# The impacts of technological and personal factors on the security awareness of smartphone users

A thesis presented in partial fulfilment of the requirements for the degree of

Master of Information Science
In
Information Technology

at Massey University,
Albany, New Zealand.

***Rawan Abdulrahman Jaber***

***2016***

# ABSTRACT

With the increasing popularity of mobile devices (e.g. smartphones) and the resulting security risk (e.g. cybercriminals seeking to compromise devices to target user information), enhanced user security awareness is critical in securing the devices and the data. This research investigates that what technological and personal factors affect smartphone users' security awareness. An online (web-based) survey was conducted between September 2015 and March 2016 to explore the impacts of technological factors (e.g. platforms and applications) and personal factors (e.g. educational and technological backgrounds, gender and age, and ethnicity) on smartphone users' security awareness. Findings from the analysis of 919 responses indicate that the factors that are statistically significant in relation to smartphone security awareness are technological backgrounds, educational levels, downloading apps, installed apps, and using cracked apps.

**Keywords**:
Security awareness
Smartphone security
Personal factors
Technological factors
Smartphone users

# ACKNOWLEDGMENTS

I would first like to express my gratitude to my supervisor, Associated Professor Ruili Wang, for the valuable and professional guidance, for encouraging me to do my best, and for supporting me with comments and suggestions that I needed to successfully complete my thesis.

I owe my special thanks to my wonderful family for supporting and encouraging me throughout the challenges that I had to encounter during the process of writing this thesis. I cannot show how grateful I am to you. Especially, my father Abdulrahman, thank you for believing in me to follow my dreams. I know that you were waiting for this moment more than I do, and I know that your soul is here and you are proud of what I've achieved. May your soul rest in eternal peace. My mother Njlaa, your prayers for me were what sustained me thus far; your support, love, concern and care was what gave me the strength to continue. The only thing I can do is dedicating this work to you both. I also thank the most wonderful and precious gift in my life, my two kids, Salam and Razan; just to let you know that you are the reasons that kept me strong during the hardest times. You are the pride and joy of my life. Thanks for just being around me during this journey and for making it full of love and happiness.

My sincere thanks also go to all my dear friends for supporting me through this journey toward my goal.

Finally, I would like to thank my home country, Saudi Arabia, for believing in me and giving me the opportunity to study abroad and achieve something valuable in my life.

Thanks you all for being by my side. This accomplishment would not have been achieved without all of you. I greatly value your support and appreciate your belief in me.

Rawan Jaber
Auckland, June 2

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# 1. Introduction

Smartphones and other mobile devices are an integral part of our daily lives today; smartphones ownership has witnessed a sharp upward trend since 2013 (Ba et al., 2013; Hrestak et al., 2014; Jang et al., 2013; Jones & Chin, 2015; Poushter, 2016). As an example, Apple recently announced that around 100 billion apps have been downloaded and installed thus far on apple devices (Statista, 2015). This tremendous increase in the number of smartphone applications is a result of the rapid development in the variety of smartphones (Chin et al., 2012; Mylonas et al., 2013). Simultaneously, the massive growth in smartphone technology presents new security concerns (Mylonas et al., 2013; Parker et al., 2015; Rodr´ıguez-Mota et al., 2016). There is a wide range of applications (hereafter referred to as 'apps') designed for different purposes (e.g. gaming and social networking) and platforms (e.g. Android and iOS). These apps are available for download from both official app stores (e.g. Apple App Store, Google Play, and Amazon App Store) and third-party or non-official app stores.

Users downloading apps from third-party sources that have a weak or non-existent app vetting policy have a higher chance of installing a malicious app on their device or having their device compromised (Chin et al., 2012; Eshmawi & Nair, 2013; Hrestak et al., 2014; Li et al., 2014; Mylonas et al., 2013). For example, a study carried out by Al-Hadadi and Al Shidhani (2013) demonstrates that most smartphone users do not have a clear idea about how to act or whom to report to if they experience any security-related incident. The study also highlights a general lack of security awareness among smartphone users. The researchers therefore recommend focusing on human or personal factors concerning security awareness, rather than attempting to improve the security measures on smartphones. Although previous research has investigated security awareness among smartphone users (see, for example, Androulidakis & Kandus, 2011; Chin et al., 2012; Felt el al., 2012; Imgraben et al., 2014; Jones & Chin, 2015; Mylonas et al., 2013), there is still a lack of research that exclusively explores smartphone security issues. Similarly, the number of scientific studies that address and consider both personal and technological factors and their impacts on smartphone users' security awareness is either very limited, mostly outdated or remotely related to the topic (see, for example, Heinrichs, 2012; Jones & Chin, 2015;

Mylonas et al., 2013; Parker et al., 2015). It is in this background that the present study attempts to investigate security awareness among smartphone users.

Although considerable theoretical and empirical literature in the field of smartphone security gives an insight into users' security awareness, there is dearth of research in areas such as personal and technological factors that may have a bearing on the extent of security awareness amongst smartphone users. This paper therefore aims to fill this research gap by focusing on personal and technological dimensions of users' smartphone security awareness. Specifically, the study investigates the effect of personal factors (such as users' ages, genders, ethnicity, personal traits, educational and technological backgrounds) and technological factors (such as the type of operating systems, installed applications, activities) on the level of security awareness of smartphone users. The research questions that this study intends to answer include:

- Do personal factors have an impact on users' smartphone security awareness?
- Do technological factors have an impact on users' smartphone security awareness?

Prior to carrying out the study, we hypothesized the following:

I. Regarding the technological factors:
- H1: There is a relationship between the platforms used and user security awareness level.
- H2: There is a relationship between the types of applications installed and user security awareness level.
- H3: There is an inverse relationship between user activities and user security awareness level.

II. Regarding the personal factors:
- H4: There is an inverse relationship between the users' ages and their level of security awareness.
- H5: Female smartphone users have a greater level of security awareness than their male counterparts.

- H6: There is a positive relationship between the users' educational backgrounds and their level of security awareness.
- H7: There is a positive relationship between the users' technological backgrounds and their level of security awareness.
- H8: All ethnic groups have, on average, a moderate level of security awareness.
- H9: There is a relationship between the users' types of personal traits and their level of security awareness.

In order to test the hypotheses listed above and to find answers to the two research questions, an online survey of smartphone users was conducted. The scope of the survey was limited to users who have a smartphone with the two most popular smartphone platforms (iOS and Android). It is expected that the outcome of this research will give a clear idea about the extent of effect of personal and technological factors on users' smartphone security awareness. The results will also help the end-users increase their security awareness.

The rest of the paper is organized as follows. Section 2 presents related theoretical and empirical work on security awareness of smartphone users, including the development of smartphones, the difference between cellphone and PC security, the extent of security awareness of smartphone users; and technological and personal factors related to smartphones security. Section 3 discusses the methodology adopted for this study and the experiments and implementation processes are laid out, including the data collection procedures, survey questionnaire description, and the pilot study that we conducted as part of the evaluation process. Section 4 provides the results and analysis of the study. It describes the statistical results, including descriptive statistics, statistical tests, testing of the hypotheses and regression analysis. This is followed by a discussion of the results and the implications they entail. After that, Section 5 presents the problems encountered during the implementation of this study, followed by the future work and recommendations. Lastly, Section 6 wraps up the conclusion of this study.

# 2. Literature review

In this section, an overview of the previous work in the field of smartphone security is reported, analysed and critiqued. The section introduces the smartphone era and the associated security threats first. It then discusses the difference between mobile security and computer security before reporting on the state of security awareness among smartphone users. The technological factors are discussed, which are the focus of this study, including operating systems (i.e. iOS and Android), apps installed and users' activities. At the end, the personal factors are also discussed, including gender, age, educational background, technological background, ethnic groups and personality.

## 2.1 The smartphone era

Smartphones are becoming increasingly popular because of the multimode functionality and mobility. The past few years have witnessed a significant growth in smartphone ownership worldwide (Poushter, 2016). The continuous addition of and improvement in functions such as advanced web browsers, modernized multimedia capture and expanded storage capacity have increased their popularity multifold (Barrera & Van Oorschot, 2011). The enormity of the world's existing mobile market can be assessed from the Microsoft report (2011), which revealed that around 4 billion mobile phones were in use around the world, 1.08 billion of these being smartphones. An ABI research (Koetsier, 2013) shows that the number of smartphone users increased to 1.4 billion in 2013, out of which 294 million were iOS and 798 million Android smartphones users. An estimate suggests that smartphone use is increasing by 30% each year, and will reach a staggering 4.4 billion users by the end of 2017 (Portio Research, 2013). Some other studies also suggest that the number of smartphone subscribers is growing at a rapid speed (Nielsen, 2011) and as many as 83% of cellphone owners today have smartphones (Experian Marketing Services, 2014). Furthermore, around 80% of the online consumers today own a smartphone (Accenture Report, 2016; GlobalWebIndex, 2016). A recent Ericsson Mobility Report (2016) shows that there are around 3.4 billion smartphone subscriptions around the world in the first quarter of 2016; the growth is expected to reach 6.3 billion by 2020. The trend has experienced more acceleration in advanced countries, as the latest Pew Research Center

Report (2015) shows that more than 64% of American adults have a smartphone device. This growing popularity of smartphones has also led to the development of a variety of smartphone applications.

Smartphones work best with multifarious applications that are especially designed for them. These applications are developed by both official and nonofficial companies. Smartphone users are becoming increasingly comfortable downloading and installing these applications from app repositories, which might either be official ones (i.e. maintained by the operating system of smartphone, e.g. Apple's App Store) or nonofficial ones (e.g. Amazon App Store for Android) (Mylonas et al., 2013). Presence of such a huge number of applications in both official and nonofficial/third-party market attracts smartphone users towards making use of these applications for their ease and comfort. Downloading and installation of these applications, however, is almost always associated with security risks (Li et al., 2014).

The smartphone applications industry poses invariable security threats to the users' cellphones and the personal information contained therein. Nonofficial applications are accompanied by the possibility of installing malwares such as Trojans (Li et al., 2014; Mylonas et al., 2013; Parker et al., 2015). Attackers can use these marketplaces as venue to initiate a security attack or a privacy attack. For example, a hacker (or cracker) uses a marketplace to gain personal or secure information (Mylonas et al., 2013). The number of malicious apps in application repositories is increasing (Mylonas et al., 2013), which compromises the users' most private information. How to prevent smartphones from an attack therefore becomes a vital challenge (La Polla et al., 2013). With nearly two billion smartphones currently in use and over 500 kinds of smartphone malware identified (including viruses, Trojan, etc.), the threat to smartphones and smartphone users is not a mere conjecture; it is real (La Polla et al., 2013; Parker et al., 2015). It can therefore be concluded that while the development of mobile technology has on the one hand resulted in a substantial convenience in people's lives, it has on the other hand brought about an inevitable risk to people's security and privacy.

## 2.2 Mobile security and PC security

Both mobile devices and personal computers are vulnerable to a wide range of security threats. Based on Symantec report (2013), the number of security threats to mobile devices is considerably low as compared to the number of threats to PCs. However, due to factors such as (i) the rapid development in mobile and smartphones field, (ii) increasing the use of smartphones for sensitive activities, and (iii) the techniques used by hackers become more sophisticated, threats to mobile phones have shown a higher growth rate in the recent years, and are now considered more dangerous than before (Hrestak, Picek, & Rumenjak, 2014; Mcafee Labs, 2016; Rodr´ıguez-Mota et al., 2016; Shedon et al., 2014; Symantec, 2013). The Symantec report (2013) also shows that a significant increase has been observed in the number of vulnerabilities in mobile devices, with 415 vulnerabilities in 2012 compared to 314 in 2011 and 163 in 2010. This shows that mobile devices are at an increased risk of security compromise. Nevertheless, a great deal of techniques and tools are being developed continuously with the claims to prevent or reduce the security threats on smartphones (Rodr´ıguez-Mota et al., 2016).

One of the main reasons behind greater security threats to mobile devices is the ever-expanding applications market. This notion is substantiated by Juniper Networks (2011) report, which verifies that the most noticeable mobile malware risk is mainly from the accelerated growth of applications in app markets. Coupled with it is the ease of installing apps from a wide range of developers, which has given rise to multifarious security issues for smartphones users (Barrera & Van Oorschot, 2011). Since an overwhelming majority of users download as well as install third-party apps for smartphones, they invariably draw the attackers' attention (La Polla et al., 2013; Parker et al., 2015). Although La Polla et al. (2013) expect "malware for smartphones to evolve in the same trend as malware for PCs" (p. 446), they argue that there are several vital differences in the security dynamics of mobile phones and PCs. For example, malware writers may make money from their illegal activities more easily on smartphones than they can do in the case of PC environments. One limitation of smartphones, is their CPUs and memory sizes, which limit possible security solutions. For example, intrusion detection algorithms cannot be operated on a smartphone easily because of the complexity of algorithms and the computing power limitation of a smartphone. Another vital difference pertains to device configuration, content protection

and user authentication, which present more difficulty on smartphones than they do on PCs (Motha et al., 2009). Additionally, many solutions that work on PCs cannot be used on smartphones. One potential threat, mentioned by McAfee Labs Report (2016), is the widespread use of wearable devices, such as smart watches and activities trackers; these wearables could work as a backdoor for the attackers to gain access into and compromising the security of integrated smartphones. The smartphones nowadays also act as collection points for smart TVs and security systems in smart homes (McAfee Labs Report, 2016), further compromising their security. This goes on to show that mobile phones are more vulnerable to malware than PCs now.

Since smartphones tend to be constantly hand for the users, this may put them under the wrong impression that their devices are more secured than PCs; this, in turn, may lead the users to trust their smartphones with valuable and sensitive information (Dagon et al., 2004). Research shows that data stored on mobile phones are more likely to be stolen or be accessed by unauthorized parties than data stored on PCs (Musbah et al., 2013). The most threats-prone smartphones, according to Musbah et al. (2013), are the ones with ports that enable the device to connect with external domains, such as Bluetooth, Wi-Fi and memory slots. They further argue that, in general, in wireless communication the sensitive and critical information is neither secured enough nor encrypted well. Besides, there are other threats that could also affect the device when installing applications on smartphones. As a remedy, Musbah et al. (2013) suggest measures such as keeping the smartphone's OS up-to-date, always letting the device in invisible mode when wireless communication is not in use, and not installing any application from untrusted sources. The Symantec report (2013), however, shows that even downloading apps from trusted resources is not immune from risk. As an example, the report cites a 2012 incidence when a malware software was masquerading as popular games such as "Super Mario Bros." and "GTA 3 - Moscow city" on Google play market.

An additional security threat to which smartphones are prone, as against PCs, is the touchscreen facility available on them. Alrowaily and Alrubaian (2011) explain that some of the Android based smartphones provide pattern recognition mechanism for unlocking the device. The smudge that the fingerprints (or finger trace) leave after unlocking the device could be misused to hack and gain access to the device, they claim.

The most significant security threat posed by smartphones as compared to PCs is personal data. Therefore, security concerns of personal data are constantly increasing (Jones & Chin, 2015). Barrera and Van Oorschot (2011) pointed out that because of advanced features available on smartphones, users tend to save their personal data in various forms onto smartphones. This implies, they argued, more privacy breakthrough and added data leakage. One example of this is cloud synchronization, which may lead to synchronization of the data to another device. Similarly, GPS apps could be used to spy on user locations and other private information. Other studies have also revealed that smartphones are more likely to attract information security risks if they are not protected well. For instance, a study by Imgraben et al. (2014) found that almost 50% of the participants did not take any security measures on their smartphones, such as locking the device by a passcode. Such practices may lead to a leakage of personal data.

Based on the above studies reported above, it is clear that both device and personal security can be compromised more on smartphones than on PCs. It is thus relatively easier to attack smartphones than it is in the case of PCs. However, there seems to be a general lack of awareness about such security threats among smartphones users.

## 2.3 Security awareness in smartphone users

Smartphones users have been reported to have relatively low security awareness, which is exacerbated by a continuous increase in risky security behaviour (Jones, Chin, & Aiken, 2014; Mylonas et al., 2013; Parker et al., 2015). Even if they do have a good level of security awareness, the security implementation and behaviour level is considered unacceptable, which means that they fail to apply security procedures into their devices (Balebako et al., 2014; Sari & Candiwan, 2014; Mylonas et al., 2013). A study by Volkamer et al. (2015) found that smartphone users' security awareness is merely limited to the threat of physical access to their devices. The study also found that smartphone users generally underestimate the security risk by believing that they do not have any valuable or interesting data to attract the attackers. Interestingly, some of the users believed that their smartphone use is secure since they had never been exposed to any security threats. Although the study's findings cannot be generalized since the sample population size was quite small, other

studies also point toward low security awareness among smartphone users. For example, Jones and Chin (2015) conducted two studies in 2011 and 2014 to measure the security practices of smartphone users; comparative analysis of two studies shows that the users' security practices and the risky behaviours worsened with the passage of time. However, the participants were limited to students with business major in only one university. Another study conducted by Androulidakis and Kandus (2011) found a significant relationship between the security awareness of smartphone users and no-smartphone users. The study hypothesized that the smartphone users of advanced OS are more likely to feel secure. However, the statistics generated from their data proved that even though advanced OS users feel secure, the actual score of their security awareness is lower than that of the users who use non-advanced OS. This low score on security consciousness makes them become more vulnerable to security attacks than others. The researchers concluded that among advanced OS users, there is a noticeable lack of security awareness and a moderate security attention. The authors conducted another study (Androulidakis & Kandus, 2012) to compare the security feeling of mobile phone users to the objectively agreed best security practice. They found negative correlation between 'feeling secure' and 'being secure' as the users who felt their mobile phones were secure tended to have less security awareness and cautiousness. This huge gap between what smartphone users think about security and what the reality is must therefore be addressed in research in order to minimize security attacks and vulnerabilities.

