Smartphone Security Risks: The Extent of User Security Awareness

Conor Murray

A dissertation submitted to the University of Dublin in partial fulfilment of the requirements for the degree of MSc in Management of Information Systems

1st September 2014

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work, and has not been submitted as an exercise for a degree at this or any other university. I further declare that this research has been carried out in full compliance with the ethical research requirements of the School of Computer Science and Statistics.

Signed: ___________________

Conor Murray

1st September 2014

Permission to lend and/or copy

I agree that the School of Computer Science and Statistics, Trinity College may lend or copy this dissertation upon request.

Signed: ___________________

Conor Murray

1st September 2014

Acknowledgement

I would first like thank the staff and lecturers of Trinity College for their help and support over the last two years.

I would like to thank my classmates, some of whom were my team-mates throughout the two year term. There were some tough long nights but we got there in the end.

I would very much like to thank my parents for their continued support and advice throughout the two year period. It was tremendous.

To everyone who took the time to take part in the survey, your input was vital and much appreciated.

Finally I would like to reserve a special thanks to my supervisor Aideen Keaney who offered great advice and support to me throughout the dissertation.

What you get by achieving your goals is not as important as what you become by achieving your goals.

Abstract

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." (Weiser, 1991, p.94).

Mark Weiser envisioned an environment where computers and communication capabilities were seamlessly integrated with human users. Smartphones, with their mobility, connectivity capabilities and growing array of sensors providing improved context awareness of the surrounding environment, are increasingly fitting this description.

However, as smartphones collect, store and transmit copious amounts of personal data, users need to be aware of the security and privacy implications of utilising this technology.

The primary objective of this research is to explore the extent to which smartphone users are aware of the potential security risks when using their smartphone. This dissertation also seeks to determine whether smartphone users are actually concerned about the risks and if they are taking any steps to protect their personal data on their smartphone.

An online survey was chosen as the most suitable strategy for answering the research question. 143 individuals, predominantly from Ireland, responded.

The findings of the survey indicated that the majority of the respondents did, in fact, have a high degree of awareness regarding security risks to their smartphone devices. It was observed that respondents did not indicate a high level of concern with respect to the security risks presented to them. The findings also suggested that the majority of users were not concerned about the privacy and protection of their personal data, with some believing that they did not have anything worth taking. Smartphone users considered security software to be unnecessary, instead relying on rudimentary screenlock or password protection mechanisms to protect the data on their smartphone.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Context and Background

"Everyone is going to have a smartphone. The trend has been mobile was winning; it's now won."

Eric Schmidt, Google Executive Chairman (Bloomberg, 2013)

In 2013, worldwide mobile phone sales totalled 1.8 billion units with smartphone sales accounting for 53.5% (Van Der Meulen and Rivera, 2014), a rise of 14% from the 2012 figure. According to the latest Commission of Communications Regulations Quarterly Report, there are 4.6 million mobile devices in Ireland, of which 2.7 million are deemed to be active smartphones, representing 58.5% of all mobile devices (Commision for Communications Regulation, 2014). This was a 12.2% annual increase in the number of active smartphones in Ireland.

Smartphones offer more advanced capabilities than a contemporary mobile phone. They are essentially powerful handheld computers with their own operating systems. As well as the traditional requirements to provide voice, SMS, MMS and video calling, they are capable of delivering an array of information processing functionalities including, but not limited to, accessing internet sites, banking and making payments, document editing, email, games and utilising location based services. As the figures above indicate, smartphones are becoming ubiquitous. A key element in their proliferation is their mobility along with the capability to provide persistent connectivity for the user.

However just as smartphones become more pervasive and powerful, those same security risks that have affected traditional PCs and desktop computers will emerge on the mobile platform in order to try to take advantage of the smartphone user. Such risks can include, for example, data leakage as a result of unauthorised access, theft or loss and digital attacks from malicious applications (malware) that may try to spy on and steal the user's personal data.

Are smartphone users aware of these risks? Are smartphone users actually concerned about these risks?

Recent research literature (Ludwig et al., 2013 , Lever et al., 2013) suggests that the prevalence of mobile malware is over-hyped; with Ludwig et al. (2013), security researchers at Google, reporting that only 0.001% of all applications downloaded by users were able to breach the “multiple layers of defence” that the platform provides as a threat prevention mechanism. This research by Google is reinforced by a paper from Lever et al. (2013), researchers at the Georgia Institute of Technology, who found that only 0.0009% of devices on a cellular network contained malware. Such a low prevalence rate may lead to the perception that there is no need for a smartphone user to be concerned about security risks to their smartphone.

There are steps that a user can take to secure their smartphone and protect the privacy of the data on it from loss, accidental or otherwise. These can range from employing a simple screen lock password, which protects unauthorised users from accessing the device, to more sophisticated measures such as remote tracking and wiping of the smartphone. Both Android and Apple provide remote tracking and wipe capabilities through their Android Device Manager and Find my iPhone features (Apple, 2014a , Google, 2014a). Are smartphone users employing any of these steps to protect their privacy and security when using their device?

This dissertation investigates whether smartphone users are aware of the potential security risks when using their smartphone, whether they are actually concerned about these risks and if they are taking any steps to protect their personal data on their smartphone.

1.2 Research Question

The primary research question being asked in this dissertation is;

"To what extent are smartphone users aware of the potential security risks when using their smartphones?"

Sub-questions that arise from this are;

- Whether there is an awareness amongst smartphone users of malicious threats and risks to their smartphone devices.
- Whether there is any concern amongst smartphone users about these threats and risks.
- What steps, if any, are smartphone users taking to protect their privacy and security when using their smartphone?

1.3 Research Interest and Beneficiaries

The popularity of smartphones continues to increase. Smartphone sales first surpassed PC sales in 2010 (Weintraub, 2011) and this is a trend that will not be reversed. As indicated in the introduction, there have been conflicting reports about the prevalence of malicious threats on smartphones and the actual security risks associated with smartphone usage. Thus it is interesting to gain an insight into the security awareness of smartphone users. Are these users aware of the potential security risks? Are they actually concerned about their possible exposure to these risks?

This research investigates user security awareness of smartphone risks and this research will benefit other researchers who are interested in carrying out studies on users and their awareness levels of security risks on smartphones.

1.4 The Scope of the Study

The study is limited to 143 smartphone users who took part on an online survey on user security awareness of smartphone risks. The survey took place between 10th June and the 21st June 2014. Although the survey was available online and invites were sent to colleagues and friends located globally, the majority of respondents were located in Ireland. Survey users had to have a smartphone but were not limited or excluded based on the smartphone operating system they had.

1.5 Chapter Structure

This dissertation is structured as follows;

- Chapter 1 : Introduction
  The introduction chapter provides background information on the dissertation and provides context for the research. The primary research question is presented along with a number of subquestions arising from the primary research topic.
- Chapter 2 : Literature Review
  The literature review chapter examines the available literature relevant to the research. It explores topics such as the definition of a smartphone, the mobile threat landscape including smartphone security risks and mobile malware threat prevalence, current literature focussing on user security awareness on smartphones and the privacy paradox; where user intention conflicts with actual user behaviour.
- Chapter 3 : Methodology and Fieldwork
  This chapter provides a brief summary of the research philosophies, methodologies and strategies available to the researcher. It explains which philosophical approach has been taken and describes the research method used to answer the research question.
- Chapter 4 : Findings and Analysis
  This chapter focuses on analysis of the data that was collected during the research.
- Chapter 5 : Conclusions and Future Work
  This chapter concludes the dissertation by summarising the findings and determining whether the data collected has answered the research question. This chapter also contains observations, discusses limitations of the study and points out potential future research areas.

2 Literature Review

2.1 Introduction

This dissertation investigates the extent to which smartphone users are aware of the potential security risks when using their smartphones, whether they are actually concerned about these risks and if they are taking any steps to protect their personal data on their smartphone.

In order to frame the topic accordingly, this literature review examines the published research with respect to the following areas:

- What is a smartphone?
- Smartphone risk landscape
- Measuring user security awareness
- User security awareness on smartphones
- The privacy paradox

2.2 What is a Smartphone?

Mobile phones are increasingly being referred to as “smartphones”. Given the continued rapid adoption rate of smartphones (Van Der Meulen and Rivera, 2013b) it is inevitable that the traditional mobile phone will eventually be replaced entirely.

A key element in the proliferation of the smartphone is their mobility along with the capability to provide pervasive connectivity for the user. Mark Weiser’s seminal paper described his vision of ubiquitous computing (also known as pervasive computing);
‘’The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.’’ (Weiser, 1991, p.94).

The essence of Weiser’s vision was an environment where computers and communication capabilities were seamlessly integrated with human users. Smartphones, with their mobility, connectivity capabilities and growing array of sensors providing better context awareness of the surrounding environment, are increasingly fitting this description. However what defines a smartphone? What makes it different from a normal mobile phone?

According to Hamblen (2009), there is no common, industry wide standard definition for a smartphone. In general, smartphones are handheld communication devices that integrate the functionality of a normal mobile phone, PDA and other devices. The user no longer needs to carry a separate mobile phone, music player, camera etc. These functionalities have converged into a single device.

Gartner (2013b) defines a smartphone as *"a mobile communications device that uses an identifiable open OS (operating system)"* where *"an open OS is supported by third-party applications written by a notable developer community."*

IDC, a major market research firm specializing in IT and telecommunications, in their older press releases defined a smartphone as a converged mobile device that features a high-level operating system to enable the device to run third-party applications (Business Wire, 2009). This definition highlights the importance of a sophisticated operating system and the extendibility of the capabilities of the device by way of third-party software applications. (Hamblen, 2009)

The lack of a common definition for a smartphone is also evident within the academic research domain. Zheng and Ni (2006) propose that the smartphone is the next-generation, multifunctional cell phone providing voice and text-messaging while also facilitating data processing through enhanced wireless connectivity. They suggest that the smartphone is a union of a powerful cell phone and a wireless-enabled PDA.

Becher et al. (2011) define a smartphone as a device which *"contains an MNO (mobile network operator) smartcard with a connection to a mobile network. Moreover, it has an operating system that can be extended with third-party software".* A Mobile Network Operator smartcard (SIM card within GSM networks) is a smartcard inside the mobile device that is controlled by a mobile network operator.

Theoharidou et al. (2012) suggest that such a definition is too broad given that these properties are also valid for feature phones which they classify as being restrained by a small screen size, having limited processing and networking capabilities and generally utilise a properietary, inadequately documented operating system.

Mylonas et al. (2013a) suggest that *"smartphones are mobile devices that combine the functionalities of cell phones and portable computers".*

However Theoharidou et al. (2012) offer a more robust definition of a smartphone;

A "smartphone is a cell phone with advanced capabilities, which executes an indentifiable operating system allowing users to exend its funtionality with third party applications that are available from an application repository".

Theoharidou et al. (2012) further expand upon this by suggesting that smartphones must include sophisticated hardware with;

- Advanced processing capabilities,
- Multiple and fast network connectivity capabilities,
- A clearly identifiable operating system (Android, iOS, Blackberry),
- An ability to install third party applications from application repositories,
- An appropriately sized screen. ("appropriately" is never further defined)

A common theme emerging from the review of the industry and academic literature regarding the definition of a smartphone is the presence of a clearly identifiable, high level operating system and the capability of the device to install third party applications from a third party source or repository.

With respect to the smartphone operating system, two candidates have emerged as the prominent platforms in the marketplace; Google Android and Apple iOS. Other platforms such as Nokia's Symbian, Blackberry's RIM and Microsoft Windows Mobile do exist but their market share is not comparable to Android and Apple (Van Der Meulen and Rivera, 2013b). Thus a brief review of the current literature describing the Android and Apple platforms will be provided.

2.2.1 Android Platform

The Android platform was unveiled on the 5th November 2007 with the founding of the Open Handset Alliance, a broad alliance of leading technology and wireless companies including Google, T-Mobile, HTC and others (Open Handset Alliance, 2007a).

Android is built on the open source Linux operating system and is developed and maintained by Google. On 12th November 2007 the Open Handset Alliance released the first free and publicly available Software Development Kit (SDK) for Android consisting of tools, documentation and emulators necessary for the development of new applications (Open Handset Alliance, 2007b).

Google's official application repository is known as the Google Play Store (Google Play Store, 2014b). Previously known as the Android Market, it was launched on 22nd October 2008 (Chu, 2008) allowing users to download applications to their Android device. Song et al. (2013) suggest that the open nature of the Android development process has influenced the way Google manages its application store because mobile operators and developers are free to utilise any software development kit of their choosing while developing applications. The omission of any pre-screening and verification process implies that anyone is allowed to post any application on the Google Play Store without much restriction. Müller et al. (2011) propose that this absence of a testing and verification process is the main differentiator between Google Play Store and other smartphone markets, thus creating a free market philosophy where the market regulates itself. Google therefore adopts an open platform strategy.

Android applications can be downloaded from the Google Play Store or via various third party application marketplaces (AppBrain, Amazon Appstore and many others) (Barrera and Van Oorschot, 2011). Google charge a $25 registration fee in order for a developer to acquire a Google Play Developer Console account (Google Support, 2014). Each Android application must be digitally signed by its developer. However because there is no requirement for a developer's digital certificate to be signed by a trusted certificate authority, these applications are usually signed with self-signed digital certificates which leads to poor source origin and integrity protection (Mylonas et al., 2012).

According to Bordianu et al. (2013), submitting an application to Google Play takes much less time than the Apple App Store, primarily due to the lack of human involvement in the validation process.

As indicated in Figure 2.1, Barrera and Van Oorschot (2011) define three software installation models based on the level of control the operating system or hardware vendor has over the installation and management of the application;

- *User control model*,
- *Guardian*,
- *Walled-garden.*

The *user control model* is where a user is given full responsibility for all application installation and security decisions. Based on this definition, Android is classified as fitting into this particular model.

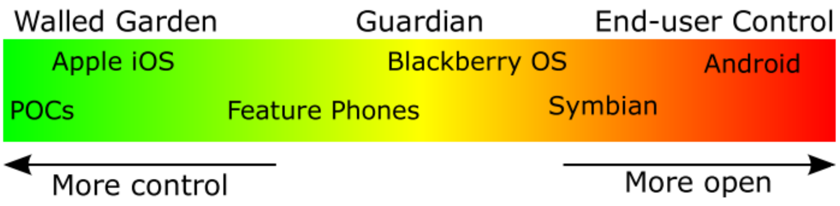


Figure 2.1 - Software Installation Models (Barrera and Van Oorschot, 2011)

While there are no officially released documented figures from Google regarding the growth, size and number of downloads from their Play Store, independent figures from Appbrain (AppBrain, 2014b) suggest there are 1,060,000 applications available on the Google Play Store, of which 81.57% are free and 18.43% are paid (AppBrain, 2014a). This is a credible figure given that Google's senior vice president, Sundar Pichai, announced in July 2013 that there were 1 million apps in the Google Play store (Warren, 2013).

According to Gartner, Android accounted for 78.4% of all smartphones sales in 2013, up from 66.4% in 2012 (Table 2.1) (Van Der Meulen and Rivera, 2014)

Table 2.1 - Worldwide Smartphone Sales to End Users by Operating System in 2013 (Thousands of Units)

Operating System	2013 Units	2013 Market Share (%)	2012 Units	2012 Market Share (%)
Android	758,720	78.4	451,621	66.4
iOS	150,786	15.6	130,133	19.1
Microsoft	30,843	3.2	16,941	2.5
BlackBerry	18,606	1.9	34,210	5
Other OS	8,821	0.9	47,203	6.9
Total	**967,776**	**100**	**680,108**	**100**

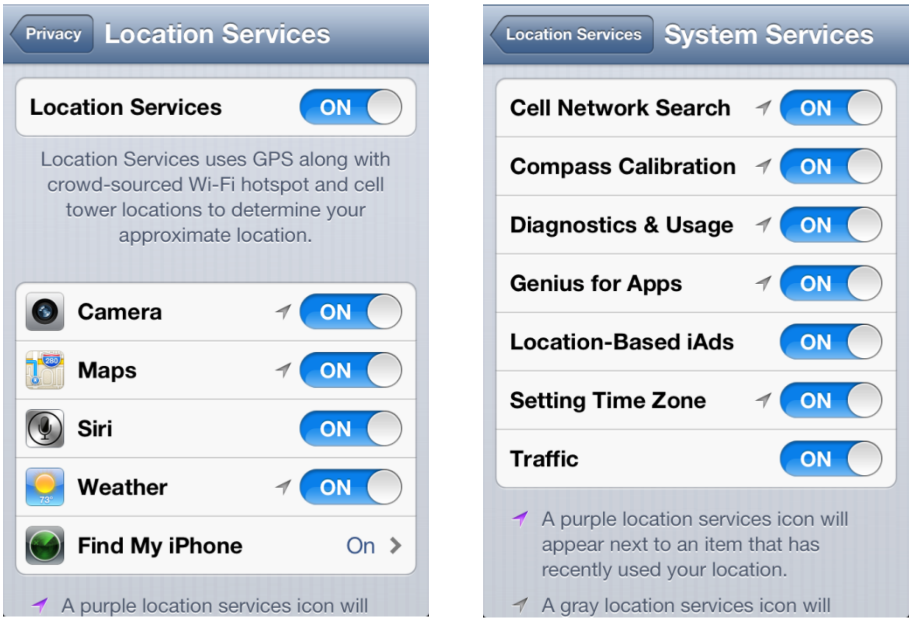
Given the growth of Android applications, as evident by the figures, this open platform/user control model appears to be a successful one. However, the open nature of the platform, coupled with its popularity and an inefficient validation process has resulted in it being a prime target for the majority of mobile malware (Trend Micro, 2013 , Symantec, 2013c , Uscilowski, 2013).

2.2.2 Apple iOS Platform

Contrary to Android, iOS is a proprietary operating system maintained by Apple. The operating system and original iPhone were released in June 2007 (Laugesen and Yuan, 2010 , West and Mace, 2010). On 10th July 2008 Apple launched the App Store allowing developers to offer or sell their applications for the iOS platform (Bordianu et al., 2013).

Song et al. (2013) state that Apple operate a closed market strategy, maintaining control of the development of the hardware, the operating system, selection of the applications, and the sale of those selected applications via its App Store distribution platform. In order to publish applications on the Apple App Store, a developer is required to have an Apple ID and become a member of the iOS Developer Program which incurs an annual fee of $99 (Apple, 2014c). Once a developer is registered, Apple provides documentation and the necessary toolset for developing iOS applications. Prior to an application being released on the App Store it must be submitted to Apple for approval. According to Barrera and Van Oorschot (2011) Apple have not released any detailed information regarding their vetting process. Bordianu et al. (2013) suggest that the process can take up to four days during which time the application is evaluated to ensure it adheres to the App Store review guidelines.

Barrera and Van Oorschot (2011) define the *walled-garden model* (Figure 2.1) as the smartphone vendor maintaining full control over third party software installation. Apple’s iOS would best fit in this particular model. However as Figure 2.2 highlights, users do still have to make some security decisions regarding whether access is permitted to location services (Apple, 2014b).



Privacy Location Services

Location Services ON

Location Services uses GPS along with crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location.

Camera ON
Maps ON
Siri ON
Weather ON
Find My iPhone On

A purple location services icon will

Location Services System Services

Cell Network Search ON
Compass Calibration ON
Diagnostics & Usage ON
Genius for Apps ON
Location-Based iAds ON
Setting Time Zone ON
Traffic ON

A purple location services icon will appear next to an item that has recently used your location.

A gray location services icon will

Figure 2.2 - Apple Location Services (Apple, 2014b)

Given the strict nature of Apple's application vetting process and their walled-garden approach regarding application distribution, the incidence of malware within the App Store is low. According to an F-Secure Report (2013), no instances of malware were reported on the iOS platform in 2013. Symantec (2013c), in their annual Internet Security Threat Report made an interesting observation; while there were more reported vulnerabilities (387) within the Apple iOS platform in 2012, there was only one malware threat created. This contrasted with Android which had only 13 vulnerabilities reported for the platform but led mobile operating systems in the amount of malware written for the platform.

While these figures seem to indicate that the Apple iOS is a safer platform for users, it is Android that is continuing to solidify its position as the number one mobile operating system for smartphones. Thus it is natural that malware writers will target the most popular platform in order to maximise their potential gain, be it financial or otherwise.

2.3 Smartphone Risk Landscape

2.3.1 What is Risk?

According to Hogben and Dekker (2010), within information security, risk is defined as the product of the likelihood and the impact of a threat against the information assets of an organization or an individual. Threats exploit one or more vulnerabilities. The likelihood of a threat is determined by the number of underlying vulnerabilities, the relative ease with which they can be exploited, and the attractiveness for an attacker to do so. The International Organization for Standardization (2008) define risk as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization or individual. Thus the measure of risk can be determined as a product of the threat, vulnerability, and the asset values (Vacca, 2012, p.386)(Figure 2.3):

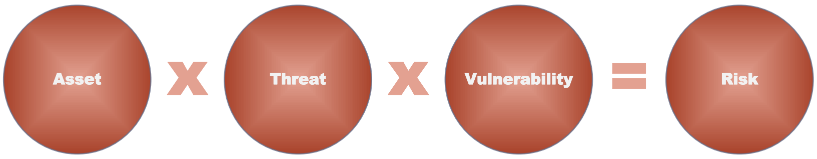


Figure 2.3 - Risk Formula

The smartphone itself would be considered an asset. The information stored on the device would also be considered an asset to the individual or organisation that owns it. Such informational assets on the smartphone may include:

- Personal data;
- Corporate intellectual property (if used for business purposes);
- Classified information;
- Financial assets such as online banking information;
- Personal and organisational reputation data.

According to the European Union Agency for Network and Information Security (2009) a threat is defined *“as any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service”.* They define a vulnerability as a weakness, design or implementation error that can exist which can lead to an unexpected and undesirable compromise of a computer system.

Mobile devices are at risk from a number of different threat vectors. Their portable nature means they are highly vulnerable to physical attacks such as unauthorised access or theft and loss, and like traditional desktop PCs they are also susceptible to digital attacks. The trend in the workplace towards BYOD (Bring Your Own Device) further increases the risk of exposure to corporate assets because such devices may not adhere to the corporate security policies that should be in place to protect such assets.

Table 2.2 summarises the top ten smartphone security risks and their associated risk rating as compiled by the European Union Agency for Network and Information Security (Enisa, 2010).

Table 2.2 - Top Ten Smartphone Security Risks

No.	Title	Risk	Description
1	Data leakage resulting from device loss or theft	High	Occurs when the smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.
2	Unintentional disclosure of data	High	Occurs when the smartphone user unintentionally discloses data on the smartphone.
3	Attacks on decommissioned smartphones	High	Occurs when the smartphone is decommissioned improperly allowing an attacker access to the data on the device.
4	Phishing attacks	Medium	Occurs when an attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.
5	Spyware attacks	Medium	Occurs when the smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.
6	Network Spoofing Attacks	Medium	Occurs when an attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.
7	Surveillance attacks	Medium	Occurs when an attacker keeps a specific user under surveillance through the target user's smartphone.
8	Diallerware attacks	Medium	Occurs when an attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.
9	Financial malware attacks	Medium	Occurs when the smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.
10	Network congestion	Low	Occurs when a network resource overload due to smartphone usage leading to network unavailability for the end-user.

As can be observed from the table, the likelihood of data leakage from theft or device loss is considered as the highest risk to the smartphone user. However the table includes a number of risks associated with threats of a digital nature. These include phishing attacks, spyware attacks, diallerware attacks and financial malware attacks.

2.3.2 The Growth of Mobile Digital Threats

The first malicious application developed for smartphones was released in June 2004. Known as Cabir, it was a proof of concept threat targeting the Symbian operating system, used by Nokia Series 60 smartphones (Symantec, 2004 , Hypponen, 2006 , Furnell, 2005a). Cabir spread via Bluetooth. Constant scanning by Cabir for Bluetooth-enabled devices resulted in it reducing the battery life of any infected smartphone (Ramu, 2012).

In 2004, Guo et al. (2004) discussed the potential damage a compromised smartphone could cause. This ranged from privacy violation, identity theft to a distributed denial of service attack on a telecoms infrastructure. As of the time of writing, there have been no reported instances of any distributed denial of service attack on a telecoms infrastructure. However as smartphones continue to become more pervasive and powerful, and malicious threats continue to evolve, the idea may not be so far-fetched. Indeed Traynor et al. (2009) were able to demonstrate that as few as 11,750 compromised mobile phones were capable of degrading the mobile service by 93% by continuously sending data messages to the cellular network servers.

As far back as 2005, Furnell (2005a) had surmised that the increasing incidence of malware on mobile devices was becoming a significant cause for concern. As the mobile threat landscape continues to evolve, various researchers have surveyed mobile malware and its transition from the Symbian platform to the Android platform (Shevchenko, 2005 , Schmidt et al., 2009 , Felt et al., 2011b). This transition is best described by Maslennikov (2013) stating that in late 2011, roughly 65% of mobile threats observed by Kaspersky targeted the Android platform. However by late 2012, that percentage had increased to 94% (Maslennikov, 2013) as highlighted in Figure 2.4. Kaspersky, like other antivirus software vendors, have various means of collecting and detecting malicious samples either via their own customers providing the malicious samples directly or through various collection entities such as honeypots and sharing samples between antivirus software vendors.

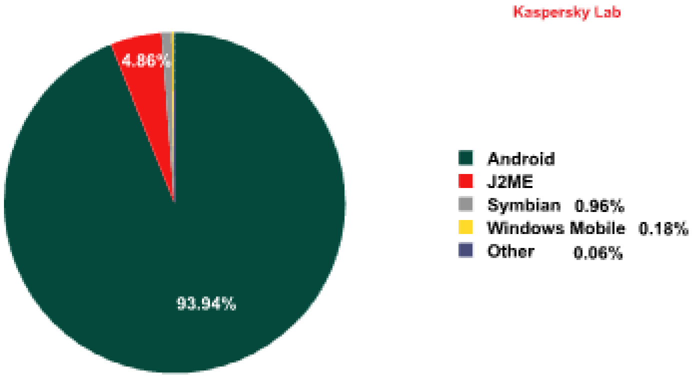


Figure 2.4 - Distribution of mobile threats by platform, 2004 – 2012 (Maslennikov, 2013)

According to a Symantec whitepaper by Uscilowski (2013) there is a *“massive growth in the volume of malware families”.* Trend Micro (2013) announced that the number of malicious and high-risk applications targeting the Android platform had surpassed the 1 million mark in September 2013.

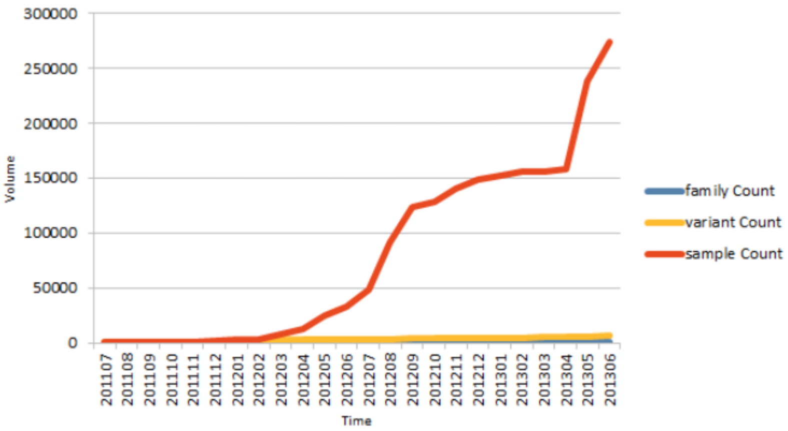


Figure 2.5 - Android Malware Growth (Uscilowski, 2013)

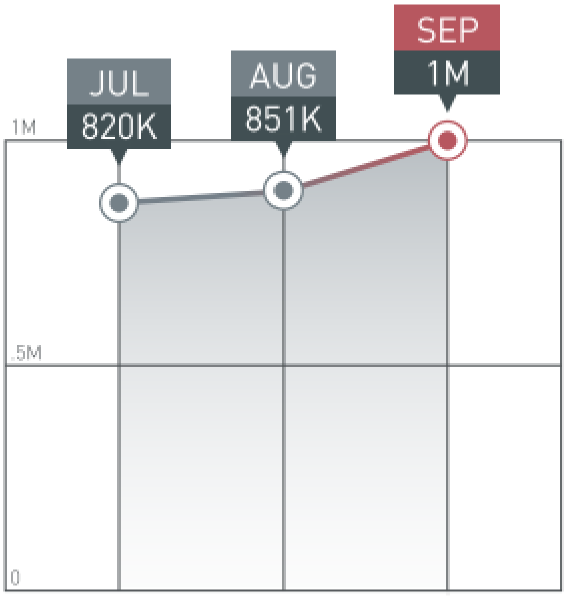


Figure 2.6 - Android Threat Volume Growth (Trend Micro, 2013)

There is a marked difference in the volume between the two graphs indicated. The graph in Figure 2.5 by Uscilowski (2013) includes a family count, a variant count and a sample count. Similar to the biological domain, computer malware can be grouped into families. For any malware family there exists a set of criteria that is found within all files in the family, such that all files in the family satisfy the set of criteria, and files that do not satisfy the set of criteria are not in the malware family (Gennari and French, 2011). A variant within a family is where a new member has new features that are not shared by every member of the family. Sample count is an indicator of the number of known malware files encountered or observed by Symantec during this time period. It can be observed in Figure 2.5 that although the family and variant count rose very slowly, the actual number of samples found increased significantly. This sample count of circa 273,000 differs greatly from the number presented in the Trend graph (Figure 2.6) which indicates Trend reached a volume of 1 million Android samples by September 2013. This is likely attributed to how each vendor defines and classifies malware (discussed in section 2.3.3) and what each vendor is including in their count. There can be disagreement as to which classification bracket certain malicious applications should be placed in. Some antivirus software companies will classify applications that contain invasive adware libraries as malware while others do not. Symantec classify these invasive adware libraries as mobile adware or “madware” (Uscilowski, 2013). Another source of disagreement is whether to consider “potentially unwanted programs” (PUPs) as malware or not. For example, an application used to “root” an Android phone would be considered suspect or unwanted were it to suddenly appear on the phone without the user’s explicit consent.

2.3.3 What is Malware?

Mell et al. (2005) define malware, also known as malicious code or malicious software, as a *“program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.”*

Symantec and Trend Micro, two antivirus (AV) software companies, classify malware rather simply as a category of malicious code that includes viruses, worms, and trojan horses (Symantec, 2014b , Trend Micro, 2014). Symantec expand somewhat on the definition suggesting malware looks to exploit existing vulnerabilities or weaknesses on systems in order to make their entry quiet and easy.

Aycock (2006), in his book, Computer Viruses and Malware, simply described malware as software whose intent or effect is malicious. For a book dedicated to malware, this seems like an over-simplistic definition. Aycock (2006) also suggests that the term malware covers a variety of threats including worms, trojan horses, virus and spyware.

Misra and Dubey (2013), in their recent book Android Security: Attacks and Defences, consider malware as software code designed to disrupt regular operations and collect sensitive and/or unauthorized information from a system/user. Malware can include viruses, worms, trojans, spyware, key loggers, adware, rootkits, and other malicious code.

Ramu (2012) proposes that malware is a malicious code that has the capability to do anything in any other program such as writing a message, stopping a running program, modifying a file etc. While this definition may not essentially be true; malicious code is not necessarily able to do anything in any other program, it does emphasise the concept that it can damage or harm other software or applications and possibly prevent them from running correctly or at all. Indeed certain malware, once it has found its way onto the host operating system, will seek out and cripple any antivirus products that do not yet detect it (Symantec, 1999 , Symantec, 2011). Ramu (2012) also suggests that malware is further classified as trojans, bots, virus, backdoor, worms, rootkits etc.

Felt et al. (2011b) present three separate types of threats posed by smartphone applications; malware, grayware and personal spyware. Their reasoning for distinguishing between the three types is based on the threat delivery method, with Felt et al. (2011b) suggesting that personal spyware and grayware have different motivations and use different attack vectors than malware. While they do not use the term malicious software, Felt et al. (2011b) do suggest that malware gains access to a device in order to steal data, damage the device, or simply to annoy the user. A user misleadingly installs the malicious application or the application exploits a weakness in order infiltrate the device. Like other researchers, they also classify malware as including trojans, worms, botnets and viruses.

It is evident from the literature that there is a consistent theme emerging regarding the definition of malware (or malicious code). It is software code that is malicious in nature. It tries to surreptitiously gain access to a device either via an exploit/vulnerability in the device or by misleading the user. It can, but not always, disrupt regular operations. Its purpose is more often than not to collect sensitive information or perform operations on the system without the user's explicit permission or consent.

2.3.4 Smartphone Malware Threat Prevalence

The word *prevalence* comes from the Latin *praevalere*, meaning *"condition of being widespread or general."* (Dictionary.com, 2014) The word is often used to describe a phenomenon that is rife in a particular community, like the prevalence of a virus or disease within a region. Thus the term has relevance and is used regularly within the broad computer security and antivirus industry when the pervasiveness of a threat or virus is being described.

Symantec apply a prevalence rating to each security threat they define. Their prevalence rating evaluates the extent to which a virus is already spreading among computer users. They base this rating upon the number of antivirus submissions they are receiving from their customer base (Symantec, 2014c).

The growth of mobile malware, specifically on the android platform, is well documented. Figures presented by Uscilowski (2013), Trend Micro (2013) and Juniper Networks (2014) would suggest that mobile malware is widespread. Juniper Networks (2014) reported that mobile malware threats grew at a rate of 614 percent between March 2012 and March 2013, demonstrating an exponentially higher cyber-criminal interest in exploiting mobile devices. Lookout (Linden, 2013) reported that the likelihood of one of their users encountering a mobile threat was 2.61%. This was a cumulative figure based on their prevalence figures for adware (1.6%) to spyware (0.1%).

