malware | 61.9% | 83.2% |
| Ransomware | 31.9% | 59.4% |
| Rootkits | 16.6% | 33.5% |
| Trojans | 61.4% | 76.1% |

**Table 9: Student Awareness Relating to Smartphone Threats**

After the Intervention students' awareness of what security software is essential to have on their smartphones also increased. Students considered the use of appropriate security software such as anti-virus software, anti-spyware software, encryption software, firewall software, and lock-screen protection essential prior to the intervention, but only had anti-virus and lock-screen protection installed on their smartphone. After the Educational Intervention, the percentage of students that use the various security software increased. Although anti-virus software and lock-screen protection were the most used security software amongst students, there was a reported increase in the use of other security software. Table 10 shows the increase in the reported adoption amongst various security software.

| Security Software | Pre-Test | Post-Test |
|---|---|---|
| Anti-Virus | 63.8% | 72.3% |
| Anti-Spyware | 16.1% | 22.6% |
| Encryption Software | 27.6% | 44.5% |
| Firewalls software | 27.1% | 34.8% |
| Lock Screen Protection | 73.8% | 78.7% |

**Table 10: Smartphone Security Software Adoption**

The level of awareness amongst students with regards to the risk applications pose to their privacy and personal information also increased. The results identified that students' awareness relating to risk increased from 86.6% to 90.3% after the Educational Intervention. Users indicated that they are more aware of risk that downloading applications from third-party marketplaces pose to their privacy. They also showed a positive improvement on the need to use encryption when storing information on their smartphones. Many students in the Pre-Test did not care for reviewing permissions requested, but after the Intervention, 60.6% of students answered that it should be reviewed.

The reported concern that students indicated they had with regards to personal information stored on their devices, and the loss thereof, in the Post-Test increased after acquiring the knowledge through the Intervention. In the Pre-Test, 77% of students stated that they were extremely concerned about their personal information. However, the percentage in the Post-Test increased to 81.3%. When users are conscious of threats they might encounter they could begin to behave in a manner that reduces the possibility of the risk.

The use of the blended learning approach accompanied with the Road Trip analogy assisted in the positive results in the study. The reflection lesson prior to the Educational Intervention assisted in creating initial awareness amongst the students and allowed them to be able to identify gaps they were unaware of. The Educational Intervention, utilising of an adaptive-like questionnaire, was used to address the gaps in knowledge students had in a specific area with the intention that, with an increase in knowledge, there will be an increase in awareness, which could result in a change of users' behaviour. From the results of the study, it can be argued that the use of the Educational Intervention had a positive impact on students' security knowledge and reported smartphone usage.

## 6 Conclusion

Through the use of an Educational Intervention it was discovered that smartphone users' knowledge could be improved and that universities should ensure that they use interventions to address the gaps in security knowledge smartphone users might have. Although there are many Educational Interventions available, what makes this intervention different is the fact that it is customised to the audience based on the results of their Pre-Test and the way they answered it.

Future research could investigate whether a broader implementation of this Educational Intervention could have the same results with a different age group of smartphone users. A similar study could be conducted with the addition of further topics such as jail-breaking or rooting of smartphones that might have been excluded with this sample of smartphone users.

# 7 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.

# 8 References

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

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

Boelens, R., Van Laer, S., De Wever, B., & Elen, J. (1998). BLENDED AND ONLINE LEARNING IN ADULT EDUCATION AND TRAINING. The Women's Review of Books, 15(5), 27. https://doi.org/10.2307/4022859

Dawson, M., Wright, J., & Omar, M. (2015). Mobile Devices: The Case for Cyber Security Hardened Systems. Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications, (January), 1103–1123. https://doi.org/10.4018/978-1-4666-8751-6.ch047

Esmaeili, M. (2014). Assessment of Users' Information Security Behavior in Smartphone Networks. ProQuest Dissertations and Theses, 146. https://doi.org/10.13140/RG.2.1.3456.7129

Felt, A., Finifter, M., Chin, E., Hanna, S., Wagner, D. (2011) A survey of mobile malware in the wild. In: Proc. of the 1st ACM workshop on security and privacy in smartphones and mobile devices (SPSM '11). ACM; p. 3-14.

Glynn, S.M. 2004. Connect concepts with questions and analogies. In Cases in middle and secondary science education, eds. T.R. Koballa and D.J. Tippins,136–142. Upper Saddle River, NJ: Pearson Education.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6771 LNCS (PART 1), 311–320. https://doi.org/10.1007/978-3-642-21793-7_35

Kruger, H., Kearney, W. (2006) A prototype for assessing information security awareness. Comput Secur 2006; 25(1):289-96.

Mylonas, A., Dritsas, S., Tsoumas, B., & Gritzalis, D. (2011). Smartphone security evaluation - The malware attack case. SECRYPT 2011 - Proceedings of the International Conference on Security and Cryptography, (July), 25–36. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-80052493767&partnerID=tZOtx3y1

RSA. (2018) Current State of Cybercrime. Retrieved 23 July 2018 from https://www.rsa.com/content/dam/premium/en/report/rsa-fraud-report-q1-2018.pdf

Sarwan, M., & Soomro, T. R. (2013). The impact of smartphone’s on Society. Proceedings of the Annual Hawaii International Conference on System Sciences, 98(2), 1734–1742. https://doi.org/10.1109/HICSS.2013.623

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

The University of Sheffield. (n.d.). Reflective Learning for Students. Retrieved June 11, 2018, from https://www.sheffield.ac.uk/lets/toolkit/learning/reflective

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: an empirical analysis. The Electronic Library, 35(6), 1177–1190. https://doi.org/10.1108/EL-09-2016-0183