Research shows that smartphone users generally underestimate the risk of getting their stored information and identities on smartphones stolen or even sold. For example, a study carried out by Imgraben et al. (2014) showed that users were unaware about the risks of revealing their personal information to a third party. The study also found that users who jailbreak/root their smartphones tend to be more likely to take risks, such as downloading apps from unauthorized app markets. The authors pointed out the need to have training programs for online security, especially for the smartphone users, in order to maintain the user knowledge about cybercrimes and the best security procedures and protection available. However, the study was conducted at just one Australian university with a relatively small sample compared to the actual number of smartphone users in Australia, which limits its

generalizability.

This is not to say that the level of security awareness among smartphone users is the same across various sections of population or that it is not increasing with the passage of time. A recent study conducted by Accenture (2016) shows that more than two-thirds of the smartphone users now have an added awareness of security, and they sometimes choose to stop using their devices over security and privacy concerns. The study, however, does not delve into the reasons for increased security awareness. Some other recent studies (see, for example, Parker et al., 2015; Sari & Candiwan, 2014) have also shown that the overall level of smartphone user awareness is now considered as satisfactory, with the security behaviour still considered merely acceptable. However, as pointed out in several studies mentioned above, the desired security awareness level needs to be improved further.

Users' reduced security awareness is also manifested in their lack of interest in apps reviews and agreement messages. The smartphone's OS could actually be the greatest risk to the device if the user keeps ignoring permission messages, suggested updates and other security procedures prompted by the OS (Shedon et al., 2014). Parker et al. (2015) reported that around 82% of smartphone users tend to ignore the license agreements and permission requests while downloading/installing apps. Correspondingly, Kato and Matsuura (2014) pointed out that by checking the permission messages when downloading and installing apps, the smartphone user can avoid any malware execution that could infect their device. However, the study did not provide much evidence regarding this practice and was focused on Android OS only, which means that it cannot be generalized to all smartphone platforms. Similarly, Mylonas et al. (2013) conducted a survey to explore the security awareness of smartphone users who download apps from official app repositories. The authors found that most of the smartphone users are never apply or enable any security controls as they trust these apps stores. Moreover, the users tend to ignore any security or agreement messages while downloading/installing apps. They were also found showing no interest in reading the reviews about apps. Likewise, Volkamer et al. (2015) reported that smartphone users tend to overestimate and trust the app repositories, apps developer and smartphone company to take the responsibility and do security checks on apps, so no malicious apps will be allowed in the stores. Similarly, a study by Felt el al. (2012) found that only a minority of smartphone dig into security as well as permission messages to

understand security and technology. As another example, Chin et al. (2012) conducted a survey to investigate the security awareness of smartphone users when they use their smartphones. The study revealed that most of the users were concerned about the physical loss or damage that could happen to their devices rather than having concerns about the internal security of the smartphones. Furthermore, regarding apps downloading and installing, smartphone users tended to have free apps from unknown developers and companies. The researchers also found that the participants' trust on apps depended on indicators such as reviews and recommendation from other users instead of understanding privacy and security indicators.

Regarding applying security controls, Parker et al. (2015) revealed that this practice is associated with language and gender factors as the non-English users seem to need extra training to fully understand the security issues in smartphones. The lack of awareness in terms of storing personal data is an alarming phenomenon, as users tend to save critical and personal data on their smartphones, which makes them a great target for hackers and malware (Sari & Candiwan, 2014). Some studies show encouraging results with regards to security awareness about personal data. For example, a survey was carried out by Androulidakis and Kandus (2011) in order to examine how saving personal data on mobile phones affects the users' security awareness. The study showed that users generally feel secure to save their personal data in their phones. It revealed that around 31% of the users knew and were moderately taking the necessary security measures and options on their devices. The findings also showed that around 78% of the users who were saving their personal data used to back up their data at least once per month. The researchers concluded that the level of the users' security awareness was at a normal and moderate level in general. Findings from this study are quite encouraging; however, the study was based on the use of mobile phones in general, with no specific focus on smartphones. The study also did not recommend any guidelines for improving users' security awareness.

In summary, the main reasons behind the low to acceptable level of security awareness and behaviour among smartphone users could be: the long time it takes to read and understand security policies and messages; the time it takes to report any security incidents to get their security problems resolved; the problem of understanding what is written; and ignoring the security messages (Balebako et al., 2014; Sari & Candiwan, 2014).

In other cases, the users just do what others are doing; for example, if an app is popular in the user's social circle, he/she will go for it without thinking about any security issues (Volkamer et al., 2015). The studies reported above indicate that in addition to the vulnerabilities of the operating system itself, smartphone users' level of security awareness also provides an opportunity to attackers.

## 2.4 Technological factors

In this section, we present and discuss previous research about technology related issues that could have an impact on the security awareness of smartphone users. The technological factors relevant to this study are: operating systems, installed apps and user activities. These aspects are discussed in the ensuing sub-sections.

### 2.4.1 Operating systems: Android and iOS

An overwhelming majority of smartphones run on either Android or iOS operating systems, presently the most popular smartphone operating systems (Balebako et al., 2014; ComScore, 2015; GlobalWebIndex, 2016; IDC Research 2015). La Polla et al. (2013) claim that future cybercriminals would more likely focus their attention to iOS and Android operating systems since these two operating systems have far more users than any other operating system. According to ABI Research, by the end of 2013 there were around 35 billion Android and 29 billion iOS applications in use (Koetsier, 2013). Another study shows that around 83% of the smartphone application downloaders use Android or Apple smartphones (Nielsen, 2011). Furthermore, a report by Nielsen (2013) shows that among the smartphone users aged 18 and above, Android and Apple are the most popular platforms with 53% and 40% use respectively. Alarmingly, the Lookout Center report (2011) shows that Android users are two and a half times more likely to have malware than before, with three out of ten likely to have web-based threats. The report estimated that in the first half of 2011, around one million Android users were affected by malware, with a considerable upward growth in the number of infected Android apps from 80 apps to over 400 apps.

Smartphones that use Android operating system are at an enhanced risk of security threat (Rodr´ıguez-Mota et al., 2016). La Polla et al. (2013) and Li et al. (2014) claim that

Android is not a very closely monitored platform, as it follows a philosophy of openness called ‘anything goes’; in other words, it has an open source attribute, which increases its vulnerability and chances of attracting hackers’ attention. This is evident from a report by Juniper Networks (2011), which shows that Android malware has risen by 400% since 2010. The report also reveals that one out of every 20 applications, which ask for user permissions, would make a call without the user interaction or even knowledge. Another shocking fact mentioned in the report is that around eight applications in Android market ask for a dangerous permission, granting which could leave the device totally broken and unusable. Of late, however, Android OS has made a noticeable progress in improving the security of its platform (Rodr´ıguez-Mota et al., 2016).

Android is not the only platform that is targeted by cybercriminals. Even though the number of observed threats on iOS is quite small as compared to Android, the platform is not immune from security compromise. One of the major threats to iPhone is jailbreak (leaving users free to unlock their iPhones and download apps without authorization by Apple) as attackers are more likely to attack the jailbroken phones and take control of them (Juniper Networks, 2011; O’Brien, 2016). Moreover, the most recent Symantec report (O’Brien, 2016) reveals that even the non-jailbroken devices could be affected by malware, as attackers mostly install the threats when the users connect their smartphones into an affected computer by cable or even wirelessly. For example, the attacker could gain access to the iOS device by simply sending a malicious file through AirDrop (the Apple file transfer protocol to exchange files wirelessly between Apple devices) that installs a malicious software on the device. O’Brian (2016) also reported that in late 2015, a serious security breach affected the App Store when it was found that a huge number of Trojan infected apps were hosted on the App Store server.

The discussion above reveals that although Android and iOS are the most popular smartphone platforms, they also have their own vulnerabilities, which are most likely to be exploited by attackers. Security threat to the smartphones, however, increases with downloading and installing applications, regardless of the operating system used as a platform.

### 2.4.2 Installed apps

Smartphone devices are actually built around, and to some extent dependent on, apps, which play a major role in the user experience. Over the years, apps have developed into extremely important and useful software for smartphone users (Nielsen, 2015). According to a recent Apple report, around 100 billion apps have been downloaded and installed so far on iPhones, most of these being games (Statista, 2015). Another source reported that 46 billion applications were downloaded in 2012 compared to 37 billion in 2011, and the number is expected to exceed 200 billion per year by the end of 2017 (Portio Research, 2013). These apps come in a variety of forms, utilities and dimensions. However, since smartphones tend to be more entertainment driven, users are more likely to use apps for entertainment purposes such as gaming and social networking; use of apps in these categories therefore keeps increasing with the passage of time (Nielsen, 2015). Accordingly, Statista website, quoting Apple, reported that the most popular apps category is gaming with around 23% of the App Store market share, followed by business apps, education apps, lifestyle apps and entertainment apps (Richter, 2015). Similarly, another study shows that gaming apps are the most downloaded apps, followed by social networking apps (Nielsen, 2015). Regardless of their nature and use, however, downloading and installing apps is not without its potential hazards.

It is commonsense that users should only install the applications that they need since the more apps they download and install, the more exposed their smartphones are to security risks (Wright, 2011). Additionally, apps should be installed only from trusted resources, as they provide the easiest way for hackers to access the phone (Ofcom, 2013). A hacker can take a very popular paid app, embed his/her own malicious code, and then offer it for free on the network or through third-party repositories. Once the user downloads the app, the hacker may be able to control the device and access whatever he/she wants without the user permission. Similarly, Symantec report (2013) shows that most of the malicious codes for mobile devices pose as legitimate apps or are imbedded into popular apps. The report also shows that 35% of the malicious code generators steal the user's information, 15% track the user, and 13% send content, messages and emails from/to the user's device. This could include sending SMS, making calls, browsing and downloading online content; the user will not notice anything until it is too late. Parker et al. (2015) as well as Ofcom's guide (2013)

therefore recommend that the users must download apps from trusted and official stores and must also check reviews about the apps.

There are several factors that a user might consider before downloading and installing an app. According to the Naked Security Survey, mentioned in Sophos report (2013), the developer's reputation (43%) is the most important factor that users take into consideration when they install apps on their device; around 29% users consider the popularity of the app, whereas 13% depend on the app's cost. A similar study by Google (2014) revealed that the most significant factor when users decide to download an app is price (82%); 62% are influenced by the description, 60% are motivated by rating or reviews and 43% decide whether they want to download the full version app or not based on the free trial version of the app. The Google study (2014) also reports different reasons for downloading apps; around 33% of smartphone users download apps because of recommendation by others, 31% because they sound interesting/fun, 24% because of familiarity with the company/brand of the app, and 18% because they give an exclusive discount/reward. Interestingly, the study shows that one in four installed apps is actually never used.

To sum up, an increasing number of applications are being installed and downloaded by billions of users every day. Different users consider different factors when installing an app. The malware and hackers thrive on such downloading and installation. The users' security is resultantly compromised. Their security is also compromised because of the nature of their activities on the smartphones.

### 2.4.3 User activities

More advanced smartphones and added availability of apps implies more use of the smartphones by the users. Statista website reports that users spend around 41 hours per month on average on their smartphones; the time spent is expected to increase over time (Richter, 2016). However, a study by Nielsen (2015) shows that regardless of how many apps there are and how many the users have installed on their smartphones, on average they access around 27 apps per month. The study also shows that the time spent per person on smartphone is progressively increasing; it rose to around 38 hours per month in late 2014 from around 23 hours per month in 2012, which is more than 36% increase in two years.

Another study reported that, on average, smartphone users spend around 14.5 hours per week (more than 2 hours per day) on their smartphones (Experian Report, 2014). Based on the most recent report of Board of Governors of the Federal Reserve System (2015), smartphone users are showing a significant attention and adaptation to a wide range of activities by using their smartphones. Text messaging, according to the report, is still one of the most frequent activities among smartphone users even with the high functionality and multitude of apps that smartphones provide. The most popular activities on smartphones, other than text messaging, are games and social networking, as mentioned earlier. Browsing, multimedia and commerce activities are also highly common among smartphones users. The report also shows that Facebook, Google, YouTube, Twitter and eBay are the most visited websites. Another report by Nielsen (2014) reveals that around 89% of the smartphone users' time is spent on watching different media through apps. Similarly, according to Pew Research Center Internet & American Life Project (2013), nearly 63% smartphone users go online via their smartphones and 52% of them check their emails. A study by Louca and Ktoridou (2014) also shows that smartphone users' main activities are Internet related. A study conducted by Sari & Candiwan (2014) on smartphone use found that around 80% used it for internet browsing, 79% for social media activities, 75% for texting, 62% for emailing, nearly 55% for calling, and 44% for gaming. The study, although based on a relatively small sample, gives a clear indication of the use preferences of smartphone users.

The embedded smartphone sensors have given rise to a new path for smartphone use (Anjum & Ilyas, 2013). These sensors track and record the physical activities of smartphone users, thereby helping them maintain a healthy lifestyle. The rapidly evolving smartphone sensor technologies (such as GPS sensors, image sensors, audio sensors, light sensors, etc.) could be used to identify the activities that the user is performing based on the sensor's activity recognition capability (Weiss & Lockhart, 2012). This means that a smartphone can now be used as sport tracker, sleep tracker, health monitor and for many other daily activities. The most recent report by Pew Research Center (2015) shows that smartphone users are using their devices for navigating different life activities, such as looking up for medical conditions, accessing learning and educational resources, searching for job opportunities and resourcing, remaining up-to-date with the latest news, routing and mapping, and connecting with online communities, etc.

It is thus clear from the discussion above that with the smartphone technology and applications available today, the user is able to do different tasks and activities. However, there is a dearth of studies that explore if these activities could have any impact on the users' security awareness. Overall, studies connecting different technological factors with smartphone users' security awareness are quite rare. There is therefore a need for more in-depth exploration of the association between technological factors and smartphone users' security awareness.

## 2.5 Personal factors

In addition to technological factors, personal factors may also play a crucial role in the extent of security awareness among smartphone users. In the following section, findings from some previous studies on the personal and personal factors in relation to the users' security awareness will be presented and discussed. The factors that will be investigated in this study are: gender, age, educational background, technological background, ethnic group and personality.

### 2.5.1 Gender

In the gender-biased society of the past, there was a clear gender gap regarding the smartphone ownership, as a majority of smartphone users tended to be male (Nielsen, 2013; Poushter, 2016). However, the two most recent Nielsen reports (2014, 2015) show that there is now gender parity as almost equal number of the two genders own a smartphone and the time they spend on using apps is also almost even. When it comes to the use of the smartphones, however, females have been found to be more likely to use smartphones (especially for online relations apps) than their male counterparts (Kim et al., 2015). The study, however, did not establish any relationship between gender and security awareness. Another study conducted by Deursen et al. (2015) revealed that males tend to use their smartphones less than females for relational and personal purposes. Females were also found to have a higher habitual addiction to using smartphones.

Regarding smartphone security, Parker et al. (2015) found that low security control adoption is related to gender, as female smartphone users tend to have a lower security

awareness and implementation. However, the study sample was limited to young Android users only rather than taking a cross-section of the population. Interestingly, another study by Jones and Heinrichs (2012) shows the opposite, i.e. men are more likely to be engaged in risky practices on their smartphones. Yet another study by Jones and Chin (2015) found that there are no differences in smartphone security practice and behaviours between the two genders. Overall, there is a noticeable lack of studies that show a relationship between gender and security awareness for smartphone users.

### 2.5.2 Age

Age is an important factor when it comes to the use of smartphones. As expected, young adults have been found to be more likely to use smartphones (Nielsen Report, 2013). Young adults aged between 18-34 tend to be the most likely group of users, and are more likely to be smartphone-dependent (Pew Research Center, 2015; Poushter, 2016). The studies, however, do not explore whether age has anything do to with the users' security awareness.

Research indicates that age has a positive impact on self-regulation in terms of smartphone use. In a recent study conducted by Deursen et al. (2015), it was revealed that older people are less likely to show addiction to using smartphones as compared to young adults. The study, however, merely focused on the habitual and addictive behaviours related to smartphone use without shedding light on security awareness in the two age groups. In a related study, Parker et al. (2015) found that younger smartphone users tend to have more security awareness. They reported that younger users have a good knowledge of malware, security apps and authentication controls; however, they also highlighted that there is still a high security risk regarding the lack of security implementation, risky activities and user complacency. They also found that student smartphone users aged between 18-22 are more likely to be engaged in risky behaviours.