However these claims have been disputed, with figures being presented by Google and in recent research literature (Ludwig et al., 2013 , Lever et al., 2013) that would suggest the prevalence of mobile malware is over-hyped. Ludwig et al. (2013), security researchers at Google, reported that only 0.001% of all applications downloaded by users were able to breach the “multiple layers of defence” that the platform provides as a threat prevention mechanism. (Figure 2.7 - Layers of Defence (Ludwig et al., 2013))

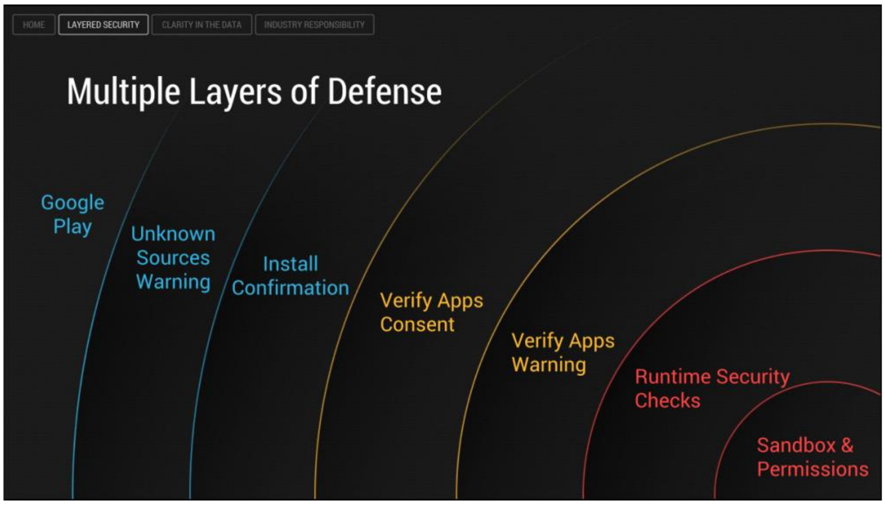


Figure 2.7 - Layers of Defence (Ludwig et al., 2013)

These “multiple layers of defence” consist of Google Play, Unknown Sources Warning, Install Confirmation, Verify Apps consent, Verify Apps warning, Runtime Security Checks and a permissions-based sandbox where the application itself runs. However a number of these layers (Unknown Source warning, Install Confirmation, Permissions) involve a confirmation dialogue box prompting the user for a decision. Research elsewhere has already shown that not only do application developers tend to request more permissions than necessary (Felt et al., 2011a), the end-user also demonstrated low attention and comprehension rates; they rarely read the questions they are being asked (Felt et al., 2012). Unfortunately once the permissions are applied, they cannot be revoked in a granular manner. This means a user must accept all the permissions that a particular application is requesting in order to use the application. Android does not allow a user to install an application but to then say "no" to that application’s permission request that it be able to read their address book, track their location, or retrieve other sensitive data about the user. Google released such a feature in Android 4.3. However this feature was later removed in Android 4.4.2 with Google stating it removed the feature because its experimental nature could break applications (Eckersley, 2013).

The results presented by Ludwig et al. (2013) indicate the low percentage (0.001%) of applications that breached their layered defence model. No figures regarding how many applications Google actually considered malicious were presented. Thus this gives no indication as to how prevalent Android malware actually is.

Google's research is reinforced by a paper from Lever et al. (2013), researchers at the Georgia Institute of Technology, who found that only 0.0009% of devices on a cellular network contained malware. Given this miniscule number, the researchers conclude that mobile application markets are providing adequate security for the majority of mobile devices. The researchers collected network traffic over the course of three months between April and June 2012 from a US network provider and identified those domain name lookup requests that were made by a mobile application. Using a set of malicious domain names sourced from various public and private datasets of known malware, they were able to cross reference the domain lookup requests made by the mobile application with this set. The subsequent figure (3,492 out of 380,537,128 devices or 0.0009%) indicated how many mobile applications were trying to make contact with known malicious domains or remote locations and thus how many devices appeared to be infected. While the methodology is sound, the monitoring of domain name lookups is somewhat limiting. If a malicious application does not make any domain name lookup requests then it will not be included or captured in the figures. A malicious application may have a hardcoded IP address and thus have no need to make a domain lookup request. Malware authors may use dynamically changing domain names and thus such domains would not be included in any known malicious domain name dataset.

According to Raiu and Emm (2013), the majority of mobile malware observed by Kaspersky in 2013 continued to be SMS trojans, whereby a malicious application surreptitiously sends SMS messages to a premium rate number thus generating revenue for the developer of the malicious application. SMS trojans tend not to have a requirement to make any domain name lookup requests and as such would not be captured in the figures.

There is little information from other independent sources regarding mobile malware infection rates. In contrast to the paper by Lever et al. (2013), an interesting paper by Truong et al. (2013) focused on data collected directly from the mobile devices themselves in order to calculate a mobile malware prevalence rate. Using two separate malware datasets they found the malware infection rates in Android to be on average 0.27% (set 1 had a rate of 0.26%, set 2 had a rate of 0.28%). While still small, this is significantly higher than the figures presented by both Google and Lever et al. (2013). Rather than detecting malware on the devices, Truong et al. (2013) used data collected from over 55,000 Android devices to enumerate the likelihood of infection for a given device. They used an application, known as Carat (Oliner et al., 2013), to intermittently collect data from a device including battery level and the names of the applications that are running on the device. They compared these running applications against lists of known malware from the Mobile Sandbox dataset and from the antivirus company McAfee to generate figures for each malware dataset (0.26% for Mobile Sandbox dataset and 0.28% for McAfee). Unfortunately their user base of 55,278 devices was rather small. It would be interesting to observe the figures were they to repeat this analysis with a larger Carat user base, something which they acknowledge themselves.

The literature reviewed thus far regarding mobile malware focuses predominantly on the Android platform and less so on the Apple platform. Given the strict nature of Apple's application vetting process and their walled-garden approach regarding application distribution, the incidence of malware within the Apple App Store is low, with Felt et al. (2011b) and Han et al. (2013), indicating there had been no known instances of any malware. Where grayware has managed to find its way onto the Apple App Store it quickly gets removed (Symantec, 2014a). In another instance, applications created by the developer *Storm8* were removed from the App Store once Apple realised they were discretely harvesting users' phone numbers and other personal information (Egele et al., 2011).

While malware does exist for the iOS platform it is not prevalent. Indeed, according to an F-Secure Report (2013), no instances of malware were reported on the iOS platform in 2013. Symantec (2013c), in their annual Internet Security Threat Report observed only one malware threat targeting the iOS platform. A key finding from Cisco's 2014 Annual Security Report indicated that 99% of all mobile malware in 2013 targeted Android devices (Cisco, 2014). These figures would suggest malware targeting iOS is not prevalent. However it does exist. Felt et al. (2011b), in their paper "*A survey of mobile malware in the wild"*, collected information about 46 pieces of malware in a period between January 2009 and June 2011, 4 for iOS, 24 for Symbian, and 18 for Android. The 4 pieces of malware they identified for iOS only spread through a specific vulnerability that was present in "rooted" or jailbroken iOS devices and none of these were listed in the App Store. A root exploit (also known as a "jailbreak") can be used by smartphone users who want to circumvent the default security mechanisms that exist on the smartphone. Apple consider such an action as an unauthorised modification of iOS and thus a violation of the iOS end-user software license agreement (Apple, 2013).

2.4 Measuring User Security Awareness

The Information Security Forum (2011) defines information security awareness as the extent to which staff understand the importance of information security, the level of information security required by the organisation and their individual security responsibilities and act accordingly. While this definition relates to staff and organisations, it can also be applied to general user security awareness with respect to smartphone usage.

Considering the measurement of user security awareness, researchers have focussed on trying to ascertain specifically what to measure. Kruger and Kearney (2006) presented a model to measure the information security awareness of an individual based on three dimensions, namely knowledge (what users know), attitude (what users think or feel) and behaviour (what users do). Like Kruger and Kearney (2006), Mathisen (2004) also focused on measuring change at the individual level, suggesting that raising the state of awareness leads to better behaviours and attitudes regarding information security. Mathisen (2004) presents a number of ways for measuring the level of security awareness including quarterly questionnaires to employees of an organisation, personal interviews with individuals and group discussions and workshops which could be used to measure awareness.

Unfortunately measuring awareness is not straightforward. When a user takes part in a security awareness program, the effectiveness of the program can be measured by determining the individuals' knowledge before and after the program. However such user knowledge does not signify that they will put it into practice. Rasmussen (1997) noted that improved awareness levels only provided temporary relief from risk because over time users found themselves returning to previous levels of awareness due to pressures of workload or productivity. Okenyi and Owens (2007) also argued that measuring user security awareness is not easy. They suggested that effective security awareness is a factor of the shared attitudes, behaviours, and practices that characterise a group or organisation.

2.5 User Security Awareness on Smartphones

"Security is a chain; it's only as secure as the weakest link."

Bruce Schneier, author and Security technologist (Schneier, 2000)

The term ‘smartphone’ could be considered somewhat disingenuous. These devices have the capacity to be much more than just a phone. The current generation of smartphones are far more powerful than the desktop computers of yesteryear. Besides being powerful, they have also become ubiquitous. Email, web browsing, games, document editing, GPS functionality and location based services are now standard fare. Online banking and making payments in shops through the use of Near Field Communications (NFC) technology is also possible (Alliance, 2011 , Rinne, 2013). The element of personalisation and intimacy takes the smartphone beyond a simple repository of phone contacts, photos and texts. It also contains emails (possibly business related), Twitter and Facebook account details; usernames and passwords for various services that the owner may use. Users may have a lot to lose if their smartphone is compromised and their private data is stolen. With the number and sophistication of IT security threats increasing (Juniper Networks, 2014 , Cisco, 2014), the security awareness of the user is a pertinent factor in the protection of their mobile device. The design and ease of use of security features within and around the smartphone also has a role to play in protecting the end user from harm.

As far back as 1975, Saltzer and Schroeder (1975) had identified psychological acceptability as one of the eight key tenets for building secure systems, suggesting that the human interface needed to be designed for ease of use to ensure users were consistently and automatically applying the protection mechanisms correctly. Such a need for technology to be presented to users in a suitable manner resulted in the emergence, in the 1980s, of a new research field called Human Computer Interaction (HCI). Taking it a step further, HCI-SEC is now a commonly used term to describe the research field concerned with the alignment of usability and security. It is an abbreviation of the acronym HCI (Human Computer Interaction) with the abbreviation SEC (Security) (Garfinkel, 2005).

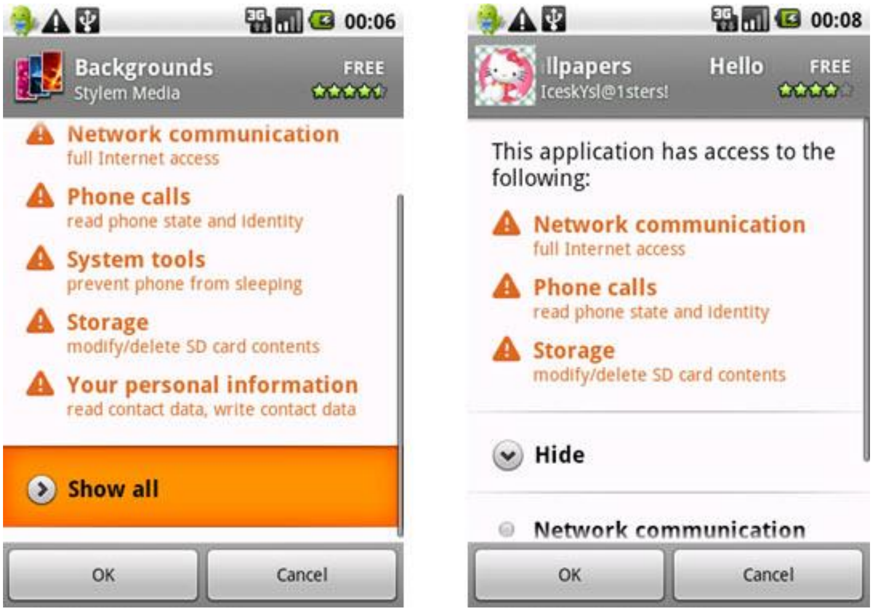
One of the most important principles to observe with respect to information security is the KISS principle (Keep It Simple Stupid). Security tends to restrict what people can do and makes systems more complex. In the seminal paper “*Why Johnny Can’t Encrypt*” by Whitten and Tygar (1999), the authors performed a case study of a security program that was considered to have a good user interface. Their purpose was to evaluate whether the software in question (Pretty Good Privacy 5.0) could be successfully used by a novice to encrypt their email. Of the 12 study participants, only 4 were successfully able to sign and encrypt an email message in the 90 minute timeframe they were allocated. 3 individuals accidentally sent the email in clear-text, thus exposing the secret they were supposed to protect. Whitten and Tygar (1999) concluded that designing usable security, that is also effective enough for those who do not understand it, requires more than just providing a simple point and click user interface. It is a specialised problem requiring specific user interface design evaluation methods tailored towards security.

Usability and security do not necessarily need to be conflicting goals when it comes to system design. Garfinkel (2005) argued that by redesigning systems with specific well-defined design patterns and revising the way functionality is implemented in today's operating systems and applications, greater alignment between usability and security could be achieved; "security and usability can be synergistically improved". Through conducting a number of studies (on remnant data of discarded hard drives) and surveys (on a set of Amazon merchants) Garfinkel (2005) was able to identify and present patterns that could be used to minimize security leaks and compromises.

Nonetheless, either system designers still appear to be making bad design decisions or normal users are not able to make adequate security decisions when presented with security controls. Steven Furnell carried out a number of studies on end-users and their ability to use and understand security on various desktop operating systems and applications. In Furnell (2005b), the security options within Microsoft Word were used to demonstrate examples of typical usability problems of such security features. Furnell et al. (2006) surveyed over 340 users in order to determine their understanding of the security features within Windows XP and three popular applications. It revealed that users faced difficulty when presented with these security features. In Furnell (2007), the author suggests that while security-related features had evolved within new releases of various desktop applications, new problems had been exposed that would still present usability problems for the end-users from a security perspective. This research suggests that end users are unable to make reasonable security decisions and utilise security controls effectively.

The academic literature focusing on the security awareness of smartphone users is somewhat limited and focuses predominantly on the Android platform. Given the nature of smartphones and how they are evolving ubiquitously, the role of the end user in protecting their smartphone from security risks and threats is important. Their own actions (inadvertently installing a malicious application, visiting a spurious website from their smartphone) can directly impact the security and privacy of their data. Thus their level of security awareness may become a potentially influencing factor in protecting themselves.

By design, Android applications do not have permission to perform any operation that would adversely impact other applications, the operating system, or the user. Thus for an application to have access to private contact data, another application's data, network access, or even writing its own data to the device storage, the application must declare that it will require the permissions to do so. When a user installs an application, they are presented with a list of permissions that application is declaring. The user must accept the permissions before the application can be installed. If the user chooses not to accept the permissions then the application will not be installed.



Network communication
full Internet access
Phone calls
read phone state and identity
System tools
prevent phone from sleeping
Storage
modify/delete SD card contents
Your personal information
read contact data, write contact data

This application has access to the following:
Network communication
full Internet access
Phone calls
read phone state and identity
Storage
modify/delete SD card contents
Network communication

Figure 2.8 - Comparison of Two Android Applications' Permissions

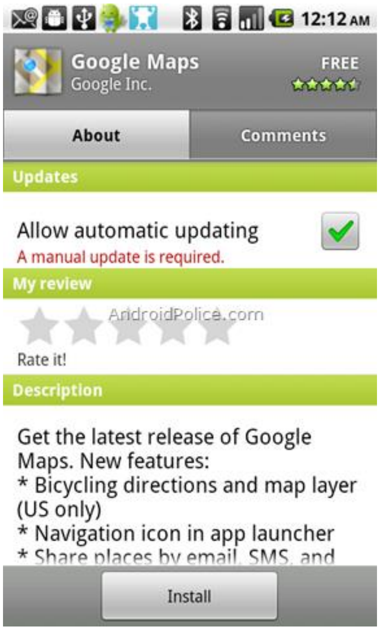
Unfortunately these permissions, and their associated risks, are not always readily understood by the end users or the developers themselves. Many users have become accustomed to accepting the terms of service and permissions that go along with the application in order to get it to install. The problem is that there may be potential security and privacy risks arising from this. When the developer fails to understand permissions correctly there is a risk that the applications they develop will simply request more permissions than strictly necessary for the application to perform its task fully. Figure 2.8 compares the permission declaration for two similar wallpaper style applications. It is evident that the application on the left is requesting more permissions than the application on the right. There may (or may not) be a legitimate reason for the application on the left to be requesting access to the user's personal data. Sometimes the application intends to send this information to a third party server or the developer inadvertently requested more permissions then the application actually needed.

This concept of over privilege was investigated by Felt et al. (2011a) in their paper "*Android Permissions Demystified*". The authors developed a tool to detect over privileges in a sample set of 940 Android applications. They observed that 341 of the 940 applications (~36%) tested had extra unnecessary permissions. However they concluded that this was attributed to developer confusion and that developers were attempting to obtain least privilege for their applications but fell short due to a general lack of developer understanding and poor API documentation.

This *Principle of Least Privilege* is a well-known principle that was described as a design concept by Saltzer and Schroeder (1975). They proposed that any program or user of a system should operate using the minimum set of privileges or requirements necessary to perform the task, thus limiting the damage that could result from any accident or error through unintentional, unwanted or improper use.

Vidas et al. (2011) also investigated this principle with respect to Android applications. Similar to Felt et al. (2011a), they developed a tool to aid a developer in specifying a minimum set of permissions required for a given application. Vidas et al. (2011) also found that some applications were requesting permissions that were not required for it to execute properly. Like Felt et al. (2011a), they concluded that existing developer APIs made it difficult for developers to determine the correct set of permissions required to adhere to the principle of least privilege.

Unfortunately the idea of permission creep or evolution of permissions is all too easy an event as applications update with new features thus seeking new permissions, application updating can be configured to occur automatically in the background and users ultimately stop paying attention altogether over time or may not even be aware of permission issues in the first place (Figure 2.9).



Google Maps
Google Inc.

Updates

Allow automatic updating ☑
A manual update is required.

My review

Rate it!

Description

Get the latest release of Google Maps. New features:
* Bicycling directions and map layer (US only)
* Navigation icon in app launcher
* Share places by email, SMS, and

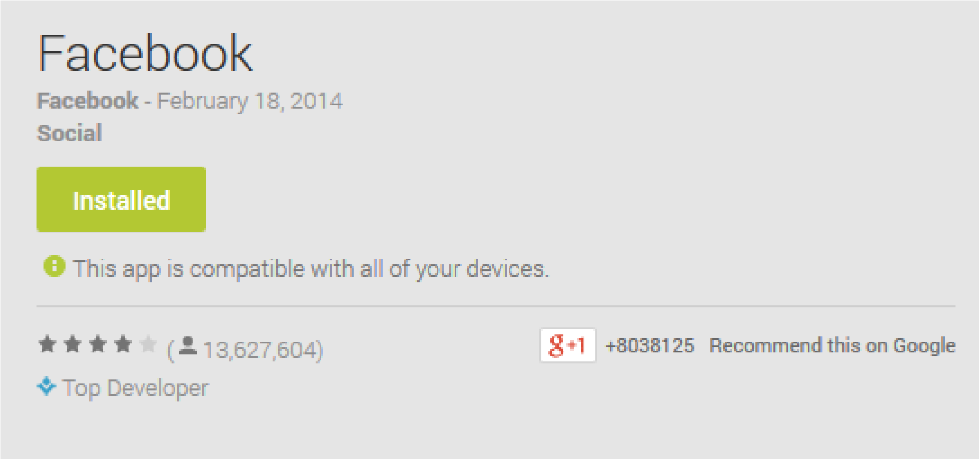
Figure 2.9 - Android Automatic Updating

When it comes to end users' comprehension and understanding of permissions, there appears to be a lack of understanding and awareness leading to a similar confusion that is faced by the developer. Felt et al. (2012), in their paper "*Android permissions: user attention, comprehension, and behavior*", examined whether the Android permissions system was an effective mechanism at warning users. The results of their studies indicated that the Android permissions system was ineffective at helping most users make a correct security decision during application installation. Indeed only 17% of the participants paid any attention to the permissions during installation. They identified a number of issues with the permissions system that impeded user awareness and comprehension including the actual permission category headings and relating the permission warnings to actual real risk.

Kelley et al. (2012) conducted a series of semi-structured interviews in order to determine end users' understanding of the permission screen presented when they install an application and whether they had an awareness of the perceived risks associated with making a decision to install the application based on those permissions. Their succinct conclusion was that "*Users do not understand Android permissions*". The permissions screen was confusing and misleading for developers and non-technical users alike. Kelley et al. (2012) suggested that permissions were generally ignored by the participants who instead relied on word of mouth, ratings and Android market reviews. Interestingly it appears that end users were generally uninformed about the existence of malware on the

Google Play market and actually believed that some form of developer and application pre-screening took place on the Google Play market. McDaniel and Enck (2010) suggest that there is a widely held expectation that security is the market’s responsibility, arguing that markets have not failed security, but instead, the failure is our expectation that these markets should do so. It must be noted that in February 2012 Google did take steps to improve security on their Play Store by introducing Bouncer. (Lockheimer, 2012). Bouncer is an automated tool that checks submitted applications for any suspicious activity. Unfortunately it has been proved relatively easy to circumvent with researchers quickly producing proof of concept evasion techniques (Oberheide and Miller, 2012 , Percoco and Schulte, 2012).

Chin et al. (2012) were interested in measuring user confidence in smartphone security and privacy. They conducted a user study on 60 participants. While they found that users were more apprehensive about using privacy and financially sensitive applications on their smartphones, however they still observed that users tended to install applications ignoring the privacy policies and EULAs. This indicated a general lack of consideration and awareness towards security and privacy issues during application installation thus increasing the risk of a malicious application being inadvertently installed on the smartphone. The authors believed that user mistrust in applications could be addressed by extending centralised markets such as Google Play with information about trusted brands. Google does have a “Top Developer” listing (Figure 2.10) described as “*Some of the best developers on Google Play, chosen by the Google Play team*” (Google Play Store, 2014a). It is noteworthy that the list is chosen by the Google Play team although the criteria for inclusion in the list are unknown. Such a listing could be considered a trusted brand and perhaps could be augmented or improved to include developers that would pass some extra validation criteria.



Facebook

Facebook - February 18, 2014

Social

Installed

This app is compatible with all of your devices.

★★★★☆ (13,627,604)

+1 +8038125 Recommend this on Google

Top Developer

Figure 2.10 - A Top Developer on Google Play

However given how simple it is to set up a website and act as a third-party application store, and with the lack of availability of Google Play Market in certain countries such as Russia and China, the idea of adding trust and recognition to Google's *user controlled model* seems like a difficult task.

In a recent paper by Mylonas et al. (2013b) entitled "*Delegate the smartphone user? Security awareness in smartphone platforms*", the authors examined the security awareness of smartphone users who installed applications from official application repositories/stores. They conducted a survey of 458 users in Greece between September and December 2011. The scope of the survey included Android, BlackBerry, Apple iOS, Symbian and Windows smartphone users. The results of their survey indicated that smartphone users believed that downloading applications from the application stores was risk-free. As with Kelley et al. (2012), the authors found that a common misconception existed amongst users about the apparent security controls in place on an official application store and thus the applications must be trustworthy; which unfortunately is not always the case. Interestingly they also noted that such users may be unable to realise that the device is much more than just a phone. As mentioned at the beginning of the section, smartphones have the capacity to be much more than just a phone. They are the amalgamation of a phone and a handheld computer and thus they are exposed to a greater set of threats than a simple phone. Mylonas et al. (2013b) also observed that users again ignored the security and permissions messages presented to them, thus violating the trust model of the smartphone security models. These models assume users will read and understand the messages presented to them in order to make an informed decision about their security and privacy. The authors suggested that users have become trained to click through disruptive messages when completing a task; an observation also noted by Motiee et al. (2010) in a study to determine whether Windows users followed the Principle of Least Privilege. Mylonas et al. (2013b) also found that users are increasingly using their smartphones for both business and personal purposes. This observation, coupled with the fact that many of the users did not consider it necessary to install any third party security software on their smartphones, increases the risk of unauthorised access to confidential data on the smartphone. This particular study took place on a sample set of participants from Greece.

2.6 The Privacy Paradox

Smartphones, with their mobility, connectivity capabilities and growing array of sensors providing better context awareness of the surrounding environment, are increasingly fitting Weiser's vision of ubiquitous computing. Weiser described such technologies as disappearing into the background while at the same time becoming intertwined with everyday life (Weiser, 1991).

The ability of the latest generation of smartphones to collect detailed information on users, coupled with the enhanced speeds at which this data can be stored and searched within large databases, creates the possibility for personal profiling and individually tailored services. Xu et al. (2011) suggested that much of the tracking and data collection is a result of businesses attempting to deliver personalised services and targeted advertising in a more effective manner. However such capabilities tend to raise concerns amongst users regarding the privacy of their information.

Westin (1967, p.7) defines privacy as *"the claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others."* Stone et al. (1983, p.460) expanded upon this, defining information privacy as *"the ability of the individual to control personally information about one's self"* while King (2013), in her paper on smartphones and privacy expectations, defines information privacy risk as *"access to one's personal information without express knowledge or consent".*

The perception of privacy and what an individual considers to be private is subjective, differing widely across populations and cultures. Research by Milberg et al. (2000) found that cultural values had a significant positive effect on information security concerns across countries. Hoofnagle et al. (2010) carried out a study to determine whether there were differing attitudes towards privacy between young adults and older adults within a group in the US. They concluded that young and old adults alike expressed similar attitudes towards privacy. However they also found that higher proportions of young adults incorrectly believed that the law protects their privacy online more than it actually does suggesting that this lack of knowledge, rather than a cavalier lack of concern regarding privacy, may be the reason they engage with the digital world in a seemingly unconcerned manner.

Public opinion surveys tend to indicate that users are concerned about the privacy of their information (Phelps et al., 2000) with a recent TRUSTe 2014 US Consumer Confidence Privacy Report TRUSTe (2014) finding that 92% of US internet users worried about their privacy online. Their major concerns were businesses sharing their personal information with other companies, and companies tracking their online behaviour to target them with advertisements and content. O' Brien and Torres (2012) investigated Facebook users' perceptions of online privacy, exploring their awareness of privacy issues and how their behaviour is influenced by this awareness. Their findings revealed that over half of Facebook users have a high level of privacy awareness. However privacy concerns were prevalent especially relating to third party access to Facebook users' information. A study by Mylonas et al. (2013b) found that 95.2% of smartphone users were concerned about their privacy. Similarly, Chin et al. (2012) found that smartphone users were apprehensive about running privacy related tasks on their phones.

However despite these high levels of privacy concerns, people continue to use these technologies that are implicated in personal data collection in a belief that perceived benefits outweigh the perceived privacy risks (Dinev and Hart, 2006). This behaviour is known as the ‘privacy paradox’ where intentions and behaviours around personal information disclosure often differ (Barnes, 2006 , Awad and Krishnan, 2006 , Spiekermann et al., 2001). Various studies have been carried out to investigate this phenomenon. Spiekermann et al. (2001) found that while most individuals stated privacy was important to them, study participants did not *“live up to their self-reported privacy preference.”* Norberg et al. (2007), in their paper *“The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors”*, found that the level of actual information disclosure exceeded the individuals’ intention to disclose. They suggested that *“behavioral intentions may not be an accurate predictor of actual behavior”.*

Not surprisingly, social networks have also been a source of research into privacy concerns and behaviours. A study by Acquisti and Gross (2006) revealed a high discrepancy between stated concerns and actual behaviour when sharing profile information on Facebook. A study carried out by Stutzman et al. (2013) involving 5076 Facebook users over a period of 2005 to 2011, indicated that the *"amount and scope of personal information that Facebook users revealed privately to other connected profiles actually increased over time -- and because of that, so did disclosures to "silent listeners" on the network: Facebook itself, third-party apps, and (indirectly) advertisers."*

This intention versus behaviour paradox also exists amongst smartphone users. In their paper, *"Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use",* Shklovski et al. (2014) revealed that while users expressed dismay when they were informed about the spurious information sharing practices of certain applications on their smartphone, they proceeded with *"business as usual when it came to using their smartphones".* Interestingly research by Keith et al. (2013) suggested that perceived privacy risk actually plays a larger role than perceived benefits in determining disclosure intentions of users. They found that only a weak, albeit significant, relationship exists between information disclosure intentions and actual disclosure. In addition, this relationship was heavily moderated by the consumer practice of disclosing false data. However it is more difficult for users to moderate what personal data the smartphone and applications are transmitting.

2.7 Summary

In summary, it can be observed that there are a number of smartphone security risks with the likelihood of data leakage from theft or device loss being the highest. However there are also a number of risks of a digital nature that could cause concern amongst smartphone users.

Android with its open platform/user control model, has emerged as the dominant mobile platform with Gartner reporting that it accounted for 78.4% of all smartphone sales in 2013 (Van Der Meulen and Rivera, 2014). The fact that it is the most common operating system for mobile devices and its open nature has also made it the prime target for the majority of mobile malware. The most prevalent operating system coupled with the ability to install software from any source results in the greatest number of threats. While malware does exist for the Apple iOS it does not do so in a widespread context (Cisco, 2014 , F-Secure Report, 2013 , Symantec, 2013c).

Focussing on measuring user security awareness, researchers have focussed on determining what exactly to measure. Kruger and Kearney (2006) identified the three dimensions of knowledge, attitude and behaviour as evaluation indicators of user security awareness while Mathisen (2004) suggested a number of methods to measure security awareness including quarterly questionnaires, personal interviews and group discussions and workshops. This would enable before and after metrics to be recorded.

The literature review surrounding user security awareness suggests a lack of security awareness amongst smartphone users. Chin et al. (2012) studied 60 participants and found that while users were more apprehensive about using privacy and financially sensitive applications on their smartphones, they still tended to ignore the privacy policies and EULAs when installing an application. A study of 458 users in Greece by Mylonas et al. (2013b) also revealed a lack of security awareness with users ignoring security messages and trusting applications from official application stores. It is evident from the research that while users express these concerns regarding the privacy of their information (Phelps et al., 2000 , TRUSTe, 2014), the reality is that their actual behaviours do not correlate with their perceived intentions. This behaviour, known as the ‘privacy paradox, has been found to be prevalent amongst users in various domains (Norberg et al., 2007 , Stutzman et al., 2013 , Shklovski et al., 2014).

3 Methodology and Fieldwork

3.1 Introduction

"All men by nature desire to know."
Aristotle, Greek philosopher

This chapter will provide a brief overview of the principal research philosophies, associated methodological approaches and strategies available in modern IS research. It will give the rationale for the methodology selected for this study and explain the philosophical basis behind this decision.

3.2 Research Philosophies and Approaches

Creswell (2012, p.3) defines research as the *"process of steps used to collect and analyse information to increase our understanding of a topic or issue".*

According to Saunders et al. (2012) there are three major ways of thinking about the research philosophy: axiology, ontology and epistemology.

Axiology refers to the study of the nature or character of values and their judgements. The role a researcher's own values play in the research process is of importance. While researchers try to be objective and balanced in their research, there is no such thing as totally impersonal objective research.

Ontology deals with the nature of social entities. It is the study of being, that is, the nature of existence, the *what is* (Crotty, 1998). Wand and Weber (1993, p.220) identify ontology as *"a branch of philosophy concerned with articulating the nature and structure of the world"*.

Objectivism is an ontological position which states that social entities (like an organisation or team) have an existence, which is independent from the people in them. It emphasises the structural aspects of management and assumes that management is similar in all organisations (Saunders et al., 2012, p.131).

Subjectivism, on the other hand, would assert that social entities or phenomena (like the organisation or team) have no independent reality but are instead created through the perceptions and actions of social actors (Saunders et al., 2012, p.132). Thus because these phenomena are constantly being generated in the minds of those who think about them, they are in a constant state of revision. Individuals place different interpretations on a situation and thus perceive things differently.

While ontology represents understanding *what is*, epistemology looks to understand *what it means to know*. Bryman and Bell (2011, p.15) propose that epistemology "*concerns the question of what is (or should be) regarded as acceptable knowledge"* in a particular discipline or field of study. With respect to this concept of what constitutes acceptable knowledge, Saunders et al. (2012) have proposed there are four philosophical positions a researcher may adopt: positivism, interpretivism, realism and pragmatism.

- Positivism
  Such a stance is usually associated with natural science research and involves empirical testing. According to Hirschheim et al. (1995, p.21) positivism claims that "all knowledge can be expressed in statements of laws and facts that are positively corroborated by measurement". Positivism assumes that the world is objective rather than subjective and that only observable phenomena will lead to the production of credible knowledge (Saunders et al., 2012, p.134). A positivist researcher tends to focus on quantitative methods used to test and verify hypotheses. Such an approach is considered to be deductive in nature, which begins by initially developing a theory and producing a hypothesis (or hypotheses) relating to the focus of the research.
- Interpretivism
  Interpretivism is concerned with seeking to understand a social actor's meaning of a situation. According to Schwandt (1994, p.118) an interpretivist believes that "*to understand this world of meaning one must interpret it".* An interpretivist tends to adopt qualitative methods when performing research. The researcher needs to make sense of the subjective meanings expressed about the phenomenon being studied (Saunders et al., 2012, p.163). Such a way of thinking is likely to be associated with an inductive approach. The inductive approach starts by looking at the focus of the research, with data being collected through investigation by various research methods and a theory is developed as a result of the subsequent data analysis.
- Realism
  Realism takes aspects from both positivist and interpretivist positions. It proposes that objects have an existence independent of human consciousness (Saunders et

al., 2012, p.136), yet also accepts that knowledge is socially created; what we regard as real is significant.

- Pragmatism

  The pragmatic approach involves using the methods which appear best suited to addressing the research problem. Pragmatic researchers therefore grant themselves the freedom to use any of the methods, techniques and procedures typically associated with quantitative or qualitative research. The mandate for a pragmatist is not to find truth or reality, the existence of which are constantly being disputed, but to simply facilitate human problem-solving (Powell, 2001, p.884). Pragmatism embraces the two extremes of positivism and interpretivism, with the former emphasising a quantitative, deductive approach and the latter a qualitative inductive approach.

In terms of the research approach, the research question is predominantly a quantitative one, thus meriting a deductive approach. However a number of the sub-questions have a qualitative aspect to them which require an inductive approach. A pragmatic researcher will use both objective and subjective reasoning when drawing conclusions and making inferences about the data collected. Such an approach will cater for the deductive and inductive aspects recognised above. Thus pragmatism has been chosen as the philosophical viewpoint for the research.

3.3 Research Methodological Choice

The next step is to determine a data collection technique. Figure 3.1 shows the basic choices between using single data collection techniques such as quantitative and qualitative research design which is known as a mono method versus using more than one data collection technique known as multiple methods.

