Research on the User Attitudes and Behaviors of Mobile Security and Antivirus

Mei-Ling Yao [1], Ming-Chuen Chuang [2] and Chun-Cheng Hsu [3]

[1,2,3] Institute of Applied Arts, NCTU, Hsinchu, Taiwan

Abstract

Diversified applications of smartphones bring convenience for life but leads to capturing the interest of hackers towards planning attacks against smartphones and the resulted benefits. Currently, research related to mobile security focuses more on technical study in order to block malicious programs, permission and privacy study etc., but less on the user experience for the mobile security application (MSA). By means of surveys, this study explores knowledge, attitudes, behaviors and user experience regarding mobile security and antivirus. From research results: 1) More than half of the respondents in this study are familiar or very familiar with computer and smartphone technology. Most of them also regard that mobile security risks are a serious issue. Compared to iOS respondents, Android respondents further regard that mobile security risk is serious, and that MSA is important, but the proportion of MSA installation is not high. Those having lower familiarity with technology regard that severity of mobile security risk is higher. 2) Males have more technical knowledge about computers and smartphones compared to females, but females pay more attention to mobile security and account for a higher proportion of MSA installation compared to males. Fewer iOS users install MSA compared to Android users, but they also have concerns about mobile security and consider installing MSA. 3) The knowledge of respondents about computer and mobile phone technologies will not affect their attitude towards mobile security risk significantly, and their attitude towards mobile security risk will not affect their installation of MSA significantly. 4) It seems that the computer antivirus software installation experience would not affect the installation intention of MSA significantly. 5) The most commonly used MSA features are: Malware prevention, safe browsing, garbage file cleanup, call and message

filter, and privacy protection. 6) Proactive alerts for intercepting threats and current security status for mobile phones could better provide users with the feeling of being protected, while providing regular security reports is less effective. Advertisements are the main reason why users feel that they are being interfered with using MSA, which developers will consider and think about how to reduce advertisement interference or operate users through different profit models.

Keywords: Mobile security, user experience, mobile antivirus, smartphone, KAB

1. Introduction

Diversified applications of smartphones bring us unprecedented convenience and user experience. Social networking, work, entertainment, learning, shopping and payment etc. can all be done using smartphones. Mobile applications have affected our daily life deeply. In 2015, the number of smartphones has exceeded that of desktop computers. Users use smartphones to perform some important and personal tasks, such as sending and receiving Emails, use of online banking, and online shopping, which show that current transaction behavior has been transited from E-Commerce to M-Commerce gradually. From an investigation with respect to use of smartphones for 3,500 end users (15-45 years old) all over the word, nearly 50% of users spend more than 5 hours in using smartphones every day, in which 25% of users spend more than 7 hours in using smartphones every day. People's reliance on smartphones is far beyond our imagination. Overall, the two most commonly used features of smartphones for users are web browsing and mobile games, followed by calling, messaging, watching videos, and visiting community websites (Counterpoint Research, 2017).

The convenience of the smartphone is undoubted, which, however, results in mobile security and privacy issues. Cyber hackers follow the App trend and extend the means of attacking against PCs (Personal Computers) by using viruses or malicious programs in the era of PC to smartphones for stealing important information or personal privacy, and even more, thereby for defrauding money. Check Point, an antivirus software company, points out that malware CopyCat has invaded smartphones running Android OS (Operating System), such that 14 million mobile devices are invaded by hackers in the world. This malware will obtain superuser permission of Android OS through Root mobile phones to download various counterfeit applications automatically, in order to know which application the user has downloaded or opened, and then remove and replace the account of the user with the account owned by the hacker. Hackers gain more than $1.5 million from revenues of those counterfeit advertisements by means of advertisement pop-ups in applications (Check Point, 2017).

On the other hand, current App developers can easily access data stored on smartphones including contact information, call history, web browsing logs, personal messages, photo and videos, financial data, GPS locations, camera or microphone logs or obtain permission etc. In many cases, the permissions requested by App developers would be more than actually needed, while those App developers are not responsible for protecting this information from hacking sufficiently, such that Apps become malicious programs. Also, users fail to fully understand the mobile security risks associated with granting these permissions (Jorgensen, 2015). Most users are unaware of the existence of smartphone malicious programs or suspicious applications in the Android app store, let alone knowing about the damages which might inflict their personal information collected and shared by these malicious programs (Kelly, 2012).