### 2.5.3 Educational background

As previously stated, the phenomenal increase in smartphone adoption and use has led to widespread security issues for both the device and the information that is contained

therein. One of the most important factors that impact the users' security awareness and behaviour is their educational background. Several studies demonstrate that well-educated users are more likely to own a smartphone and be smartphone-dependent (Pew Research Center 2015; Poushter, 2016). It is expected that educated smartphone users must have applied some security and privacy settings; however, data show that a huge percentage of the users are still not aware about or tend to ignore the potential security risks (Jones et al., 2014). The study by Jones et al. (2014) found that even though the users already know the consequences of security problems and attacks, their awareness is not reflected on applying/following security procedures on their smartphones. The study, however, does not explore the reasons behind this behaviour. Similarly, a study by Jones and Heinrichs (2012) shows that students in general tend to be careless and unaware of security awareness.

A comparison of the two studies carried out by Pew Research Center (2012, 2013) on smartphone use shows some interesting findings. The older study showed that around 61% of college level users were more likely to own a smartphone, with 36% of high school grade and only 21% with no high school diploma users tending to have a smartphone. The more recent study shows an increase in all of the categories with 70%, 46% and 36% respectively. The latter report also reveals that users with upper educational spectrum and upper end of income are more likely to own an iPhone rather than an Android smartphone. The studies, however, do not explore the dimension of security awareness vis-à-vis the users' educational background.

### 2.5.4 Technological background

Living in the digital era requires computer literacy, i.e. being able to deal with computers and other technology devices to perform day-to-day activities and tasks (Cullen & Cobb, 2011). Saadi (2009) defines computer literacy as "the ability to achieve desired outcomes via a computer" (p. 5). Computer literacy is strongly related to information literacy, which is "understanding how to assess, interpret, and generate meaningful responses to volumes of data" (Saadi, 2009, p. 5). As a consequence, both computer and information literacy determine the level of technological literacy or background of a person. According to Maryland Technology Literacy Consortium (TLC) computer skills guidance, "technology literacy is the ability of an individual, working independently and with others,

to responsibly, appropriately and effectively use technology tools to access, manage, integrate, evaluate, create and communicate information" (n.d., p. 1). TLC categorizes the levels of user skills into (a) basic: foundational and primary computer literacy skills; (b) intermediate: the computer skills are more advanced than the foundational, and (c) proficient: the computer literacy and skills are extremely advanced and well covered and applied into educational and work settings. All these definitions imply that being computer and technology literate can help a user become aware of the security risks that his/her device is exposed to.

The level of computer literacy is not equal between the two genders, however. A recent study by Patrick and Ngozi (2014) revealed a significant difference between males and females in relation to computer literacy. Males were found to be more interested in technology and more likely to dominate the computer resources. However, the study was conducted within Nigerian universities only and hence cannot be generalized. Another study by Ikolo and Okly (2012) found that despite differences between males and females in relation to computer literacy, both the genders show interest in getting more information through becoming more involved with computers and technology. The study is, however, silent about the security aspect of these smartphone users.

Studies on users' technological background and the resulting impact on their security awareness are quite rare. The only noteworthy study was carried out by Mylonas et al. (2013), which indicated that the technological background of the smartphone users would have a small impact on their security awareness. The study, however, found a noticeable low security adoption in all groups. It is pertinent to mention here that the study merely focused on the Android users and is hence is not a true representation of the phenomenon.

### 2.5.5 Ethnic group

It has been shown that ethnic and cultural factors do have an impact on users' security awareness level (Drevin et al., 2011). Regarding smartphone ownership, the US, Europe and Middle East tend to be the areas where people are more likely to own a smartphone as compared to Latin America, Asia-Pacific and Africa (Poushter, 2016). A report by Nielsen (2014) shows that around 63% of White users, 72% of African American users, 67% of Hispanic users and around 78% of Asian users owned smartphones. The

report found the Hispanics to use apps and spend time on their smartphones (about 37 and a half hours per month on average) more than any other race or ethnicity. Moreover, another report by Nielsen (2015), revealed in the last quarter of 2014, shows that multicultural consumers are leading the smartphone penetration growth as following: 86% Asian/Pacific Islanders, 83% African Americans, 82% Hispanic, 87% others, 75.7% Native American and 74.2% White. Furthermore, a recent report by Lookout (2014) shows that North America (Canada, US and Mexico) and Europe (France, Germany, UK and Spain) malware encounter rates are still low compared to Asia (Japan, China, Russia and Korea) due to the popularity of third-party app stores, excluding Japan as it has the lowest malware encounter rate due to strict regularities. Also, according to the most recent Pew Research Center report (2015), around 13% Latinos and 12% African Americans own smartphones compared with 4% of Whites. Another report by Pew Research Center (2013) shows that nearly 53% White, non-Hispanic users own a smartphone, compared with 64% Black, non-Hispanic users and 60% Hispanic users. Compared to an older study by the same organization (2012), a slight increase was observed in the number of users in each ethnicity group with around 42% of White, non-Hispanic, 47% of Black, non-Hispanic users and 49% of Hispanic users owning a smartphone. The report also shows that African-Americans are more likely to have an Android smartphone. However, Parker et al. (2015) reported that an increase has been witnessed in smartphone ownership in the developing countries, which puts them at a higher security risk.

There is also a diversity regarding apps use among different ethnicities, according to the Nielsen report (2015). The study shows that African-Americans are at the top when it comes to spending time on using apps with nearly 43 hours/month, followed by Hispanics who spend around 41 hours/month, while Asian-Americans and White population spend 37 hours/month and 35 hours/month respectively.

The reports and studies above, however, do not establish a clear link between ethnicity or cultural background and level of security awareness. To conclude, there are limited studies that link ethnicity with smartphone security awareness.

### 2.5.6 Personality

Personality can be defined as "a set of individual characteristics which may determine behavior, predispose and even be positively associated to some psychosomatic conditions" (Preedy & Watson, 2010, p. 4285). With the technological era and the introduction of smartphones, a change has been observed in individuals' personality traits and their habits and interactions with the environment in general (Kim et al., 2015).

Over the years, psychologists and researchers (see, for example, Digman, 1990; Goldberg, 1990) have agreed to describe human personality through five factors. These factors are known as the five-factor model (FFM) or the big five, and include conscientiousness, extroversion, neuroticism, openness to experience and agreeableness. Devaraj et al. (2015) are one of the first researchers who applied the FFM of personality in the IS field to see how each factor could influence technology acceptance. They found that FFM is very useful in order to predict the user's behaviour, attitude and beliefs and the relation between the intention to use (technology acceptance) and the real system use. They summarized the five factors as:

(1) Conscientiousness: the degree of motivation, goal-managing and organization behaviour.
(2) Extroversion: the degree of sociability and being ambitious (whereas introverts tend to be the opposite, being shy and quiet).
(3) Neuroticism (emotional instability): it can be represented by insecurity, hostility and anxiousness. Besides, Costa and McCrae (as cited in Hughes et al., 2012) stated that people with high neuroticism levels may be sensitive and nervous and tend to be more worried, while people with low levels have a good control over emotions and stability.
(4) Openness to experience: represented by flexibility and acceptance of new thoughts and ideas. Costa and McCrae mentioned that people who tend to have a high openness level show more interest and seek for new experiences, while those who have low level of openness are linked to preferring familiarity and convention.
(5) Agreeableness: it is about how friendly people are. People who tend to have a high rating are usually kind and warm (Hughes et al., 2012).

A study by Kim et al. (2015) shows that conscientiousness, openness and extraversion have an association with owning a smartphone more than the other factors. However, the researchers did not measure those factors in order to find out the level of the users' security awareness. Another study by Moore and McElroy (2012) investigated how different personality factors can affect the use of Facebook. They found a significant relation between the personality and the type of wall posting, and level of regret of inappropriate content. This means that users' personality can influence their behaviour.

It has been argued that personality types and characters may impact the technology acceptance of smartphone users (Özbek et al., 2014). Özbek et al. (2014) point out that the acceptance might be different according to the personality type, as the users who tend to show agreeableness perceive the smartphone technology as useful. On the other hand, they report, users who are more neurotic perceive the smartphone technology as less useful. In addition, the users who are open and have more attraction to new things and are willing to try different things perceive the technology of smartphones as an easy thing to use. The study, however, did not cover all the personality dimensions that were stated.

Use of smartphones can lead to different reactions among different users. According to a report by Pew Research Center (2015), the use of smartphone affects users' happiness by 77% and productivity by 79%. On the other hand, around 15% of the users reported that they feel angry when they use their smartphones. The report also shows that young users are more likely to be distracted and frustrated, in addition to sometimes being grateful. In general, the younger users tend to experience a wider range of emotions and moods than the older users.

Personality factors have been widely used to measure and predict both the human attitude and behaviour psychologically. However, there is not much concentration on the technology field. With limited number of studies showing a connection between the smartphone and user personalities and how that could influence the user's security awareness, further investigations are needed.

To conclude, this section investigated the previous literature related to this study's research topic. The literature review clearly demonstrates that the number of studies that link both technological and personal factors with smartphone security awareness is quite

limited. In order to fill this research gap, there is a need for in-depth exploration of the association between technological and personal factors in relation to smartphone users' security awareness.

# 3. Research methodology

In order to examine how different technological and personal factors impact smartphone users' security awareness, a mixed methods research design was applied. Specifically, a combination of descriptive and explanatory methods was used; the methods allowed for asking questions from the research participants and describing their responses. In the descriptive methods paradigm, survey questionnaire was used to collect data. The reason for choosing survey over other descriptive methods was the ease of administration and the swiftness of response it provides in studying groups of individuals (Jackson, 2014). The explanatory method, on the other hand, afforded an opportunity to measure and observe if there is a relation between the various factors under study and the security awareness of smartphone users. The independent variables in the data collection process were the technological and personal factors that came under the purview of this study. Users' security awareness constituted the dependent variable. Both independent and dependent variables have been implicitly and operationally defined in the literature review section above.

This section comprises a description and discussion of data collection methods and procedures in order to ensure the validity, reliability and accuracy of the data. Details about the survey are also included to help determine whether the results are statistically significant or not. The section also explains the questionnaire items of the survey. The section ends with a detailed discussion of the pilot study that was conducted to ensure that the final survey questionnaire is improved and refined.

## 3.1 Data collection

In order to collect the data for this study, an online (web-based) survey was used, which is available online and can be accessed (if not targeted) by anyone. The survey was conducted from September 2015 to March 2016. Online survey was considered to be a better option than paper-based survey in terms of advantages such as ease of use, cost-effectiveness, functionality, and flexibility. Online survey is now deemed as an effective tool to conduct and produce a questioner, and is widely used in many different research fields and topics (Srivatanakul & Wiwatwattana, 2014). The significant growth in online communities and social sites around the world makes online survey more noticeable and

easily accessible to a wider range of participants (Lumsden et al., 2006). Besides, it is considered as the cheapest tool for data collecting and processing, and provides a wider sample coverage compared to paper-based survey (Kapis & Korojelo, 2011).

The survey was developed using Google Forms, which is a free survey-building tool, is easy to deal with, and can handle as much responses as needed with no extra cost ("Google Forms", n.d.). The survey developed for this study (see Appendix F) targeted random smartphone users. It was released and advertised by using different social media websites and applications to make sure that it reaches as wider variety of users as possible. The duration of the survey completion was around 7-9 minutes on average. A pilot study was carried out before the final administration of the survey in order to ensure its reliability and validity (Androulidakis & Kandus, 2011). Details about the pilot study are discussed later in this section.

## 3.2 Questionnaire description

As discussed above, the survey was conducted using an online questionnaire (Appendix F). The questionnaire consisted of 31 closed-ended questions structured as different types of questions (multiple choices, semantic differential, measurement questions, etc.) covering several aspects of smartphone users' security awareness. The questions were designed according to the overall aim of the study to be able to find specific answers related to the research questions. The questionnaire consisted of three main sections; each section was related to a specific topic. The main parts are explained below.

a. General information: This set of questions (Q1 to Q5) are aimed at collecting information related to the personal factors, including the users' gender, age, cultural background, education level, and personality.

b. Technological information: A total of five questions are included in this part. Question 6 is, in a way, associated with both personal and technological factors (it asks about the users' IT level), and works as a logical transition from personal to technological factors questions. Question 7 relates to finding whether the user has a smartphone or not; if

not, the survey will end; otherwise, the response will be counted. Questions 8 helps categories the users by platforms. Questions 9 and 10 are related to the user activity factor to identify the amount of time spent on smartphone and the use pattern. These questions helped relate this information with other questions to find out if this will have any impact on security awareness.

c. Security awareness: This part contains some questions related to technological factors and some related to determining and measuring the security awareness level of the smartphone users, to be able to find whether they understand the security issues their smartphones could be exposed to. Questions 11, 12 and 13 are about the different procedures that the users apply/use to protect their devices. Questions 14 and 15 are related to the users' internet connectivity habits. Another group of questions (16, 17, 18, 19, 26 and 27) are used to find whether the users know or even care about how to perform and configure the security and privacy settings on their smartphone; if they are aware about protecting their smartphones' information from being lost or stolen; whether they are using/following any procedures regarding that; and whether this would have an impact on their security risk understanding. Questions 20, 21, 23 and 25 are designed to determine the actual situation of the smartphone users' security awareness by getting an idea about what they think about security risks.

   Questions 22, 24, 30 and 31 are related to the technological factor 'installed application' to test the users' security risk consciousness when downloading/installing apps as well as to determine which kind of application repositories the user uses to download smartphone applications from, i.e. whether they use official or nonofficial stores. These set of questions are also aimed at finding about the users' behaviours and the factors that could influence their decision when downloading apps. Questions 28 and 29 are intended to see if the users pay attention to security or privacy massages and the license and user agreements when downloading or installing apps.

At the end of the questionnaire, free text space has been provided for the users to leave any additional information, comments or suggestions they would like to write.

## 3.3 Pilot study

Conducting pilot studies are strongly advised in quality research to test the survey, spot any weaknesses, and get feedback to improve the final version (Kothari, 2009). A pilot study was therefore conducted to evaluate the questionnaire. The questionnaire content was shown to targeted experts in the research and IT fields as well as to a group of smartphone users who were similar to our target respondents. The pilot study engaged 43 participants, including 38 females and 5 males. They were aged between 16-54 years old. Out of the total participants, 29 were using iOS based smartphones and 13 Android based smartphones. The questionnaire was administered as an online survey. The questions were almost similar to the final version of the questionnaire that was used to conduct the actual survey. In addition, a compulsory open-ended question was added at the end that asked the users to give suggestions and comments in order to refine and improve the questionnaire. The final results of the pre-test study helped us in different ways, such as: refining the questions that some of the users had difficulties with or were ambiguous about; adjusting some of the predefined answers in order to cover all the desired answers; and finding out if the survey time was reasonable or not (Oates, 2006).

To sum up, this section presented the methods and procedures followed to ensure the validity, reliability and accuracy of our data. The section also reported on the questionnaire's elements distribution to show how we targeted each factor in the survey. Lastly, the section provided results of the pilot study that was conducted in order to evaluate the questionnaire.

# 4. Result analysis and discussion

This section outlines the primary statistical findings that were obtained, which include: 1) descriptive statistics for the survey's questions; 2) statistical tests; 3) testing of the hypothesis; and 4) regression analysis. This is followed by a discussion of answers to our research questions and what we have concluded from the findings of this study. As stated earlier, a total of 919 responses to the survey questionnaire were received. In order to investigate the smartphone users' security awareness concerning personal and technological factors, we tried to find correlations between the responses we had received and then analyzing the data. Quantitative data analysis software SPSS (Statistical Package for Social Science) version 23 was used to investigate and analyze the data and to perform the major statistical tests to ensure the validity and statistical significance of our results. We also used Microsoft Excel to produce some of the charts.

## 4.1 Statistical results

### 4.1.1 Descriptive statistics

In this section, descriptive statistics (including frequency and percentage) for each question on the survey are provided.

Frequency tables (provided in Appendix A) indicate that 75.8% of the respondents were female, 49.9% were between 25 and 34 years of age and 35.4% were between 16 and 24 years of age, 79.4% were of Middle Eastern/Arab origin, and 70.2% had a Bachelor's or higher degree. The respondents represent many different personality types, including 27.1% describing themselves as a conscientiousness personality and 27.7% describing themselves as extroverts. The results are shown in figures 1, 2, 3 and 4 below.