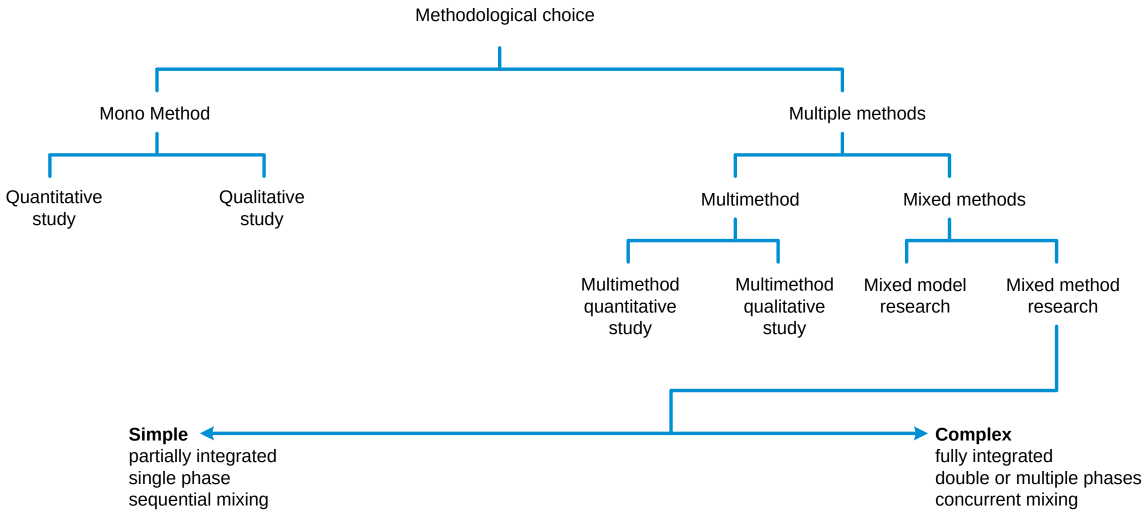


Figure 3.1 - Methodological choice (Saunders et al., 2012, p.165)

The primary objective of the research is to explore the extent to which smartphone users are aware of the potential security risks when using their smartphone. Thus the nature of the research is an exploratory study. A mono method research design is being taken with respect to the data collection and analysis.

3.4 Research Strategy

The research strategy is defined as a plan of action to achieve a goal (Saunders et al., 2012, p.173). While different research strategies tend to be principally linked with quantitative, qualitative or multiple method research designs, it should be recognised that a particular research strategy should not be seen as being superior or inferior to any other. Thus the choice of strategy is guided by the research question and objectives of the study. The following lists some of the more commonly used strategies:

- Experiment
- Survey
- Archival Research

- Case Study
- Ethnography
- Action research
- Grounded Theory

The survey, which is usually associated with deductive research (Saunders et al., 2012, p.176), was chosen as the most suitable strategy for answering the research question. Survey research involves the collection of information from a sample of individuals through their response to various questions. There are two types of survey questions typically used in survey research; closed-ended and open-ended questions. Closed-ended question formats provide respondents with a list of answer choices from which they must choose to answer the question, while open-ended questions allows respondents to freely answer the question as they want without limiting their response (Dillman et al., 2009). Open ended questions are commonly used in qualitative research; however they can also be used in quantitative research to allow the researcher gain more information and insight into an issue.

Evans and Mathur (2005) and Selm and Jankowski (2006) highlight a number of benefits of online surveys including:

- Global reach – opportunity for a large audience for the survey.
- Flexibility – in how the survey can be delivered to the respondent.
- Low administration cost.
- Convenience – respondents can answer the survey at a convenient time for themselves.
- Ease of data entry and analysis – as the survey is online it is relatively easy for the data to be recorded, tabulated and analysed using tools (for example SPSS).
- Anonymity for the respondent.
- Absence of interviewer bias.

3.5 Time Horizon

There are typically two time horizons to consider;

- A **Cross-sectional study** involves research being conducted over a short period of time and represents a snapshot of the particular phenomena being investigated. These studies often employ the survey strategy (Saunders et al., 2012, p.190).
- A **Longitudinal study** tends to observe a phenomenon over a longer period of time tracking the development or changes to it. It would be considered as adopting a diary perspective.

Based on the time constraints that apply in this research, a cross-sectional time horizon is being adopted.

3.6 Sample Population

The sample population being targeted were smartphone users. Being an online survey it was available for distribution to a wide audience of the researcher's friends, family and colleagues, many of whom are located in various countries around the world. It was hoped that this may provide extra insight into the potential differences between various demographical regions and their awareness and concerns about smartphone security.

3.7 Sampling

As it is impractical to collect data on the entire population of smartphone users, a sample needs to be selected. There are two type of sampling techniques:

- Probability sampling, where each unit of the population has a known nonzero chance of being selected for the sample.
- Non probability sampling, where the samples are gathered in a process that does not give equal chance to all individuals from the population.

A non-probability sampling technique called convenience sampling was chosen because the researcher was unable to access the target population using other sampling techniques within the time frame and financial constraints of the study. Convenience sampling involves selecting subjects because of their convenient accessibility and proximity to the researcher. The drawbacks with this method are sampling bias and that the sample is unlikely to be representative of the entire population. The sample that was used for the research included:

- Family, friends and classmates.
- Work colleagues.
- Facebook friends and acquaintances.
- Twitter followers.

A number of participants did subsequently share the survey link with their friends and work colleagues thus there was a snowball effect with respect to the sampling. However this was not an intentional technique as the researcher had not specifically asked participants to do so.

3.8 Limitations of Chosen Methodology

While an online survey does afford a number of advantages as indicated in a previous section, there are a number of limitations to this approach. These include;

- Potentially ambiguous questions – the biggest drawback is the capacity to do it badly (Saunders et al., 2012, p.178) because the researcher is not there to clarify any questions that the respondent does not understand.
- Impersonal – the lack of human contact can limit the ability to further probe for more in-depth details the way an open-ended interview or focus group may be able to (Evans and Mathur, 2005).
- Low response rate – online surveys tend to have a lower response rate (Sauermann and Roach, 2013 , Rogelberg and Stanton, 2007) and thus can serve to undermine the perceived credibility and actual generalizability of the collected data.

In order to alleviate any potentially ambiguous questions a pilot survey was sent out to a limited number of individuals in order to solicit feedback and ensuring that respondents would not have problems in answering the questions (Saunders et al., 2012, p.451). Further details on piloting the survey and how the questions were modified following feedback are discussed in section 3.10.2.

In order to mitigate the risk of a low response rate, the survey was distributed to a large number of recipients via electronic means as dictated by the ethics approval. The importance of the research was indicated in the distribution email which also included the researchers contact details in case of further queries from participants. After the first week a reminder email was sent out and the links on the social media sites were refreshed to ensure they re-appeared. To avoid risk of spamming and annoying individuals, only one reminder email was sent out.

3.9 Ethics Approval

Any research project that involves human participation must have independent review by a Research Ethics Committee before its commencement. On 1st May 2014 an application for ethics approval was submitted to the Trinity College Dublin Research Ethics Committee. The ethics approval application form included a link to a preview mode of the survey to allow the Ethics Committee to review the survey questions.

On 20th May 2014 ethics approval was granted to proceed with distributing the survey. The Ethics Approval form is attached in Appendix A - Ethics Application Form.

3.10 Research Strategy - Online Survey

An online survey was developed in order to gather information about smartphone users, their usage of the smartphone and their awareness of the potential security risks associated with smartphone usage. The survey was designed and delivered using SurveyMonkey (www.surveymonkey.com) which provides an online questionnaire hosting service to registered users.

3.10.1 Survey Design

The survey consisted of a total of 42 questions. The questions were divided into sections which focussed on a specific area;

- Smartphone Usage (4 questions)
  To gain an understanding of what type of smartphone the user owned, what they used it for and what data they stored on it.
- Smartphone Applications (8 questions)
  To gain an understanding as to where the user downloaded applications from, what factors they would consider when installing an application and whether they believed applications they downloaded underwent a prior security review.

- User Security Awareness (7 questions)
  To gain an understanding of the user's general security awareness associated with smartphone usage.
- Smartphone Security Mechanisms (4 questions)
  Determine what (if any) security mechanisms the user employed on their smartphone in order to protect themselves.
- Smartphone Security Risk Scenarios (11 questions)
  This section outlined a number of potential scenarios that could compromise the security of a user's smartphone. Smartphone users were asked whether they were aware the particular scenario could happen and whether they were concerned about it happening to them.
- Demographics (4 questions)
  A number of questions to aid in determining the demographical breakdown of the individuals that took part in the survey.

The full list of survey questions are provided in Appendix B - Survey Questionnaire. The question types were predominantly multiple-choice questions with either single answer or multiple answer choices. A number of questions required the usage of a Likert unipolar ordinal scale to measure the degree of concern the user had regarding the statement being made. Dillman et al. (2009) suggest that the challenge is to choose an appropriate scale length that respondents will be able to place themselves on the scale but not so many that the categories begin to lose their meaning or become ambiguous. Thus a five point scale was chosen for the questions with a rating scale as follows;

- Extremely concerned
- Very concerned
- Moderately concerned
- Slightly concerned
- Not at all concerned

A smartphone security survey of US consumers carried out by the Ponemon Institute (2011) presented a number of scenarios illustrating a range of security issues and risks. Individuals were asked whether the specific risk could happen to them, if the risk had actually happened to them and what their level of concern was about the risk. A number of these scenarios were deemed appropriate to the research and thus utilised in this survey.

3.10.2 Piloting the Survey

A pilot study refers to a mini-study in which the proposed questionnaire and all implementation procedures are tested on a sample of the survey population. The purpose is to identify potential problems with the survey, such as ambiguous or badly worded questions, and related implementation procedures (Dillman et al., 2009).

Prior to distributing the survey, a pilot survey was created using Survey Monkey and presented to six participants in order to receive their feedback. Given the number of questions in the survey, it was requested that particular attention be paid to how long it took to complete the survey. Overall the feedback was positive and the time taken to complete the survey was not deemed to be a potentially inhibitive factor. A number of comments were made;

- There was some ambiguity regarding the question about Bluetooth. The reviewer wondered whether the question was asking if Bluetooth was always set as on/off or what was the setting at the point of completion of survey. After consultation it was felt that the question was clear enough as it was and thus was not modified.
- Two reviewers queried the option choices for the question "*What do you use (or have you used) your Smartphone for?*" One reviewer was not sure where video chat (Skype/FaceTime) fitted in. The other reviewer questioned whether the choice "Watching TV/films" also included YouTube, suggesting that if this was the case that "media clips" should be added. The survey question was modified to accommodate these changes.
- A technically competent and security aware reviewer queried one of the scenarios that was being presented;
  "*Financial applications for Smartphones can be infected with specialised malware designed to steal credit card numbers and online banking credentials. Were you aware that this could happen?*"
  They suggested that it appeared as if the scenario presented a situation where legitimate financial applications on the Smartphone could become infected with malware. However this is not the case. The reality is that an unaware user may inadvertently download a trojanised financial application which passes itself off as legitimate one on an application store/marketplace. This raised an interesting point regarding the accuracy of the question being asked. Thus the question was rephrased based on further discussions.

3.10.3 Survey Issuance and Closure timelines

Once ethics approval was granted the survey could be distributed to the sample population. In accordance with ethics, the Symantec HR manager signed the Informed Consent Form to approve the distribution of the survey link via company email.

The survey was distributed via the following channels;

- Participant email to family, friends and classmates.
- Participant email to work colleagues.
- Posting on social media site Facebook.
- Posting on personal Twitter feed to followers.

As per ethics guidelines, the online survey included the participant information sheet and declaration form which detailed the background to and the procedures of the research.

The survey opened on 10th June 2014 for a period of 2 weeks. It was closed on the 21st June having received 152 responses. After the first week a reminder email was sent out and the links on the social media sites were refreshed to ensure they re-appeared. Data collected was extracted from SurveyMonkey.

4 Findings and Analysis

4.1 Introduction

This chapter presents the findings of the research and explains how the data was prepared, analysed and interpreted. As outlined in the methodology chapter, the survey was designed and delivered using SurveyMonkey (www.surveymonkey.com).

A combination of both Microsoft Excel and IBM SPSS Statistics version 22 were used to carry out the analysis of the data.

4.2 Data Preparation

Once the survey was closed, the data was reviewed in SurveyMonkey. All response data was exported to Microsoft Excel in both coded numerical format and actual answer test formats. Both formats were needed at the later stage when preparing the data for import into SPSS which did require an element of work.

Preparing the data for import into SPSS from the Excel sheet was a time-consuming but worthwhile exercise as it allowed for a low level review of the data. Each question was optional, thus when a record was empty it indicated that the respondent decided not to answer the specific question. Missing data was coded as the numerical value 99 to indicate these situations. Once the Excel data was imported into SPSS, further preparatory work needed to be carried out. There were a total of 94 data variables, each of which corresponded to a particular question. For example the question, “Do you use your Smartphone for personal use, business use or both?” was given the variable name “os_personal_business”. Each variable needed to have a label, an associated value and a measurement variable defined for it. For measurement SPSS distinguishes three levels:

- Nominal;
  The answers given have no logical order. A typical example is the gender.
- Ordinal;
  With an ordinal scale there is a logical order, but no numbers are asked for. A typical example is a scale like: bad - neutral - good.
- Scale;
  Chosen if a number is being requested. A typical example would age

Once the measurement variables have been defined the data is ready for further analysis.

4.3 Survey Findings

In total there were 152 responses to the survey. Of the 152 respondents, one individual did not agree to the terms and conditions and thus did not proceed any further. The second question asking the respondent whether they had a smartphone resulted in three individuals responding with a “No” and thus took no further part in the survey. Given that the survey was entitled “Smartphone User Security Awareness” it would seem unusual that a respondent who did not own a smartphone would have proceeded past the terms and conditions of the survey. Of the remainder, a further five individuals exited the survey prematurely without submitting their data. This resultant sample set of 143 respondents were included in the analysis.

The survey questions were divided into sections which focussed on a specific area;

- Demographics,
- Smartphone Usage,
- Smartphone Applications,
- User Security Awareness,
- Smartphone Security Mechanisms,
- Smartphone Security Risk Scenarios

The following sub-sections discuss the findings and analysis of the survey data in relation to the specific focus areas of the survey.

4.3.1 Demographics

Four questions were asked in order to determine the profile of the survey respondents. Information about gender, age, country of residence and level of IT expertise was requested from the survey respondents.

Of the 143 survey respondents 75% were male, while 24% were female. Two individuals, representing 1% of the respondents, did not specify their gender (Appendix C - Table 7.1). In terms of age distribution, over half (53%) of the respondents were aged between 25 and 34 years of age, followed by 34% aged between 35 and 44 years of age (Appendix C - Table 7.2).

With respect to geographical dispersion, survey respondents were predominantly located in Ireland (87%) (Appendix C - Table 7.3).

Respondents were also asked to rate their level of IT expertise. 69% of all respondents rated themselves as having either an excellent or good level of IT expertise. The percentage breakdown is displayed in Figure 4.1.

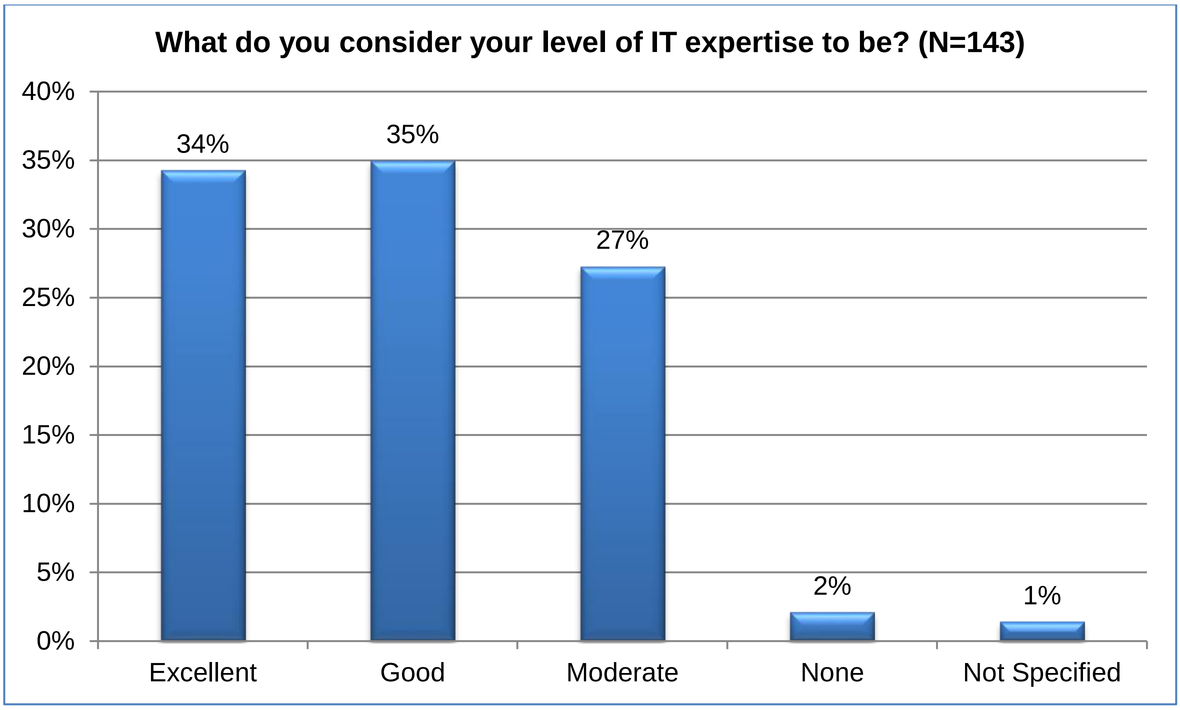


Figure 4.1 - What do you consider your level of IT expertise to be?

In summarising the demographic breakdown, the majority of respondents are situated in Ireland within an age range and level of IT expertise close to that of the researcher. Although the survey was presented online and distributed to a wide audience of the researcher's friends, family and colleagues, the sample set does appear have inherent bias and could not be considered to be representative of the larger population of smartphone users.

4.3.2 Smartphone Usage

The survey respondents were asked a number of questions regarding their smartphone usage. The popularity of the smartphone operating systems in the sample set is depicted in Figure 4.2.

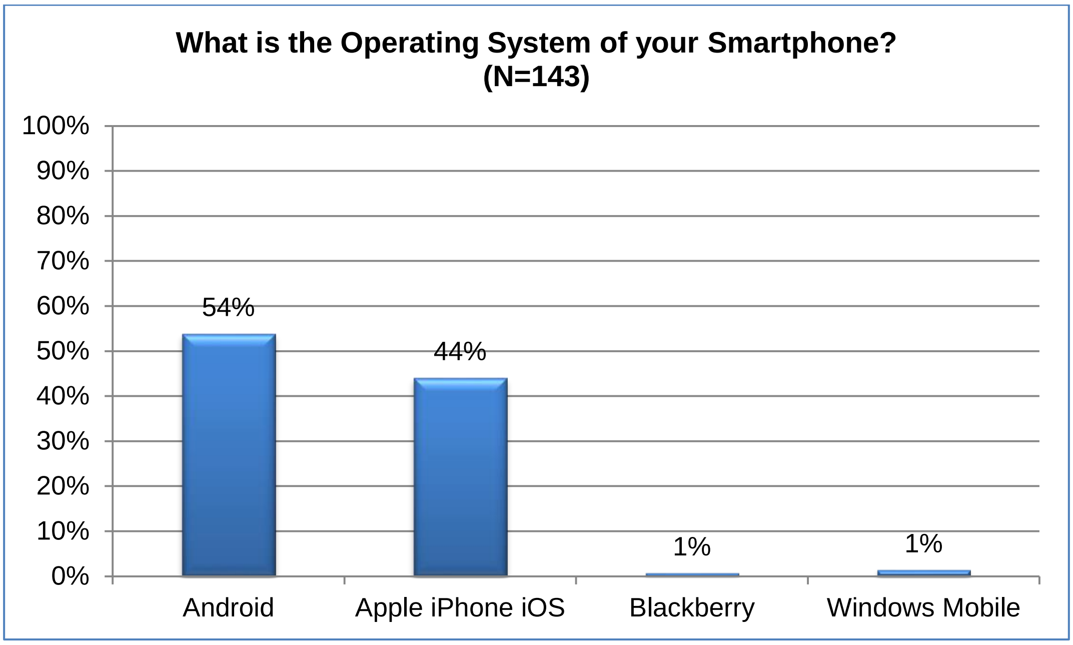


Figure 4.2 - What is the Operating System of your Smartphone?

Not surprisingly, Android is the most popular operating system within the sample set. However the figures for Android are not as high as those reported by Gartner who suggest that Android accounts for 78.6% of all smartphones (Van Der Meulen and Rivera, 2013b , Van Der Meulen and Rivera, 2013c , Van Der Meulen and Rivera, 2013a). Apple iPhone users accounted for 44% of the survey respondents.

Figure 4.3 presents the operating system popularity per gender. The figures suggest that females in the sample set tend to prefer using an Apple iPhone over Android. Indeed of the 34 females in the survey set, 19 (56%) were using Apple iPhones versus 15 (44%) that were using Android. This is at odds with the overall operating system popularity breakdown within the sample set.

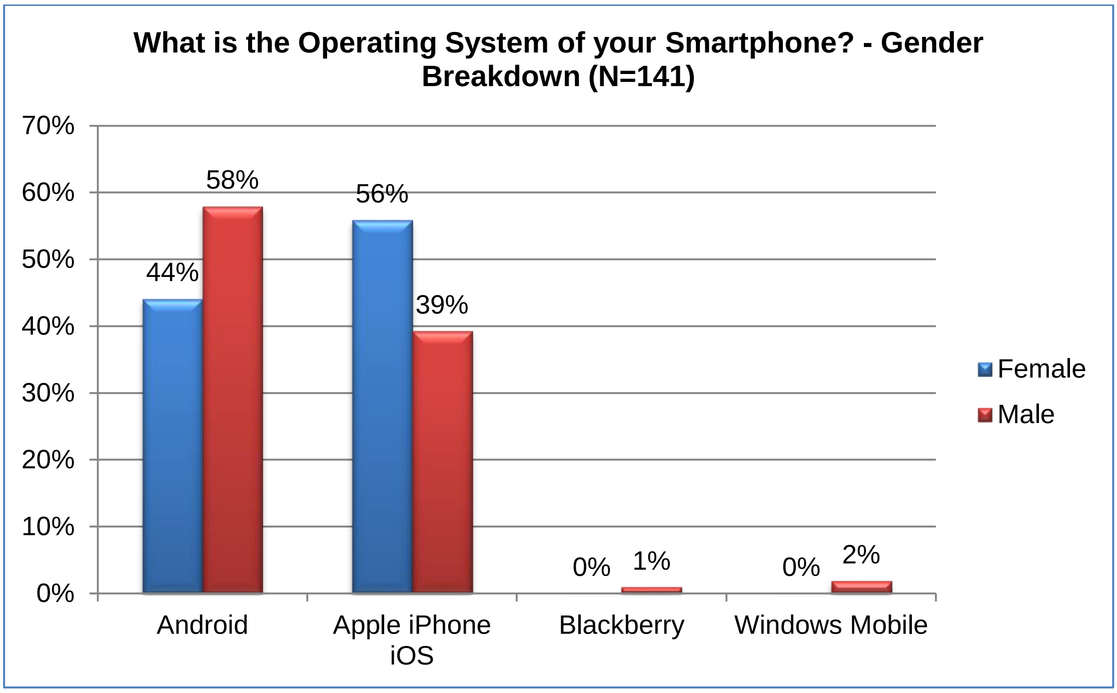


Figure 4.3 - What is the Operating System of your Smartphone? - Gender Breakdown

When asked whether they use their smartphones for personal use, business use or both, 49% of survey respondents indicated that they were using their smartphones for both personal and business use (Figure 4.4).

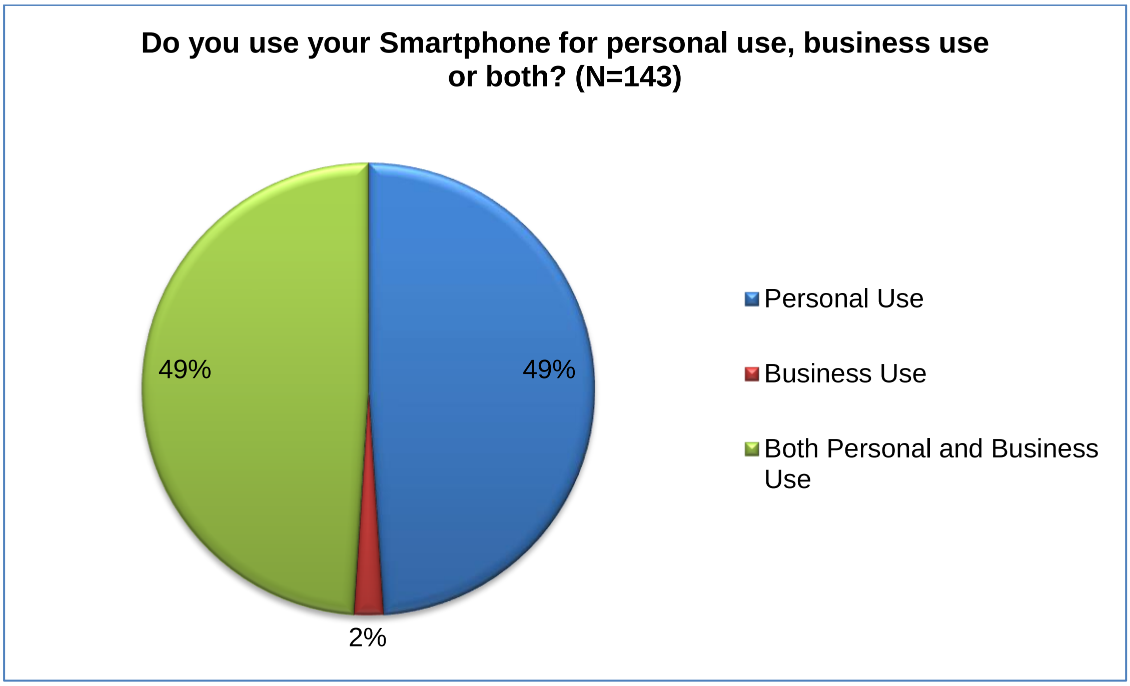


Figure 4.4 - Do you use your Smartphone for personal use, business use or both?

This figure would reflect the increasing tendency towards using personal smartphones for business purposes. The BYOD (Bring Your Own Device) trend, highlighted by Gartner as one of the top 10 strategic trends for 2014, increases the risk of exposure to corporate assets. This is because users' smartphones may not adhere to the corporate security policies that should be in place to protect such assets (Gartner, 2013a).

Survey respondents were asked what specifically they were using their smartphone for. Besides phone usage, the most popular uses of the smartphone were internet browsing (100%), camera (99%), texting (97%), maps and navigation (94%), calendar (90%) and personal email (89%). 70% of the survey respondents were banking online or paying bills with their smartphone, while just over half (52%) had shopped online with their smartphone (Figure 4.5).

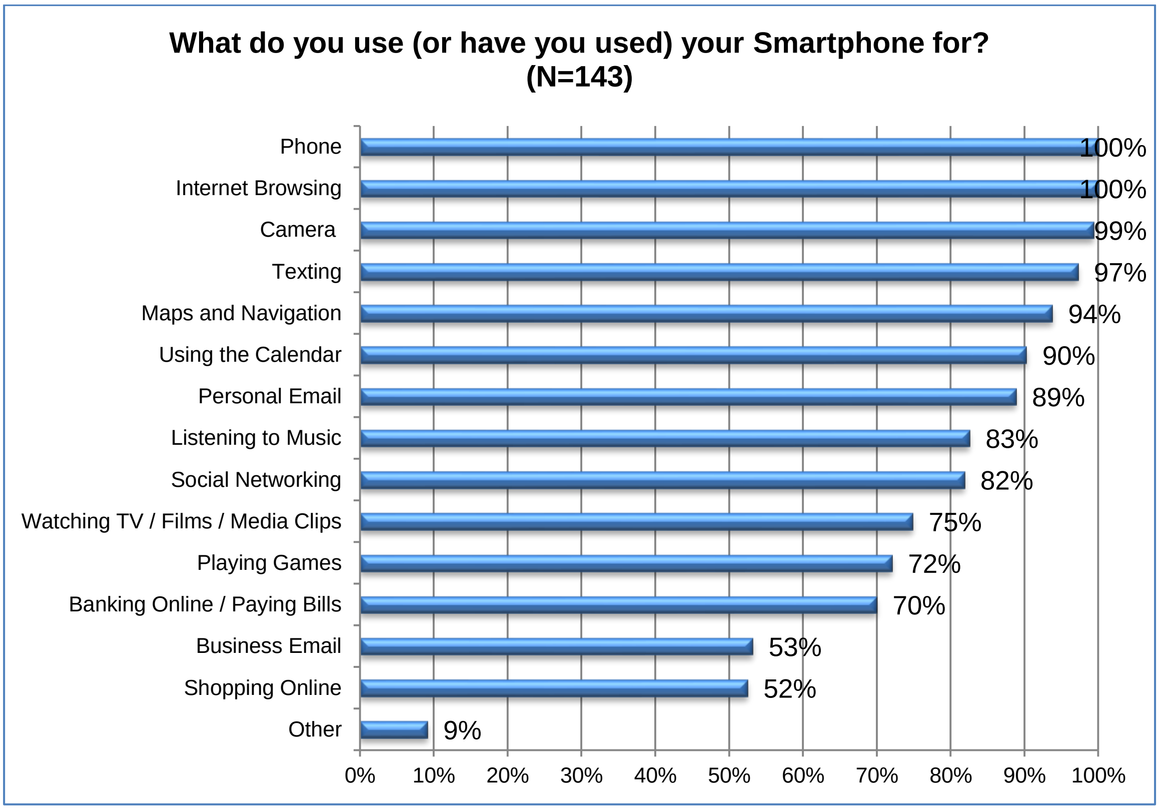


Figure 4.5 - What do you use (or have you used) your Smartphone for?

As shown in Figure 4.6, the data most often stored on smartphones by survey respondents included photos (99%), contact lists (89%), email addresses (77%) and music/videos (73%). Only 14% stored passwords or pin numbers on their smartphone while 10% stored credit/debit card numbers.

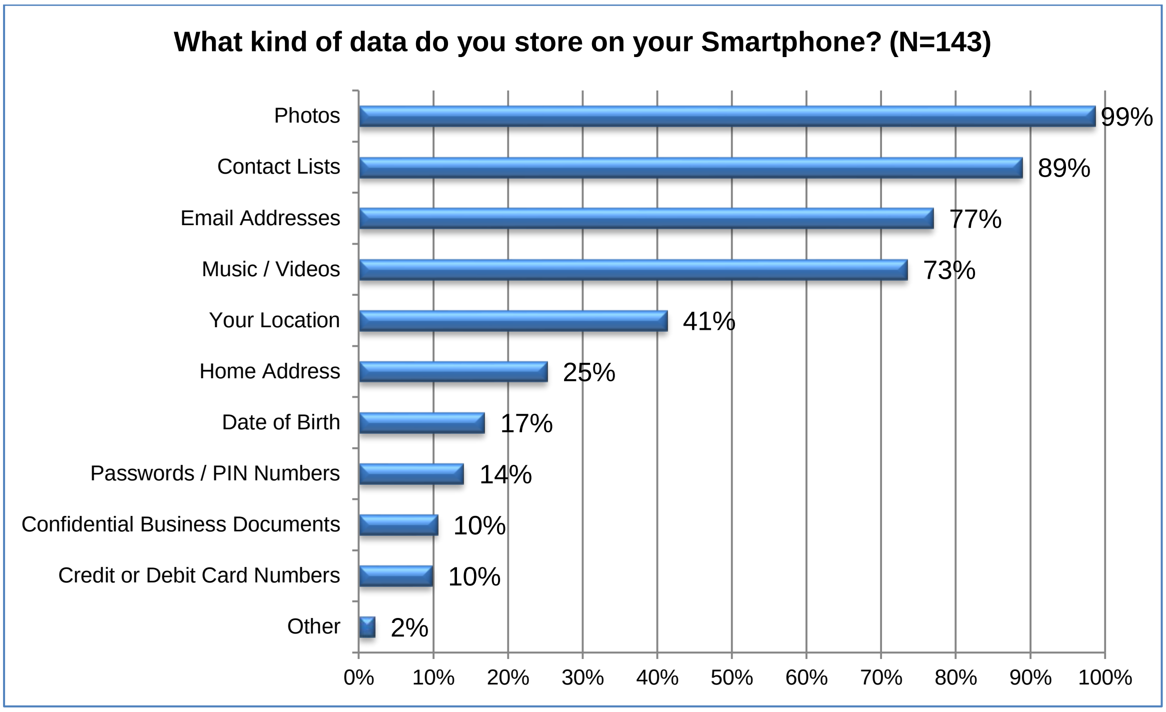


Figure 4.6 - What kind of data do you store on your Smartphone?

Summarising the Smartphone Usage section, it can be observed that Android is the most popular Smartphone platform amongst survey respondents at 54%, albeit this figure is not as high as Gartner's figures of 78.4% (Van Der Meulen and Rivera, 2014). The Apple iPhone was more popular amongst females with 56% of female survey respondents preferring it to Android. 49% of all participants were using their smartphone for both personal and business use with 53% using their smartphone to send and receive business emails.

4.3.3 Smartphone Applications

When asked whether they installed applications on their smartphone, 98% of the respondents indicated that they did so. Given that applications enhance the user experience of the smartphone it was perhaps more surprising that 2% of the survey respondents did not install applications. However one respondent, who indicated that they did not do so, subsequently specified in a separate question that they installed applications from the *"Company IT"* suggesting they might have forgotten to answer the question or decided not to.

As indicated in Figure 4.7, the overwhelming majority of respondents (99%) download applications from the official app stores (Google Play, Apple App Store) signifying a measure of trust in the official application stores.

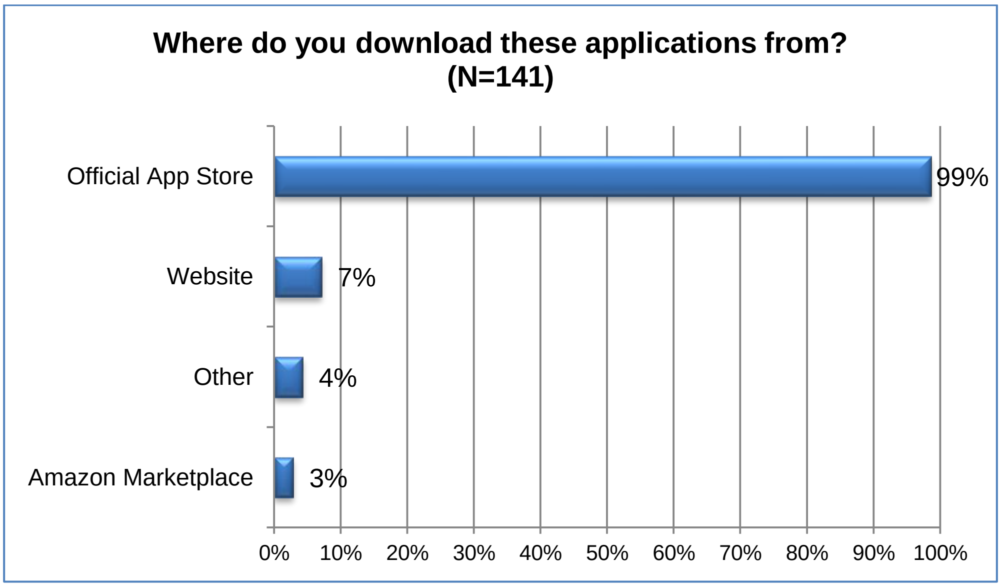


Figure 4.7 - Where do you download these applications from?