In spite of approximately 200 or more MSAs being available on Google Play, most of which are provided in freemium, but none seem to be successful in attracting the interest and user attention as only very few of them download regularly. User habits in using PCs should be transferred to the use of smartphones. However, the users seem to fail to apply their antivirus experience with PCs to smartphones. There are many reasons which cause neglect of mobile security. For example, users may have insufficient knowledge of mobile security risks, or do not understand the impacts of these risks on them, or current MSA designs fail to satisfy users. In order to explore what the users think of mobile security risks, this study intends to use surveys to understand the following issues:

1) Do users value mobile security with respect to knowledge, attitude and behavior, and what are their knowledge, attitudes and behaviors?
2) Are there different knowledge, attitudes and behaviors for different user groups?
3) What is the relationship between knowledge, attitude and behavior for mobile security?
4) Does installation experience of computer antivirus software affect intention of MSA installation?
5) What are experiences of users with respect to MSA?

2. Literature Review

Both smartphones and computers face many threats to information security, such as loss, theft or damage of smartphones, and mobile threat types that are completely different compared to

Table 1: Different types of malware activities

Data theft	Surveillance	Impersonation	Financial loss	Botnet activities
Account Contact data Call history Email File document International Mobile Equipment Identity (IMEI) Telephone number	Sound Camera Call Location SMS	Social media Sending mail Fishing SMS	Ransomware Fake Antivirus software Making expensive calls Sending SMS results in tariff consumption (premium SMS) Stealing transaction identification numbers (TANs)	Fraud Distributed denial of service attack (DDos attack) Sending SMS results in tariff consumption (premium SMS)

traditional computer threats, such as malicious programs, hacker attacks, eavesdropping, monitoring, tracking, and account theft, social engineering, fishing mails and increasing money frauds etc. (Theoharidou, 2012). Users believe that the data stored in smartphones is private and needs to be protected. However, smartphones are prone to theft, loss and damage, which results in a very significant security risk for both individuals and company organizations. (Mansfield-Devine et al, 2012) (Urban, 2012). Different from OS's of computers, those smartphones are not developed that maturely, so that users have to be restricted in order to ensure their mobile security. (Botha et al, 2009). Therefore, users feel that setting up security control on a smartphone is not easy (Furnell, 2006). Security controls include but are not limited to the following categories: password authentication, PIN (Personal Identification Number), firewall, remote management, encryption and antivirus software. Passwords are more complicated and more secure than PIN numbers. However, as users are eager to enjoy the convenience without a rigorous password setting, the purpose of password protection is not achieved accordingly (Landman, 2010).

There are many types of mobile security threats, which may be divided into physical threats, network-based threats, system-based threats, and application-based threats, which are explained as follows (Hao et al, 2016):

1) Physical threats: Compared with computers, the portability and convenience of smartphones result in their easy loss or theft. Hackers can use malicious programs for connection to computers, install malicious programs on or steal data from smartphones, while the use of smartphone authentication or encryption allows for enhanced protection and prevents hackers from being able to easily hack into smartphones.
2) Network-based threat: Smartphones can be connected to the outside world through Wi-Fi and Bluetooth. Each type of communication has its own potential security vulnerability and allows for easy eavesdropping through the use of tools such as Wifite. Therefore, users are advised to connect to and use WPA2 trust network, or other more secure network security protocols.

3) System-based threat: Smartphone manufacturers sometimes generate vulnerabilities in smartphones accidentally. For example, a serious security vulnerability named No iOS Zone has been found for iOS. This vulnerability would connect to other iOS devices in a fabricated network automatically thus making iOS devices crash repeatedly to the point that they are unavailable for use (Amit, 2015). To avoid such threats, a timely smartphones system update is required to ensure the security of the smartphone.
4) Application-based threats: As system security is vulnerable, applications may not be updated timely and result in potential security issues. Use of software that is not updated timely would increase the chance of being attacked by hackers, or the application itself is malware. If a smartphone is infected with a malicious program, data could be stolen, more malicious programs would be installed, expensive SMS texts would be sent and result in tariff consumption or the smartphone would be monitored remotely, all of which could result in loss of money or loss of data. Therefore, it is important to detect and defend against malicious programs on smartphones.

Malicious program is a type of evil, intrusive or troubling software or program code (for example: Trojan, rootkit, and backdoor), which uses the smartphone without the consent of the user. Malicious programs usually use malicious file attachments or links in spam Emails for connection to infected websites. According to the influence of different malware attacks, malicious programs can be divided into 5 types as listed in table 1 (Polla, 2013):

1) Data theft: Theft of accounts and contact data etc.
2) Behavior monitoring: Monitoring of call histories or geographic locations etc.
3) Counterfeit for fraud: Counterfeiting of identity for fraud.
4) Loss of money: Ransomware or delivery of expensive SMS.
5) Botnet: Controlling of mobile phones to perform malicious actions.