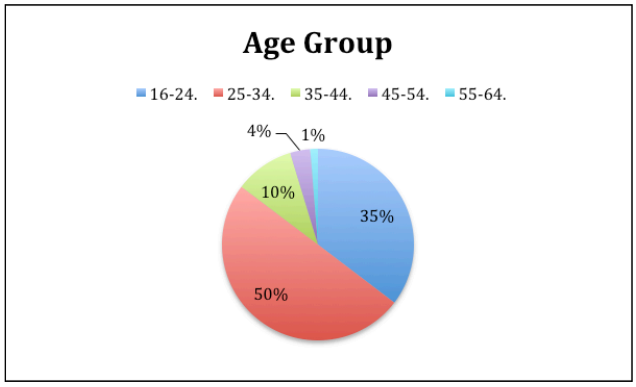


**Figure 1. Age distribution**

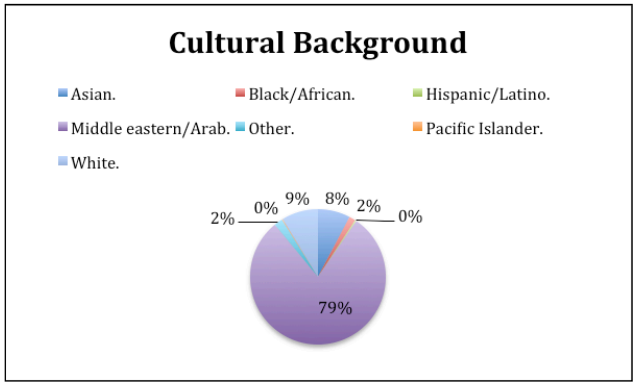


**Figure 2. Ethnic group distribution**

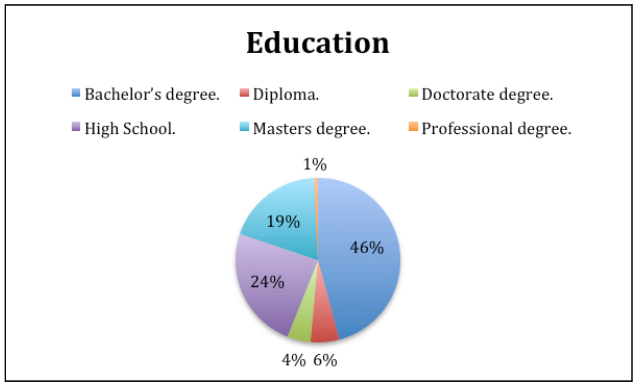


**Figure 3. Education distribution**

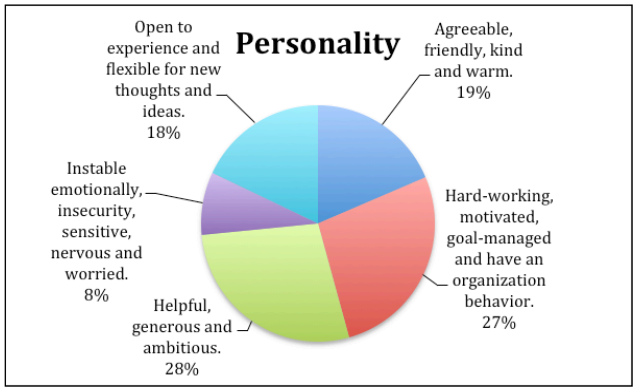


**Figure 4. Personality distribution**

As shown in Fig5, the average respondent considers himself/herself to be intermediate in regards to IT (54.1%), with more users identifying as basic (30.8%) than proficient (15.1%). A significant finding is the fact that 98.5% of respondents use a smartphone. These numbers align with current statistics on the growing popularity and use of smartphones (Barrera & Van Oorschot, 2011; Experian Marketing Services, 2014). The sample, however, has a higher rate of cell phone use than that surveyed by the Pew Research Centre report (2015), which found 64% of American adults having a smartphone device. While a study by Koestsier (2013) found that Androids are more frequently used than iPhones, this study found more iPhone users than Android users, as out of the smartphone users, 66.1% use an iPhone and 32.1% use an Android. As shown in Fig6, almost a quarter (24.5%) of users spend 1-3 hours per day on their phone, 34.2% spend 4-6 hours, 16.9% spend 7-9 hours, and 24.5% report using their phone "almost all the time". A strong majority (68.9%) of the respondents report using the updated or latest version of their smartphone OS.

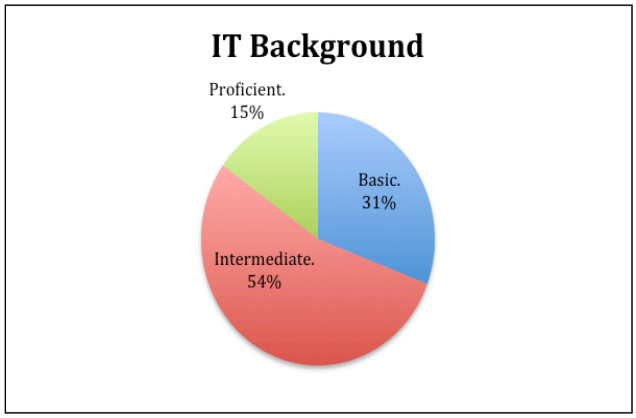


**Figure 5. IT background distribution**

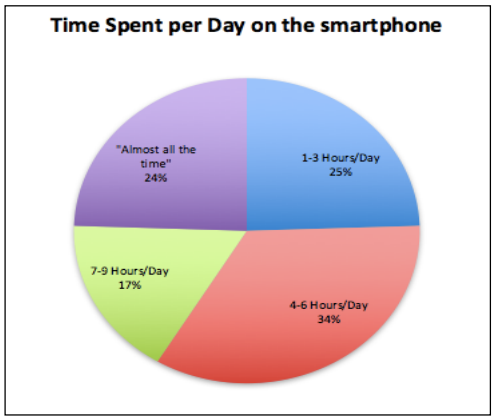


**Figure 6. Time spending/day**

A review of existing literature reveals that sharing of phones and passwords leaves smartphone users vulnerable to security risks (Barrera & Van Oorschot, 2011; Imgraben et al., 2014). Moreover, the touchscreen facility of smartphones renders the possibility of using fingerprint smudges to determine passwords (Alrowaily & Alrubaian, 2011; Aviv et al., 2010). Results of the survey show that a majority (87.5%) of the survey respondents keep their phones password protected. Almost half of respondents (49.2%) reported that they sometimes share their pin key or password with others, while 42.3% informed that they never share this information. Only 12.5% reported that they let others use their phone, while 44.6% allow others to use their phone only when they are present, and 24.4% sometimes allow others to use their phone. While a majority of the respondents (62.6%) reported that they have never lost their smartphone, 17.4% revealed that they have lost it whereas 18.5%

reported that they lost it but got it back. Regarding internet connection, 83.2% keep their phone connected all the time and 15.2% only connect when they need to. A majority of the respondents connect their phones to public networks, with 42.1% reporting doing it regularly and 41.6% intermittently.

A majority of the survey respondents (63.9%) have configured the privacy and security settings on their phones, while 15.8% know how but don't care and 15.5% don't know how but would like to learn. Most of the respondents back-up their phones less than once a month (19%) or less (41.9%), with 25.6% never backing up their phones. Almost half of the respondents (44.8%) informed that their smartphones do not need an antivirus, while 16.9% reported that they didn't know if their phones needed one and 16.1% reported they know they can, but they don't use an antivirus. A majority of the respondents (64.7%) are aware that their phone has security risks. Other half of the respondents perceive their security risks to be average (36.0%) or high (17.3%), with 21.7% reporting to not know their security risk and 23.5% perceiving their risk to be low.

Mylonas et al. (2013) argue that downloading apps opens smartphones to the possibility of installing malwares, such as Trojans. A strong majority (95.3%) of the survey respondents download smartphone apps from official stores and believe that these stores do a security check/test on apps before release (58.9%). Most respondents (66.6%) do not download or install pirated/illegal copy/cracked apps. Answers varied with regard to perception of the ability of smartphones to be hacked/hijacked by malware, virus, Trojans, or the like, with 29.7% reporting to not know, 29.7% reporting that it could not happen, and 39.1% reporting that it could happen. However, 61.5% report feeling comfortable saving critical or private data to their phones. Very few respondents (14.4%) always read the security/privacy/permission messages during downloading/installing apps, with 41.2% never reading the message and 42.9% sometimes reading the message. This aligns with Felt et al.'s (2012) finding that only a small percentage of users review the security of permission messages. Similarly, 60.6% of respondents click agree without reading the license/user agreement message when installing apps. Most respondents (62.2%) do not use all the apps downloaded on their smartphones. Lastly, when downloading apps, the factors of consideration for the respondents are shown in Fig7.

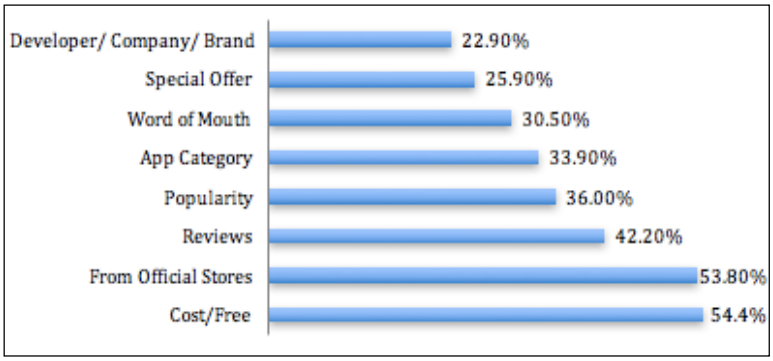


**Figure 7. User's considerations when downloading apps**

### 4.1.2 Statistical tests

In this section, we will correlate the various variables and provide Pearson's correlation coefficient, two tailed p-value, and n-value for each correlation. In order to do this, the data were assigned numerical values in the cleaning process. To run statistical tests, the data were first coded numerically. The codes are given in Appendix G.

❖ **Addressing research question 1**

The salient personal factors chosen for this study (age, education, and IT background) will be correlated with select variables of security awareness (e.g. antivirus use, backup, awareness of security risks, perception of smartphone security risks, thinking smartphone has been attacked by malware, reading security messages, etc.). For both gender and ethnicity, a difference in means t-test will be used to assess the relationship with these security awareness variables.

- ***Age:*** For age, correlation was tested with each of the following: antivirus, backup, aware of security risks, perception of security risks, reading security messages, reading license messages, and perception of malware attack. Of these, the only correlation that is statistically significant (at the 0.05 level) is the correlation between age and reading security messages. Supporting statistics are provided in the table below:

**Table 1: Age correlation table**

| AGE | Pearson Correlation | Sig (2-tailed) | N |
|---|---|---|---|
| Antivirus | -.012 | .729 | 905 |
| Backup | -.003 | .929 | 905 |
| AwareSecRisk | .054 | .018 | 905 |
| ThinkSmartRisk | .049 | .138 | 905 |
| ReadSecMess | .082* | .013 | 905 |
| ReadLicMess | .048 | .145 | 905 |
| AttackMalware | .033 | .316 | 905 |

- ***Education***: Correlation of education as a variable was tested with each of the following: antivirus, backup, awareness of security risks, perception of security risks, reading security messages, reading license messages, and perception of malware attack. Of these, the only correlation that is statistically significant (at the 0.05 level) is the correlation between education and antivirus usage. Supporting statistics are provided in the table below:

**Table 2: Education correlation table**

| EDUCATION | Pearson Correlation | Sig (2-tailed) | N |
|---|---|---|---|
| Antivirus | .077* | .020 | 905 |
| Backup | -.017 | .605 | 905 |
| AwareSecRisk | .004 | .897 | 905 |
| ThinkSmartRisk | .003 | .938 | 905 |
| ReadSecMess | .034 | .303 | 905 |
| ReadLicMess | .027 | .413 | 905 |
| AttackMalware | .061 | .065 | 905 |

- ***IT background:*** For IT proficiency, correlation was tested between this variable and each of the following: antivirus, backup, awareness of security risks, perception of security risks, reading security messages, reading license messages, and perception of malware attack. Of these, all variables except perception of malware

attack were significant. Backup, awareness of security risks, reading security messages, and reading license messages were statistically significant at the 0.01 level and antivirus use and perception of smartphone security risks were correlated at the 0.05 level. Supporting statistics are provided in the table below:

**Table 3: IT background correlation table**

| IT BACKGROUND | Pearson Correlation | Sig (2-tailed) | N |
|---|---|---|---|
| Antivirus | -.072** | .030 | 905 |
| Backup | .180** | .000 | 905 |
| AwareSecRisk | .106** | .001 | 905 |
| ThinkSmartRisk | .078* | .018 | 905 |
| ReadSecMess | .190** | .000 | 905 |
| ReadLicMess | .103** | .002 | 905 |
| AttackMalware | .024 | .470 | 905 |

- ***Gender:*** Because gender is not an ordinal variable, a t-test was used to assess differences between male and female respondents. For the t-test, the SPSS output (see Appendix B) provides that equal variances cannot be assumed for four of the variables: antivirus, backup, reading security messages, and reading license messages. For the remainder of the variables, equal variances can be assumed (based on a statistically significant, >0.05 Levene's Test for the Equality of Variances). For variables with a statistical significance greater than 0.05, we conclude that there is no statistical significance between males and females in the sample. Therefore, we can conclude that there is a statistically significant difference between genders for backup, awareness of security risks, perceptions of security risks, and perceptions of malware attack. Supporting statistics are provided in the table below:

**Table 4: Gender t-test table**

| GENDER | Levene's Test Outcome | Sig (2-tailed) of T-test for Equality of Means |
|---|---|---|
| Antivirus | Equal variances not assumed | .297 |

| | | |
|---|---|---|
| Backup | Equal variances not assumed | .022 |
| AwareSecRisk | Equal variances assumed | .029 |
| ThinkSmartRisk | Equal variances assumed | .039 |
| ReadSecMess | Equal variances not assumed | .750 |
| ReadLicMess | Equal variances not assumed | .254 |
| AttackMalware | Equal variances assumed | .002 |

- ***Ethnicity:*** Again, because ethnicity is not an ordinal variable, a t-test was used to assess differences between the ethnicities. Because 79.4% of respondents identified themselves as Middle Eastern, the tests were conducted to compare the difference between respondents who identify as Middle Eastern and all other respondents. For the t-test, the SPSS output provides that equal variances cannot be assumed for five of the variables: antivirus, awareness of security risks, perceptions of security risks, reading security messages, and perceptions of attack by malware. For the remainder of the variables, equal variances can be assumed (based on a statistically significant, >0.05 Levene's Test for the Equality of Variances). For variables with a statistical significance greater than 0.05, we conclude that there is no statistical significance between males and females in the sample. Therefore, we can conclude that there is a statistically significant difference between Middle Easterners and non-Middle Easterners for antivirus, perceptions of security risks, reading security messages, and reading license messages. Supporting statistics are provided in the table below:

**Table 5: Ethnicity t-test table**

| **Ethnicity** | **Levene's Test Outcome** | **Sig (2-tailed) of T-test for Equality of Means** |
|---|---|---|
| Antivirus | Equal variances not assumed | .042 |
| Backup | Equal variances assumed | .265 |
| AwareSecRisk | Equal variances not assumed | .681 |

| | | |
|---|---|---|
| ThinkSmartRisk | Equal variances not assumed | .010 |
| ReadSecMess | Equal variances not assumed | .000 |
| ReadLicMess | Equal variances assumed | .000 |
| AttackMalware | Equal variances not assumed | .944 |

- ***Personality:*** Because personality is not an ordinal variable and there were more than two possible responses, ANOVA was used to assess differences between the five personality types. For the t-test, the SPSS output below personality is not statistically significant for the security risk factors with the exception of Attack by Malware. Therefore, we cannot conclude that there is a statistically significant difference between personality types for backup, awareness of security risks, and perceptions of security risks. Supporting statistics are provided in the table below:

**Table 6: Personality t-test table**

ANOVA

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Antivurus | Between Groups | .772 | 4 | .193 | .575 | .681 |
| | Within Groups | 302.174 | 900 | .336 | | |
| | Total | 302.946 | 904 | | | |
| AwareSecRisk | Between Groups | .445 | 4 | .111 | .492 | .742 |
| | Within Groups | 203.367 | 900 | .226 | | |
| | Total | 203.812 | 904 | | | |
| ThinkSmartRisk | Between Groups | 8.578 | 4 | 2.144 | 2.067 | .083 |
| | Within Groups | 933.665 | 900 | 1.037 | | |
| | Total | 942.243 | 904 | | | |
| ReadSecMess | Between Groups | 5.289 | 4 | 1.322 | 2.715 | .029 |
| | Within Groups | 438.297 | 900 | .487 | | |
| | Total | 443.587 | 904 | | | |
| ReadLicMess | Between Groups | 4.086 | 4 | 1.021 | 2.209 | .066 |
| | Within Groups | 416.102 | 900 | .462 | | |
| | Total | 420.188 | 904 | | | |
| AttackMalware | Between Groups | 6.778 | 4 | 1.694 | 2.472 | .043 |
| | Within Groups | 617.050 | 900 | .686 | | |
| | Total | 623.828 | 904 | | | |

To summarize, based on the correlations and t-tests presented within this section, the following relationships are statistically significant:

- Older respondents are more likely to read security messages.
- More educated respondents are more likely to use antivirus.
- The more IT proficient the respondent, the more likely he/she is to backup, be aware of security risks, perceive security risks to be greater, and read security and license messages.
- The more IT proficient a respondent, the less likely he/she is to use anti-virus.
- Male respondents are more likely to back up their phones, have a higher awareness of security risks, perceive greater security risks, and perceive greater chances of malware attack.
- Middle Eastern respondents are more likely to use antivirus, perceive less security risk, are less likely to read security messages, and are less likely to read license messages.

❖ **Addressing research question 2**

Answers related to security awareness (e.g., antivirus use, backup, awareness of security risks, perception of smartphone security risks, thinking that the smartphone has been attacked by malware, reading security messages, installed applications) were compared for smartphone type, for installed applications, and for activities on smartphone.