Figure 4.8 indicates that 69% of the respondents believed applications downloaded from the official application stores were safe. Interestingly, 57% of respondents were unaware of any security review mechanisms in place on the official application stores prior to them downloading an application to their smartphone (Figure 4.9). These findings may suggest that users trust the official application stores while not necessarily knowing whether any security reviews actually take place on the applications uploaded to those stores.

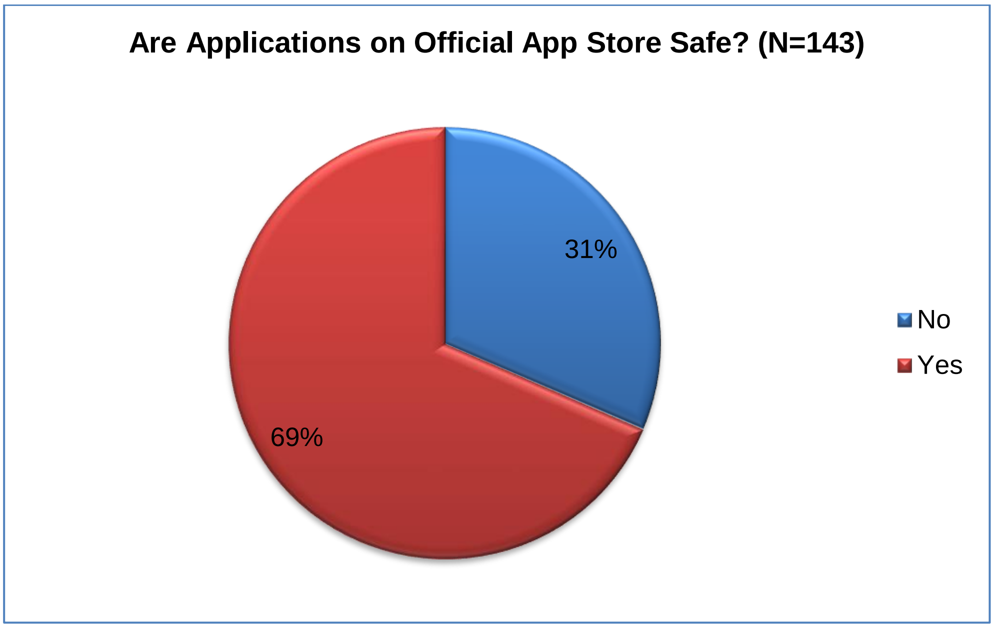


Figure 4.8 - Are Applications On Official App Store Safe?

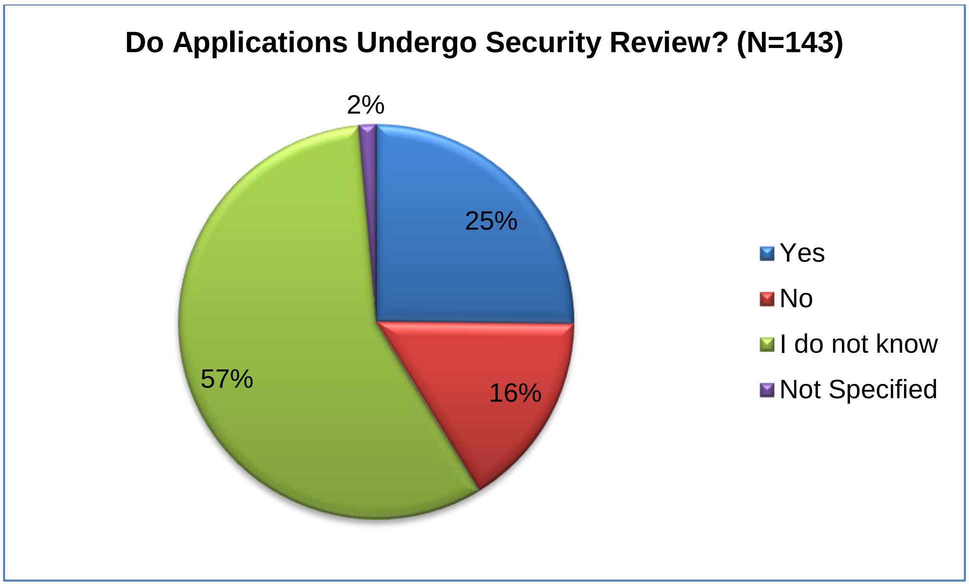


Figure 4.9 - Do Applications Undergo Security Review?

When the survey results are further broken down, it can be observed that 44% of Android users do not believe applications from the Google Play store are safe, whereas only 8% of Apple iPhone iOS users do not trust the applications from the Apple App Store (Figure 4.10)

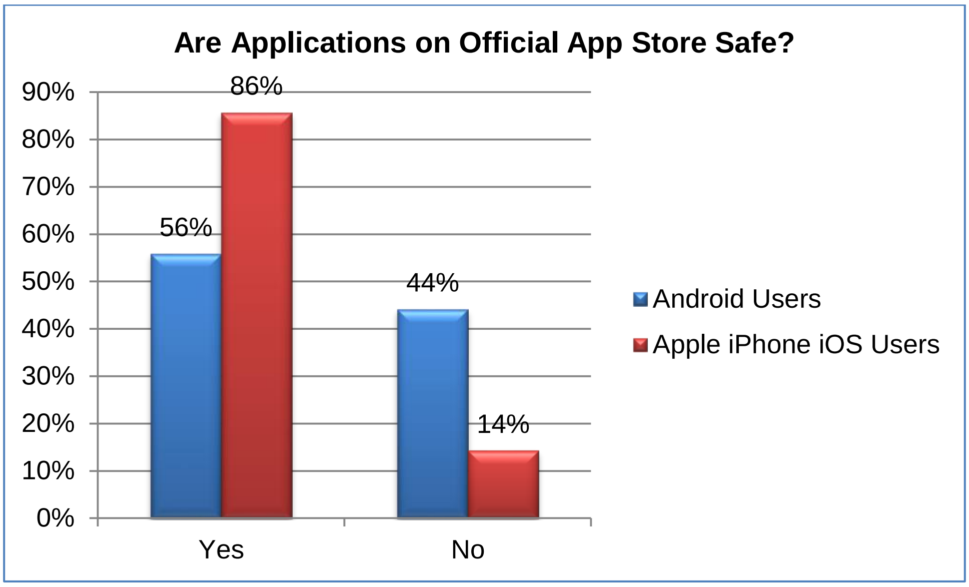


Figure 4.10 - Are Applications on Official App Store Safe?

Given the abundant reporting of fake malicious applications on the Google Play market, this lack of trust may be well placed. Google's open market strategy and omission of any pre-screening and verification process implies that anyone is allowed to post any application on Google's Play Store without much restriction. As discussed in the literature review, Google did take steps to improve security on their Play Store by introducing Bouncer in February 2012. (Lockheimer, 2012). However researchers have found that it can be circumvented (Oberheide and Miller, 2012 , Percoco and Schulte, 2012). In contrast, Apple's strict vetting process and walled-garden approach regarding application distribution has resulted in minimal instances of malware within the Apple App Store with F-Secure Report (2013) reporting no instances of malware on the iOS platform in 2013.

Survey respondents were asked about the main factors they considered when installing an application. Unsurprisingly, price, at 66%, was the main factor considered when making a decision whether to install an application (Figure 4.11).

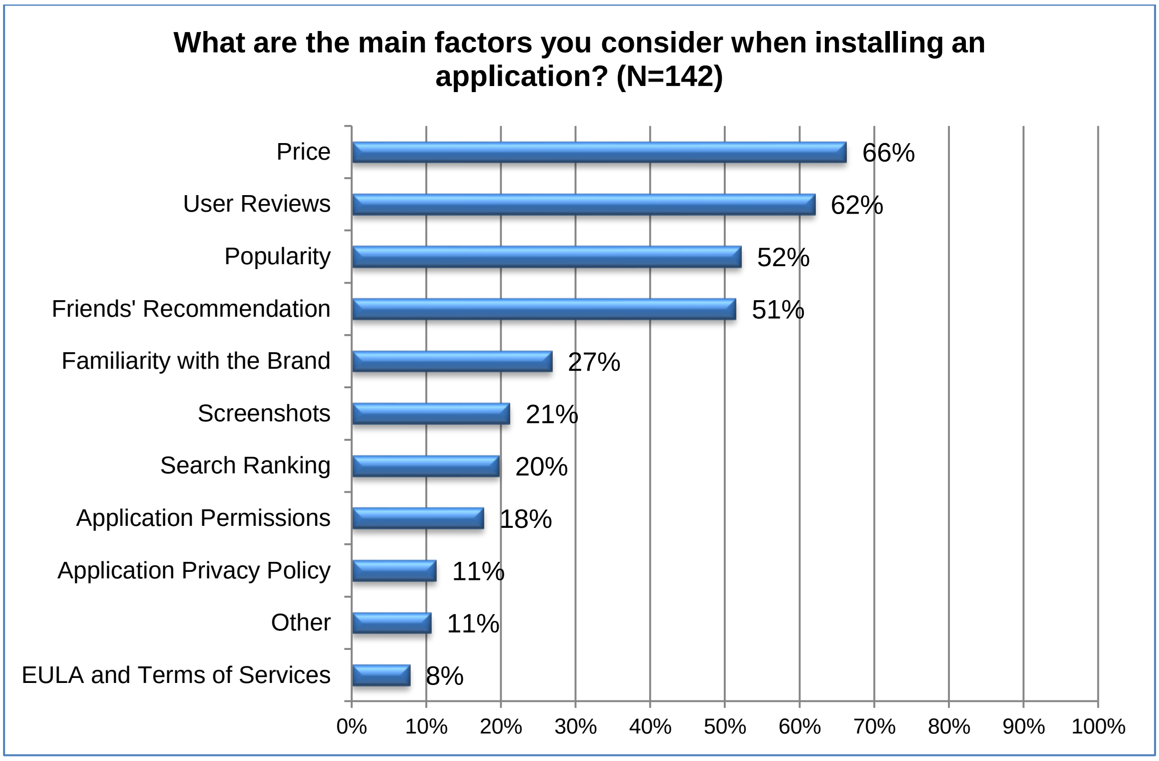
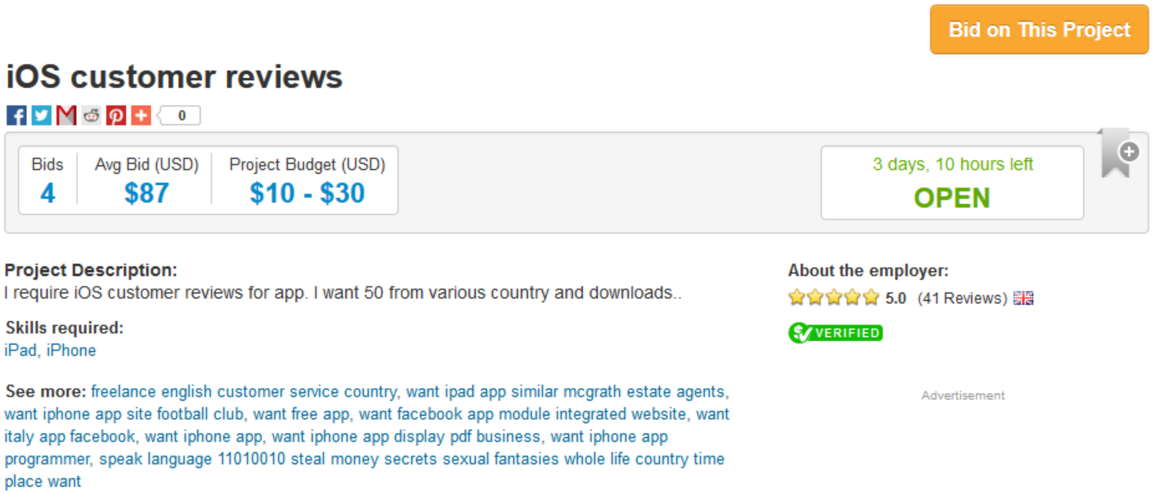


Figure 4.11 - What are the main factors you consider when installing an application?

62% of survey respondents relied on user reviews when considering installing an application on their smartphone. Forman et al. (2008) have shown that consumer ratings and reviews do have an impact on the purchase decision of a consumer. Thus, while there is a benefit to having ratings and reviews for smartphone applications, there is a need to ensure these are genuine. While fake reviews are nothing new to Amazon, this practice has become more commonplace on both the Google Play Store and Apple App Store with companies specifically set up to sell fake reviews (Orland, 2014 , Kimura, 2014) and developers often looking to purchase fake reviews from freelance marketplaces (Figure 4.12).



iOS customer reviews

Bids	Avg Bid (USD)	Project Budget (USD)
4	$87	$10 - $30

3 days, 10 hours left
OPEN

Project Description:
I require iOS customer reviews for app. I want 50 from various country and downloads..

Skills required:
iPad, iPhone

See more: freelance english customer service country, want ipad app similar mcgrath estate agents, want iphone app site football club, want free app, want facebook app module integrated website, want italy app facebook, want iphone app, want iphone app display pdf business, want iphone app programmer, speak language 11010010 steal money secrets sexual fantasies whole life country time place want

About the employer:
★★★★★ 5.0 (41 Reviews)

VERIFIED

Advertisement

Figure 4.12 - Developer Purchasing Fake iOS Reviews

The survey revealed that a low proportion of survey respondents considered the application’s privacy policy (11% of respondents), EULA or terms of service (8% of respondents) as factors that influenced their installation of an application on their smartphone.

Survey users who specifically owned an Android smartphone were asked whether application permissions were a factor of consideration when installing an application. Only 32% of survey respondents within this group regarded it as a factor of consideration.

Figure 4.13 presents the survey responses with respect to the attention respondents pay to security and EULA/terms of service (agreement) messages during application installation. These survey questions specifically asked the respondents whether they paid attention to security messages and licencing agreements/terms of service messages that appear while installing an application on your Smartphone. Not surprisingly, respondents paid more attention to security messages with 51% of users always examining the security messages while only 19% always scrutinized the EULA/terms of service messages.

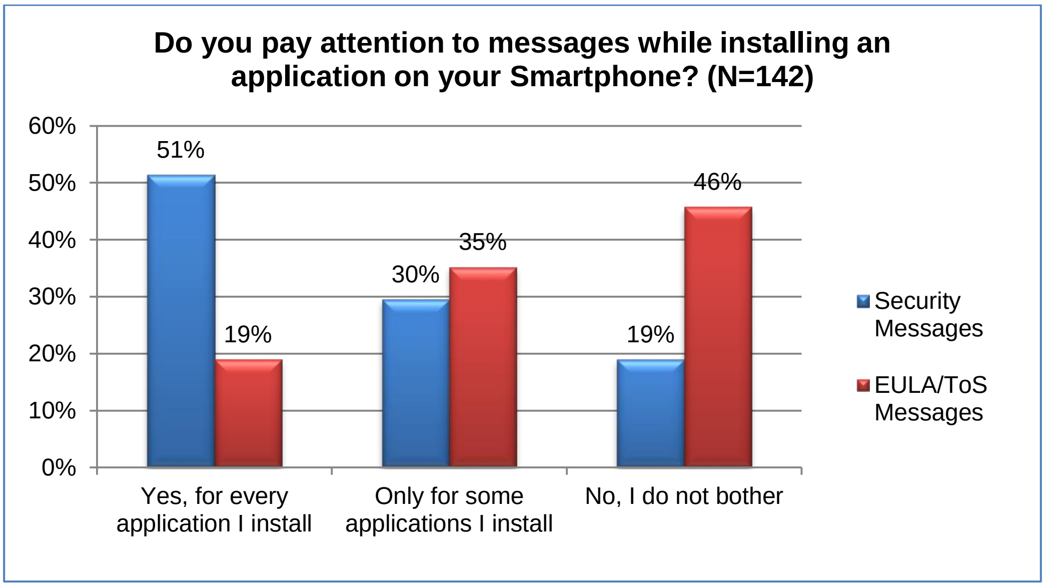


Figure 4.13 - Do you pay attention to messages while installing an application on your Smartphone?

As discussed in the literature review, the security models of both Android and Apple iOS prompts the user with certain security or EULA messages during the installation phase. These models assume the users will examine these messages and make informed decisions. Android, in particular, requires that the user accepts the permissions that the application is requesting before the specific application can be installed. Thus the onus is on the user to understand the security messages. Ignorance of such messages can inadvertently result in the user allowing an application elevated privileges and/or access to confidential data.

The survey findings would indicate that smartphone users are ignoring privacy and security related factors when it comes to choosing to download and install an application on their smartphone, preferring instead to rely predominantly on price, user reviews, popularity and friends' recommendations when making a decision. These findings are comparable to similar research conducted by Mylonas et al. (2013b) and Kelley et al. (2012) who concluded that permissions were ignored, with their participants trusting word of mouth, ratings and application store reviews.

4.3.4 User Security Awareness

Survey respondents were asked a number of questions in relation to their general security awareness associated with smartphone usage.

84% of survey respondents were aware that applications did require the user to allow the specific application access to the private data stored on the phone (Figure 4.14). This percentage was larger than expected, suggesting that the survey users did have an element of security awareness regarding the fact that applications were requesting permission to access their private data. However this seems to conflict with the survey findings with only 18% of respondents paying attention to the permissions an application requested and 51% of the users always paying attention to the security messages during application installation.

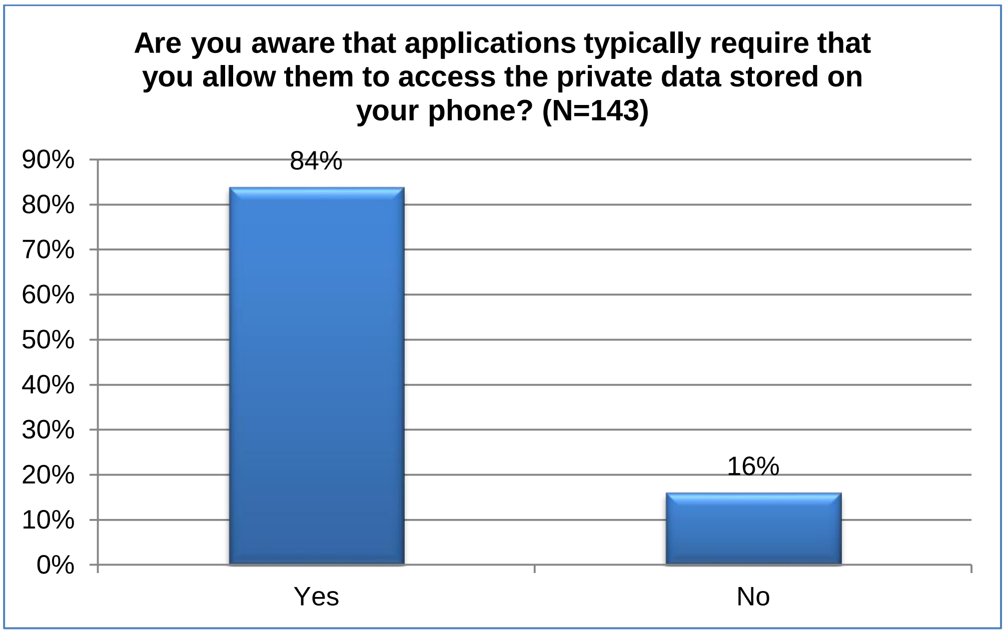


Figure 4.14 - Are you aware that applications typically require that you allow them to access the private data stored on your phone?

When asked how concerned they were about the privacy and protection of their personal data on their smartphone, only 30% of the respondents suggested they were either very/extremely concerned (Figure 4.15). It can also be observed in Figure 4.15 that survey respondents appear to have chosen the middle ground when answering this particular question. Given that the majority of survey respondents (71%) have never been infected by a malicious application (Figure 4.17), it may well be that there has been no defining event to have caused them to alter their level of concern.

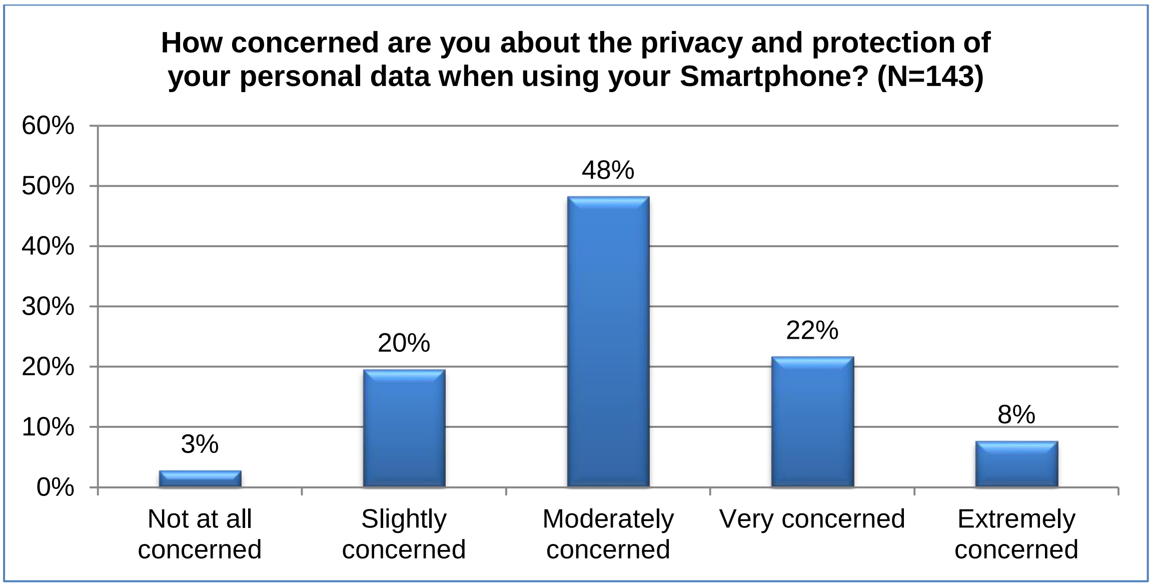


Figure 4.15 - How concerned are you about the privacy and protection of your personal data when using your Smartphone?

An inferential statistical analysis was performed using the Chi-square test to determine whether there was any relationship between a respondents' awareness of applications requesting permissions and their actual concern regarding the privacy of their personal data (Table 4.1). The null hypothesis H_0 was that awareness was independent of the concern while the alternate hypothesis H_1 was that awareness and concern were dependent. The Chi-square value was calculated to be 5.773 with a df (degree of freedom) of 4. The resultant probability value was 0.217. This p-value, being higher than 0.05, leads us to accept the null hypothesis H_0 and conclude that there is no evidence of a relationship between awareness and concern.

Table 4.1 - Respondent Privacy Awareness vs. Concern

		How concerned are you about the privacy and protection of your personal data when using your Smartphone?					
		Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned	Total
Aware Apps require Access to Private Data	Yes	2	24	61	25	8	120
	No	2	4	8	6	3	23
	Total	4	28	69	31	11	143

Similarly a Chi-square test was performed to determine whether there was any relationship between a respondent's awareness of applications requesting permissions and their consideration of application permissions when installing an application (**Error! eference source not found.**). The null hypothesis H_0 was that awareness was independent of considering permissions while the alternate hypothesis H_1 was that awareness and consideration of permissions were dependent. The Chi-square value was calculated to be 3.278 with a df (degree of freedom) of 1. The resultant probability value was 0.070. This p-value, being higher than 0.05, leads us to accept the null hypothesis H_0 and conclude that there is no evidence of a relationship between awareness and consideration of permissions.

Table 4.2 - Respondent Privacy Awareness vs. Considering Permission at Install

		Do you consider application permissions when installing?		
		Yes	No	Total
Aware Apps require Access to Private Data	Yes	24	96	120
	No	1	22	32
	Total	25	118	143

When asked whether they were aware of the existence of malicious applications on the smartphone, 83% of survey respondents indicated an awareness of the existence of such applications (Figure 4.16).

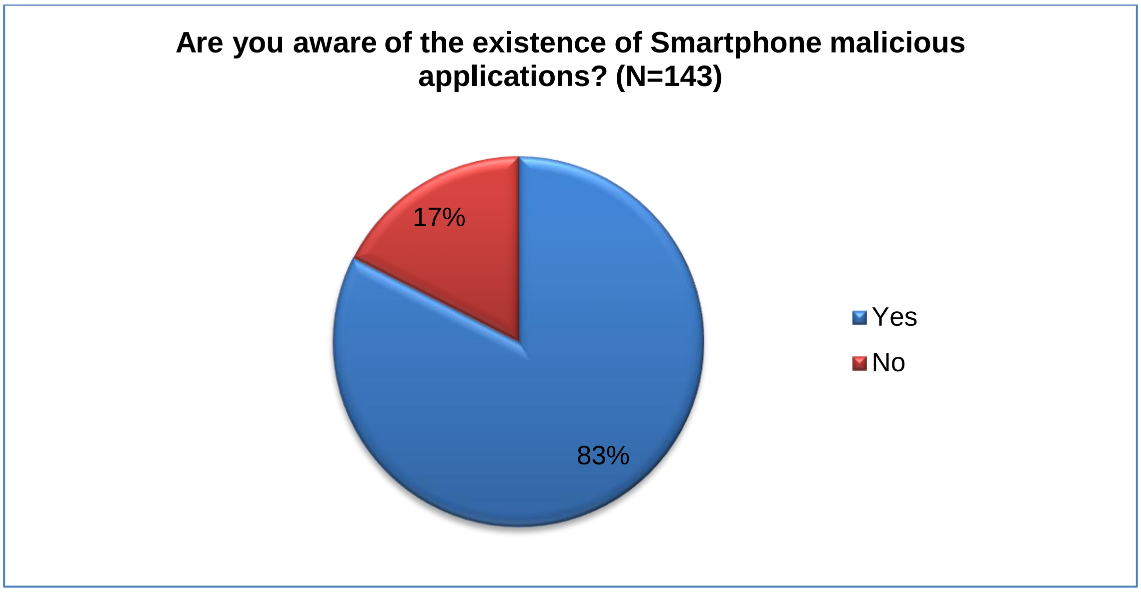


Figure 4.16 - Are you aware of the existence of Smartphone malicious applications?

Only 5% of survey respondents had knowingly experienced a malicious application infection on their smartphone while 24% of respondents did not know whether they had (Figure 4.17). Of the 5% that did, survey respondents were asked how they became aware of the malicious application. Various responses included;
“Via IT dept”,
“Antivirus Tools”,
“Huge data bill”,
“Pop-up ads”,
“Strange apps installing themselves and performance issues”

Interestingly 2 (of 7 overall) individuals had indicated that they had experienced a malicious application on their Apple iPhone.

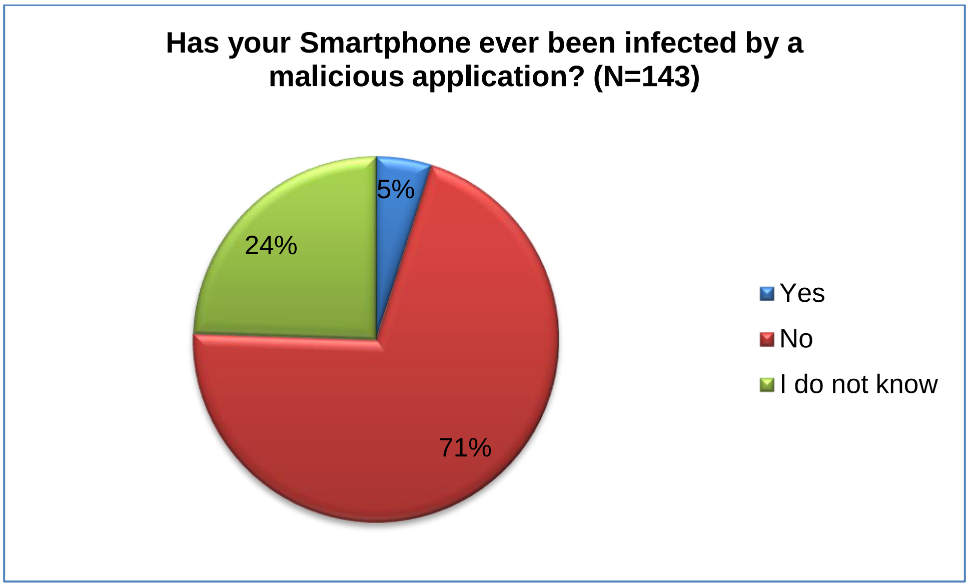


Figure 4.17 - Has your Smartphone ever been infected by a malicious application?

Survey respondents were asked whether they had recorded/noted their smartphone's IMEI (International Mobile Equipment Identity) number. The purpose of an IMEI is to identify a mobile device make and model. It also enables the network operator to accurately identify the device thus can be used to block stolen smartphones. 49% of respondents, a surprisingly high number, had noted their IMEI number with 40% not recording it and only 11% not aware what the IMEI number was (Figure 4.18). These figures significantly contrast with a study by the Hong Kong Office of the Privacy Commissioner for Personal Data (2012) where only 9.5% of their respondents had noted their IMEI number.

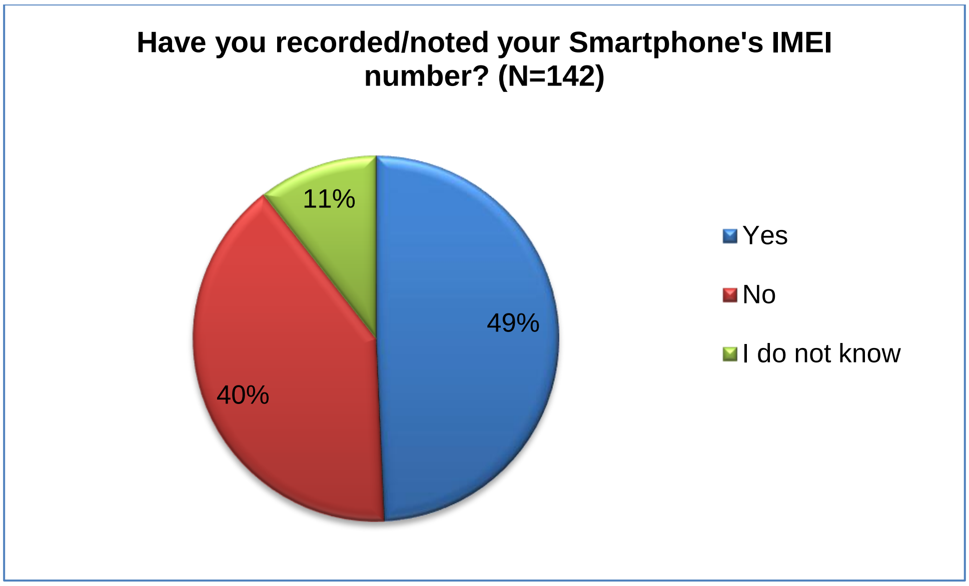


Figure 4.18 - Have you recorded/noted your Smartphone's IMEI number?

When asked whether they had Bluetooth enabled on their Smartphone. Figure 4.19 shows that 68% of survey respondents indicated that they did not have it enabled. This may suggest a heightened awareness of the risks or that they are turning it off to conserve battery power. Bluetooth has been shown to be vulnerable to security exploitations in the past. As discussed in the literature review, the first known malicious application for smartphones, Cabir, spread via Bluetooth (Symantec, 2004 , Hypponen, 2006 , Furnell, 2005a). Other Bluetooth threats such as blue jacking (essentially Bluetooth spam) and blue bugging (an attacker can remotely access a user’s smartphone and use its features) do exist. The only way to completely prevent potential exploitation is to switch off Bluetooth when it is not being used. Placing it into an invisible or undetectable mode as 10% of survey respondents have done still will not mitigate the risk.

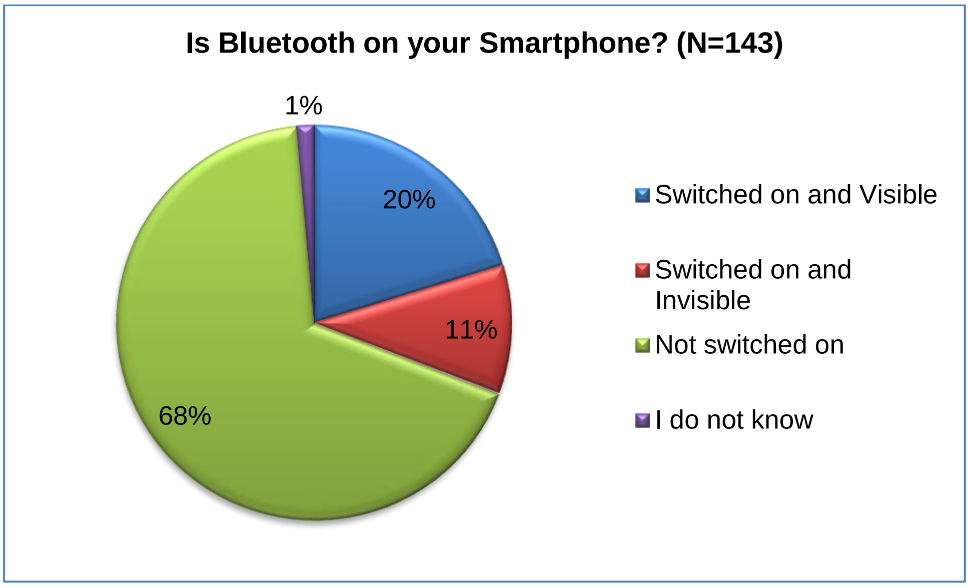


Figure 4.19 - Is Bluetooth on your Smartphone?

4.3.5 Smartphone Security Mechanisms

In this section of the survey a number of questions were asked to determine what (if any) security mechanisms the user employed on their smartphone in order to protect themselves.

When it comes to protecting the security of the smartphone there are numerous mechanisms that can be utilised from a simple screenlock to remote tracking and remote software wipe. Employing more than one mechanism in a layered approach to protecting IT devices and systems is a well regarded approach to protecting the confidentiality and security of those systems (National Security Agency, 2012). This concept is also good practice for smartphone users to adopt.