Mobile security should be a comprehensive approach that involves considerations with respect to technology, behavior, philosophy and organization etc. (Zafar & Clark, 2009). Compared to researches on mobile security technologies such as firewall or antivirus, there are fewer researches with respect to human factors. However, it is important to analyze and understand the opinions of users because technologies cannot solve all security issues completely (Ophoff & Robinson, 2014). Scholars in the field of social psychology have established a model for assessing information security awareness based on knowledge, attitude and behavior (KAB) to understand the relationship between these three factors. Knowledge will trigger changes on attitudes eventually thus affecting changes of user behaviors gradually. In KAB theory, knowledge is related to what people know, attitude is related to what people think, and behavior is related to what people do

(Kruger & Kearney, 2008).

Operating systems of smartphones are mainly divided into two categories: Android and iOS. Google released the first Android smartphone in 2008. Since Android is an open Linux operating system, anyone is allowed to develop Android Apps. Despite the official Google Play store, developers can still publish Apps anywhere. Google mainly benefits from advertisement revenues, and accordingly, provides open and free platforms and services for everyone to use. Apple provides users with complete services through integration of software and hardware. Only people who participate in iOS Developer Program are allowed to develop iOS Apps and publish Apps through Apple App Store. Some corporate organizations are allowed to participate in iOS Developer Enterprise Program, so that they can develop and publish their own Apps for their employees to use. It can be seen from the above that mobile applications are developed by third-party developers; users can download, through mobile application stores, and install those applications in smartphones. However, it is difficult for users to understand which personal information may be collected, or which hidden features may be provided by App developers. Therefore, there are often security threats and privacy issues in using applications. The number of Android malicious programs is quite amazing (Felt, 2011) because anyone can develop, design and publish their own Apps. Although Android Google Play began support of malicious program scanning in 2012, the effectiveness was not good because preventing users from downloading malicious programs could not be performed comprehensively (Percoco, 2012). Compared to Android, there are far fewer iOS malicious programs because all Apps on the Apple App Store need to be reviewed to ensure actual consistency with what is described. This means that these reviewed Apps should be isolated from malicious features. However, there are still some malicious programs or spyware programs that can penetrate into the App Store (Bonnington, 2012).

King (2012) compared concerns and expectations of 13 Android and 11 iOS users with respect to privacy. She assumed that iOS users should trust Apps more because Apple has the review process. From her research result, users would feel more secure as they know that Apps have been reviewed. Android users also believe that Google has reviewed Apps on the Google Play Store. Benenson (2013) et al. compared 506 Android and 216 iOS users with respect to differences in mobile security and privacy and found that people who are more interested in technology tend to use iOS. 38% of Android respondents install mobile antivirus software; among users who install Apps, 20% of Android users and 5% of iOS users are aware of privacy issues, such as disclosure of personal data and permissions etc. Obviously, the proportion of Android users is higher than that of iOS users, that is, Android users are more concerned about privacy issues.

Many researches for mobile security focus on privacy related issues and make discussion based on

permission disclosure screen of Android as the main topic. Android is an open platform. In the App development process, users will be notified of which permissions will be used by the App to be installed through the permission disclosure screen. Many users would ignore the permission list described on this screen. Only 17% of users would read carefully, and more than 75% of users have no idea about security risks which may be inflicted due to the granting of permission (Felt, 2012). Most users ignore the Android permission disclosure screen and tend to choose Apps based on easily understandable criteria, such as App ranking, user appraisal and word of mouth, due to poor knowledge about the impact of permission (Kelley, 2012). As such, due to usability issues of default permission disclosure screen of Android OS, users cannot understand which personal privacy security issues may arise when they agree that the App to be installed is allowed to access their photos, GPS locations, cameras, and other features. Harbach et al. (2014) tried to present certain privacy risks in a specific approach, such as personal example. For example, when a system requests permission to "Read contact data", the data of three friends will be selected from the contact data in the smartphone randomly and displayed on an interface, so that users will be more alert to the privacy risk for disclosure of this warning message.