Before initiating this step, we needed to create an index variable of security awareness (composite of security awareness variables). In order to do this, 15 variables were aggregated. Variables in which a high score indicated a security risk were added, and variables in which a low security indicated a security risk were subtracted. Specifically, the following variables were added: sharing passwords, allowing others to use the phone, constant connection to the internet, connecting to public internet, lost phone in the past, downloading apps, use of cracked apps, and attacked by malware. The following variables were subtracted to develop the index: password protecting the phone, configuring privacy settings, backing-up the phone, using an antivirus, updating the phone, reading security messages, and reading license messages. The security index message was calculated for

each respondent. The index mean was -1.27, with a range from -11 to 9. For these numbers, 9 indicates the highest security risk and -11 indicates the lowest security risk.

In order to address research Q2, a difference in means t-test was conducted to assess the differences between iPhone and Android users in terms of security awareness index. There is no statistically significant difference in the security awareness scores of iPhone (M=-1.33, SD=3.12) and Android (M=-1.17, SD=3.27) users (t=-.721, p=.471). Next, correlation was calculated for downloading cracked apps and the security awareness index, which indicated a strong statistically significant relationship (r=.337, n=897, p=.000). Similarly, the correlation between downloading apps and the security awareness index was calculated and found to be statistically significant (r=.089, n=897, p=.008). The relationship between using all downloaded apps and the security awareness index was not found to be statistically significant (r=-.058, n=897, p=.085). No significant relationship was found between time spent on one's phone and security awareness (r=.047, n=897, p=.161).

### 4.1.3 Testing the hypotheses

In this section, we report on the testing of our statistical hypotheses. A hypothesis testing is the process of checking or finding out whether our research results are supporting what we hypothesized earlier (Jackson, 2016). Hypotheses testing details are given below:

- H1: There is a relationship between platform used and user security awareness (2-tailed).

Running correlation between OS and the security awareness index reveals that there is no statistically significant relationship between the two variables (r=0.28, n=897, p=.406). We therefore reject this hypothesis.

- H2: There is a relationship between installed applications and user security awareness (2-tailed).

This hypothesis is tested using the relationship between each downloaded apps (Q22), cracked apps (Q24), and use of all apps (Q30). There is a statistically significant relationship between downloading apps and the security awareness index (r=.089, n=897, p=.008). There

is also a statistically significant relationship between using cracked apps and the security awareness index (r=.337, n=897, p=.000). However, the relationship between using all apps on the phone and the security awareness index is not statistically significant (r=-.058, n=897, p=.085). Based on these data, we reject the hypothesis relating use of all apps to security awareness, but we fail to reject the hypothesis based on downloading apps and use of cracked apps.

- H3: There is an inverse relationship between the user activities and user security awareness (1-tailed).

There is no statistically significant relationship between user activities and user security awareness (r=.047, n=897, p=.161). Based on these data, we reject the hypothesis that there is a relationship between frequency of user activity and user security awareness.

- H4: There is an inverse relationship between age of smartphone users and user security awareness (1-tailed).

There is no statistically significant relationship between age and the security awareness index (r=0.046, n=897, p=.166). Based on these data, we reject the hypothesis that there is an inverse relationship between the age of smartphone users and their security awareness.

- H5: Female smartphone users have greater security awareness than male smartphone users.

There is a statistically significant relationship between gender— males (M=-1.70, SD=3.27) and females (M=-1.14, SD=3.11)— in regards to the security awareness index (t=2.22, p=.027). The means indicate that females have a higher security awareness index mean than males. This provides that females have less security awareness than males. Based on this, we reject the hypothesis that female smartphone users have greater security awareness than male smartphone users.

- H6: There is a positive relationship between educational attainment and user security awareness (1-tailed).

There is a statistically significant relationship between educational attainment and the security awareness index (r=-.046, n=897, p=.166). As a higher security awareness index number indicates a greater risk, the negative correlation coefficient indicates that there is an inverse relationship between educational attainment and security risk. Thus, the greater one's educational attainment, the less security risk he/she has in relation to smartphones. Based on these data, we fail to reject the hypothesis that there is a positive relationship between educational attainment and user security awareness.

- H7: There is a positive relationship between technological background and user security awareness (1-tailed).

There is a statistically significant relationship between IT background and the security awareness index (r=-.245, n=897, p=.000). The correlation coefficient indicates an inverse relationship between the technological background and the security awareness index, which provides that the greater one's technological background, the less of a security risk he/she has in relation to smartphone use. Based on these data, we fail to reject the hypothesis that there is a positive relationship between technological background and user security awareness.

- H8: All ethnic groups will have moderate security awareness.

There is no statistically significant relationship between ethnicity— Middle Eastern (M=-1.21, SD=3.12) and non-Middle Eastern (M=-1.55, SD=3.28)— in regards to the security awareness index (t=1.28, p=.203). Based on these data, we reject the null hypothesis relating to ethnicity and security awareness.

- H9: There is a relationship between personality and user security awareness.

The figure below reveals that there is a relationship between personality and security awareness index measures. Respondents who identified or tended to be neurotic, who are "emotionally unstable, insecure, sensitive, nervous, and worried" had the highest security awareness index means, indicating that these individuals were at the most risk, followed by those with agreeable, friendly, kind, and warm personalities.

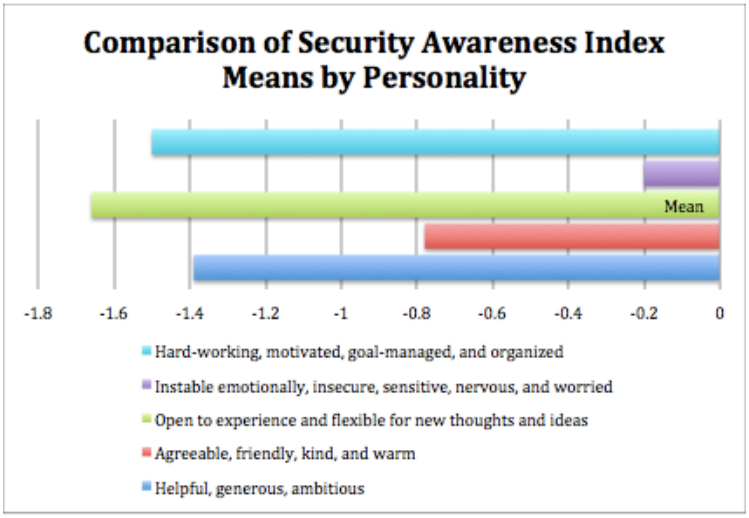


**Figure 8. Comparison of security awareness index means by personality**

### 4.1.4 Regression analysis

In this section, we discuss the regression analysis that we ran, in which security awareness index variable is the dependent variable and the following are used as independent variables: platform, applications, user activities, age, gender, education, technological background, ethnicity, and personality. However, we did not include the installed applications and user activities factors; since most of the respondents use their phones for multiple tasks, it would difficult to differentiate security risks or awareness for a single task.

A multiple linear regression was calculated to predict smartphone awareness index measures based on OS, age, gender, education level, IT background, ethnicity, and personality. The regression model tested in SPSS is as follows:

$$SecurityAwareIndex = \beta 0 + \beta 1\ OperatingSystem + \beta 2\ Age + \beta 3\ Female + \beta 4\ Educ + \beta 5\ ITProficiency + \beta 6\ MiddleEastern + \varepsilon$$

A significant regression equation was found (F(7,889)=9.218, p<.000), with an R2of 0.68. Respondents' predicted security awareness index score is .921+.253 (OS)-.038 (AGE)+.438 (FEMALE)-.123 (EDUC)-1.113(IT) .357(ETHNICITY) (as mentioned before in the codebook). Security awareness index scores increased with .253 index points with use of non-iPhone operating systems and .438 for females. Security awareness index scores

decreased .038 with age group increase, .123 with educational attainment degree increase, 1.113 with one unit increase in IT proficiency, and .357 with being non-Middle Eastern. IT background was the only significant predictor of security awareness index scores ($\beta$=-2.232, p<.000).

## 4.2 Discussion

In this section, the findings of the study are discussed with a view to determining the extent to which the different personal and technological factors, which are the focus of this study, have an impact on smartphone users' security awareness. The discussion is centered around answers to the research questions this study set out with. Each research question is answered below based on the findings of the study.

1) Do different personal factors (e.g., educational and technological background, gender, age) have an impact on users' smartphone security awareness?

Findings from the data reveal that some personal factors do impact users' security awareness. Regarding age, for instance, the older respondents were found to be more likely to read security messages. The previous studies focused on the age brackets for likely smartphone use (Nielsen, 2013; Pew Research Center, 2013), and smartphone dependency in youth vs. late adulthood (Deursen et al., 2015; Pew Research Centre, 2015). The findings of this study regarding age are noteworthy because they indicate more responsibility regarding security among older population. The findings contradict those of an earlier study by Parker et al. (2015) where younger smartphone users were found to have more security awareness as opposed to older users.

In relation to educational background, more educated respondents in this study were found to be more likely to use antivirus. This is in contrast to the findings of studies carried out by Jones et al. (2014) and Jones and Heinrichs (2012). Jones et al. argued that although educated, most smartphone users do not show enough awareness about potential security risks, and those who are aware do not apply it on their smartphones in terms of security procedures. Similarly, Jones and Heinrichs (2012) found students generally careless and

unaware of security awareness. This study, however, although limited in scope, makes it clear that the higher the educational background of the respondents, the more likely they are to use antivirus.

Concerning IT background, we found that the more IT proficient the respondent, the more likely he/she is to backup, be aware of security risks, perceive security risks to be greater, and read security and license messages. Ironically, however, the more IT proficient a respondent, the less likely he/she is to use anti-virus. The technological background-related finding of this study is quite important as there is an acute dearth of empirical literature that deals with this aspect of security awareness. The only other study, carried out by Mylonas et al. (2013), also found a small impact of technological background of the smartphone users on their security awareness. However, the findings of our study are more significant because it focusses on both Android and iOS users whereas Mylonas et al. (2013) merely focused on Android users.

Regarding gender, male respondents were found more likely to back up their phones, have a higher awareness of security risks, perceive greater security risks, and perceive greater chances of malware attack. This is a significant finding because although some recent studies (see, for example, Deursen et al., 2015; Kim et al., 2015) found that females are more likely than males to own, use and feel addicted to smartphones, the studies did not show any relationship between gender and security awareness. Additionally, this finding of our study is also contradictory to Jones and Heinrichs's (2012) study who found men more likely to be engaged in risky practices on their smartphones. Interestingly, while Jones and Chin (2015) found no differences between the two genders with regard to smartphone security practice and behaviour, our study clearly shows that men are far smarter than women (at least in the context of the Middle East) when it comes to smartphone security awareness.

In relation to ethnicity, it was found that Middle Eastern respondents are more likely to use antivirus, perceive less security risk, are less likely to read security messages, and are less likely to read license messages. The findings are consistent with studies carried out on other ethnicities (Drevin et al., 2011; Lookout, 2014; Nielsen, 2014, 2015; Pew Research Center, 2013, 2015) that show that ethnic background has an impact on the security awareness of smartphone users. Although some studies have also investigated the diversity

concerning the use of apps among different ethnicities (see, for example, Nielsen, 2015), apps use did not come under the purview of our study.

This study set out to test several hypotheses based on the personal factors associated with the security awareness of smartphone users. Some of these hypotheses were found valid whereas others were found invalid. Our findings reject the hypothesis that there is an inverse relationship between the age of smartphone users and user security. The findings also reject the hypothesis that female smartphone users have greater security awareness than male smartphone users. On the other hand, the findings proved the hypothesis that there is a positive relationship between technological background and user security awareness. The findings also proved the hypothesis that there is a positive relationship between educational attainment and user security awareness. The null hypothesis relating to ethnicity and security awareness, however, could not be proved. Finally, a relationship was found between personality and security awareness index measures. In this regard, respondents who identified as neurotic had the highest security awareness index means, indicating that these individuals were at the most risk, followed by those with agreeable personalities. This study therefore corroborates some of the findings of studies carried out in the past (Kim et al., 2015; Moore & McElroy, 2012; Özbek et al., 2014) on the association between personality type and the extent of security awareness among smartphone users.

2) Do different technological factors (e.g., operating systems, installed apps, types of connected network, and user activities) have on impact on users' smartphone security awareness at the time they install third-party applications?

In the literature review section, we carried out a detailed review of the different operating systems used by the smartphone users and the various threats that these operating systems are prone to. Empirical studies (Juniper Networks, 2011; La Polla et al., 2013) were cited to show that Android users are at a comparatively increased risk of security threat. This study found that regardless of the operating system that the respondents use, it does not impact their security awareness. This finding has implications for users of operating systems that are more vulnerable. It was also found that the use of cracked apps increases one's security risk, as does downloading apps. This finding corroborates the findings and

recommendations of some other studies carried out in the past (O'Brian, 2016; Ofcom, 2013; Wright, 2011). It highlights the importance of downloading only required apps (Wright, 2011), downloading them from trusted sources (Ofcom, 2013), determining the developers' reputation (Sophos Report, 2013), and remaining vigilant about malicious apps imbedded as legitimate apps (Symantec Report, 2013). Interesting, however, the findings revealed that using all apps on the phone is not a significant factor in security awareness, nor is time spent on one's phone. While it has been shown that using all apps and spending more time on the phone could lead to increased security risk (Louca & Ktoridou, 2014), this study failed to establish a relationship between these user activities and their smartphone security awareness.

Regarding the statistical hypotheses that were set in regards to the second research question, some were proved valid whereas others were found invalid. We reject the hypothesis that there is a relationship between platform used and security awareness. We also reject the hypothesis that there is a relationship between using all apps on one's phone and security awareness. However, the hypothesis that there is a relationship between downloading apps and security awareness as well as between using cracked apps and security awareness was proved. Finally, we reject the hypothesis that there is a relationship between frequency of user activity and user security awareness.

To conclude, in this section we displayed the descriptive statistics related to our survey's questions followed by the statistical tests, which addressed both research questions. This section also displayed the results pertaining to the testing of the hypotheses, followed by a discussion of the regression analysis. Finally, we discussed answers to our research questions and what we have concluded from the findings of this study. In summary, the factors that are statistically significant in relation to smartphone security awareness are technological backgrounds, educational levels, downloading apps, and installed apps, using cracked apps in specific.

# 5. Problems, future work and recommendations

In this section we describe the problems and limitations that were faced during the conduct of this research, the way they affected the overall study, and how we may possibly avoid them in the future. We also incorporate some suggestions and improvements for future work on the topic. Lastly, some recommendations are given on how this study can be used and further areas that it can lead to for research.

## 5.1 Problems and limitations

While due care was taken in designing and conducting this study, we believe there are a few limitations of the study that should be taken into consideration when conducting future work in this area. Firstly, there is a limitation with regard to the demographics of the study pertaining to the ethnicity of the respondents. Around 80% of the sample is comprised of respondents from the Middle Eastern origin; the second largest group comprised of around 8% of the respondents. It would therefore be hard to generalize the findings to other ethnic groups. Although the study was not designed with the aim of focusing on Middle Eastern respondents, the data proved otherwise. This limitation was countered through dividing the respondents into those of Middle Eastern and non-Middle Eastern origin. However, despite our study's findings not necessarily translatable to other ethnic groups, the salient aspect of the findings is that the study gives an insight into the smartphone security awareness of the large Middle Eastern group. The study is also significant because there is a noticeable lack of research on participants from Middle Eastern origin.

Secondly, the lack of studies on the Middle East region in computer and security-related human behaviour did not allow us to have an in depth look at some of the technological and personal factors. Due care was, however, taken to give a comprehensive review of theoretical and empirical literature that is available in the field.

Thirdly, we believe that semi-structured interviews with some selected respondents would have given more depth to the study. However, despite our initial plans to do so, it could not be materialized because of paucity of time.

Finally, collecting the data took more time than we expected. It was examination period in most of the areas, and the youth was busy in preparing for and taking exams, so

they took a long time in responding to the survey questionnaire. For any future work of this nature, it is advisable to choose the timing of sending out the survey carefully.

## 5.2 Future work

As the sample of the study was selected randomly, future work in the area can conduct and apply the same survey to specific cultural and demographic profile of respondents – as subgroups – in order to get a comparable data from different backgrounds and then explore and compare their security awareness. Also, since other operating systems are contending for taking a place in the market, future studies could focus on other platforms and expand on the research area. In addition, the number of respondents could be increased to get results that are more generalizable. Finally, with the rapid growth in the IT research field, we need to keep track of the most recent studies to build stronger evidences.

## 5.3 Recommendations

The findings of this study are expected to provide valuable information to different organizations in determining how they could increase and raise the security awareness of smartphone users. They could do so by designing appropriate security awareness programs and campaigns in light of this study's findings that some factors are more important and have more influence on the users' security behaviour.