As Figure 4.20 depicts, 85% of respondents have activated screenlock or password protection on their smartphone with 55% employing a SIM card PIN number. Given that the SIM card can simply be removed from the smartphone it may be surprising that this figure is not higher, this could suggest that users are less concerned about their SIM being taken.

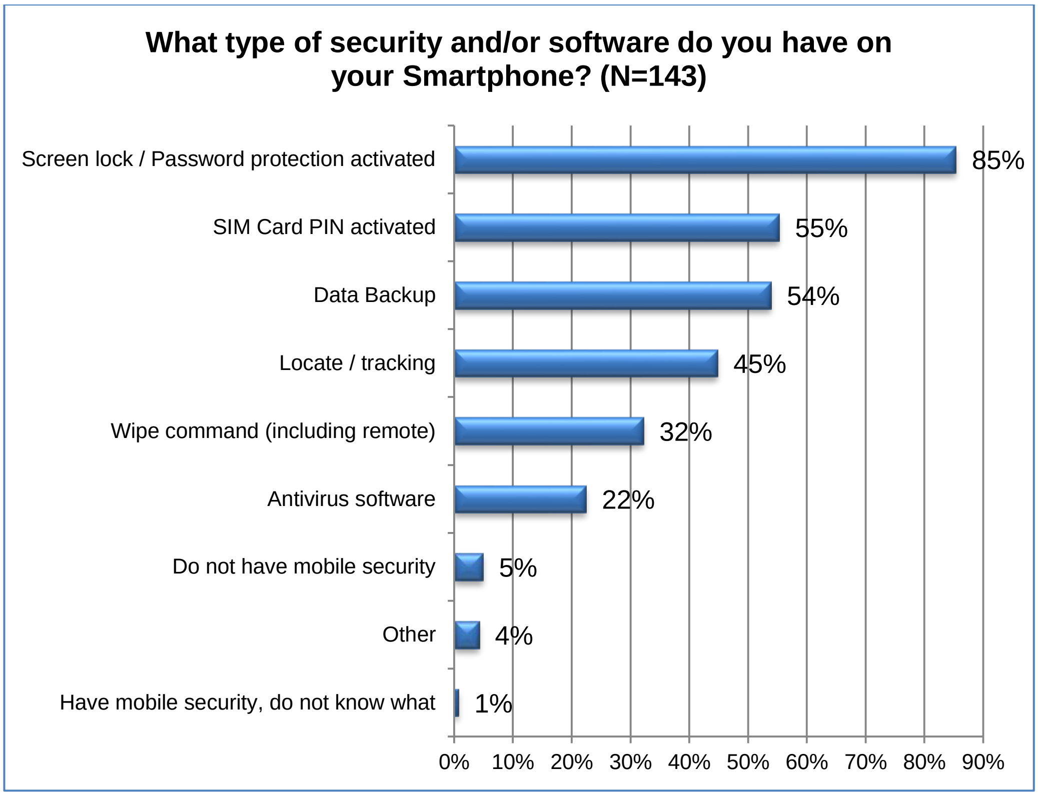


Figure 4.20 - What type of security and/or software do you have on your Smartphone?

Focussing on the two most popular protection mechanisms employed by users, a cross-tabulation was performed using SIM Card Pin activated as the second variable.

Table 4.3 - Screen Lock vs. SIM Card

N=143		SIM Card PIN activated		
		Yes	No	Total
Screen lock / Password protection activated	Yes	52%	34%	85%
	No	3%	11%	15%
	Total	55%	45%	100%

Table 4.3 shows that only 52% of total survey respondents activated both security mechanisms indicating that users are not employing the layered approach to security that would be considered good practice. 11% of respondents had activated neither screen lock nor SIM card protection. Given that 49% of survey respondents had previously indicated that they were using their smartphones for both personal and business use, the lack of security controls do represent a risk to organisations where such practices occur. On a personal level the 11% of respondents who activated neither security mechanism are leaving themselves open to easy compromise of their device and data should their smartphone be physically stolen.

Survey respondents were asked whether they considered smartphone antivirus security software essential. As Figure 4.21 portrays, respondents were evenly split on this particular question.

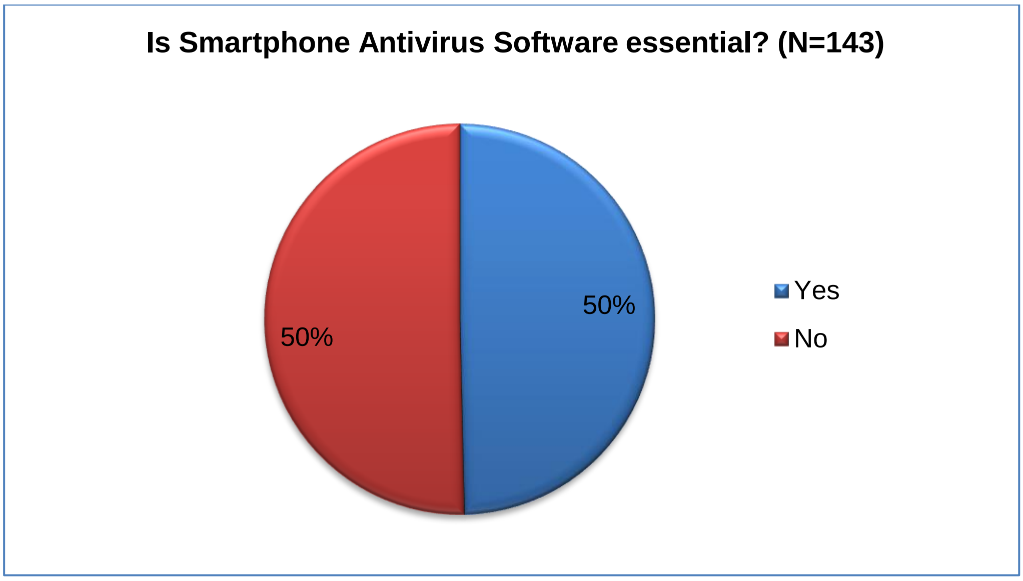


Figure 4.21 - Is Smartphone Antivirus Software essential?

Respondents who believed smartphone antivirus security software was not essential were asked to briefly explain why they felt that way. Of the 49 who answered, 15 commented about having an Apple iPhone and believing it to be safe from harm.
"Apple is safer than PC",
"I believe Apple is fairly safe",
"Trust in the walled garden that is the iOS App Store",
"I know of no iOS viruses",
"I presume Apple iOS is a safer OS"

These users may not be incorrect is their assumption. As indicated in the literature review, while malware does exist for the iOS platform it is not prevalent (F-Secure Report, 2013 , Symantec, 2013c). Indeed Cisco indicated that 99% of all mobile malware in 2013 targeted Android devices (Cisco, 2014). The 4 pieces of malware that Felt et al. (2011b) collected for iOS only spread through a specific vulnerability that was present in "rooted" or jailbroken iOS devices and none of these were listed in the Apple App Store. When survey users were asked whether their smartphones were jailbroken, only 1.6% of Apple iPhone iOS users responded that theirs was (Table 4.4).

Table 4.4 - Smartphone Rooted/Jailbroken

N=141		**Is your Smartphone rooted/jailbroken?**			
		Yes	No	I do not know what that means	Total
What is the Operating System of your Smartphone?	Android	10.7%	74.7%	14.7%	75
	Apple iPhone iOS	1.6%	73%	25.4%	63
	Blackberry	0%	100%	0.0%	1
	Windows Mobile	0%	100%	0.0%	2

Other users who did not consider smartphone antivirus security software to be essential commented:
“Do not know enough about it really”,
“Never considered installing it”,
“I do not have sufficiently private information on the device to justify cost of antivirus software”,
“Never heard of it”,
Wasn't aware such a thing existed”,
“There is none that I’m aware of for iOS devices”,
“Never really thought about it assume Apple have some security built in”,
“I’m not familiar with it. Never crossed my mind to use it”,
“Wasn't aware of antivirus for iPhone”,
“Never thought of it before”,
“I had not thought of it or was not aware of the need of it!”,
“I do now!”

This suggests a lack of awareness of security software for smartphones amongst 9% of survey respondents. Other respondents simply did not see a need to have such software installed as they did not consider their data valuable enough to anyone:
“Good luck to anyone who wants to steal from me, there is very little to take.”
“I do not have sufficiently private information on the device to justify cost of antivirus software.”
“I don't have personal data on my phone that I'm concerned about other people seeing.”
“I don't think I keep any valuable data on my phone.”

Other users commented that technological parameters (battery life, device performance) and the fact they were never affected by smartphone malware as influencing factors in their decision not to install antivirus security software on their smartphones. Nonetheless smartphone antivirus security software offers an extra layer of defence against potentially malicious applications.

Interestingly, when asked on which devices they used security software, 100% of survey respondents used some form of security software on their PC/Laptop/Desktop while only 31% found it necessary to install it on their smartphone (Figure 4.22). This indicates an element of inconsistency amongst the users with respect to the security awareness of the threats and controls that exist on the two platforms. When the 7% of users were asked to specify what other devices they used security software on, 60% of those users mentioned tablet, which is also another mobile device.

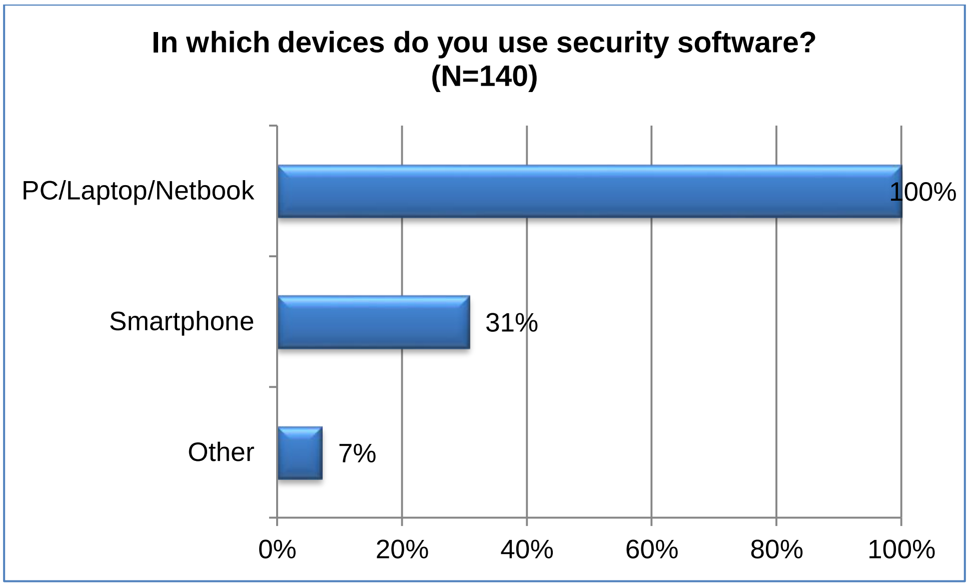


Figure 4.22 - In which devices do you use security software?

4.3.6 Smartphone Security Risk Scenarios

The survey respondents were presented with five potential scenarios that could compromise the security of a smartphone. The respondents were first asked whether they were aware that the particular scenario could happen and secondly, the level of concern that they had regarding that scenario actually happening to them. A Likert unipolar ordinal scale was used to measure the level of concern users had regarding the statement being made. A five point scale was used with a rating as follows;

- Extremely concerned
- Very concerned
- Moderately concerned
- Slightly concerned
- Not at all concerned

The five smartphone security risk scenarios presented to the survey respondents were:

1. Smartphones can be infected by malware that makes use of premium services or numbers resulting in unexpected monthly charges.
2. Smartphone applications may contain spyware that can access the private information contained on a smartphone.

3. Malicious financial/banking applications, posing as legitimate ones but instead designed to steal your credit card numbers and online banking credentials, may be present on App stores.
4. A Smartphone can be disposed of or transferred to another user without properly removing sensitive data, thus allowing an intruder to access private data on the device.
5. A Smartphone can connect to the Internet through local public Wi-Fi hotspots that are insecure, thus potentially exposing your personal and financial data.

Figure 4.23 summarises the survey respondents' level of awareness regarding the five smartphone security risk scenarios. It can be observed that generally there is a high level of awareness amongst the survey respondents regarding the various security risk scenarios presented. Survey respondents were most aware that they are vulnerable to exposing their confidential data when connecting to the Internet through an insecure public WiFi hotspot (84%) while there was also a high level of awareness regarding improper disposal of their smartphone (82%).

It is somewhat surprising that not more respondents were aware of premium rate malware (also known as SMS trojans) given that the majority of mobile malware observed by Kaspersky in 2013 were SMS trojans (Raiu and Emm, 2013).

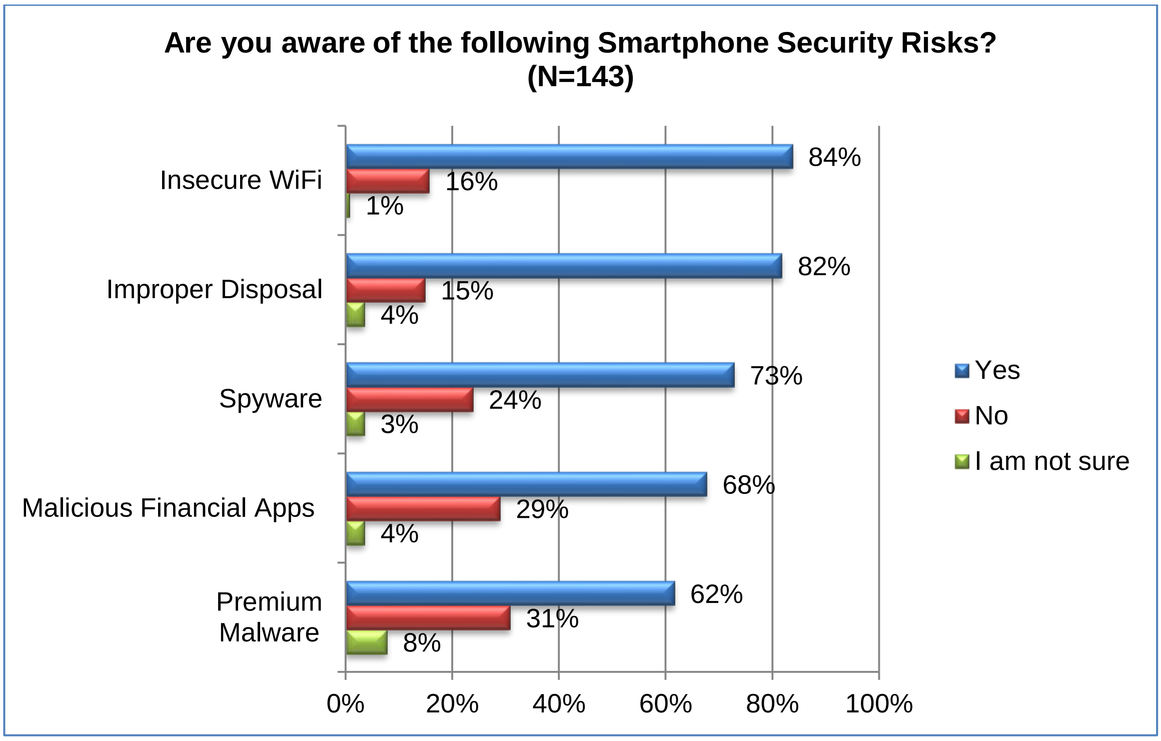


Figure 4.23 - Smartphone Security Risk Awareness

Although the level of concern questions were open to all survey respondents, the decision was made that if a respondent had indicated they were not aware of the particular security risk then their subsequent level of concern regarding that risk would be excluded from the data analysis. In essence, an individual cannot be concerned about something they are not actually aware of. Table 4.5 provides a breakdown of the level of concern amongst this group of survey respondents regarding the smartphone security risk scenarios.

Table 4.5 - Smartphone Security Risk Level of Concern

		How concerned are you about the following Smartphone Security Risks?					
		Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned	N=
Risk	Premium Malware	10%	25%	32%	25%	8%	88
	Spyware	5%	26%	25%	34%	10%	103
	Malicious Financial Apps	18%	19%	21%	24%	18%	95
	Improper Disposal	22%	16%	24%	22%	16%	116
	Insecure WiFi	16%	21%	26%	24%	13%	118

In order to present the data more appropriately, “Not at all concerned” and “Slightly concerned” were grouped into “Low Level of Concern” while “Very concerned” and “Extremely concerned” were aggregated into “High Level of Concern”. “Moderately concerned” was relabelled to “Moderate Level of Concern”. A clustered bar chart was produced in order to present the levels of concern amongst the risk aware survey respondents regarding each of the security risks (Figure 4.24).

As Figure 4.24 depicts, the risk aware survey respondents were most concerned about the threat of spyware applications accessing the private information contained on their smartphone (44%), followed by the threat malicious financial applications posed to their smartphone (42%). However it still must be noted that for each of the security risk scenarios presented, the figures show that less than half of the respondents actually had a high level of concern suggesting that the majority of survey respondents were not too concerned about the security risks actually happening to them.

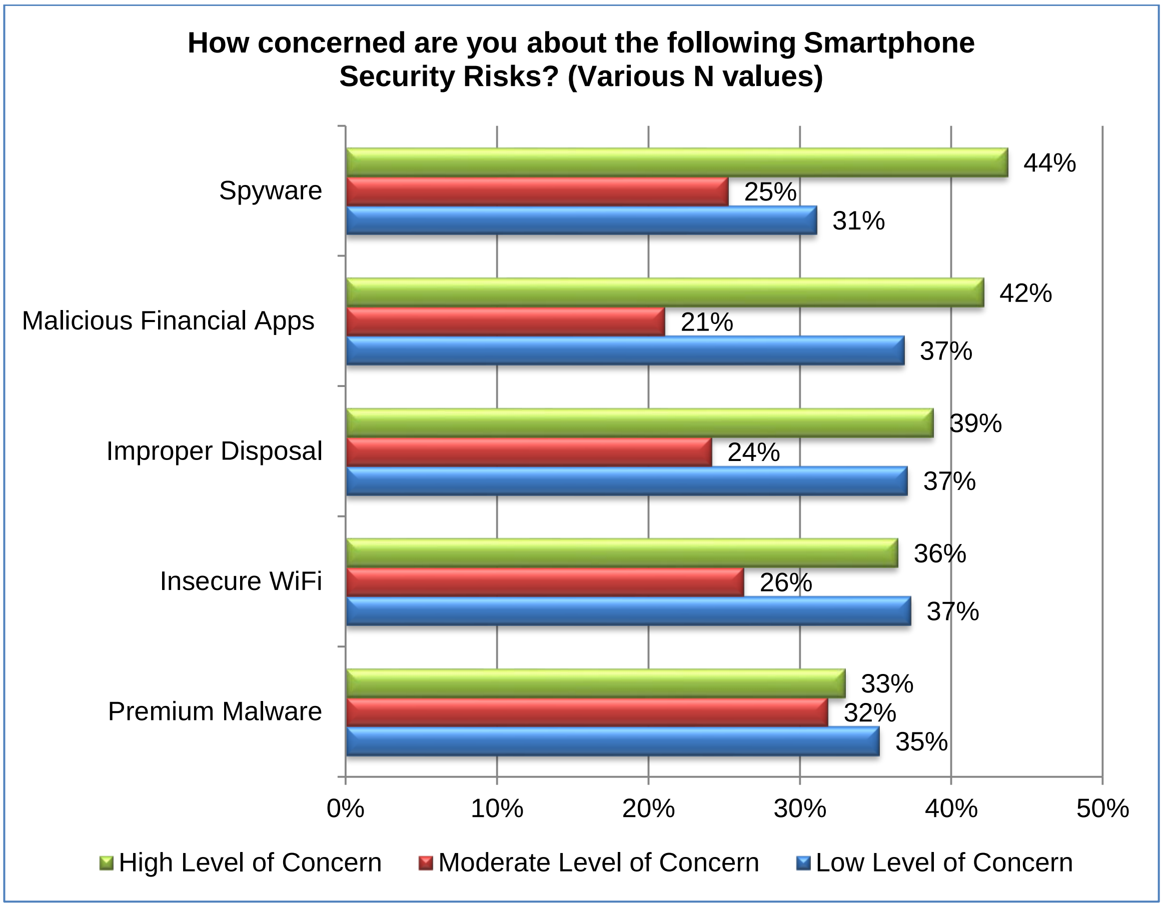


Figure 4.24 - Smartphone Security Risk Level of Concern

Figure 4.25 presents a graph indicating the percentage of overall users who were aware of the specific risk versus those that indicated a high level of concern regarding the risk. Each bar is displayed as a percentage of the overall sample set of 143 survey respondents (100% represents the 143 respondents). Therefore the “high level of concern” figures are percentages of the total survey respondents whether they were aware of the specific risk or not.

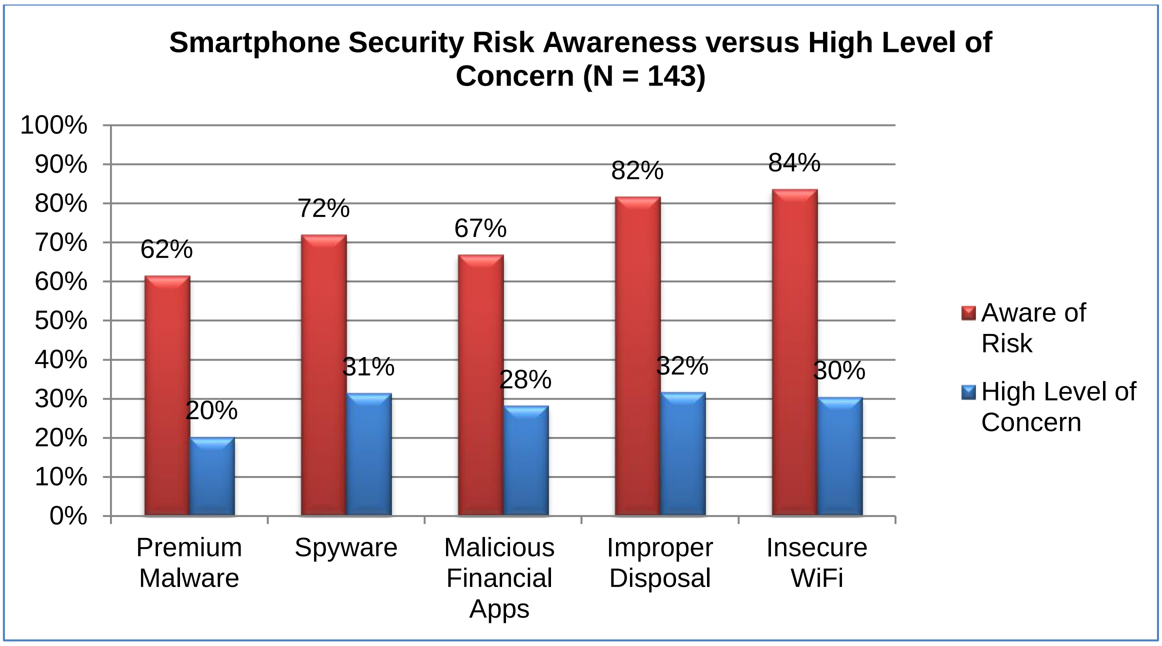


Figure 4.25 - Smartphone Security Risk Awareness versus High Level of Concern

As Figure 4.25 illustrates, and previously mentioned when discussing Figure 4.23, the overall level of awareness of the security risks is high. We can also observe from this graph that there is generally not a high level of concern amongst the users in the sample set with respect to the security risks. Of the total sample set of survey respondents, users were most concerned about improper disposal, spyware and insecure WiFi respectively. However these percentages were still quite low, hovering around the 31% figure.

For each of the specific security risks, a Chi-square test was performed to determine whether the fact that the respondent was aware of each risk had an impact on their level of concern towards that risk. The p-values for each security risk are presented in Table 4.6. In each case the null hypothesis H_0, that the respondent awareness and privacy concern were independent of each other, was accepted due to the fact that all p-values were greater than 0.05.

Table 4.6 - Respondent Awareness of Risk vs. Concern

		How concerned are you about the following Smartphone Security Risks?				
		Low Level of Concern	Moderate Level of Concern	High Level of Concern	Total (N)	p-value
Number of Respondents who were Aware of the Particular Security Risk	Premium Malware	31	28	29	88	0.345
	Spyware	32	26	45	103	0.545
	Malicious Financial Apps	35	20	40	95	0.588
	Improper Disposal	43	28	45	116	0.920
	Insecure WiFi	44	31	43	118	0.863

Survey respondents were asked whether their current awareness of and concern about mobile security and privacy threats, such as those described in the survey, impacted their decision to install mobile security protection on their smartphone. As Figure 4.26 depicts, 37% of respondents indicated that they were aware of the privacy and security risks involved with using their smartphone but did not believe that a mobile security product was necessary. 34% of respondents suggested they would not consider emailing, shopping or banking online without using having mobile security installed. Interestingly, of the 7 respondents whose smartphone had previously been infected by a malicious application, 5 considered themselves to be aware enough of the privacy and security risks to not require a mobile security product. Had these individuals “learnt their lesson” and were now more cautious in their approach or did they still believe in their own due diligence when using a smartphone?

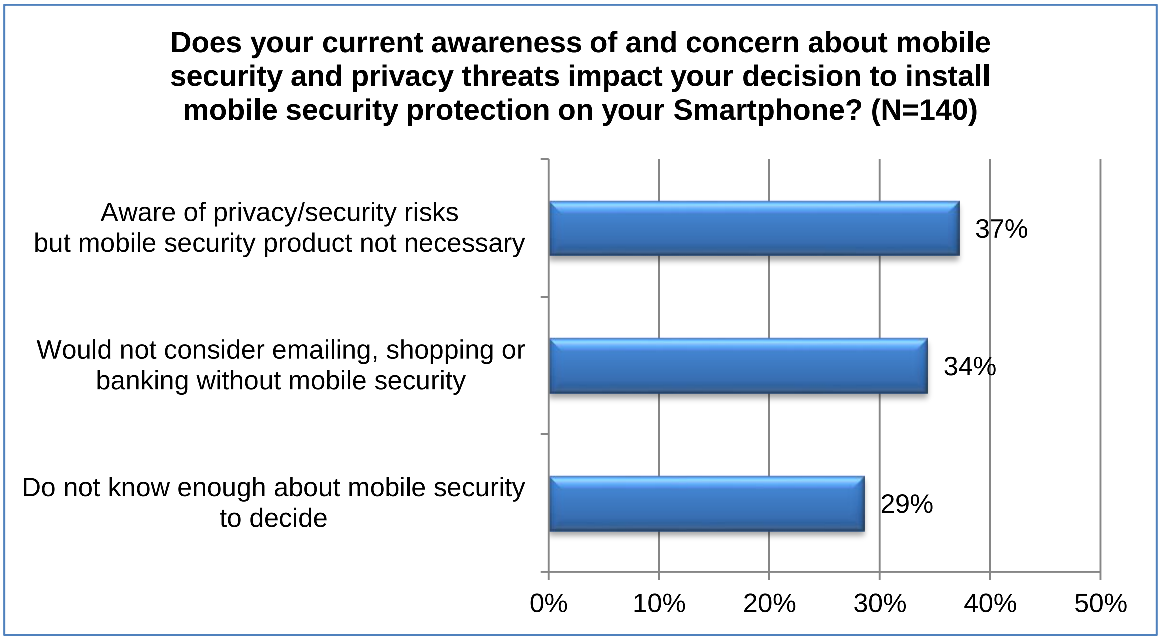


Figure 4.26 - Does your current awareness of and concern about mobile security and privacy threats impact your decision to install mobile security protection on your Smartphone?

The smartphone operating system of the respondents may be an influencing factor in their decision regarding the actual need for a mobile security product. As has been indicated, the incidence of malware within the Apple App Store is low (F-Secure Report, 2013) thus Apple iPhone users may not believe such a product is necessary. As indicated in Figure 4.27, this does appear to be the case with 32% of Apple iPhone users aware of the risks involved versus 23% who would not consider performing certain tasks without a mobile security product installed. In contrast, 39% of Android users were aware of the risks involved and did not consider a mobile security product necessary. However a larger proportion, 45%, would not carry out certain tasks without a mobile security product installed.

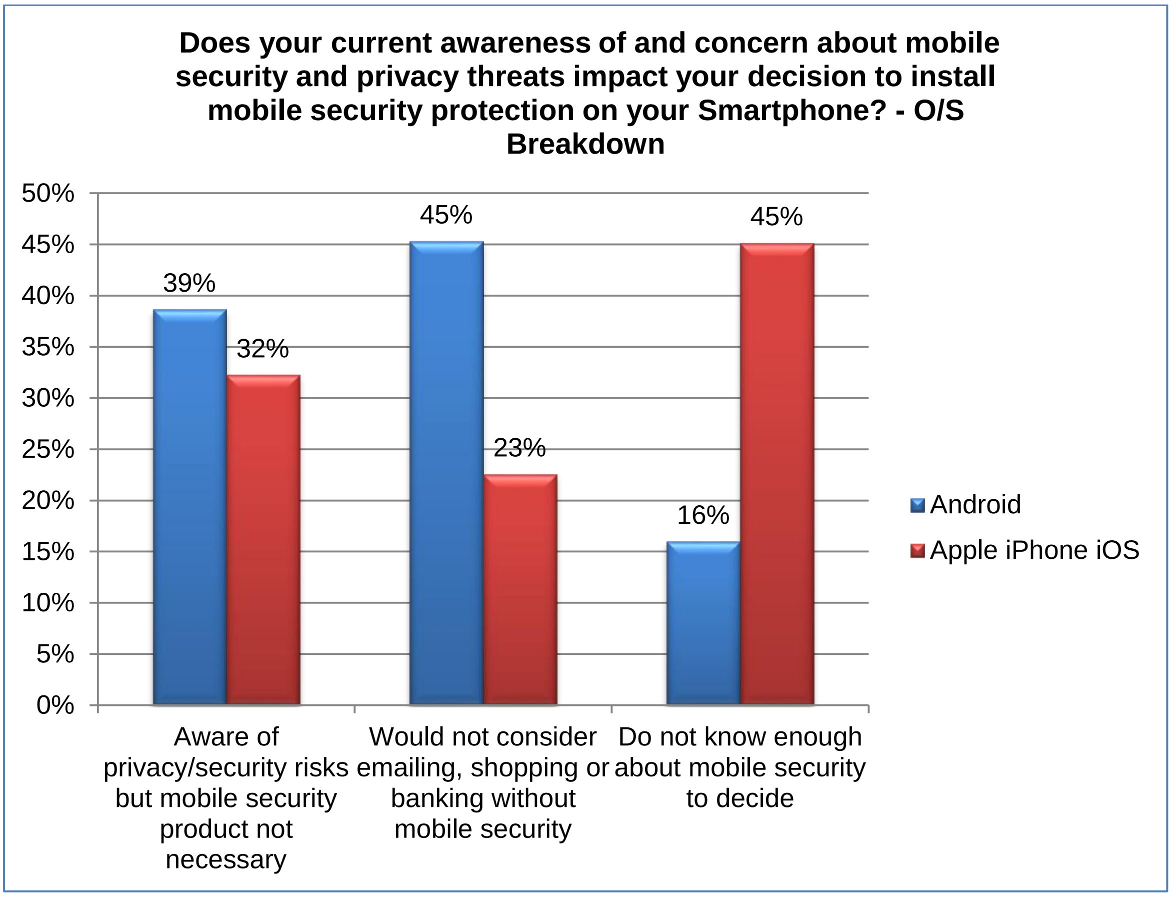


Figure 4.27 - Does your current awareness of and concern about mobile security and privacy threats impact your decision to install mobile security protection on your Smartphone? - O/S Breakdown

5 Conclusions and Future Work

5.1 Introduction

This chapter discusses the conclusions, identifies a number of limitations of the research and presents potential opportunities for further research in the area.

5.2 Conclusions

As indicated in chapter 1, the primary research question being asked in this dissertation is;

"To what extent are smartphone users aware of the potential security risks when using their smartphones?"

Given the nature of smartphones and how they are evolving ubiquitously, the role of the end user in protecting their own smartphone from security risks and threats is important. Their own actions (inadvertently installing a malicious application, visiting a spurious website from their smartphone) can directly impact the security and privacy of their data. Thus the extent of their security awareness becomes a key factor in protecting themselves.

A number of sub-questions arose that would help in providing an answer to the primary research question;

- Whether there is an awareness amongst smartphone users of malicious threats and risks to their smartphone devices.
- Whether there is any concern amongst smartphone users about these threats and risks.
- What steps, if any, are smartphone users taking to protect their privacy and security when using their smartphone?

In order to address the main research question and associated sub-questions, an online survey was used to collect data. Of the 152 responses, 143 were deemed valid and thus used as the sample set from which the data was analysed.

5.2.1 To what extent are smartphone users aware of the potential security risks when using their smartphones?

The findings of the survey indicated that the majority of the smartphone users did, in fact, have a high degree of awareness regarding security risks to their smartphone devices.

Five smartphone security risk scenarios were presented to survey respondents. It was observed that generally there was a high level of awareness amongst the survey respondents regarding the various security risk scenarios presented. Most respondents were aware of the fact that they were vulnerable to exposing their confidential data when using insecure public WiFi hotspots. In July 2014, Dublin Bus announced that free WiFi was available for all passengers across its entire bus fleet (Dublin Bus, 2014). Many public places like hotels, bars and cafes also offer free WiFi to their customers. During the months of October and November 2013, an Irish security firm carried out an audit of the publicly accessible WiFi networks of ten Dublin hotels. Within a short period of time, they found that they were able to exploit flaws within those WiFi networks and gain access to users' web traffic and sensitive information including emails, credit card details and passwords (Carty, 2013). Although the onus should be on the business that is providing the WiFi to ensure it is secure using security protocols like WPA2, this is often bothersome as it relies on providing each user with a key before they can connect. Thus the WiFi is left unsecured and exposed. While user awareness of insecure WiFi hotspots was high, they may be unaware of the ease to which the WiFi points can be breached. This would be a topic for further research. There are a number of steps users can take to mitigate this risk however;

- Using a VPN;
  The most secure way to browse on a public network is to use a virtual private network. A VPN routes traffic through a secure network even on public Wi-Fi.
- Disable automatic connecting to WiFi hotspots;
  Automatically connecting to any available WiFi hotspot can be a privacy risk. The device may connect to a public network which could result in personal information being exposed or leaked.
- Use security software;
  Although the findings indicated that respondents were evenly split on whether smartphone security software was essential, a layered approach to security is

good practice. Such software can help provide protection for users while using public WiFi networks.

There was also a high degree of awareness regarding improper disposal of smartphones potentially exposing sensitive data. Users were least aware of premium rate malware (also known as SMS trojans) which is surprising given that the majority of mobile malware observed in 2013 was actually premium rate malware (Raiu and Emm, 2013).

A high percentage (83%) of survey respondents also indicated that they were aware of the existence of smartphone malicious applications. This figure was comparable to a study carried out by Mylonas et al. (2013b) where 81.4% of Greek smartphone users were aware of the existence of such malicious applications.

When asked whether they were aware that applications required the user to grant them access to the private data stored on the phone. 84% of survey respondents indicated that they were aware. This suggested that survey users were aware of the fact that applications were requesting permission to access their private data. However this finding conflicted with observations elsewhere in the survey, whereby only 18% of respondents indicated that they paid attention to the permissions an application requested and approximately half (51%) of the survey respondents indicating that they always pay attention to security messages during installation.

These findings suggest that there is evidence of the privacy paradox in operation. As discussed in the literature review, research (Acquisti and Gross, 2006 , Dinev and Hart, 2006) on the privacy paradox has found that users' actual behaviours during privacy transactions contradict with their concerns on privacy risks when disclosing personal information. While users complain about the risks of disclosing such information their beahviours are influenced by low-level rewards and the perceived benefits (Norberg et al., 2007 , Shklovski et al., 2014). In the case of these survey findings, users indicated an awareness that applications required access to the personal data yet only 18% of respondents actually paid attention to what permissions the application asked for. Some respondents did not consider their data valuable enough to anyone:
"I don't have personal data on my phone that I'm concerned about other people seeing."
"I don't think I keep any valuable data on my phone."

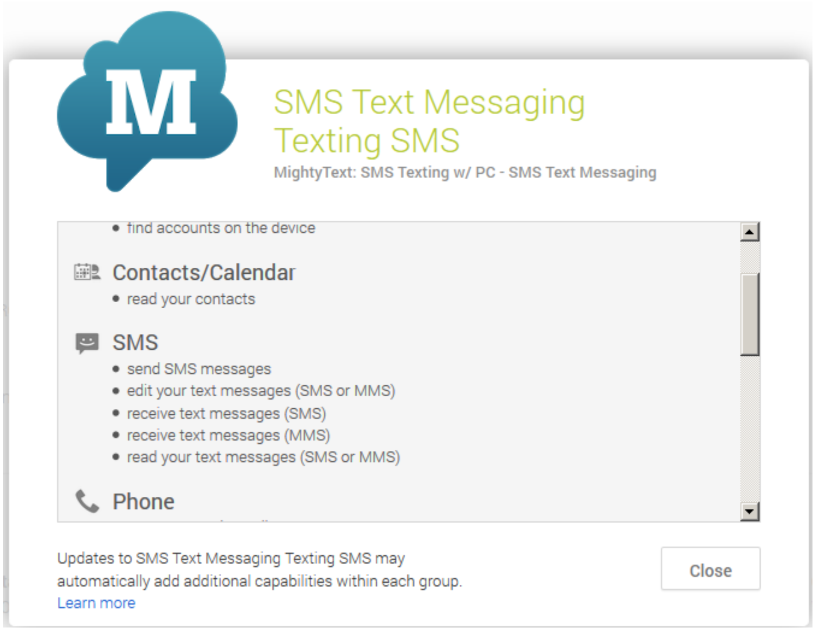
These users tend to believe that their own personal data, photos, contact lists and email addresses are not important enough to be stolen or used elsewhere. However this is not true. This is information about the user, their demographics, behaviours and habits. While the user may think it has little to no value, it is valuable to individuals and companies who are building a profile about the user or simply who want to use that data for nefarious purposes.

When it came to EULA/Terms of Service messages, only 19% indicated they always examine them. This is not surprising and compares with similar research in the area (Vidas et al., 2011 , Felt et al., 2012 , Kelley et al., 2012 , Chin et al., 2012). Such behaviour may be explained by the fact that users have become accustomed to clicking through messages and accepting the terms of service and permissions when installing software and applications (Motiee et al., 2010).

Unfortunately this gives rise to potential security and privacy risks as users blindly click through the installation of the application without really comprehending what it is they are accepting or allowing the application to do. When the developer fails to understand and apply permissions correctly, or chooses not to, there is a risk that the applications they develop will simply request more permissions than strictly necessary for the application to perform its task fully. This idea of permission creep or evolution of permissions is all too easy an event as applications update with new features thus seeking new permissions. Application updating can also be configured to occur automatically in the background and users ultimately stop paying attention altogether over time or may not even be aware of permission issues in the first place.

While the results indicate that survey users were aware that applications were requesting permission to access their data, it also indicated that only 18% of respondents actually paid attention to the permissions an application requested. It was observed that within this survey group, the chi-square test that was conducted indicated that there was no correlation between user awareness of an application requesting access to their private data and their consideration of permissions at install time. Both Google and Apple are attempting to address these concerns through modifications and “improvements” to their prospective platforms.

In an attempt to make it easier for users and developers to understand what an application has access to, Google recently made changes to how permissions are displayed (Google, 2014b). Application permissions are now organised into group of related permissions. For example, an application that wants to read incoming SMS messages would require the “Read SMS messages” permission. With this new change, SMS related permissions are bundled into an “SMS” permission group. If the user installs the application, they are giving it access to all SMS-related permissions. Essentially if they approve one, they approve them all (Figure 5.1).



SMS Text Messaging Texting SMS

MightyText: SMS Texting w/ PC - SMS Text Messaging

- find accounts on the device

Contacts/Calendar

- read your contacts

SMS

- send SMS messages
- edit your text messages (SMS or MMS)
- receive text messages (SMS)
- receive text messages (MMS)
- read your text messages (SMS or MMS)

Phone

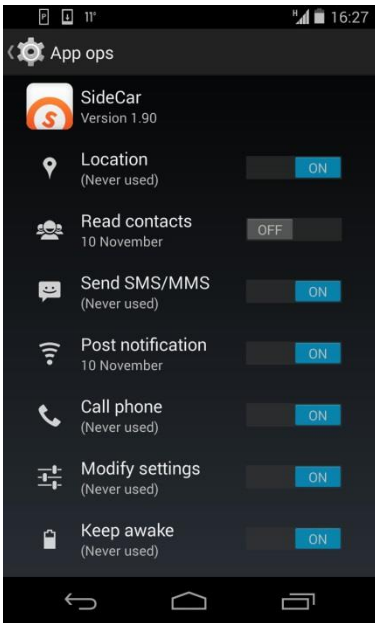
Updates to SMS Text Messaging Texting SMS may automatically add additional capabilities within each group.
Learn more

Figure 5.1 - Android Permission Groups

Although the core concept is good; making the permissions more understandable for users, the implementation exposes security and privacy issues. The problem is that permission groups can contain basic permissions as well as potentially risky permissions. A user might not want the application to have the ability to send SMS messages, thus potentially incurring monetary charges. However the application can automatically update and gain the ability to perform other SMS related tasks such as sending SMS messages without requesting permission.

Users should have control over the data they are sharing. A better approach would be to provide the users with the ability to choose the explicit permissions they want the application to have access to. Currently Android does not allow a user to install an application and subsequently decide which permissions the application can be granted.

Google actually released a feature in Android 4.3 called App Ops which allowed users to manually enable and disable application permissions, thus potentially preventing the application from collecting or accessing sensitive data (Figure 5.2).



App ops

SideCar
Version 1.90

Location
(Never used)
ON

Read contacts
10 November
OFF

Send SMS/MMS
(Never used)
ON

Post notification
10 November
ON

Call phone
(Never used)
ON

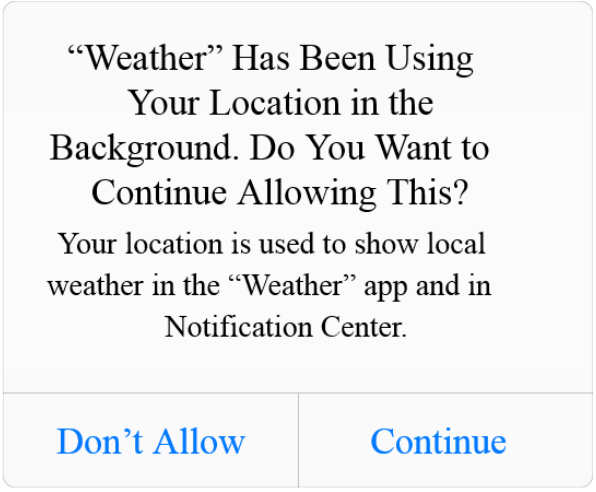
Modify settings
(Never used)
ON

Keep awake
(Never used)
ON

Figure 5.2 - Android App Ops Feature

This was seen as a positive move by the Electronic Frontier Foundation. However this feature was later removed in Android 4.4.2 with Google stating it removed the feature because its experimental nature could break applications (Eckersley, 2013). It could be argued that there is no motivation for Google to prevent users from blocking applications from accessing the Internet. In-app advertising is a revenue generating model for developers and Google want to gather information about users' behaviours. Allowing users to disable such a feature on an application, while beneficial to the user, might not be in Google's best interest.

Apple are also taking steps to further increase transparency surrounding application permissions. In previous iOS versions, once a user granted permission for an application to use personal information, that permission remained in place until the user manually revoked it in iOS Settings or uninstalled the application. With iOS 8 users will have the option of allowing an application to access location data, but only "While [app is] In Use." Users will also be reminded which application have already been granted that permission via a prompt that will ask the user if they want to "continue allowing" the application to use location information in the background (Figure 5.3).



“Weather” Has Been Using Your Location in the Background. Do You Want to Continue Allowing This?

Your location is used to show local weather in the “Weather” app and in Notification Center.

Figure 5.3 - Apple Location Reminder

While the survey findings indicate a high level of awareness amongst respondents of smartphone security risks, another aspect is whether smartphone users are actually concerned about these threats and risks. With respect to the five smartphone security risk scenarios there was not a high level of concern amongst the respondents. They were mostly concerned with improper disposal (32%), spyware (31%) and insecure WiFi (30%). These percentages are low. When asked how concerned they were about the privacy and protection of their personal data on their smartphone, only 30% of the respondents suggested they were either very/extremely concerned.

It was also observed that within this survey group, the chi-square tests that were conducted indicated that there was no correlation between user awareness of a risk and their associated concern about that particular risk. This adds further weight to the privacy paradox discussed previously.

The low level of concern may be due to the fact that respondents have not had anything detrimental occur to cause them to change their level of concern. The majority (71%) of respondents indicated that their smartphone had never been infected by a malicious application. However given that only 22% of respondents surveyed actually had antivirus software on their smartphone, they cannot be certain that they do not have any malicious or privacy invading applications on their smartphone.

Are smartphone users taking any steps to protect their privacy and security, and if so what are they?

Survey respondents were asked what security measures they employed on their smartphone in order to protect themselves. These measures can range from a simple screenlock or password to more sophisticated mechanisms like remote tracking and software wipe. 85% of respondents had activated screenlock or password protection on their smartphone while 55% employed a SIM card PIN number. Given that the SIM card can simply be removed from the smartphone it may be surprising that this figure is not higher, this could suggest that users are less concerned about their SIM being taken although SIM cards can still contain personal data. Using more than one protection mechanism, known as defence in depth, is considered good practice (National Security Agency, 2012). Focussing on the two most popular and easy to implement security mechanisms, it was found that only 52% of respondents activated both with 11% decinding not to use either of these. Survey results indicated that almost half were using the phone for both personal and business use. Thus the lack of security controls can represent a risk to organisations where such practices occur, increasing the likelihood of unauthorised access to data. This workplace trend towards “Bring Your Own Device” (BYOD) is likely to continue as organisations look to raise employee productivity. However BYOD impacts the traditional security model of protecting the organisation’s perimeter by blurring the definition of that perimeter. Organisations will want to protect their assets and thus mobile device management (software that secures, monitors, manages and supports mobile devices within an organisation) should be utilised. Through such software, organisations may insist on the installation of security software on mobile devices that contain work related data. Wilson and Hash (2003, p.7) in their report on security awareness and training pointed out that *“learning is a continuum; it starts with awareness, builds to training and evolves into education.”* Organisations should be developing security awareness and training programs tailored towards mobile devices and ensure their employees take part in the programs. Such programs can educate the users about the security risks and include best practices that users should adopt to protect their own and the company’s assets.

The smartphone IMEI number can be used to identify a mobile device and model thus enabling a network operator to block stolen smartphones, as long as the legitimate owner can provide the IMEI. A surprisingly high number of survey respondents had indicated that they had recorded their IMEI number. While the figure was still less than half (49%), this was considerably higher than that from a study by the Hong Kong Office of the Privacy Commissioner for Personal Data (2012) where only 9.5% of their respondents had done so.

5.2.2 Further Observations of Interest

The findings of the survey indicated that the vast majority (99%) of the respondents downloaded applications from the official app stores. 69% of these users believed applications downloaded from the official app stores were safe. However 57% of the respondents did not know whether there were any security review mechanisms in place on these official app stores. Mayer et al. (1995) defines trust as the "*willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."*

Based on this definition, the findings would suggest that users trust the official application stores. Is this trust misplaced?

From a negative perspective these official application stores represent a single large attack vector for malicious applications. If a malicious application is submitted to the store, users who download and install the application may be affected by whatever underlying malevolent activities the application performs, potentially compromising the security and privacy of the user. Unfortunately there have been numerous instances reported where fake malicious applications have appeared on the Google Play Market (Symantec, 2013b , Symantec, 2013e , Symantec, 2013d , Symantec, 2013a). RiskIQ (2014) reported that malicious mobile applications in the Google Play market increased 400% in 2013. However Riskiq did not provide actual figures thus the baseline figure may have been low to begin with. Spurious applications have also been found in the past on Amazon (Symantec, 2013b) and Apple App Store (TechCrunch, 2012), albeit in far fewer numbers than Google Play.

Although it only takes one wrong click to get infected; as discussed in the literature review, the reality is that the risk of exposure to a malicious application through an official store such as Google Play or Apple App Store is low. By default an Android phone does not allow users to install applications from unknown sources and most users would not have a need to do so. However users in certain countries do not have access to the official app stores. Thus they rely on installing applications from third-party websites which tend to not have the same level of due diligence that the likes of Apple App Store or Google Play. As indicated in section 5.4, there is an opportunity for further research in this area.

The majority of survey respondents did not install security software on their smartphones. This contrasted with the finding that 100% of the respondents did use some form of security software on their Pc/Laptop/desktop indicating either a lack of awareness or concern regarding the threats and controls that exist on the smartphone. Respondents were evenly split at 50% each as to whether they considered antivirus software to be essential with some users indicating that they did not feel they had anything worthwhile or important enough to be stolen. Other users suggested that technological parameters (battery life, device performance) and the fact they had never been affected by smartphone malware were factors that influenced their decision not to install antivirus software on their smartphone.

5.3 Limitations of Research

The research does have a number of limitations.

According to Saunders et al. (2012, p.671), generalisability is the extent to which the findings of a research study are applicable to other settings. This particular research looked at the extent of user awareness of potential security risks when using their smartphones. While the study would be of interest to fellow researchers involved in smartphone security, it is not possible to generalise the findings of the research due to a number of constraints:

- Convenience sampling was used because the researcher was unable to access the target population using other sampling techniques within the time frame and financial constraints of the study. The drawbacks with this method are sampling bias and that the sample is unlikely to be representative of the entire population.
- A sample set of 143 respondents were included in the analysis which, given the sampling mechanism used, would not fully represent the smartphone user population.
- An online survey was used as the distribution method. Such methods tend to have a low response rate (Sauermann and Roach, 2013 , Rogelberg and Stanton, 2007) and thus can serve to undermine the perceived credibility and actual generalisability of the collected data.

The research focussed more on utilising a quantitative data analysis approach as opposed to a qualitative data one. It was observed that respondents to a number of the Likert scale questions tended to group around the “moderately concerned” response. This seemed to suggest a certain “sit on the fence” demeanour with respect to the question at hand. A number of questions in the survey were also open-ended and some of the responses to these questions were interesting. Further interviews with individuals may have provided extra insight into their security awareness in general. It would have provided an opportunity for the researcher to explore more regarding the “sit on the fence” behaviour for some of the questions and may have resulted in other findings or concerns that were not captured by the online survey.

Another minor limitation was observed regarding the survey design. A number of the questions asked respondents whether they were aware that a particular risk could happen. These were followed by asking the respondents how concerned they were about that risk happening to them. It could be argued that a user would not be concerned about something they have no awareness of, thus skip logic could have been used to redirect individuals who answered no to the risk awareness question away from the subsequent level of concern question about the risk.

5.4 Future Research Opportunities

This study is based on a convenience sample frame of users predominantly situated in Ireland. As indicated in the methodology chapter such an approach is likely to introduce sampling bias and that the sample is unlikely to be representative of the entire population.

There is certainly scope to perform a similar study in different demographical locations. This would be interesting because, due to various issues (political and otherwise), users in certain countries do not have access to the official app stores. Thus they rely on installing applications from third-party websites which tend to not have the same level of due diligence that the likes of Apple App Store or Google Play Store would have. Indeed according to a recent report by Lookout (2014), the encounter rate of malware drastically changes depending on your geographical location. In the US it is only 4%, while in Russia and China it is 63% and 28% respectively. Would users in those regions have the same high level of awareness and low level of concern?

Furthermore as this research used a survey, which is predominantly a quantitative data analysis technique, there is scope to explore the findings further with interviews and workshops to garner more qualitative responses.

5.5 Concluding Remarks

Smartphones have become ubiquitous and as the prevalence of smart devices, in general, continues to grow, they will become more ingrained in everyday life. Already there are smart watches and wearable devices that allow people to monitor and track many aspects of their lives, experiences and achievements. Given the amount of personal data being generated and transmitted by such devices, privacy and security become important considerations for users. (Barcena et al., 2014)

In the workplace, the trend towards “Bring Your Own Device” will see more and more smartphones being used for both personal and business use. Organisations will want to protect their assets and thus mobile device management (software that secures, monitors, manages and supports mobile devices within an organisation) and security awareness programs tailored towards mobile devices will also emerge.

This dissertation surveyed a sample set of users drawn from convenience sampling. It found that there was a high level of awareness and generally a low level of concern amongst the respondents with respect to the smartphone security risks. However the threat landscape is a continually evolving one and users need to remain vigilant. The “bad guys” have already turned their attention to the smart device domain. It only takes one wrong click to have your personal data stolen.

6 References

Acquisti, A. & Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy enhancing technologies, 2006. Springer, 36-58.

Alliance, S. C. 2011. The Mobile Payments and NFC Landscape: A US Perspective. *Smart Card Alliance*.

Appbrain. 2014a. *Free vs. paid Android apps* [Online]. Available: http://www.appbrain.com/stats/free-and-paid-android-applications [Accessed 19th January 2014].

Appbrain. 2014b. *Number of available Android applications* [Online]. Available: http://www.appbrain.com/stats/number-of-android-apps [Accessed 19th January 2014].

Apple. 2013. *Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues* [Online]. Apple. Available: http://support.apple.com/kb/ht3743 [Accessed 26th March 2014].

Apple. 2014a. *Find My iPhone, iPad, and Mac* [Online]. Available: http://www.apple.com/icloud/find-my-iphone.html [Accessed 22nd July 2014].

Apple. 2014b. *iOS 6: Understanding Location Services* [Online]. Available: http://support.apple.com/kb/HT5467 [Accessed 20th January 2014].

Apple. 2014c. *iOS Developer Program* [Online]. Available: https://developer.apple.com/programs/ios/ [Accessed 20th January 2014].

Awad, N. F. & Krishnan, M. S. 2006. The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly,* 30**,** 13-28.

Aycock, J. 2006. *Computer Viruses and malware*, Springer.

Barcena, M. B., Wueest, C. & Lau, H. 2014. *How Safe is Your Quantified Self?* [Online]. Symantec. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf [Accessed 6th August 2014].

Barnes, S. B. 2006. A privacy paradox: Social networking in the United States. *First Monday,* 11.

Barrera, D. & Van Oorschot, P. 2011. Secure software installation on smartphones. *Security & Privacy, IEEE,* 9**,** 42-48.

Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S. & Wolf, C. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. Security and Privacy (SP), 2011 IEEE Symposium on, 22-25 May 2011 2011. 96-111.

Bloomberg. 2013. *Ask a Billionaire: Eric Schmidt's 2014 Predictions* [Online]. Bloomberg. Available: http://www.bloomberg.com/video/ask-a-billionaire-eric-schmidt-s-2014-predictions-pmV~qd7qTeipbjKx6_wW1Q.html [Accessed 2nd February 2014].

Bordianu, V., Benchea, R. & Gavrilut, D. 2013. Google and Apple Markets; Are Their Applications Really Secure? *Virus Bulletin***,** 51-56.

Bryman, A. & Bell, E. 2011. *Business Research Methods 3e*, Oxford university press.

Business Wire. 2009. *IDC Predicts Worldwide Mobile Phone Shipments To Fall 8.3% in 2009* [Online]. Available: http://www.businesswire.com/news/home/20090311006368/en/IDC-Predicts-Worldwide-Mobile-Phone-Shipments-Fall#.UuO1qrTFLOE [Accessed 25th January 2014].

Carty, E. 2013. Free wifi ‘putting users at risk from hackers’. *Irish Examiner*.

Chin, E., Felt, A. P., Sekar, V. & Wagner, D. 2012. Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security.* Washington, D.C.: ACM.

Chu, E. 2008. *Android Market: Now available for users* [Online]. Available: http://android-developers.blogspot.ie/2008/10/android-market-now-available-for-users.html [Accessed 25th January 2014].

Cisco. 2014. *Cisco 2014 Annual Security Report* [Online]. Cisco. Available: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf [Accessed 26th March 2014].

Commision for Communications Regulation 2014. Irish Communications Market: Key Data Report – Q1 2014. Commision for Communications Regulation,.

Creswell, J. W. 2012. Educational research : planning, conducting, and evaluating quantitative and qualitative research. 4th ed. Boston: Pearson.

Crotty, M. 1998. *The foundations of social research: Meaning and perspective in the research process*, Sage.

Dictionary.Com 2014. Online Etymology Dictionary.

Dillman, D. A., Smyth, J. D. & Christian, L. M. 2009. Internet, mail, and mixed-mode surveys: The tailored design method . Hoboken. NJ: Wiley.

Dinev, T. & Hart, P. 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research,* 17**,** 61-80.

Dublin Bus. 2014. *All Aboard with Free Wi-Fi on all routes* [Online]. Available: http://www.dublinbus.ie/en/News-Centre/Media-Releases-Archive1/All-aboard-Dublin-Bus-with-Free-Wi-Fi-on-all-routes/ [Accessed 23rd August 2014].

Eckersley, P. 2013. *Google Removes Vital Privacy Feature From Android, Claiming Its Release Was Accidental* [Online]. Electronic Frontier Foundation. Available: https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy-features-android-shortly-after-adding-them [Accessed 22nd July 2014].

Egele, M., Kruegel, C., Kirda, E. & Vigna, G. 2011. PiOS: Detecting Privacy Leaks in iOS Applications. *NDSS.* The Internet Society.

Enisa. 2010. *Top Ten Smartphone Risks* [Online]. Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks [Accessed 3rd May 2014].

European Union Agency for Network and Information Security. 2009. *Glossary* [Online]. Available: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary [Accessed 3rd May 2014].

Evans, J. R. & Mathur, A. 2005. The value of online surveys. *Internet Research,* 15**,** 195-219.

F-Secure Report. 2013. *Mobile Threat Report* [Online]. F-Secure. Available: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf [Accessed 20th January 2014].

Felt, A. P., Chin, E., Hanna, S., Song, D. & Wagner, D. Android permissions demystified. Proceedings of the 18th ACM conference on Computer and communications security, 2011a. ACM, 627-638.

Felt, A. P., Finifter, M., Chin, E., Hanna, S. & Wagner, D. 2011b. A survey of mobile malware in the wild. *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices.* Chicago, Illinois, USA: ACM.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. 2012. Android permissions: user attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security.* Washington, D.C.: ACM.

Forman, C., Ghose, A. & Wiesenfeld, B. 2008. Examining the Relationship Between Reviews and Sales: The Role of Reviewer Identity Disclosure in Electronic Markets. *Information Systems Research,* 19**,** 291-313.

Furnell, S. 2005a. Handheld hazards: The rise of malware on mobile devices. *Computer Fraud & Security,* 2005**,** 4-8.

Furnell, S. 2005b. Why users cannot use security. *Computers & Security,* 24**,** 274-279.

Furnell, S. 2007. Making security usable: Are things improving? *Computers & Security,* 26**,** 434-443.

Furnell, S. M., Jusoh, A. & Katsabas, D. 2006. The challenges of understanding and using security: A survey of end-users. *Computers & Security,* 25**,** 27-35.

Garfinkel, S. 2005. *Design principles and patterns for computer systems that are simultaneously secure and usable.* Massachusetts Institute of Technology.

Gartner. 2013a. *Gartner Identifies the Top 10 Strategic Technology Trends for 2014* [Online]. Available: http://www.gartner.com/newsroom/id/2603623 [Accessed 1st July 2014].

Gartner. 2013b. *IT Glossary* [Online]. Available: http://www.gartner.com/it-glossary/smartphone [Accessed 15th January 2014].

Gennari, J. & French, D. Defining malware families based on analyst insights. Technologies for Homeland Security (HST), 2011 IEEE International Conference on, 15-17 Nov. 2011 2011. 396-401.

Google. 2014a. *Android Device Manager* [Online]. Available: https://support.google.com/accounts/answer/3265955?hl=en [Accessed 22nd July 2014].

Google. 2014b. *Review app permissions* [Online]. Available: https://support.google.com/googleplay/answer/6014972?p=app_permissions [Accessed 20th August 2014].

Google Play Store. 2014a. *Featured App Lists* [Online]. Available: https://support.google.com/googleplay/android-developer/answer/1295940?hl=en [Accessed 7th March 2014].

Google Play Store. 2014b. *Google Play Store* [Online]. Available: https://play.google.com/store [Accessed 18th January 2014].

Google Support. 2014. *Developer Registration* [Online]. Available: https://support.google.com/googleplay/android-developer/answer/113468?hl=en&ref_topic=3450781&rd=1 [Accessed 19th January 2014].

Guo, C., Wang, H. J. & Zhu, W. Smart-phone attacks and defenses. HotNets III, 2004.

Hamblen, M. 2009. *Cell phone, smartphone -- what's the difference?* [Online]. computerworld. Available: http://www.computerworld.com/s/article/9129647/Cell_phone_smartphone_what_s_the_difference_? [Accessed 15th January 2014].

Han, J., Kywe, S. M., Yan, Q., Bao, F., Deng, R., Gao, D., Li, Y. & Zhou, J. Launching generic attacks on ios with approved third-party applications. Applied Cryptography and Network Security, 2013. Springer, 272-289.

Hirschheim, R., Klein, H. K. & Lyytinen, K. 1995. *Information systems development and data modeling: conceptual and philosophical foundations*, Cambridge University Press.

Hogben, G. & Dekker, M. 2010. Smartphones: Information security risks, opportunities and recommendations for users. *European Network and Information Security Agency,* 710.

Hong Kong Office of the Privacy Commissioner for Personal Data 2012. *Report on Privacy Awareness Survey on Smartphones and Smartphone Apps*, Office of the Privacy Commissioner for Personal Data.

Hoofnagle, C. J., King, J., Li, S. & Turow, J. 2010. How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*.

Hypponen, M. 2006. Malware goes mobile. *Scientific American,* 295**,** 70-77.

Information Security Forum 2011. The 2011 Standard of Good Practice for Information Security.

International Organization for Standardization 2008. Information technology - Security techniques - Information security risk management (ISO/IEC 27005:2008).

Juniper Networks. 2014. *Third Annual Mobile Threats Report* [Online]. Available: http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf [Accessed 26th January 2014].

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B. & Greer, C. 2013. Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies,* 71**,** 1163-1173.

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N. & Wetherall, D. 2012. A conundrum of permissions: Installing applications on an android smartphone. *Financial Cryptography and Data Security.* Springer.

Kimura, H. 2014. *Meet the Fakers - Profiles of Suspected Fake Apple App Store User Accounts* [Online]. Available: http://blog.sensortower.com/blog/2014/03/21/meet-the-fakers-profiles-of-suspected-fake-apple-app-store-user-accounts/ [Accessed 7th July 2014].

King, J. “How Come I’m Allowing Strangers To Go Through My Phone?”—Smartphones and Privacy Expectations. Symposium on Usable Privacy and Security (SOUPS), 2013.

Kruger, H. A. & Kearney, W. D. 2006. A prototype for assessing information security awareness. *Computers & Security,* 25**,** 289-296.

Laugesen, J. & Yuan, Y. What factors contributed to the success of Apple's iPhone? Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010 Ninth International Conference on, 2010. IEEE, 91-99.

Lever, C., Antonakakis, M., Reaves, B., Traynor, P. & Lee, W. The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers. 20th Annual Network & Distributed System Security Symposium, 2013.

Linden, J. 2013. *Lookout Tours the Current World of Mobile Threats* [Online]. Lookout. Available: https://blog.lookout.com/blog/2013/06/05/world-current-of-mobile-threats/ [Accessed 28th January 2014].

Lockheimer, H. 2012. *Android and Security* [Online]. Available: http://googlemobile.blogspot.ie/2012/02/android-and-security.html [Accessed 7th March 2014].

Lookout. 2014. *Mobile Threats, Made to Measure* [Online]. Available: https://www.lookout.com/static/ee_images/Mobile_Threats_Made_to_Measure_Lookout_Report_2013.pdf [Accessed 6th August 2014].

Ludwig, A., Davis, E. & Larimer, J. 2013. Android – practical security from the ground up. *Virus Bulletin.* Berlin.

Maslennikov, D. 2013. *Mobile Malware Evolution: Part 6* [Online]. Securelist. Available: http://www.securelist.com/en/analysis/204792283/Mobile_Malware_Evolution_Part_6 [Accessed 22nd January 2014].

Mathisen, J. 2004. Measuring Information Security Awareness. A survey showing the Norwegian way to do it.

Mayer, R. C., Davis, J. H. & Schoorman, F. D. 1995. An Integrative Model of Organizational Trust. *The Academy of Management Review,* 20**,** 709-734.

Mcdaniel, P. & Enck, W. 2010. Not So Great Expectations: Why Application Markets Haven't Failed Security. *Security & Privacy, IEEE,* 8**,** 76-78.

Mell, P., Kent, K. & Nusbaum, J. 2005. *Guide to malware incident prevention and handling*, US Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Milberg, S. J., Smith, H. J. & Burke, S. J. 2000. Information privacy: Corporate management and national regulation. *Organization science,* 11**,** 35-57.

Misra, A. & Dubey, A. 2013. *Android Security: Attacks and Defenses*, Auerbach Pub.

Motiee, S., Hawkey, K. & Beznosov, K. Do windows users follow the principle of least privilege?: investigating user account control practices. Proceedings of the Sixth Symposium on Usable Privacy and Security, 2010. ACM, 1.

Müller, R. M., Kijl, B. & Martens, J. K. 2011. A comparison of inter-organizational business models of mobile App Stores: there is more than open vs. closed. *Journal of theoretical and applied electronic commerce research,* 6**,** 63-76.

Mylonas, A., Dritsas, S., Tsoumas, B. & Gritzalis, D. 2012. On the feasibility of malware attacks in smartphone platforms. *E-Business and Telecommunications.* Springer.

Mylonas, A., Gritzalis, D., Tsoumas, B. & Apostolopoulos, T. 2013a. A Qualitative Metrics Vector for the Awareness of Smartphone Security Users. *In:* FURNELL, S., LAMBRINOUDAKIS, C. & LOPEZ, J. (eds.) *Trust, Privacy, and Security in Digital Business.* Springer Berlin Heidelberg.

Mylonas, A., Kastania, A. & Gritzalis, D. 2013b. Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security,* 34**,** 47-66.

National Security Agency. 2012. *Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments* [Online]. Available: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf [Accessed 22nd July 2014].

Norberg, P. A., Horne, D. R. & Horne, D. A. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs,* 41**,** 100-126.

O' Brien, D. & Torres, A. M. 2012. Social Networking and Online Privacy: Facebook Users' Perceptions. *Irish Journal of Management,* 31**,** 63-97.

Oberheide, J. & Miller, C. 2012. Dissecting the android bouncer. *SummerCon2012, New York*.

Okenyi, P. O. & Owens, T. J. 2007. On the Anatomy of Human Hacking. *Information Systems Security,* 16**,** 302-314.

Oliner, A., Iyer, A. P., Stoica, I., Lagerspetz, E. & Tarkoma, S. 2013. Carat: Collaborative Energy Diagnosis for Mobile Devices.

Open Handset Alliance. 2007a. *Industry Leaders Announce Open Platform for Mobile Devices* [Online]. Open Handset Alliance. Available: http://www.openhandsetalliance.com/press_110507.html [Accessed 18th January 2014].

Open Handset Alliance. 2007b. *Open Handset Alliance Releases Android SDK* [Online]. Available: http://www.openhandsetalliance.com/press_111207.html [Accessed 18th January 2014].

Orland, K. 2014. *Pay to rank: Gaming the App Store in the age of Flappy Bird* [Online]. Available: http://arstechnica.com/gaming/2014/02/pay-to-rank-gaming-the-app-store-in-the-age-of-flappy-bird/ [Accessed 7th July 2014].

Percoco, N. & Schulte, S. 2012. Adventures in BouncerLand: Failures of Automated Malware Detection within Mobile Application Markets. *Black Hat USA 2012*.

Phelps, J., Nowak, G. & Ferrell, E. 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing,* 19**,** 27-41.

Ponemon Institute. 2011. *Smartphone Security - Survey of US Consumers* [Online]. Available: aa-download.avg.com/filedir/other/Smartphone.pdf.

Powell, T. C. 2001. Competitive advantage: Logical and philosophical considerations. *Strategic Management Journal,* 22**,** 875-888.

Raiu, C. & Emm, D. 2013. *Kaspersky Security Bulletin 2013* [Online]. Available: http://media.kaspersky.com/pdf/KSB_2013_EN.pdf [Accessed 27th January 2014].

Ramu, S. 2012. Mobile Malware Evolution, Detection and Defense.

Rasmussen, J. 1997. Risk management in a dynamic society: a modelling problem. *Safety science,* 27**,** 183-213.

Rinne, J.-P. 2013. The Current State of NFC Payments in Finland: An exploratory study on the attitudes and opinions towards NFC payments.