Foregoing in view, there is a need for taking steps to ensure the device and personal information security of smartphone users. In order to defend against smartphone threats, a user himself/herself has the foremost responsibility and must be educated to gain the best security awareness and practice. Therefore, the security controls within smartphones should be simple to understand by average users (Parker et al., 2015). The security indicators on the apps repositories should be redesigned and the smartphone users should be educated on how to use them (Mylonas et al., 2013). Better security literacy among smartphone users may also go a long way in ensuring that their devices are protected from hackers and malware (Kato & Mastura, 2014). Besides, as recommended by Rodr´ıguez-Mota et al. (2016), one of the most effective solutions to security problems in smartphones

– especially Android – is the use of application management, as it could restrict or even inhibit the infected app from infecting the device. Such application management should therefore be ensured in all smartphones. Furthermore, there must be focus on establishing campaigns to raise security awareness among smartphone users (Mylonas et al., 2013; Parker et al., 2015; Sari & Candiwan, 2014; Volkamer et al., 2015). Additionally, there must be a centralized and trusted organization at the government level to deal with any security incidents (Al-Hadadi & Al Shidhani, 2013). Also, governments should collaborate with the private sector to provide users with the best security practice. Such a collaboration could ensure an easier and more effective discovery and solution of new security incidences. Security awareness campaigns in this regard will definitely help in increasing smartphone security awareness and practice among users.

# 6. Conclusion

To conclude, the main aim of this study was to examine and find out the impacts of different personal and technological factors on the security awareness of smartphone users. The results show that the factors that are statistically significant in relation to smartphone security awareness are technological background, educational level, downloading apps, and using cracked apps. Regarding downloading apps and the use of cracked apps, these findings align with the existing literature. The literature provides that 1) individuals at the most security risk often have the least security awareness (Androulidakis & Kandus, 2011; Imgraben et al., 2014) and 2) individuals who download apps, especially cracked apps, have the greatest security risk (Mylonas et al., 2013). Therefore, the finding of this research that individuals who download apps and/or use cracked apps have the least security awareness is supported by the literature. Furthermore, the finding that educational level and technological background both increase one's security awareness aligns with the findings of Al-Hadadi and Al Shidhani (2013). However, although Reinfelder et al. (2014) found that Android users have a greater awareness of smartphone security risks, this research did not find a statistically significant difference between the two platforms.

Overall, the findings of the study reveal that a number of personal and technological factors affect smartphone users' security awareness. There is therefore a need for taking appropriate steps, as recommended in the above section, to enhance the security awareness of smartphone users, especially in the context of Middle East.

# REFERENCES


Accenture. (2016). *Igniting growth in consumer technology [Report]*. Retrieved June 7, 2016, from https://www.accenture.com/t20160108T124537__w__/us-en/_acnmedia/PDF-3/Accenture-Igniting-Growth-In-Consumer-Technology.pdf#zoom=50

Al-Shidhani, A., & Al-Hadadi, M. (2013). *Smartphone security awareness: Time to act*. Paper presented at the 2013 International Conference on Current Trends in Information Technology (CTIT 2013), Dubai, UAE.

Alrowaily, K., & Alrubaian, M. (2011). *Oily residuals security threat on smart phones*. Paper presented at the First International Conference on Robot, Vision and Signal Processing (RVSP), Kaohsiung City, Taiwan.

Androulidakis, I., & Kandus, G. (2012). Feeling secure vs. being secure: The mobile phone user case. In C. K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush & A. Al-Nemrat (Eds.), *Global security, safety and sustainability & e-Democracy* (Vol. 99, pp. 212-219). Berlin, Germany: Springer.

Anjum, A., & Ilyas, M. U. (2013). *Activity recognition using smartphone sensors*. Paper presented at the Consumer Communications and Networking Conference (CCNC), IEEE.

Aqel, M., Hirzallah, N., & Nseir, S. (2013). *Issues with various security threats on mobile phones*. Paper presented at the Palestinian International Conference on Information and Communication Technology (PICICT 2013), Gaza, Palestinian Territories.

Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). *Smudge attacks on smartphone touch screens*. Paper presented at the the 4th USENIX conference on Offensive technologies, Washington, DC.

Balebako, R., Marsh, A., Lin, J., Hong, J. I., & Cranor, L. F. (2014). *The privacy*

*and security behaviors of smartphone app developers.* Proceedings of workshop on usable security (USEC), San Diego, CA: Carnegie Mellon University.

Barrera, D., & Van Oorschot, P. (2011). Secure software installation on smartphones. *IEEE Security & Privacy Magazine, 9*(3), 123-134.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computer & Security, 28*, 3-4.

Canalys. (2011). *Mobile security investment to climb 44% each year through 2015*. Retrieved from http://www.canalys.com/static/press_release/2011/mobile-security-forecast.pdf

Chin, E., Felt, A. P., Sekary, V., & Wagner, D. (2012). *Measuring user confidence in smartphone security and privacy*. Paper presented at the SOUPS '12 Proceedings of the Eighth Symposium on Usable Privacy and Security Washington, DC, USA.

comScore. (2015). comScore reports November 2014 U.S. smartphone subscriber market share. Retrieved June 9, 2016, from http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-November-2014-US-Smartphone-Subscriber-Market-Share

Cullen, T. A., & Cobb, I. C. (2011). Computer literacy needs in a traditional library literacy program: Results of a needs analysis. *TechTrends, 55*(6), 25-32.

Deursen, A. J. A. M. v., Bolle, C. L., Hegner, S. M., & Kommers, P. A. M. (2015). Modeling habitual and addictive smartphone behavior: The role of smartphone usage types, emotional intelligence, social stress, self-regulation, age, and gender. *Computers in Human Behavior, 45*, 411-420.

Devaraj, S., Easley, R. F., & Crant, L. M. (2008). Research note: How does personality matter? Relating the five-factor model to technology acceptance and use. *Information System Research, 19*(1), 93-105.

Drevin, L., Flowerday, S., Kruger, H., & Steyn, T. (2011). *An assessment of the role of cultural factors in information security awareness*. Paper presented at the Information Security South Africa (ISSA), Johannesburg, South

Africa.

Duggan, M., & Smith, A. (2013). *Cell internet use 2013 [Report]*. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_CellInternetUse2013.pdf

Enck, W., Ongtang, M., & McDaniel, P. (2009). *On lightweight mobile phone application certification*. Paper presented at the CCS '09 16th ACM Conference on Computer and Communications Security 2009 Chicago, IL, USA.

Ericsson. (2016). *Ericsson mobility report [Report]*. Retrieved from http://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

Experian Marketing Services (2014). *Millennials come of age[Report]*. Experian Marketing Services.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android permissions: User attention, comprehension, and behavior*. Paper presented at the SOUPS '12 Proceedings of the Eighth Symposium on Usable Privacy and Security Washington, DC, USA.

Field, A. (2005). *Discovering statistics using IBM SPSS statistics, and sex and drugs and rock 'n' roll [2nd edition]*: Los Angeles, LA: Sage.

GlobalWebIndex (GWI). (2016). *GWI device [Report]*. Retrieved June 11, 2016, from http://insight.globalwebindex.net/device

Google. (2015). *Mobile app marketing insights: How consumers really find and use your apps*[Report]. Google.

Google Forms. (n.d.). Retrieved July 01, 2015, from https://goo.gl/DYFITN

Hrestak, D., Picek, S., & Rumenjak, Ž. (2015). *Improving the android smartphone security against various malware threats.* Paper presented at the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Opatija, Croatia.

Hughes, D. J., Rowe, M., Batey, M., & Lee, A. (2012). A tale of two sites: Twitter vs. Facebook and the personality predictors of social media usage. *Computers in Human Behavior, 28*(1), 561-569.

Ikolo, V. E., & Okiy, R. B. (2012). Gender differences in computer literacy among clinical medical students in selected southern Nigerian universities. *Library Philosophy and Practice, 58*, 73-87.

Jackson, S. L. (2016). *Research methods and statistics: A critical thinking approach [5th edition]*: Boston, MA: Cengage Learning.

IDC Research. (2015). Smartphone OS market share, 2015 Q2. Retrieved from http://www.idc.com/prodserv/smartphone-os-market-share.jsp

Imgraben, J., Engelbrecht, A., & Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour and Information Technology, 33*, 1347-1360.

Jang, Y.-T., Chang, S. E., & Tsai2, Y.-J. (2013). *Smartphone security: Understanding smartphone users' trust in information security management*. Security and Communication Networks.

Jones, B., Chin, A., & Aiken, P. (2014). Risky business: Students and smartphones. *TechTrends, 58*(6), 73-83.

Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. *International Journal of Information Management, 35*(5), 561-571.

Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems, 53*(2), 22-30.

Juniper Networks Global Threat Center. (2011). *Malicious mobile threats report 2010/2011: An objective briefing on the current mobile threat landscape*. Juniper Networks Global Threat Center Research.

Kandus, G., & Androulidakis, I. (2011). *A survey on saving personal data in the mobile phone*. Paper presented at the Sixth International Conference on Availability, Reliability and Security (ARES 2011), Vienna, Austria.

Kandus, G., & Androulidakis, I. (2011). *Ramifications of mobile phone advanced O/S on security perceptions and practices*. Paper presented at the Third International Workshop on Cyberspace Safety and Security (CSS), Milan, Italy.

Kapis, K., & Korojelo, S. P. (2011). Enhanced authentication on Targeted Online Surveys: A case of online course evaluation system. In A. Abd Manaf, A. Zeki, M. Zamani, S. Chuprat & E. El-Qawasmeh (Eds.), *Informatics engineering and information science* (Vol. 251, pp. 22-32). Berlin, Germany: Springer.

Kato, M., & Matsuura, S. (2014). *Improve user's security literacy by experiencing behavior of pseudo android malware.* Paper presented at the IEEE 38th Annual International Computers, Software and Applications Conference, Vasteras, Sweden.

Kim, Y., Briley, D. A., & Ocepek, M. G. (2015). Differential innovation of smartphone and application use by sociodemographics and personality. *Computers in Human Behavior, 44*, 141-147.

Koetsier, J. (2013). *We will download 70 billion mobile apps in 2013 (50% Android, 41% iOS).* Retrieved April 29, 2015, from http://venturebeat.com/2013/03/04/we-will-download-70-billion-mobile-apps-in-2013-50-android-41-ios/

Koetsier, J. (2013). *800 million Android smartphones, 300 million iPhones in active use by December 2013, study says*. Retrieved May11, 2015, from http://venturebeat.com/2013/02/06/800-million-android-smartphones-300-million-iphones-in-active-use-by-december-2013-study-says/

Kothari, C. R. (2009). *Research methodology: Methods and techniques.* New Delhi, India: New Age International Publishers.

La Polla, M., Martinelli, F., & Sgandurra, D. (2013). A survey on security for mobile devices: Communications surveys & tutorials. *IEEE, 15*(1), 34-57.

Li, X.-T., Ren, S., Cheng, W., Xiang, L.-S., & Liu, X.-Y. (2014). Smartphone: Security and privacy protection. In Q. Zu, M. Vargas-Vera, & B. Hu (Eds.), *Pervasive computing and the networked world: Joint international conference, Vina del Mar, Chile – Revised selected papers* (pp. 289-302). Cham, Vietnam: Springer.

Lookout. (2011). *Lookout mobile threat report* [Report]: Lookout.

Lookout. (2014). *Mobile threats, made to measure: The specialization of mobile threats around the world* [Report]: Lookout.

Louca, S., & Ktoridou, D. (2014). *Understanding young cypriots smartphone apps utilization: Extent and frequency.* Paper presented at the Interactive Mobile Communication Technologies and Learning (IMCL), 2014 International Conference on Interactive Mobile Communication Technologies and Learning, Thessaloniki, Greece.

Lumsden, J., Flinn, S., Anderson, M., & Morgan, W. (2006). What difference do guidelines make? An observational study of online-questionnaire design guidelines put to practical use. In T. McEwan, J. Gulliksen & D. Benyon (Eds.), *People and computers XIX: The bigger picture* (pp. 69-83). London, England: Springer.

Maryland Technology Literacy Consortium (TLC). (n.d.). *Definition of Technology Literacy.* Retrieved July 20, 2015, from http://www.montgomeryschoolsmd.org/departments/techlit/docs/Definition%20of%20Technology%20Literacy.pdf

McAfee Labs. (2016). *2016 threats predictions [Report]*: McAfee Labs.

Mitchell, E., Monaghan, D., & O'Connor, N. E. (2013). Classification of sporting activities using smartphone accelerometers. *Sensors, 13*(4), 5317-5337.

Moore, K., & McElroy, J. C. (2012). The influence of personality on Facebook usage, wall postings, and regret. *Computers in Human Behavior, 28*(1), 267-274.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computer & Security, 34*, 47-59.

Mylonas, A., Gritzalis, D., Tsoumas, B., & Apostolopoulos, T. (2013). *A qualitative metrics vector for the awareness of smartphone security users.* Heidelberg, Germany: Springer.

Nielsen. (2011). *State of the media Q3 2011: The mobile media report*. Nielsen.

Nielsen. (2012). *The mobile consumer: A global snapshot* [Report]. Neilson.

Nielsen. (2013). *Mobile majority: U.S. smartphone ownership tops 60%*. Retrieved March 15, 2015, from http://www.nielsen.com/us/en/newswire/2013/mobile-majority--u-s--smartphone-ownership-tops-60-.html

Nielsen. (2014). *An era of growth* [Report]. Nielson.

Nielsen. (2015a). *Smartphone owners are as diverse as their devices* [Report]: Nielsen.

Nielsen. (2015b). *So many apps, so much more time for entertainment [Report]*: Nielsen.

Oates, B. J. (2006). *Researching information systems and computing*. London, UK: SAGE Publications Ltd.

Ofcom. (2013). *Safer smartphones: A guide to keeping your device secure*. Retrieved from http://consumers.ofcom.org.uk/files/2013/10/mobile-guideV8.pdf

Özbek, V., Alnıaçık, Ü., Koc, F., Akkılıç, M. E., & Kas, E. (2014). The impact of personality on technology acceptance: A study on smart phone users. *Procedia - Social and Behavioral Sciences, 150*, 541-551.

Parker, F., Ophoff, J., Belle, J.-P. V., & Karia, R. (2015). *Security awareness and adoption of security controls by smartphone users.* Paper presented at the Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa.

Patrick, O., & Ngozi, B. N. (2014). Computer literacy among undergraduate students in Nigeria universities. *British Journal of Education, 2*(2), 1-8.

Pew Research Center. (2012). *Smartphone ownership update: September 2012 / Two-thirds of young adults and those with higher income are smartphone owners [Report]*. (2012). Pew Research Center.

Pew Research Center. (2013). *Smartphone ownership - 2013/ Update [Report]*. Pew Research Center.

Pew Research Center. (2015). U.S smartphone use in 2015 [Report].

Portio Research. (2013). Mobile applications futures 2013-2017 [Report]. Portio

Research.

Poushter, J. (2016). *Smartphone ownership and internet usage continues to climb in emerging economies [Report]*. Retrieved from http://www.pewglobal.org/files/2016/02/pew_research_center_global_technology_report_final_february_22__2016.pdf

Preedy, V., & Watson, R. (2010). Personality type. (In V. Preedy & R. Watson (Eds.), *Handbook of disease burdens and quality of life measures* (pp. 4285-4285). New York, NY: Springer.

Reinfelder, L., Benenson, Z., & Gassmann, F. (2014). Differences between Android and iPhone users in their security and privacy awareness. In C. Eckert, S. Katsikas & G. Pernul (Eds.), *Trust, privacy, and security in digital business* (Vol. 8647, pp. 156-167) New York, NY: Springer.

Richmond, H. (2011). The growth of mobile marketing and tagging. Retrieved May 18, 2015 from: http://tag.microsoft.com/community/blog/the_growth_of_mobile_marketing_and_tagging.aspx

Richter, F. (2016). *Twice the time: Same number of apps*. Retrieved June 7, 2016, from https://www.statista.com/chart/3570/app-usage-in-the-united-states/

Rodr´ıguez-Mota, A., Escamilla-Ambrosio, P. J., Aguirre-Anaya, E., Acosta-Bermejo, R., & Villa-Vargas, L. A. (2016). *Improving android mobile application development by dissecting malware analysis data.* Paper presented at the 4th International Conference in Software Engineering Research and Innovation, Puebla, Mexico.

Saadi, M. L. (2009). View from Bangladesh: The new literacy. *Ubiquity - The ACM IT Magazine and Forum*.

Sari, P. K., & Candiwan, S. R. (2014). Measuring information security awareness of Indonesian smartphone users. *Telkomnika, 12*(2), 493-500.

Sheldon, R., Steele, C., & Phifer, L. (2014). Creating a secure foundation for mobile applications. In E. Demaitre (Ed.), *Mobile application delivery: The next frontier* (pp. 1-13). Newton, MA: TechTarget.

Sophos. (2013). *Security threat report 2013: New platforms and changing threats* [Report]: Sophos.

Srivatanakul, T., & Wiwatwattana, N. (2014). Uses of online survey: A case study in Thailand. In K. Tuamsuk, A. Jatowt & E. Rasmussen (Eds.), *The emergence of digital libraries: Research and practices* (pp. 243-251): Springer International Publishing.

Statista. (2015). *Cumulative number of apps downloaded from the Apple app store from July 2008 to June 2015*. Retrieved June 7, 2016, from https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

Symantec. (2013). *Internet security threat report 2013* [Report] (Vol. 18): Symantec Corporation.