Riskiq. 2014. *RiskIQ Reports Malicious Mobile Apps in Google Play Have Spiked Nearly 400 Percent* [Online]. Symantec. Available: http://www.riskiq.com/company/press-releases/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400 [Accessed 4th July 2014].

Rogelberg, S. G. & Stanton, J. M. 2007. Introduction understanding and dealing with organizational survey nonresponse. *Organizational Research Methods,* 10**,** 195-209.

Saltzer, J. H. & Schroeder, M. D. 1975. The protection of information in computer systems. *Proceedings of the IEEE,* 63**,** 1278-1308.

Sauermann, H. & Roach, M. 2013. Increasing web survey response rates in innovation research: An experimental study of static and dynamic contact design features. *Research Policy,* 42**,** 273-286.

Saunders, M., Lewis, P. & Thornhill, A. 2012. *Research Methods for Business Students*, Prentice Hall.

Schmidt, A.-D., Schmidt, H.-G., Batyuk, L., Clausen, J. H., Camtepe, S. A., Albayrak, S. & Yildizli, C. Smartphone malware evolution revisited: Android next target? Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on, 2009. IEEE, 1-7.

Schneier, B. 2000. *Secrets \& Lies: Digital Security in a Networked World*, John Wiley \&amp; Sons, Inc.

Schwandt, T. A. 1994. Constructivist, interpretivist approaches to human inquiry. *Handbook of qualitative research (1994) Denzin, Norman K.; Lincoln, Yvonna S.. Thousand Oaks: Sage Publications.*

Selm, M. & Jankowski, N. 2006. Conducting Online Surveys. *Quality and Quantity,* 40**,** 435-456.

Shevchenko, A. 2005. *An overview of mobile device security* [Online]. Securelist. Available: http://www.securelist.com/en/analysis?pubid=170773606 [Accessed 22nd January 2014].

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H. & Borgthorsson, H. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. Proceedings of the 32nd annual ACM conference on Human factors in computing systems, 2014. ACM, 2347-2356.

Song, C., Park, K. & Kim, B. C. 2013. Impact of Online Reviews on Mobile App Sales: Open Versus Closed Platform Comparison.

Spiekermann, S., Grossklags, J. & Berendt, B. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. Proceedings of the 3rd ACM conference on Electronic Commerce, 2001. ACM, 38-47.

Stone, E. F., Gueutal, H. G., Gardner, D. G. & Mcclure, S. 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology,* 68**,** 459.

Stutzman, F., Gross, R. & Acquisti, A. 2013. Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality,* 4**,** 2.

Symantec. 1999. *Trojan.KillAV* [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2002-071813-0943-99 [Accessed 25th January 2014].

Symantec. 2004. *SymbOS.Cabir* [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2004-061419-4412-99 [Accessed 21st January 2014].

Symantec. 2011. *Trojan.Badfaker* [Online]. Available: http://www.symantec.com/security_response/writeup.jsp?docid=2011-072908-3121-99 [Accessed 25th January 2014].

Symantec. 2013a. *Another Fake Application for Android Found on Google Play* [Online]. Symantec. Available: http://www.symantec.com/connect/blogs/another-fake-application-android-found-google-play [Accessed 4th July 2014].

Symantec. 2013b. *Busy August for One-Click Fraud Scammers on Google Play* [Online]. Symantec. Available: http://www.symantec.com/connect/blogs/busy-august-one-click-fraud-scammers-google-play [Accessed 4th July 2014].

Symantec. 2013c. *Internet Security Threat Report* [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf [Accessed 20th January 2014].

Symantec. 2013d. *Japanese One-Click Fraud on Google Play Leads to Data Stealing App* [Online]. Symantec. Available: http://www.symantec.com/connect/blogs/japanese-one-click-fraud-google-play-leads-data-stealing-app [Accessed 4th July 2014].

Symantec. 2013e. *Yet Another Bunch of Malicious Apps Found on Google Play* [Online]. Symantec. Available: http://www.symantec.com/connect/blogs/yet-another-bunch-malicious-apps-found-google-play [Accessed 4th July 2014].

Symantec. 2014a. *Instagram Users Compromise Their Own Accounts for Likes* [Online]. Available: http://www.symantec.com/connect/blogs/instagram-users-compromise-their-own-accounts-likes [Accessed 25th March 2014].

Symantec. 2014b. *Malware* [Online]. Symantec. Available: http://us.norton.com/security_response/malware.jsp [Accessed 25th January 2014].

Symantec. 2014c. *Prevalence* [Online]. Symantec. Available: http://www.symantec.com/security_response/glossary/define.jsp?letter=p&word=prevalence [Accessed 25th January 2014].

Techcrunch. 2012. *Apple Kicks Chart Topping Fakes Out Of App Store* [Online]. Available: http://techcrunch.com/2012/02/03/app-store-fakes/ [Accessed 4th July 2014].

Theoharidou, M., Mylonas, A. & Gritzalis, D. 2012. A Risk Assessment Method for Smartphones. *In:* GRITZALIS, D., FURNELL, S. & THEOHARIDOU, M. (eds.) *Information Security and Privacy Research.* Springer Berlin Heidelberg.

Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., Mcdaniel, P. & La Porta, T. On cellular botnets: measuring the impact of malicious devices on a cellular network core. Proceedings of the 16th ACM conference on Computer and communications security, 2009. ACM, 223-234.

Trend Micro 2013. TrendLabs 3Q 2013 Security Roundup - The Invisible Web Unmasked. Trend Micro.

Trend Micro. 2014. *Malware* [Online]. Trend Micro. Available: http://about-threats.trendmicro.com/us/definition/malware [Accessed 25th January 2014].

Truong, H. T. T., Lagerspetz, E., Nurmi, P., Oliner, A. J., Tarkoma, S., Asokan, N. & Bhattacharya, S. 2013. The Company You Keep: Mobile Malware Infection Rates and Inexpensive Risk Indicators. *arXiv preprint arXiv:1312.3245*.

Truste 2014. TRUSTe 2014 US Consumer Confidence Privacy Report.

Uscilowski, B. 2013. Mobile Adware and Malware Analysis. Symantec.

Vacca, J. R. 2012. *Computer and information security handbook*, Newnes.

Van Der Meulen, R. & Rivera, J. 2013a. *Gartner Says Asia/Pacific Led Worldwide Mobile Phone Sales to Growth in First Quarter of 2013* [Online]. Gartner. Available: http://www.gartner.com/newsroom/id/2482816 [Accessed 13th January 2014].

Van Der Meulen, R. & Rivera, J. 2013b. *Gartner Says Smartphone Sales Accounted for 55 Percent of Overall Mobile Phone Sales in Third Quarter of 2013* [Online]. Gartner. Available: http://www.gartner.com/newsroom/id/2623415 [Accessed 13th January 2014].

Van Der Meulen, R. & Rivera, J. 2013c. *Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First*

Time [Online]. Gartner. Available: http://www.gartner.com/newsroom/id/2573415 [Accessed 13th January 2014].

Van Der Meulen, R. & Rivera, J. 2014. *Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013* [Online]. Gartner. Available: http://www.gartner.com/newsroom/id/2665715 [Accessed 21st July 2014].

Vidas, T., Christin, N. & Cranor, L. Curbing android permission creep. Proceedings of the Web, 2011.

Wand, Y. & Weber, R. 1993. On the ontological expressiveness of information systems analysis and design grammars. *Information Systems Journal,* 3**,** 217-237.

Warren, C. 2013. *Google Play Hits 1 Million Apps* [Online]. Available: http://mashable.com/2013/07/24/google-play-1-million/ [Accessed 19th January 2014].

Weintraub, S. 2011. *Industry first: Smartphones pass PCs in sales* [Online]. Available: http://fortune.com/2011/02/07/industry-first-smartphones-pass-pcs-in-sales/ [Accessed 7th July 2014].

Weiser, M. 1991. The Computer for the 21st Century. *Scientific american,* 265**,** 94-104.

West, J. & Mace, M. 2010. Browsing as the killer app: Explaining the rapid success of Apple's iPhone. *Telecommunications Policy,* 34**,** 270-286.

Westin, A. F. 1967. Privacy and freedom.

Whitten, A. & Tygar, J. D. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, 1999. McGraw-Hill.

Wilson, M. & Hash, J. 2003. Building an Information Technology Security Awareness and Training Program. *NIST Special Publication,* 800**,** 50.

Xu, H., Luo, X., Carroll, J. M. & Rosson, M. B. 2011. The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems,* 51**,** 42-52.

Zheng, P. & Ni, L. M. 2006. Spotlight: the rise of the smart phone. *Distributed Systems Online, IEEE,* 7.

7 Appendices

7.1 Appendix A - Ethics Application Form

School of Computer Science and Statistics

Research Project Proposal

1. Title of project:
The Security Awareness of the Smartphone User

2. Purpose of project including academic rationale:
Smartphones have grown tremendously in popularity in recent years. The global smartphone market topped 1 billion shipments for the first time in 2013. As smartphones become more ubiquitous it is likely that they will be increasingly targeted by malicious individuals intent on stealing a user's personal and private data. The purpose of this research is to investigate to what extent smartphone users are aware of the security risks associated with smartphone usage and what preventative behaviours they employ.

3. Brief description of methods and measurements to be used:
The data collection will be done via online questionnaire on SurveyMonkey.
The survey can be seen on
https://www.surveymonkey.com/s.aspx?PREVIEW_MODE=DO_NOT_USE_THIS_LINK_FOR_COLLECTION&sm=DnMN2rVdGBxt7JGvDy2TTRRhmGEKFI3jb5FE8SSs1Vw%3d
Please note this is the preview mode of the survey.

4. Participants - recruitment methods, number, age, gender, exclusion/inclusion criteria, including statistical justification for numbers of participants:

- Any participant can answer the survey once they read the participant information sheet and are at least 18 years old and agree to the declarations within the Informed Consent Form displayed on the survey.
- An invitation email will be sent to friends and colleagues asking for their participation in the online survey.
- A permission letter will be sent to the Symantec Human Resources Manager in order to receive permission for their prospective employees to take part in the Survey.
- Candidate recruitment will be via email (fellow classmates on my course, friends and family, work mailing list pending the permission from Symantec HR Manager).

5. Debriefing arrangements:
Given the nature of the survey regarding privacy risks for Smartphone users, I will provide some information links at the end of the survey for respondents who are interesting in learning more about the threats and how they can protect themselves on their mobile devices.

6. A clear concise statement of the ethical considerations raised by the project and how you intend to deal with them:

I can certify that no actual or potential ethical issues have been identified as resulting from the research proposal. There are no risks to the participant. In the unlikely event that a participant is concerned after completing the survey they are provided with a number of information links that can provide some guidance as to how they can protect themselves on their mobile devices.

7. Cite any relevant legislation relevant to the project with the method of compliance e.g. Data Protection Act etc.

The SurveyMonkey questionnaire and responses can only be accessed using my own personal SurveyMonkey account, which is protected by strong password. The questionnaire and the access to the responses will be done via secure and encrypted Internet access - i.e. https (please note this will be available only after I receive Ethics approval and the survey is actually published).

Data confidentiality will be provided to the fullest extent possible by law under the terms defined by the data protection act 1988.

School of Computer Science and Statistics

Participant Information Sheet

Title

The Security Awareness of the Smartphone User

Researcher Contact Details

Name: Conor Murray

Email: murrac13@tcd.ie

Background of Research

Smartphones have grown tremendously in popularity in recent years. The global smartphone market topped 1 billion shipments for the first time in 2013. As smartphones become more ubiquitous it is likely that they will be increasingly targeted by malicious individuals intent on stealing a user's personal and private data. The purpose of this research is to investigate to what extent smartphone users are aware of the security risks associated with smartphone usage.

Publication

Results of the survey will form part of a dissertation for the degree of Masters of Science in Management of Information Systems at the School of Computer Science and Statistics, Trinity College Dublin. This dissertation will be submitted to the School of Computer Science and Statistics in September 2014.

Procedures of this Study

- This study is based on an online survey that should take no more than 15 minutes to complete.
- Participation is voluntary.
- Individual responses are aggregated anonymously and research reported on the aggregate results
- Your responses will be treated with full confidentiality and, if published, will not be identifiable as yours.
- Each question is optional. Feel free to omit a response to any question; however I would be grateful if all questions were responded to.
- You have the right to withdraw from the survey at any time during the process by clicking the "Exit This Survey" button and your answers will not be recorded.

Potential Conflict of Interest

I would like to declare a potential conflict of interest in that a number of participants completing this survey will be colleagues of mine working at Symantec.

Other Information

- I am required to inform you that, in the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities.

- Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.

School of Computer Science and Statistics

Participant Informed Consent Form

DECLARATION

- I am 18 years or older and am competent to provide consent
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- Since this research involves viewing materials via a computer monitor I understand that if I or anyone in my family has a history of epilepsy then I am proceeding at my own risk.

Researcher Contact Details

Name: Conor Murray

Email: murrac13@tcd.ie

Supervisor Contact Details

Name: Aideen Keaney

Email: akeaney@tcd.ie

By submitting this form you are indicating that you have read the description of the study, are over the age of 18, and that you agree to the terms as described.

Thank you in advance for your participation!

Conor Murray

School of Computer Science and Statistics

Participant Email for Survey

Hello,

My name is Conor Murray and I am a student in the School of Computer Science and Statistics, at Trinity College Dublin. I am researching to what extent Smartphone users are aware of the security risks associated with smartphone usage. I am inviting participants to complete an online survey in order to gain an insight into how individuals use their Smartphone and their understanding and awareness of Smartphone security risks.

The survey forms part of my final year research project for my masters in the Management of Information Systems.

The survey is online and takes no longer than 15 minutes to complete. I hope that you will find this an interesting exercise and it will help me in completing my research.
I would be very grateful if you could take the time to complete the survey.
The web link to the online survey is:

https://www.surveymonkey.com/<Full URL to be added once Ethics approval is received>

I attach an information sheet for survey participants, which explains the background to the research, the procedure, important notes and what happens to the survey findings.
Should you have any questions please do not hesitate to contact me.

Kindest Regards,

Conor Murray

School of Computer Science and Statistics

Symantec Human Resources (Board of Management) Informed Consent Form

Dear Sir/Madam,

I am working on a research project for my masters in Management of Information Systems at Trinity College Dublin. The purpose of this research is to investigate to what extent smartphone users are aware of the security risks associated with smartphone usage.

I would like to request permission to provide your employees with a link to my online survey at

https://www.surveymonkey.com/<Full URL to be added once Ethics approval is received>

I have also attached the following documents for your perusal:

• An information sheet, also provided online within the survey, which explains the background to the research question, the procedure, and what happens to the survey findings
• An informed consent form which is also provided online at the initiation of the survey and must be accepted prior to survey commencement.

If the above request meets your approval, could I ask that you please sign the form below and return to me?
Should you have any questions please do not hesitate to contact me.

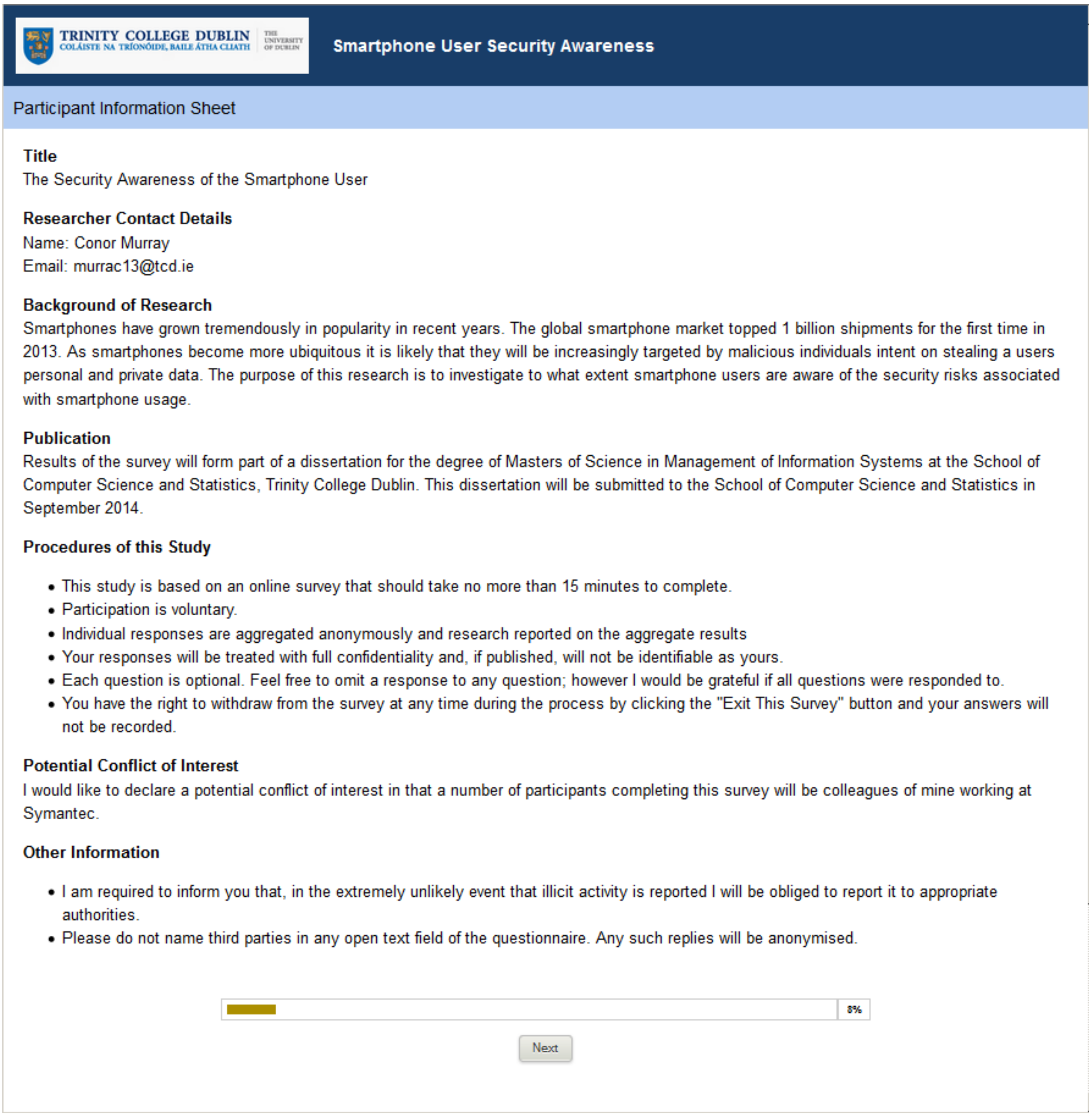
Kindest Regards,
Conor Murray

Declaration:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that the data is used for scientific purposes and I have no objection that the data is published in scientific publications in a way that does not reveal the identity of the participant.
- I understand that the participation of my employee/s is fully anonymous and that no personal details about them will be recorded.
- I understand that if illicit activities are identified, these will be reported to appropriate authorities.
- I have received a copy of this agreement.

PARTICIPANT'S NAME (PRINTED):
PARTICIPANT'S SIGNATURE:
PARTICPANT'S ROLE:
DATE:

7.2 Appendix B - Survey Questionnaire



Smartphone User Security Awareness

Participant Information Sheet

Title
The Security Awareness of the Smartphone User

Researcher Contact Details
Name: Conor Murray
Email: murrac13@tcd.ie

Background of Research
Smartphones have grown tremendously in popularity in recent years. The global smartphone market topped 1 billion shipments for the first time in 2013. As smartphones become more ubiquitous it is likely that they will be increasingly targeted by malicious individuals intent on stealing a users personal and private data. The purpose of this research is to investigate to what extent smartphone users are aware of the security risks associated with smartphone usage.

Publication
Results of the survey will form part of a dissertation for the degree of Masters of Science in Management of Information Systems at the School of Computer Science and Statistics, Trinity College Dublin. This dissertation will be submitted to the School of Computer Science and Statistics in September 2014.

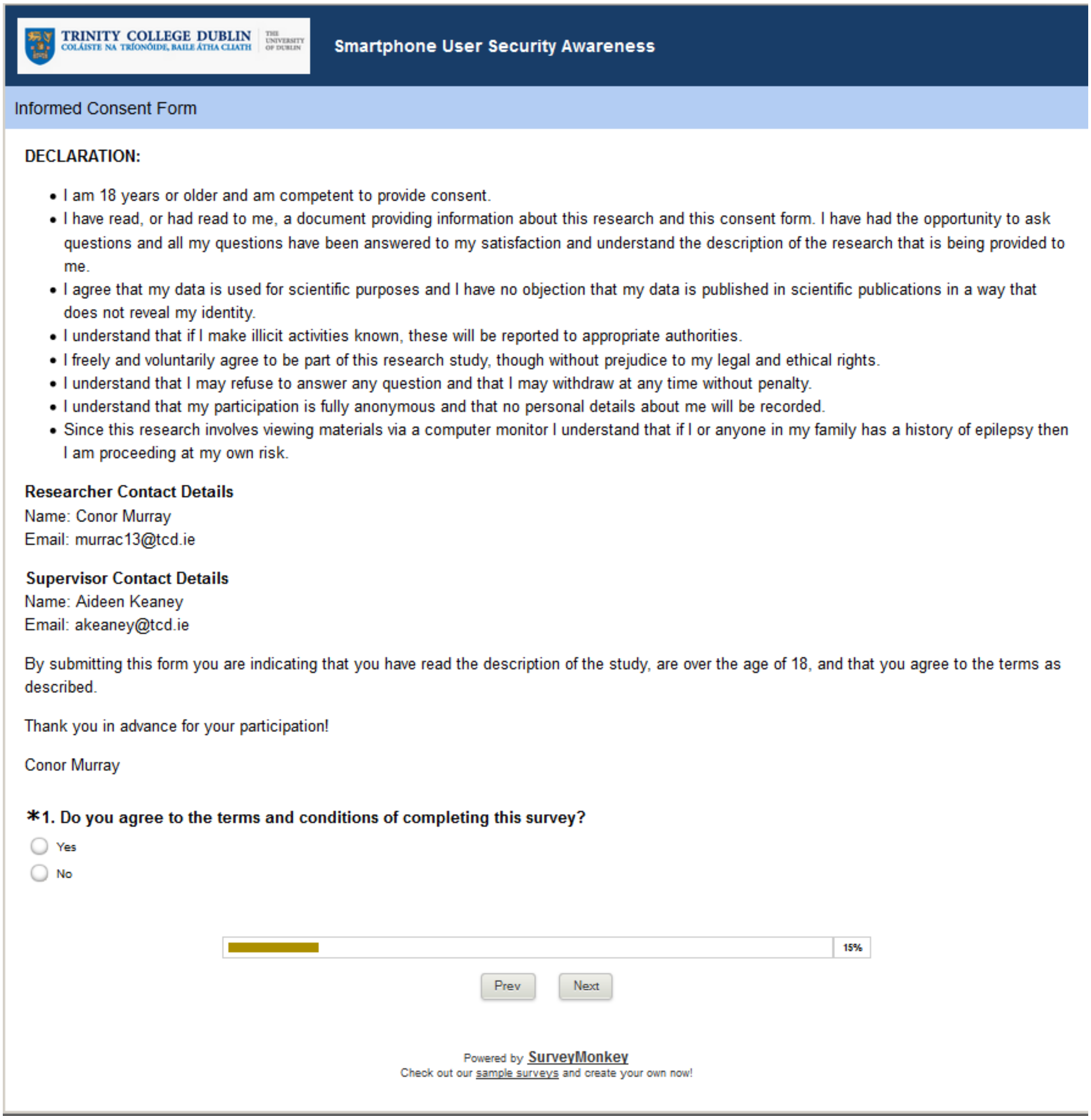
Procedures of this Study

- This study is based on an online survey that should take no more than 15 minutes to complete.
- Participation is voluntary.
- Individual responses are aggregated anonymously and research reported on the aggregate results
- Your responses will be treated with full confidentiality and, if published, will not be identifiable as yours.
- Each question is optional. Feel free to omit a response to any question; however I would be grateful if all questions were responded to.
- You have the right to withdraw from the survey at any time during the process by clicking the "Exit This Survey" button and your answers will not be recorded.

Potential Conflict of Interest
I would like to declare a potential conflict of interest in that a number of participants completing this survey will be colleagues of mine working at Symantec.

Other Information

- I am required to inform you that, in the extremely unlikely event that illicit activity is reported I will be obliged to report it to appropriate authorities.
- Please do not name third parties in any open text field of the questionnaire. Any such replies will be anonymised.


TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH
THE UNIVERSITY OF DUBLIN
Smartphone User Security Awareness

Informed Consent Form

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- Since this research involves viewing materials via a computer monitor I understand that if I or anyone in my family has a history of epilepsy then I am proceeding at my own risk.

Researcher Contact Details
Name: Conor Murray
Email: murrac13@tcd.ie

Supervisor Contact Details
Name: Aideen Keaney
Email: akeaney@tcd.ie

By submitting this form you are indicating that you have read the description of the study, are over the age of 18, and that you agree to the terms as described.

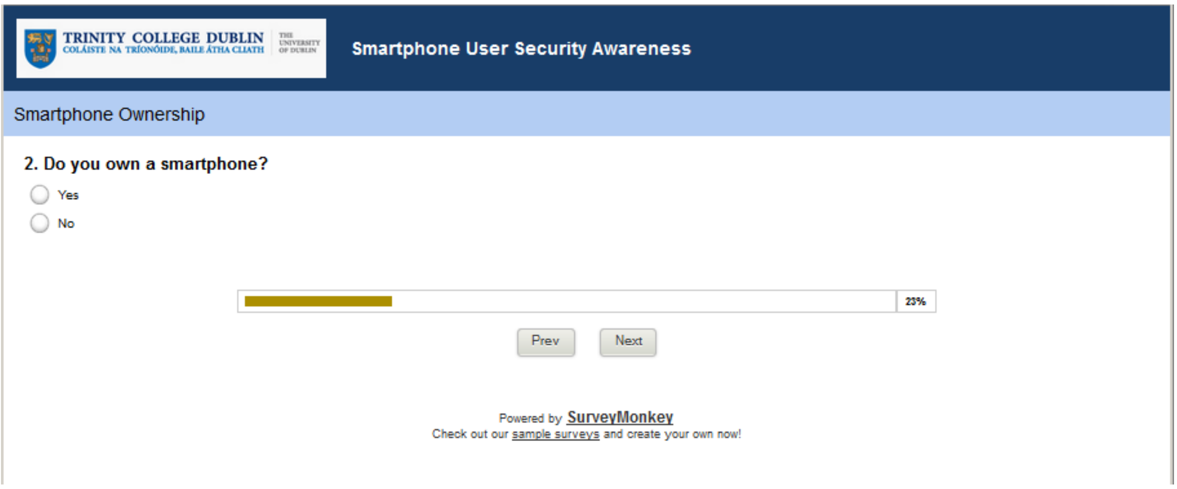
Thank you in advance for your participation!

Conor Murray

***1. Do you agree to the terms and conditions of completing this survey?**

○ Yes
○ No

15%
Prev
Next
Powered by SurveyMonkey
Check out our sample surveys and create your own now!

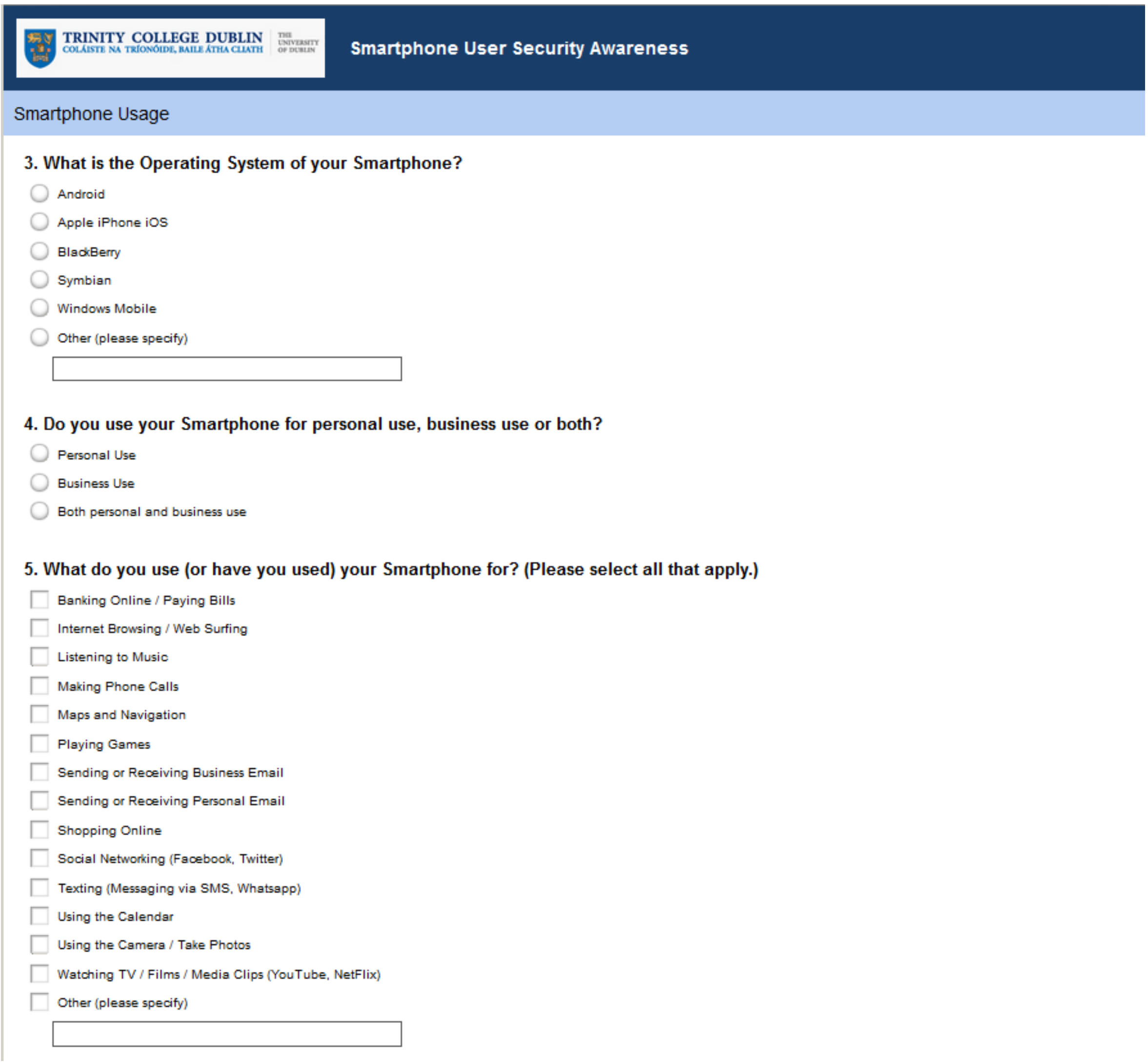

TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH
THE UNIVERSITY OF DUBLIN
Smartphone User Security Awareness

Smartphone Ownership

2. Do you own a smartphone?

○ Yes
○ No

23%
Prev
Next
Powered by SurveyMonkey
Check out our sample surveys and create your own now!