System, B. o. G. o. t. F. R. (2015). *Consumers and mobile financial services 2015* [Report]: Board of Governors of the Federal Reserve System.

Volkamer, M., Renaud, K., Kulyk, O., & Emeröz, S. (2015). A socio-technical investigation into smartphone security. In S. Foresti (Ed.), *Proceedings of security and trust management: 11th international workshop, Vienna, Austria Proceedings* (pp. 265-273). Cham, Vietnam: Springer.

Weiss, G. M., & Lockhart, J. W. (2012). *The impact of personalization on smartphone-based activity recognition*. Paper presented at the AAAI workshop: Technical report.

Wright, J. (2011). Using your smartphone securely. *OUCH!* Retrieved from http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201102_en.pdf

# APPENDICES

## Appendix A: Descriptive Statistics

**What is your gender?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Female. | 697 | 75.8 | 75.8 | 75.8 |
| | Male. | 222 | 24.2 | 24.2 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**What is your age group?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 16-24. | 325 | 35.4 | 35.4 | 35.4 |
| | 25-34. | 459 | 49.9 | 49.9 | 85.3 |
| | 35-44. | 92 | 10.0 | 10.0 | 95.3 |
| | 45-54. | 31 | 3.4 | 3.4 | 98.7 |
| | 55-64. | 12 | 1.3 | 1.3 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Please specify your cultural background (ethnicity):**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Asian. | 71 | 7.7 | 7.7 | 7.7 |
| | Black/African. | 14 | 1.5 | 1.5 | 9.2 |
| | Hispanic/Latino. | 3 | .3 | .3 | 9.6 |

| | | | | | |
|---|---|---|---|---|---|
| | Middle eastern/Arab. | 730 | 79.4 | 79.4 | 89.0 |
| | Other. | 19 | 2.1 | 2.1 | 91.1 |
| | Pacific Islander. | 2 | .2 | .2 | 91.3 |
| | White. | 80 | 8.7 | 8.7 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**What is the highest degree/level you have completed?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Bachelor's degree. | 421 | 45.8 | 45.8 | 45.8 |
| | Diploma. | 52 | 5.7 | 5.7 | 51.5 |
| | Doctorate degree. | 42 | 4.6 | 4.6 | 56.0 |
| | High School. | 222 | 24.2 | 24.2 | 80.2 |
| | Master's degree. | 175 | 19.0 | 19.0 | 99.2 |
| | Professional degree. | 7 | .8 | .8 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Which one is more suitable to describe you the most:**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Agreeable, friendly, kind and warm. | 171 | 18.6 | 18.6 | 18.6 |
| | Hard-working, motivated, goal-managed and have an organization behavior. | 249 | 27.1 | 27.1 | 45.7 |

| | | | | | |
|---|---|---|---|---|---|
| | Helpful, generous and ambitious. | 255 | 27.7 | 27.7 | 73.4 |
| | Instable emotionally, insecurity, sensitive, nervous and worried. | 79 | 8.6 | 8.6 | 82.0 |
| | Open to experience and flexible for new thoughts and ideas. | 165 | 18.0 | 18.0 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**IT background**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Basic. | 283 | 30.8 | 30.8 | 30.8 |
| | Intermediate. | 497 | 54.1 | 54.1 | 84.9 |
| | Proficient. | 139 | 15.1 | 15.1 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Are you using a smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | No. | 14 | 1.5 | 1.5 | 1.5 |
| | Yes. | 905 | 98.5 | 98.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**What is your smartphone operating system/platform?**

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Valid | Android (Samsung, Sony, Acer, Asus, htc, Huawei, LG, Motorola, ZTE, Kyocera). | 295 | 32.1 | 32.1 | 32.1 |
| | IOS (iPhone). | 607 | 66.1 | 66.1 | 98.2 |
| | Others. | 17 | 1.8 | 1.8 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**On average, how long do you spend on your smartphone per day?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1-3 hours. | 225 | 24.5 | 24.5 | 24.5 |
| | 4-6 hours. | 314 | 34.2 | 34.2 | 58.7 |
| | 7-9 hours. | 155 | 16.9 | 16.9 | 75.5 |
| | almost all the time. | 225 | 24.5 | 24.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Is your smartphone protected by password/passcode/pin key/fingerprint?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | I don't know how. | 8 | .9 | .9 | 2.4 |
| | No. | 93 | 10.1 | 10.1 | 12.5 |
| | Yes. | 804 | 87.5 | 87.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you share your pin key/password with others?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Always. | 64 | 7.0 | 7.0 | 8.5 |
| | Never. | 389 | 42.3 | 42.3 | 50.8 |
| | Sometimes. | 452 | 49.2 | 49.2 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you allow others to use your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Always. | 64 | 7.0 | 7.0 | 8.5 |
| | Never. | 115 | 12.5 | 12.5 | 21.0 |
| | Only when I am present. | 410 | 44.6 | 44.6 | 65.6 |
| | Sometimes. | 316 | 34.4 | 34.4 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you keep your smartphone connected to the Internet all the time?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No, only when I need to. | 140 | 15.2 | 15.2 | 16.8 |
| | Yes. | 765 | 83.2 | 83.2 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you connect to public networks?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No. | 136 | 14.8 | 14.8 | 16.3 |
| | Sometimes. | 382 | 41.6 | 41.6 | 57.9 |
| | Yes. | 387 | 42.1 | 42.1 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Have you ever lost your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Almost got lost, but I got it back. | 170 | 18.5 | 18.5 | 20.0 |
| | No. | 575 | 62.6 | 62.6 | 82.6 |
| | Yes. | 160 | 17.4 | 17.4 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you know how to configure the privacy and security setting on your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No, I don't care. | 31 | 3.4 | 3.4 | 4.9 |
| | No, I wish to know how. | 142 | 15.5 | 15.5 | 20.3 |
| | Yes, I know and I did. | 587 | 63.9 | 63.9 | 84.2 |
| | Yes, I know but I don't care. | 145 | 15.8 | 15.8 | 100.0 |

| | | | | |
|---|---|---|---|---|
| Total | 919 | 100.0 | 100.0 | |

**How often do you back-up your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | 2-3 times/month. | 110 | 12.0 | 12.0 | 13.5 |
| | Less often. | 385 | 41.9 | 41.9 | 55.4 |
| | Never. | 235 | 25.6 | 25.6 | 81.0 |
| | once/month. | 175 | 19.0 | 19.0 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you use an antivirus on your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | I don't know if my phone is applicable. | 155 | 16.9 | 16.9 | 18.4 |
| | No, I know there is but I don't use it. | 148 | 16.1 | 16.1 | 34.5 |
| | No, my smartphone platform does not need one. | 412 | 44.8 | 44.8 | 79.3 |
| | Yes. | 190 | 20.7 | 20.7 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Are you aware that your smart phone has security risk?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No. | 310 | 33.7 | 33.7 | 35.3 |
| | Yes. | 595 | 64.7 | 64.7 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**You think your smartphone security risk is:**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Average. | 331 | 36.0 | 36.0 | 37.5 |
| | High. | 159 | 17.3 | 17.3 | 54.8 |
| | I Do not know. | 199 | 21.7 | 21.7 | 76.5 |
| | Low. | 216 | 23.5 | 23.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**You usually download smartphone's apps (applications) from:**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Non-official stores (amazon appstore, Cydia, etc.). | 29 | 3.2 | 3.2 | 4.7 |
| | Official stores (app store, Samsung Apps Store, android market, etc.). | 876 | 95.3 | 95.3 | 100.0 |

| | | | | |
|---|---|---|---|---|
| Total | 919 | 100.0 | 100.0 | |

**Do you think the official app stores are used to do a security check/test on apps before release?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | I don't care. | 70 | 7.6 | 7.6 | 9.1 |
| | I don't know. | 222 | 24.2 | 24.2 | 33.3 |
| | No. | 72 | 7.8 | 7.8 | 41.1 |
| | Yes. | 541 | 58.9 | 58.9 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Are you used to downloading and installing pirated/illegal-copy/cracked apps?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | I don't know what is this. | 141 | 15.3 | 15.3 | 16.9 |
| | No. | 612 | 66.6 | 66.6 | 83.5 |
| | Yes. | 152 | 16.5 | 16.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you think your smartphone could be attacked/ hijacked (by malware, virus, Trojan, etc.)?**

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|
| Valid | 14 | 1.5 | 1.5 | 1.5 |

| | | | | | |
|---|---|---|---|---|---|
| | I don't know. | 273 | 29.7 | 29.7 | 31.2 |
| | No. | 273 | 29.7 | 29.7 | 60.9 |
| | Yes. | 359 | 39.1 | 39.1 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you save critical/private data on your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No. | 340 | 37.0 | 37.0 | 38.5 |
| | Yes. | 565 | 61.5 | 61.5 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Is your smartphone OS up-to-date (updated to the latest version)?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | I don't know. | 101 | 11.0 | 11.0 | 12.5 |
| | No. | 171 | 18.6 | 18.6 | 31.1 |
| | Yes. | 633 | 68.9 | 68.9 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you read the security/ privacy/ permission messages during downloading/installing apps?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | Always. | 132 | 14.4 | 14.4 | 15.9 |

| | | | | | |
|---|---|---|---|---|---|
| | Never. | 379 | 41.2 | 41.2 | 57.1 |
| | Sometimes. | 394 | 42.9 | 42.9 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you read the license/user agreement messages during installing apps?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | It depends on the type of the app. | 251 | 27.3 | 27.3 | 28.8 |
| | No, I click agree right away. | 557 | 60.6 | 60.6 | 89.4 |
| | Yes, I read it carefully before I agree. | 97 | 10.6 | 10.6 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Do you use all the apps downloaded on your smartphone?**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | | 14 | 1.5 | 1.5 | 1.5 |
| | No. | 572 | 62.2 | 62.2 | 63.8 |
| | Yes. | 333 | 36.2 | 36.2 | 100.0 |
| | Total | 919 | 100.0 | 100.0 | |

**Please rate the reasons that you look for when you download apps: [Reviews]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 327 | 35.6 | 42.4 | 42.4 |
| | 2.0 | 114 | 12.4 | 14.8 | 57.2 |
| | 3.0 | 93 | 10.1 | 12.1 | 69.3 |
| | 4.0 | 41 | 4.5 | 5.3 | 74.6 |
| | 5.0 | 69 | 7.5 | 8.9 | 83.5 |
| | 6.0 | 18 | 2.0 | 2.3 | 85.9 |
| | 7.0 | 23 | 2.5 | 3.0 | 88.8 |
| | 8.0 | 28 | 3.0 | 3.6 | 92.5 |
| | 9.0 | 19 | 2.1 | 2.5 | 94.9 |
| | 10.0 | 39 | 4.2 | 5.1 | 100.0 |
| | Total | 771 | 83.9 | 100.0 | |
| Missing | System | 148 | 16.1 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Word of mouth (some one suggestion)]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 235 | 25.6 | 30.5 | 30.5 |
| | 2.0 | 160 | 17.4 | 20.8 | 51.2 |
| | 3.0 | 124 | 13.5 | 16.1 | 67.3 |
| | 4.0 | 48 | 5.2 | 6.2 | 73.5 |
| | 5.0 | 64 | 7.0 | 8.3 | 81.8 |
| | 6.0 | 19 | 2.1 | 2.5 | 84.3 |
| | 7.0 | 28 | 3.0 | 3.6 | 87.9 |
| | 8.0 | 25 | 2.7 | 3.2 | 91.2 |
| | 9.0 | 23 | 2.5 | 3.0 | 94.2 |

| | | | | | |
|---|---|---|---|---|---|
| | 10.0 | 45 | 4.9 | 5.8 | 100.0 |
| | Total | 771 | 83.9 | 100.0 | |
| Missing | System | 148 | 16.1 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Cost/free]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 436 | 47.4 | 54.4 | 54.4 |
| | 2.0 | 120 | 13.1 | 15.0 | 69.4 |
| | 3.0 | 66 | 7.2 | 8.2 | 77.7 |
| | 4.0 | 37 | 4.0 | 4.6 | 82.3 |
| | 5.0 | 30 | 3.3 | 3.7 | 86.0 |
| | 6.0 | 13 | 1.4 | 1.6 | 87.6 |
| | 7.0 | 11 | 1.2 | 1.4 | 89.0 |
| | 8.0 | 14 | 1.5 | 1.7 | 90.8 |
| | 9.0 | 14 | 1.5 | 1.7 | 92.5 |
| | 10.0 | 60 | 6.5 | 7.5 | 100.0 |
| | Total | 801 | 87.2 | 100.0 | |
| Missing | System | 118 | 12.8 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Developer/company/brand]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 173 | 18.8 | 22.9 | 22.9 |
| | 2.0 | 143 | 15.6 | 19.0 | 41.9 |

| | | | | | |
|---|---|---|---|---|---|
| | 3.0 | 118 | 12.8 | 15.6 | 57.6 |
| | 4.0 | 55 | 6.0 | 7.3 | 64.9 |
| | 5.0 | 70 | 7.6 | 9.3 | 74.1 |
| | 6.0 | 23 | 2.5 | 3.1 | 77.2 |
| | 7.0 | 34 | 3.7 | 4.5 | 81.7 |
| | 8.0 | 32 | 3.5 | 4.2 | 85.9 |
| | 9.0 | 23 | 2.5 | 3.1 | 89.0 |
| | 10.0 | 83 | 9.0 | 11.0 | 100.0 |
| | Total | 754 | 82.0 | 100.0 | |
| Missing | System | 165 | 18.0 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [From official stores]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 415 | 45.2 | 53.8 | 53.8 |
| | 2.0 | 101 | 11.0 | 13.1 | 66.9 |
| | 3.0 | 76 | 8.3 | 9.9 | 76.8 |
| | 4.0 | 31 | 3.4 | 4.0 | 80.8 |
| | 5.0 | 40 | 4.4 | 5.2 | 86.0 |
| | 6.0 | 8 | .9 | 1.0 | 87.0 |
| | 7.0 | 12 | 1.3 | 1.6 | 88.6 |
| | 8.0 | 17 | 1.8 | 2.2 | 90.8 |
| | 9.0 | 18 | 2.0 | 2.3 | 93.1 |
| | 10.0 | 53 | 5.8 | 6.9 | 100.0 |
| | Total | 771 | 83.9 | 100.0 | |
| Missing | System | 148 | 16.1 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Popularity]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 280 | 30.5 | 36.0 | 36.0 |
| | 2.0 | 124 | 13.5 | 15.9 | 51.9 |
| | 3.0 | 140 | 15.2 | 18.0 | 69.9 |
| | 4.0 | 54 | 5.9 | 6.9 | 76.9 |
| | 5.0 | 65 | 7.1 | 8.4 | 85.2 |
| | 6.0 | 18 | 2.0 | 2.3 | 87.5 |
| | 7.0 | 18 | 2.0 | 2.3 | 89.8 |
| | 8.0 | 23 | 2.5 | 3.0 | 92.8 |
| | 9.0 | 15 | 1.6 | 1.9 | 94.7 |
| | 10.0 | 41 | 4.5 | 5.3 | 100.0 |
| | Total | 778 | 84.7 | 100.0 | |
| Missing | System | 141 | 15.3 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Interesting]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 372 | 40.5 | 47.1 | 47.1 |
| | 2.0 | 146 | 15.9 | 18.5 | 65.7 |
| | 3.0 | 95 | 10.3 | 12.0 | 77.7 |
| | 4.0 | 40 | 4.4 | 5.1 | 82.8 |
| | 5.0 | 32 | 3.5 | 4.1 | 86.8 |

| | | | | | |
|---|---|---|---|---|---|
| | 6.0 | 14 | 1.5 | 1.8 | 88.6 |
| | 7.0 | 11 | 1.2 | 1.4 | 90.0 |
| | 8.0 | 25 | 2.7 | 3.2 | 93.2 |
| | 9.0 | 20 | 2.2 | 2.5 | 95.7 |
| | 10.0 | 34 | 3.7 | 4.3 | 100.0 |
| | Total | 789 | 85.9 | 100.0 | |
| Missing | System | 130 | 14.1 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Usefulness ]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 355 | 38.6 | 46.1 | 46.1 |
| | 2.0 | 115 | 12.5 | 14.9 | 61.0 |
| | 3.0 | 84 | 9.1 | 10.9 | 71.9 |
| | 4.0 | 41 | 4.5 | 5.3 | 77.3 |
| | 5.0 | 55 | 6.0 | 7.1 | 84.4 |
| | 6.0 | 17 | 1.8 | 2.2 | 86.6 |
| | 7.0 | 13 | 1.4 | 1.7 | 88.3 |
| | 8.0 | 18 | 2.0 | 2.3 | 90.6 |
| | 9.0 | 23 | 2.5 | 3.0 | 93.6 |
| | 10.0 | 49 | 5.3 | 6.4 | 100.0 |
| | Total | 770 | 83.8 | 100.0 | |
| Missing | System | 149 | 16.2 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [Special offer]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 196 | 21.3 | 25.9 | 25.9 |
| | 2.0 | 139 | 15.1 | 18.4 | 44.3 |
| | 3.0 | 122 | 13.3 | 16.1 | 60.4 |
| | 4.0 | 54 | 5.9 | 7.1 | 67.6 |
| | 5.0 | 79 | 8.6 | 10.4 | 78.0 |
| | 6.0 | 26 | 2.8 | 3.4 | 81.5 |
| | 7.0 | 31 | 3.4 | 4.1 | 85.6 |
| | 8.0 | 28 | 3.0 | 3.7 | 89.3 |
| | 9.0 | 22 | 2.4 | 2.9 | 92.2 |
| | 10.0 | 59 | 6.4 | 7.8 | 100.0 |
| | Total | 756 | 82.3 | 100.0 | |
| Missing | System | 163 | 17.7 | | |
| Total | | 919 | 100.0 | | |

**Please rate the reasons that you look for when you download apps: [App category (game, travel, study, etc.)]**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 1.0 | 260 | 28.3 | 33.9 | 33.9 |
| | 2.0 | 146 | 15.9 | 19.1 | 53.0 |
| | 3.0 | 112 | 12.2 | 14.6 | 67.6 |
| | 4.0 | 50 | 5.4 | 6.5 | 74.2 |
| | 5.0 | 54 | 5.9 | 7.0 | 81.2 |
| | 6.0 | 20 | 2.2 | 2.6 | 83.8 |
| | 7.0 | 24 | 2.6 | 3.1 | 86.9 |
| | 8.0 | 24 | 2.6 | 3.1 | 90.1 |
| | 9.0 | 27 | 2.9 | 3.5 | 93.6 |

| | | | | | |
|---|---|---|---|---|---|
| | 10.0 | 49 | 5.3 | 6.4 | 100.0 |
| | Total | 766 | 83.4 | 100.0 | |
| Missing | System | 153 | 16.6 | | |
| Total | | 919 | 100.0 | | |

# Appendix B: T-Test

**Independent Samples Test**

| | | Levene's Test for Equality of Variances | | t-test for Equality of Means | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | 95% Confidence Interval of the Difference | |
| | | F | Sig. | t | df | Sig. (2-tailed) | Mean Difference | Std. Error Difference | Lower | Upper |
| Antivurus | Equal variances assumed | .081 | .776 | 1.033 | 903 | .302 | .0465 | .0451 | -.0419 | .1350 |
| | Equal variances not assumed | | | 1.045 | 369.684 | .297 | .0465 | .0445 | -.0410 | .1341 |
| BackUp | Equal variances assumed | 3.776 | .052 | -2.344 | 903 | .019 | -.1736 | .0740 | -.3189 | -.0283 |
| | Equal variances not assumed | | | -2.293 | 350.014 | .022 | -.1736 | .0757 | -.3225 | -.0247 |
| AwareSecRisk | Equal variances assumed | 24.164 | .000 | -2.191 | 903 | .029 | -.0808 | .0369 | -.1532 | -.0084 |
| | Equal variances not assumed | | | -2.266 | 383.532 | .024 | -.0808 | .0357 | -.1509 | -.0107 |
| ThinkSmartRisk | Equal variances assumed | 11.680 | .001 | -2.070 | 903 | .039 | -.1643 | .0793 | -.3200 | -.0086 |
| | Equal variances not assumed | | | -2.199 | 402.178 | .028 | -.1643 | .0747 | -.3111 | -.0174 |
| ReadSecMess | Equal variances assumed | 2.121 | .146 | .308 | 903 | .758 | .0168 | .0546 | -.0903 | .1239 |
| | Equal variances not assumed | | | .318 | 382.740 | .750 | .0168 | .0528 | -.0870 | .1207 |
| ReadLicMess | Equal variances assumed | 2.962 | .086 | 1.108 | 903 | .268 | .0588 | .0531 | -.0454 | .1630 |
| | Equal variances not assumed | | | 1.143 | 381.425 | .254 | .0588 | .0515 | -.0424 | .1600 |
| AttackMalware | Equal variances assumed | 9.143 | .003 | -3.144 | 903 | .002 | -.2023 | .0644 | -.3287 | -.0760 |
| | Equal variances not assumed | | | -3.067 | 348.629 | .002 | -.2023 | .0660 | -.3321 | -.0726 |

# Appendix C: SPSS Regression Output

**Model Summary**

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .260[a] | .068 | .060 | 3.06002 |

a. Predictors: (Constant), Personality, Gender, Ethnicity, Educ, IT, OS, Age

**ANOVA[a]**

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 604.178 | 7 | 86.311 | 9.218 | .000[b] |
| | Residual | 8324.357 | 889 | 9.364 | | |
| | Total | 8928.535 | 896 | | | |

a. Dependent Variable: VAR00001

b. Predictors: (Constant), Personality, Gender, Ethnicity, Educ, IT, OS, Age

**Coefficients[a]**

| Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | .921 | .621 | | 1.483 | .138 |
| | OS | .253 | .209 | .040 | 1.208 | .227 |
| | Age | -.038 | .139 | -.010 | -.272 | .785 |
| | Gender | .438 | .241 | .059 | 1.818 | .069 |
| | Educ | -.123 | .107 | -.041 | -1.148 | .251 |
| | IT | -1.113 | .158 | -.232 | -7.046 | .000 |
| | Ethnicity | -.357 | .261 | -.045 | -1.366 | .172 |
| | Personality | .016 | .066 | .008 | .238 | .812 |

a. Dependent Variable: VAR00001

# Appendix D: Security Questions Correlation Matrix (Negative Impact)

**Correlations**

| | | SharePass | OthersUse | ConnectIntAll | ConnectPub | Lost | DownloadAppsFrom | CrackedApp | AttackMalware |
|---|---|---|---|---|---|---|---|---|---|
| SharePass | Pearson Correlation | 1 | .287** | .114** | .036 | .030 | .076* | .068* | -.009 |
| | Sig. (2-tailed) | | .000 | .001 | .275 | .363 | .022 | .040 | .787 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| OthersUse | Pearson Correlation | .287** | 1 | .047 | -.006 | .007 | -.043 | -.004 | .028 |
| | Sig. (2-tailed) | .000 | | .155 | .868 | .832 | .192 | .914 | .403 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| ConnectIntAll | Pearson Correlation | .114** | .047 | 1 | .000 | .106** | -.078* | .015 | -.025 |
| | Sig. (2-tailed) | .001 | .155 | | .992 | .001 | .018 | .645 | .459 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| ConnectPub | Pearson Correlation | .036 | -.006 | .000 | 1 | .054 | -.011 | .109** | -.030 |
| | Sig. (2-tailed) | .275 | .868 | .992 | | .102 | .735 | .001 | .366 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| Lost | Pearson Correlation | .030 | .007 | .106** | .054 | 1 | -.014 | .099** | .038 |
| | Sig. (2-tailed) | .363 | .832 | .001 | .102 | | .679 | .003 | .247 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| DownloadAppsFrom | Pearson Correlation | .076* | -.043 | -.078* | -.011 | -.014 | 1 | .129** | -.028 |
| | Sig. (2-tailed) | .022 | .192 | .018 | .735 | .679 | | .000 | .394 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| CrackedApp | Pearson Correlation | .068* | -.004 | .015 | .109** | .099** | .129** | 1 | .116** |
| | Sig. (2-tailed) | .040 | .914 | .645 | .001 | .003 | .000 | | .000 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |
| AttackMalware | Pearson Correlation | -.009 | .028 | -.025 | -.030 | .038 | -.028 | .116** | 1 |
| | Sig. (2-tailed) | .787 | .403 | .459 | .366 | .247 | .394 | .000 | |
| | N | 905 | 905 | 905 | 905 | 905 | 905 | 905 | 905 |

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

# Appendix E: Security Questions Correlation Matrix (Positive Impact)

**Correlations**

| | | ConfigPriv | BackUp | Antivurus | Updated | ReadSecMess | ReadLicMess |
|---|---|---|---|---|---|---|---|
| ConfigPriv | Pearson Correlation | 1 | .213** | -.068* | .097** | .187** | .092** |
| | Sig. (2-tailed) | | .000 | .042 | .004 | .000 | .006 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |
| BackUp | Pearson Correlation | .213** | 1 | -.041 | .128** | .168** | .103** |
| | Sig. (2-tailed) | .000 | | .223 | .000 | .000 | .002 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |
| Antivurus | Pearson Correlation | -.068* | -.041 | 1 | -.028 | -.107** | -.113** |
| | Sig. (2-tailed) | .042 | .223 | | .402 | .001 | .001 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |
| Updated | Pearson Correlation | .097** | .128** | -.028 | 1 | -.002 | -.019 |
| | Sig. (2-tailed) | .004 | .000 | .402 | | .957 | .573 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |
| ReadSecMess | Pearson Correlation | .187** | .168** | -.107** | -.002 | 1 | .471** |
| | Sig. (2-tailed) | .000 | .000 | .001 | .957 | | .000 |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |
| ReadLicMess | Pearson Correlation | .092** | .103** | -.113** | -.019 | .471** | 1 |
| | Sig. (2-tailed) | .006 | .002 | .001 | .573 | .000 | |
| | N | 905 | 905 | 905 | 905 | 905 | 905 |

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

*. Correlation is significant at the 0.05 level (2-tailed).

## Appendix F: Survey of Impacts of Technological and Personal Factors on the Security Awareness of Smartphone Users

---

**Thank you for taking the time to complete the survey.**
**This survey is conducted as part of Masters research Project to assess the Impacts of Technological and Personal Factors on the Security Awareness of Smartphone Users.**

**All data and measurements obtained from this research study will be stored confidentially.**

**This survey is conducted by:**
**Mrs. Rawan Jaber (mrs.rawan.jaber@gmail.com )**
**and Associated Professor Ruili Wang (R.Wang@massey.ac.nz)**
**Massey University / New Zealand**

**If you have any question or suggestion, please contact us.**

---

❖ **General Information:**

- What is your gender?
  - Male.
  - Female.

- What is your age group?
  - 16-24.
  - 25-34.
  - 35-44.
  - 45-54.
  - 55-64.

- Please specify your cultural background (ethnicity):
    - White.
    - Black/African.
    - Hispanic/Latino.
    - Asian.
    - Pacific islander.
    - Middle eastern/Arab.
    - Other.

- What is the highest degree/level you have completed?
    - High school.
    - Diploma.
    - Bachelor's degree.
    - Master's degree.
    - Professional degree.
    - Doctorate degree.

- Which one is more suitable to describe you the most:
    - Conscientiousness: Hard working, motivated, goal-managed and has an organization behavior.
    - Extroversion: Helpful, generous and ambitious.
    - Neuroticism: Instable emotionally, insecurity, sensitive, nervous and worried.
    - Openness: Open to experience and flexible for new thoughts and ideas.
    - Agreeableness: Agreeable, friendly, kind and warm.

❖ **<u>Technological Information:</u>**

- At which level do you consider your knowledge in Information Technology?
    - Basic.
    - Intermediate.
    - Proficient.

- Are you using a smartphone?
    - Yes.
    - No.

- What is your smart phone operating system/platform?
    - IOS (iPhone).
    - Android (Samsung, Sony, Acer, Asus, htc, Huawei, LG, Motorola, ZTE, Kyocera).
    - Others.

- On average, how long do you spend on your smartphone per day?
    - 1-3 hours
    - 4-6 hours.
    - 7-9 hours.
    - Almost all the time.

- By using your smartphone, you often do: [you can select more than one]
    - Basics functions (calling, texting).
    - Surfing the Internet & emails.
    - Social networking (Facebook, twitter, Instagram, WeChat, Snap Chat, etc.).
    - Playing games.
    - Listening to audios/music.
    - Watching videos/media.
    - Online banking (shopping, money transferring, electronic payment, etc.).
    - Photographing.
    - Health/activities tracking.
    - Learning.

❖ **Security awareness:**

- Is your smartphone protected by password/passcode/pin key/fingerprint?
    - Yes.

- No.
- I don't know how.

- Do you share your pin key with others?
  - Always.
  - Sometimes.
  - Never.

- Do you allow others to use your smartphone?
  - Always.
  - Only when I am present.
  - Sometimes.
  - Never.

- Do you keep your smartphone connected to the Internet all the time?
  - Yes.
  - No, only when I need to.

- Do you connect to public networks?
  - Yes.
  - No.
  - Sometimes.

- Have you ever lost your smartphone?
  - Yes.
  - No.
  - Almost got lost, but I got it back.

- Do you know how to configure the privacy and security setting on your smartphone?
  - Yes, I know and I did.
  - Yes, I know but I don't care.

- No, I wish to know how.
- No, I don't care.

- How often do you back-up your smartphone?
  - Never.
  - 2-3 times/month.
  - Once/month.
  - Less often.

- Do you use an antivirus on your smartphone?
  - Yes.
  - No, my smartphone platform does not need one.
  - No, I know there is but I don't use it.
  - I don't know if my phone is applicable.

- You think your smartphone security risk is:
  - High.
  - Average.
  - Low.
  - I Do not know

- Are you aware that your smart phone has security risk?
  - Yes.
  - No.

- You usually download smartphone's apps (applications) from:
  - Official stores (app store, Samsung Apps Store, android market, etc.).
  - Non-official stores (amazon appstore, Cydia).

- Do you think the official appstores are used to do a security check/test on apps before release?
  - Yes.
  - No.

- I don't care
- I don't know.

- Are you used to downloading and installing pirated/illegal-copy/cracked apps?
  - Yes.
  - No.
  - I don't know what is this.

- Do you think your smartphone could be attacked/ hijacked (by malware, virus, Trojan, etc.)?
  - Yes.
  - No.
  - I don't know.

- Do you save critical/private data on your smartphone?
  - Yes.
  - No.

- Is your smartphone operating system up-to-date (updated to the latest version)?
  - Yes.
  - No.
  - I don't know.

- Do you read the security/privacy/ permission messages during downloading/installing apps?
  - Always.
  - Sometimes.
  - Never.

- Do your read the license/user agreement message during installing apps?
  - Yes, I read it carefully before I agree.
  - No, I click agree right away.
  - It depends on the type of the app.

- Do you use all the apps downloaded on your smartphone?
    - Yes.
    - No.

- Please rate the reasons you look for when you download apps:

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Reviews | | | | | | | | | | |
| Word of mouth (some one suggestion) | | | | | | | | | | |
| Cost/free | | | | | | | | | | |
| Developer/company/brand | | | | | | | | | | |
| From official stores | | | | | | | | | | |
| Popularity | | | | | | | | | | |
| Interesting | | | | | | | | | | |
| Usefulness | | | | | | | | | | |
| Special offer | | | | | | | | | | |
| App category (game, travel, study, etc.) | | | | | | | | | | |

Finally,

Thank you.

If you have comments or suggestions, please write it down.

If you do not mind, please provide your e-mail for any further information.

## Appendix G: Codebook

**Codebook:**

**Gender:** Female=1, Male =0

**Age:** 16-24=1, 25-34=2, 35-44= 3, 45-54=4, 55-64=5

**Ethnicity:** ME/Arab=1, White=2, Asian=3, Black/African American=4, Other=5, Pacific Islander=6, Hispanic/Latino=7

**Education:** Diploma=1, HS=2, BA=3, MA=4, Prof=5, Doc=6

**Personality:** Helpful, generous, ambitious=1, agreeable, friendly, kind, and warm=2, open to experience and flexible for new thoughts and ideas=3, instable emotionally, insecurity, sensitive, nervous, and worried=4, hard-working, motivated, goal-managed, and have an organization behavior=5

**IT background:** Basic=1, Intermediate=2, Proficient=3

**Smartphone User:** Yes=1, No=0

**Operating System**: IOS(iPhone)=1, Android=2, Others=3

**Time Spent on Smartphone**: 1-3 hours=1, 4-6 hours=2, 7-9 hours=3, almost all the time=4

**Activity:** Basic functions=1,

**Password Protected:** Yes=1, No=0

**Share Password:** Never=0, Sometimes=1, Always=2

**Allow Others to Use:** Never=0, Sometimes=1, Only when I am present=2, Always=3

**Always Connected to Internet:** No, only when I need to=0, Yes=1

**Lost Smartphone:** No=0, Almost lost it, got it back=1, Yes=2

**Configure Privacy Settings:** No, I don't care=0, No, I wish to know how=1, Yes, I know but I don't care= 2, Yes, I know and I did=3

**Back-Up:** Never=0, Less often=1, Once a month=2, 2-3 times/month=3

**Antivirus**: No, I know there is but I don't use it=0, No, my smartphone platform does not need one=1, I don't know if my phone is capable=2, Yes=3

**Aware of Security**: No=1, Yes=1

**Perception of Smartphone Security Risks**: I don't know=0, Low=1, Average=2, High=3

**Download Apps From**: Official Stores=1, Non-official Stores=2

**Official App Store Security Test:** No=0, I don't care=1, I don't know=2, Yes=3

**Cracked App:** No=0, I don't know what this is=1, Yes=2

**Think Attacked by Malware**: No=0, I don't know=1, Yes=2

**Updated:** No=0, I don't know=1, Yes=2

**Read Security Privacy Messages:** Never=0, Sometimes=1, Always=2

**Read License Messages**: No, I click agree right away=0, It depends on the type of app=1, Yes, I read it carefully before I agree=2

**Use All Apps:** No=0, Yes=1