TRINITY COLLEGE DUBLIN COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH THE UNIVERSITY OF DUBLIN

Smartphone User Security Awareness

Smartphone Usage

3. What is the Operating System of your Smartphone?

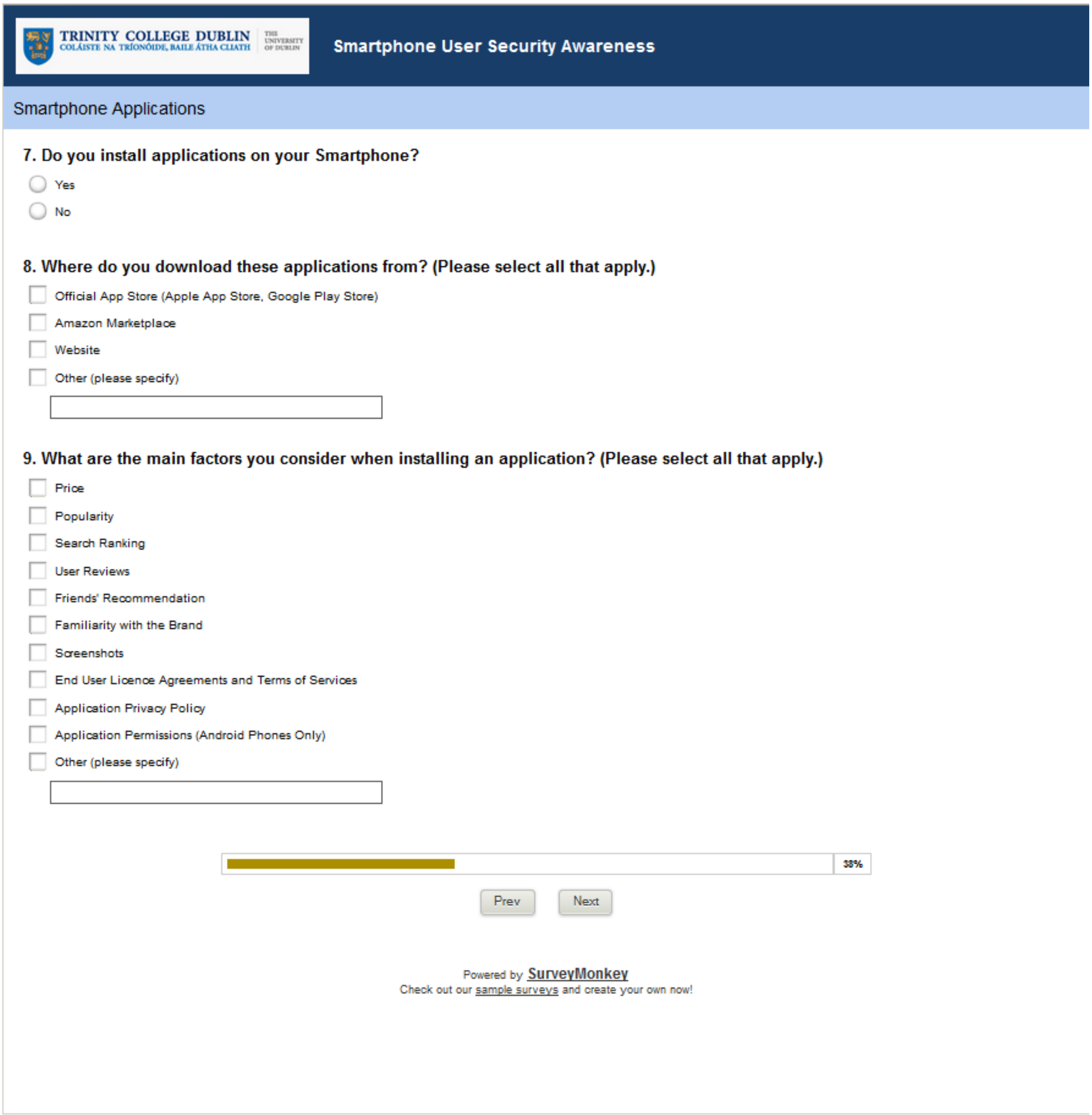
○ Android
○ Apple iPhone iOS
○ BlackBerry
○ Symbian
○ Windows Mobile
○ Other (please specify)

4. Do you use your Smartphone for personal use, business use or both?

○ Personal Use
○ Business Use
○ Both personal and business use

5. What do you use (or have you used) your Smartphone for? (Please select all that apply.)

□ Banking Online / Paying Bills
□ Internet Browsing / Web Surfing
□ Listening to Music
□ Making Phone Calls
□ Maps and Navigation
□ Playing Games
□ Sending or Receiving Business Email
□ Sending or Receiving Personal Email
□ Shopping Online
□ Social Networking (Facebook, Twitter)
□ Texting (Messaging via SMS, Whatsapp)
□ Using the Calendar
□ Using the Camera / Take Photos
□ Watching TV / Films / Media Clips (YouTube, NetFlix)
□ Other (please specify)



Smartphone User Security Awareness

Smartphone Applications

7. Do you install applications on your Smartphone?

○ Yes
○ No

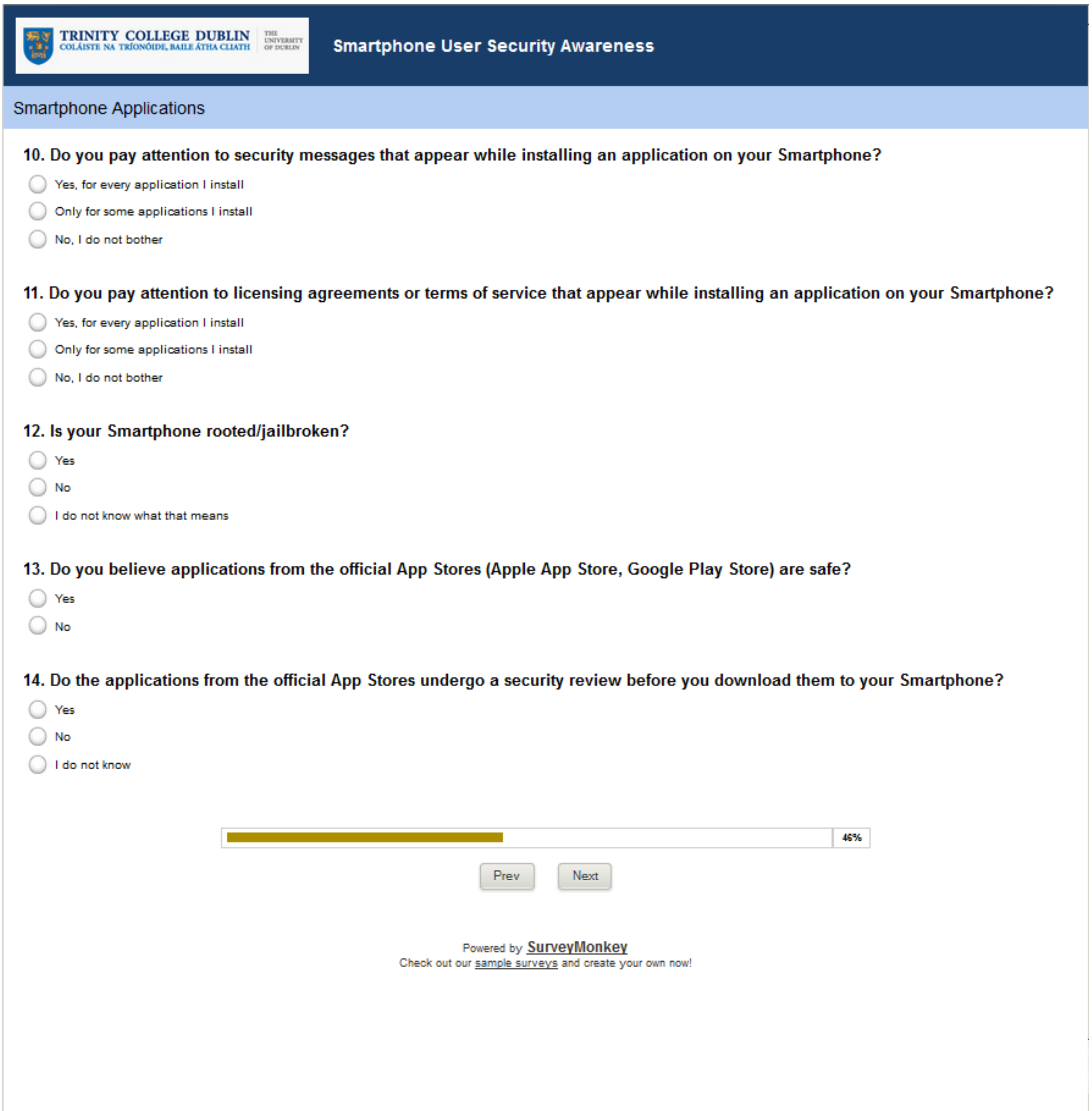
8. Where do you download these applications from? (Please select all that apply.)

□ Official App Store (Apple App Store, Google Play Store)
□ Amazon Marketplace
□ Website
□ Other (please specify)

9. What are the main factors you consider when installing an application? (Please select all that apply.)

□ Price
□ Popularity
□ Search Ranking
□ User Reviews
□ Friends' Recommendation
□ Familiarity with the Brand
□ Screenshots
□ End User Licence Agreements and Terms of Services
□ Application Privacy Policy
□ Application Permissions (Android Phones Only)
□ Other (please specify)

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Smartphone Applications

10. Do you pay attention to security messages that appear while installing an application on your Smartphone?

○ Yes, for every application I install
○ Only for some applications I install
○ No, I do not bother

11. Do you pay attention to licensing agreements or terms of service that appear while installing an application on your Smartphone?

○ Yes, for every application I install
○ Only for some applications I install
○ No, I do not bother

12. Is your Smartphone rooted/jailbroken?

○ Yes
○ No
○ I do not know what that means

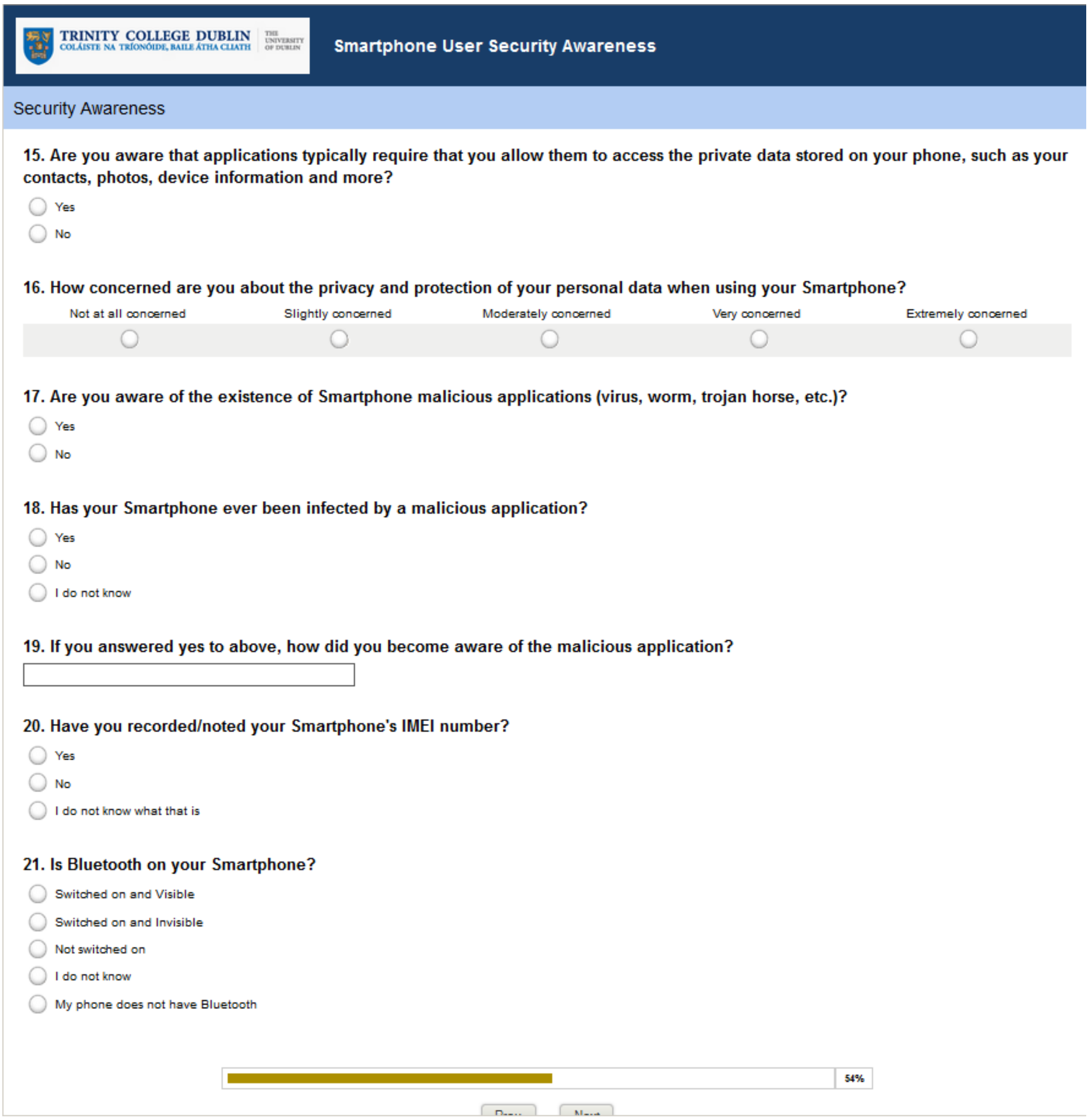
13. Do you believe applications from the official App Stores (Apple App Store, Google Play Store) are safe?

○ Yes
○ No

14. Do the applications from the official App Stores undergo a security review before you download them to your Smartphone?

○ Yes
○ No
○ I do not know

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Security Awareness

15. Are you aware that applications typically require that you allow them to access the private data stored on your phone, such as your contacts, photos, device information and more?

○ Yes
○ No

16. How concerned are you about the privacy and protection of your personal data when using your Smartphone?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

17. Are you aware of the existence of Smartphone malicious applications (virus, worm, trojan horse, etc.)?

○ Yes
○ No

18. Has your Smartphone ever been infected by a malicious application?

○ Yes
○ No
○ I do not know

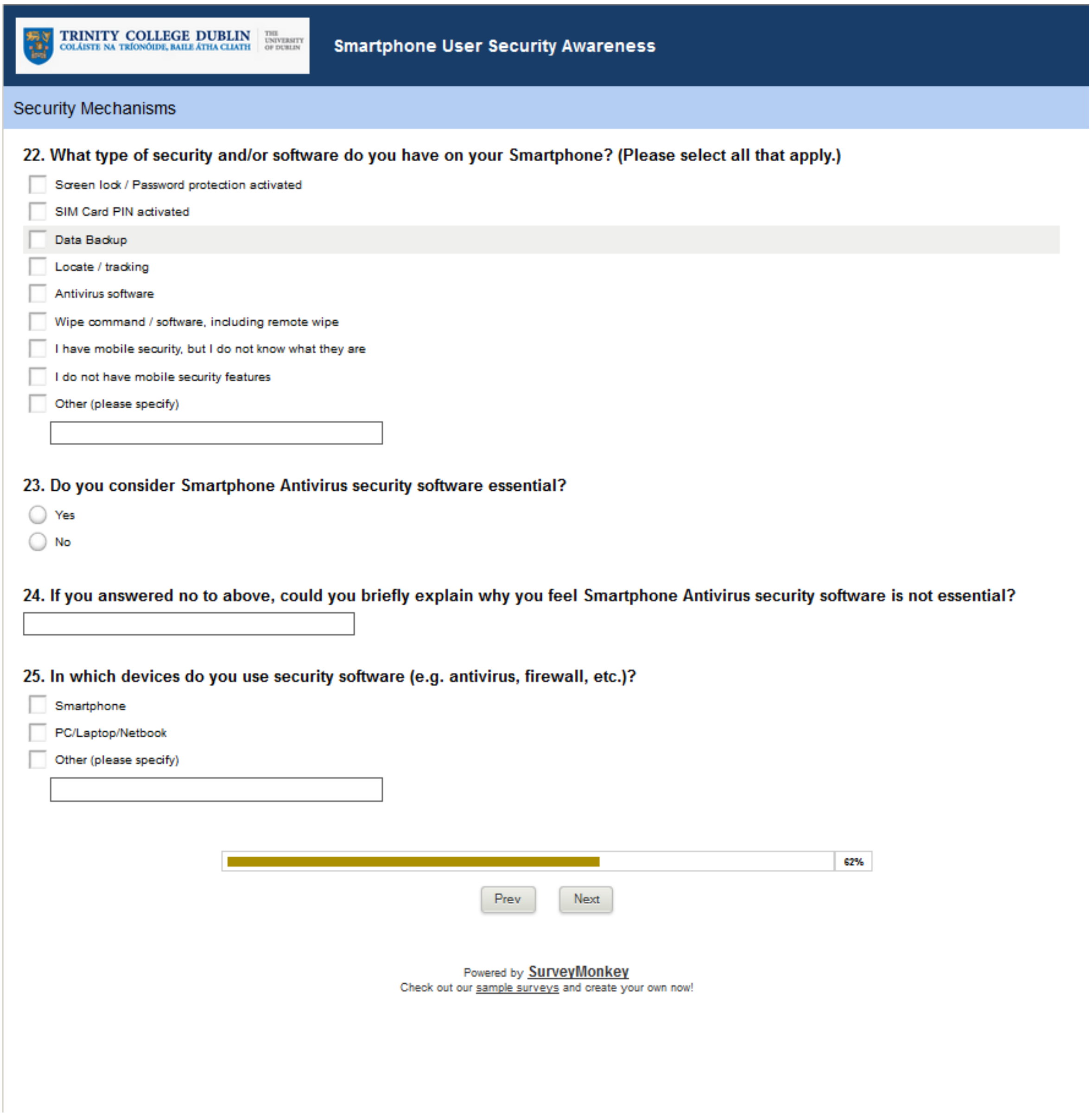
19. If you answered yes to above, how did you become aware of the malicious application?

20. Have you recorded/noted your Smartphone's IMEI number?

○ Yes
○ No
○ I do not know what that is

21. Is Bluetooth on your Smartphone?

○ Switched on and Visible
○ Switched on and Invisible
○ Not switched on
○ I do not know
○ My phone does not have Bluetooth



Smartphone User Security Awareness

Security Mechanisms

22. What type of security and/or software do you have on your Smartphone? (Please select all that apply.)

□ Screen lock / Password protection activated
□ SIM Card PIN activated
□ Data Backup
□ Locate / tracking
□ Antivirus software
□ Wipe command / software, including remote wipe
□ I have mobile security, but I do not know what they are
□ I do not have mobile security features
□ Other (please specify)

23. Do you consider Smartphone Antivirus security software essential?

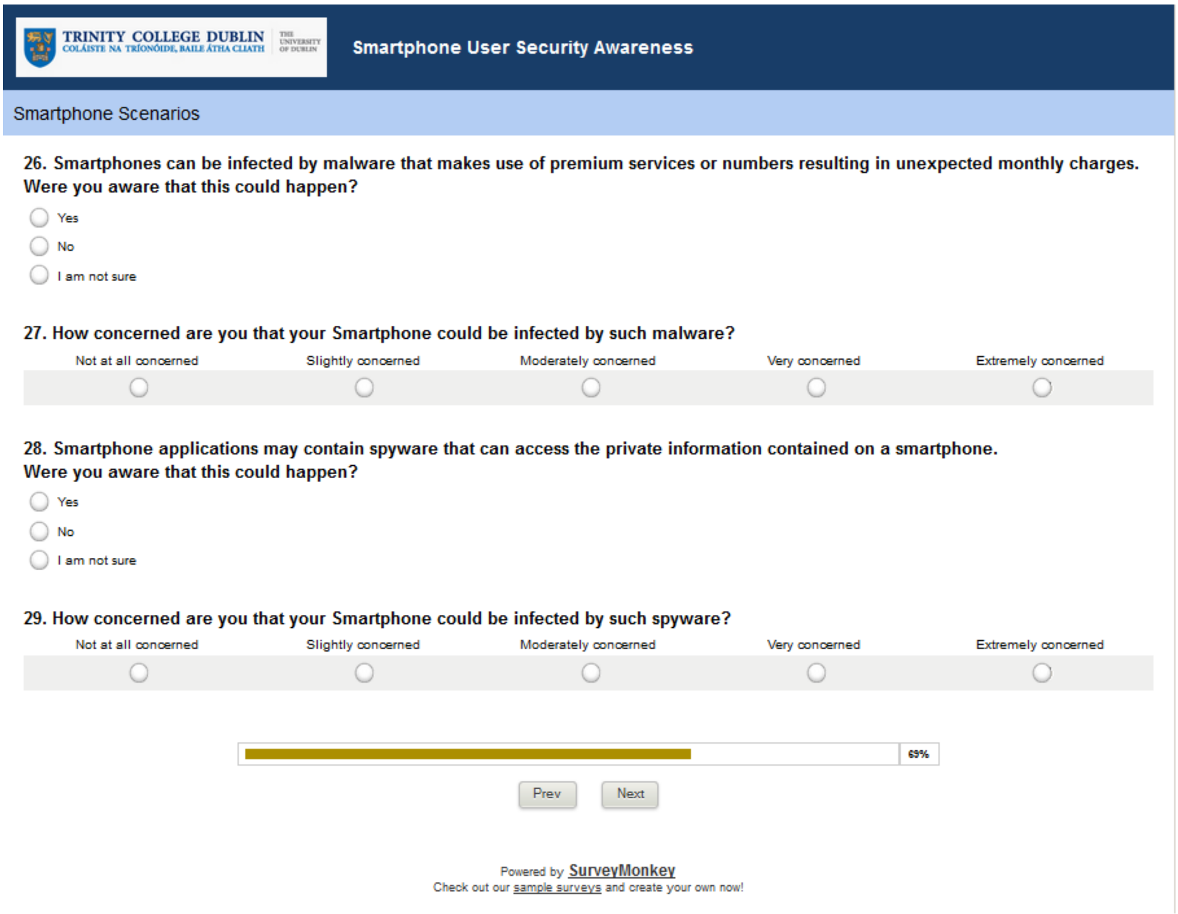
○ Yes
○ No

24. If you answered no to above, could you briefly explain why you feel Smartphone Antivirus security software is not essential?

25. In which devices do you use security software (e.g. antivirus, firewall, etc.)?

□ Smartphone
□ PC/Laptop/Netbook
□ Other (please specify)

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Smartphone Scenarios

26. Smartphones can be infected by malware that makes use of premium services or numbers resulting in unexpected monthly charges. Were you aware that this could happen?

○ Yes
○ No
○ I am not sure

27. How concerned are you that your Smartphone could be infected by such malware?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

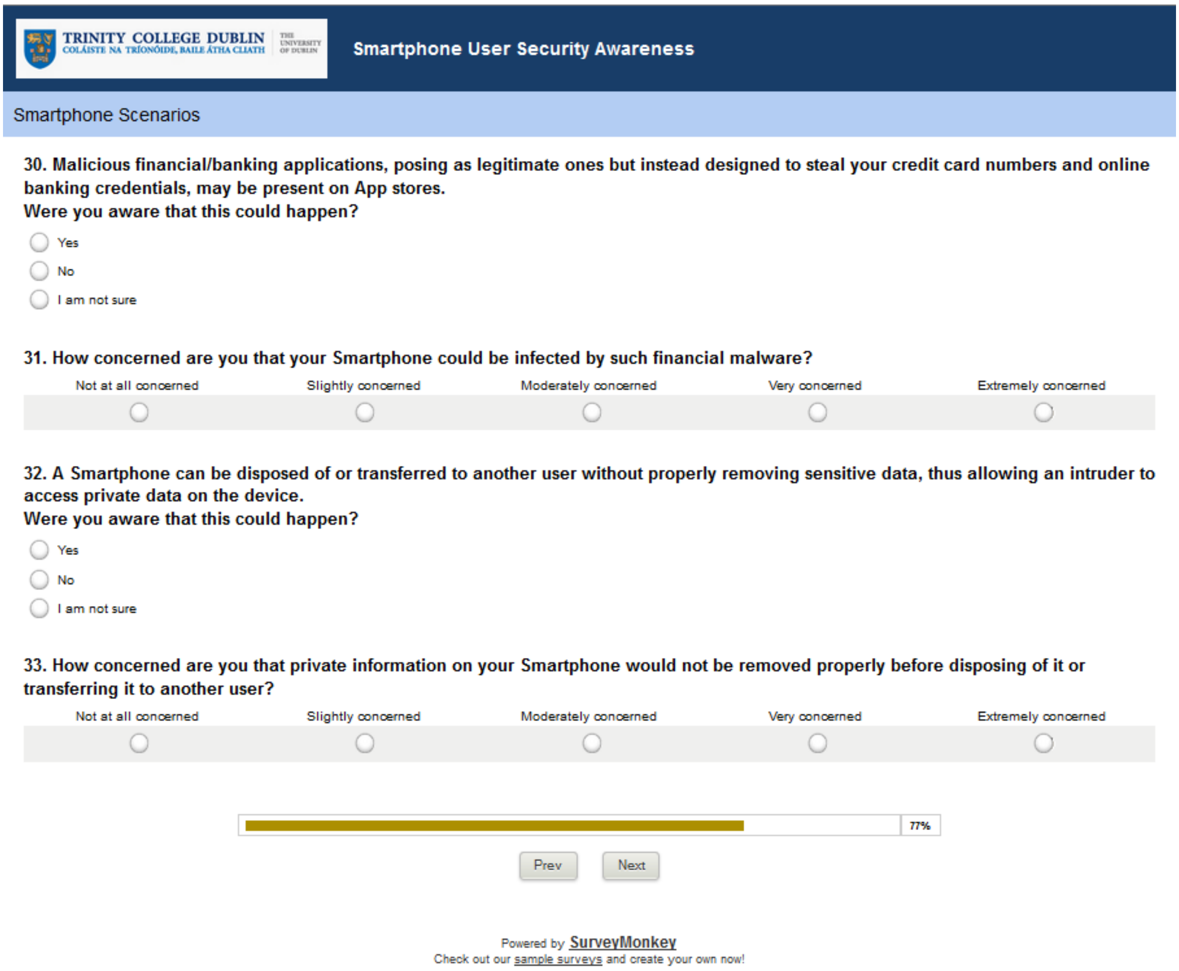
28. Smartphone applications may contain spyware that can access the private information contained on a smartphone. Were you aware that this could happen?

○ Yes
○ No
○ I am not sure

29. How concerned are you that your Smartphone could be infected by such spyware?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Smartphone Scenarios

30. Malicious financial/banking applications, posing as legitimate ones but instead designed to steal your credit card numbers and online banking credentials, may be present on App stores.
Were you aware that this could happen?

○ Yes

○ No

○ I am not sure

31. How concerned are you that your Smartphone could be infected by such financial malware?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

32. A Smartphone can be disposed of or transferred to another user without properly removing sensitive data, thus allowing an intruder to access private data on the device.
Were you aware that this could happen?

○ Yes

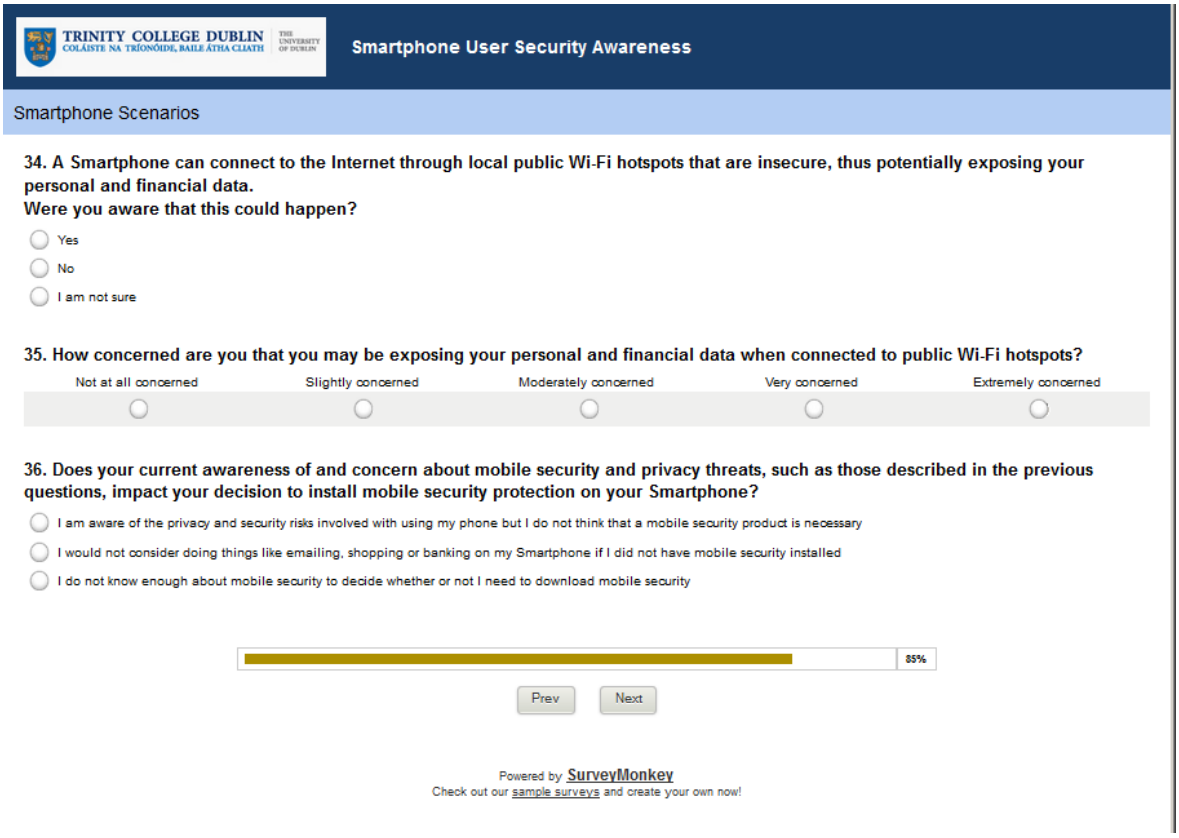
○ No

○ I am not sure

33. How concerned are you that private information on your Smartphone would not be removed properly before disposing of it or transferring it to another user?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Smartphone Scenarios

**34. A Smartphone can connect to the Internet through local public Wi-Fi hotspots that are insecure, thus potentially exposing your personal and financial data.
Were you aware that this could happen?**

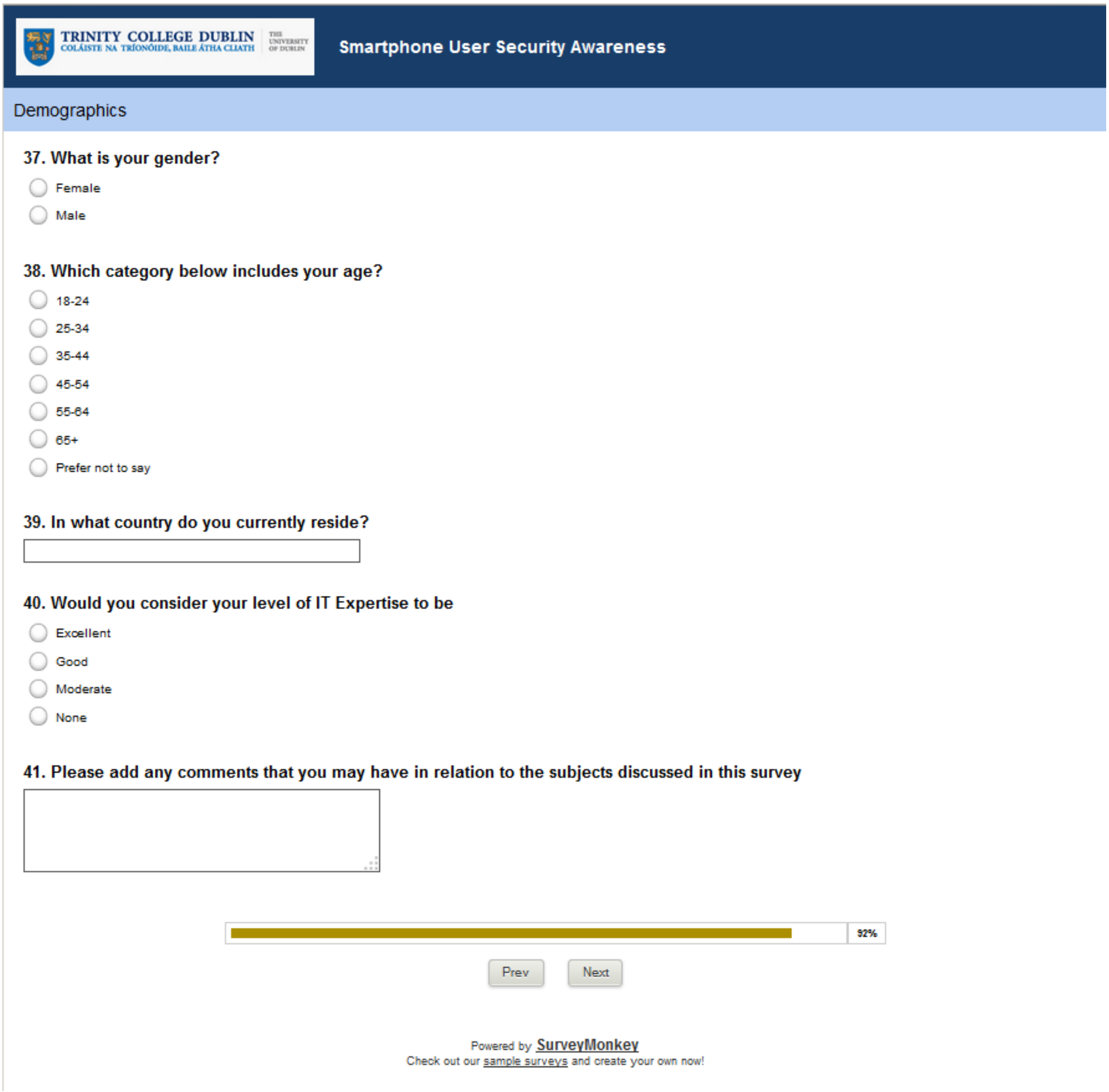
○ Yes
○ No
○ I am not sure

35. How concerned are you that you may be exposing your personal and financial data when connected to public Wi-Fi hotspots?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
○	○	○	○	○

36. Does your current awareness of and concern about mobile security and privacy threats, such as those described in the previous questions, impact your decision to install mobile security protection on your Smartphone?

○ I am aware of the privacy and security risks involved with using my phone but I do not think that a mobile security product is necessary
○ I would not consider doing things like emailing, shopping or banking on my Smartphone if I did not have mobile security installed
○ I do not know enough about mobile security to decide whether or not I need to download mobile security



Smartphone User Security Awareness

Demographics

37. What is your gender?

○ Female
○ Male

38. Which category below includes your age?

○ 18-24
○ 25-34
○ 35-44
○ 45-54
○ 55-64
○ 65+
○ Prefer not to say

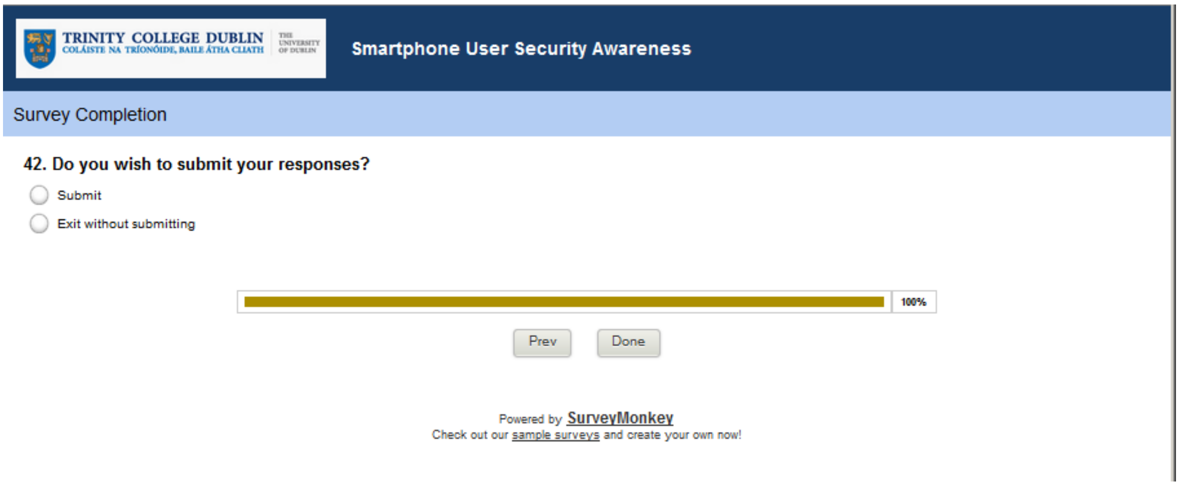
39. In what country do you currently reside?

40. Would you consider your level of IT Expertise to be

○ Excellent
○ Good
○ Moderate
○ None

41. Please add any comments that you may have in relation to the subjects discussed in this survey

Powered by SurveyMonkey
Check out our sample surveys and create your own now!



Smartphone User Security Awareness

Survey Completion

42. Do you wish to submit your responses?

○ Submit
○ Exit without submitting

Powered by SurveyMonkey
Check out our sample surveys and create your own now!

7.3 Appendix C - Survey Tables and Graphs

Table 7.1 - Gender (N=143)

Gender	Frequency	Percent
Female	34	24%
Male	107	75%
Not Specified	2	1%
Total	143	100%

Table 7.2 - Age Category Distribution (N=141)

Age Group	% Breakdown	Female	Male	Total
18-24	1%	1	0	1
25-34	53%	20	55	75
35-44	34%	9	39	48
45-54	7%	1	9	10
55-64	4%	3	3	6
65+	1%	0	1	1
Total	100%	34	107	141

Table 7.3 - Country of Residency (N=143)

Country of Residency	Frequency	Percent
Ireland	124	87%
USA	2	1%
China	2	1%
India	6	4%
Austria	1	1%
Spain	1	1%
UK	3	2%
Finland	1	1%
Not Specified	3	2%
Total	143	100%