In spite of studies by scholars on privacy security issues caused by Android OS and permission detection and protection approaches suggested by them, hackers may still develop malicious programs to avoid being blocked by these mechanisms (Trend Micro, 2012). Furthermore, mobile security risks are usually multi-faceted. Different mobile applications and user behaviors may bring users different risks. The privacy and permission issues of mobile devices are just a part of many security risks. A single risk remediation approach is insufficient for users. Therefore, installation of installing a legitimate MSA is still very important for alerting users or preventing malicious programs from attacks.

Jorgensen et al. (2015) found that general users recognize similar mobile security risk categories as experts, including personal data privacy, data authenticity and integrity, mobile phone usability and stability, as well as loss of money, respectively through interviews with 19 information security experts and surveys of 350 Android users. Among them, for personal data privacy, personal identification numbers, passwords, financial information, messages, mails and chat histories, personal photos and videos, geographic locations, contacts and files are more important. Chin et al. (2012) studied differences in attitudes of users with respect to security and privacy between smartphones and computers, and found that users would regard that the risk of smartphones is higher than that of computers when performing tasks related to privacy, banking transactions, online shopping, and health records etc. They worry about theft of mobile phones, data loss, malicious programs, or cyber-attacks.

Ophoff et al. (2014) performed a mobile phone security awareness survey for 619 users in South Africa and found that most of the respondents believe that the App downloaded from the official application store is secure and has been tested. Female respondents are more confident than males that Apps downloaded from official application store are secure. 76.3% of the users knew existence of malicious programs. Particularly, males who are more familiar with technical knowledge or information security understand more about malicious programs. However, they often ignore privacy and security risks when installing Apps; only very few users will pay attention to privacy and security risks before installing Apps. The key factors considered when users install Apps are as following in order: usefulness, price, ranking and review, popularity, as well as usability. 61.4% of the respondents know MSA, 50.52% of them have searched for free MSA, but only 27.3% of the respondents have MSA installed. Among those who feel that MSA is very important, only 42.11% have MSA-installed, and tend to choose free MSA.

3. Methodology

In order to understand knowledge, attitudes and behaviors of users regarding mobile security and MSA, as well as whether there is significant correlation between these three aspects, survey was conducted by means of questionnaires.

3.1 Questionnaire Design

Based on knowledge, attitudes, and behaviors of users regarding mobile security and MSA, these three aspects are designed as questions for questionnaires, and the author invites three experts specialized in MSA to conduct test prior to answering questions. After deleting questions with no discrimination rate, 35 items of questionnaire for users are formed. Questions in Questionnaires are formed of yes/no questions, single-choice questions, multi-choice questions, and three or five level Likert scale etc., which are summarized in the following sections:

1) Profile of respondent: Single-choice questions involving in gender, age, education level, occupation, average time spent in mobile phone every day, mobile phone brand, and years of experience in using smartphone.
2) Questions about knowledge of respondent: What is the familiarity with technology (5-level scale from very familiar to unfamiliar)? Is MSA known? Which mobile security threats have been heard? Also, what are the consequences of a smartphone being attacked by hackers?
3) Questions about the attitudes of respondents: Motivation for understanding technology, opinions for severity with respect to mobile security risks (5-level scale from very serious to

very not serious), opinions about importance of MSA (5-level scale from very important to very unimportant), and whether friends or family members will be recommended to use MSA.

4) Questions about the behavior of respondents: Whether or not to click on advertisement links in apps or web pages (usually, occasionally, never), whether or not to click on unknown links in mail or messages (usually, occasionally, never), whether or not there is experience with respect to the installation in apps downloaded from non-Google Play or the Apple app store (usually, occasionally, never), whether computer antivirus software is installed or not, or whether MSA is installed. If antivirus software is installed, is it a paid version or a free version, what is the purchase channel and what is the reason?
5) MSA experience: Frequency of use, top used features, perception of being protected, which designs make you perceptive of being protected, whether or not there is interference and what its cause is.

3.2 Participant Sampling and conducting survey

Compared to computer antivirus software, general people use MSA less frequently. Nevertheless, netizens are more likely to be familiar with computer, smartphone or network technology, so this study is targeted towards netizens in Taiwan. The survey link is published on social networking websites to seek volunteers to take part. The term of the survey is 3 days. In this study, respondents are invited through a publishing survey on social networking websites, and the ideas of a wider range of user groups may be covered, including input from users with a varying degree of technology familiarity.

3.3 Data Analysis

The analysis of survey results will analyze differences in ideas, attitudes or behaviors of different groups with respect to mobile security, as well as the significance of their differences based on different user groups, such as different genders, different familiarities with technology, different views on the severity with respect to mobile security risk and importance of MSA etc.

4. Results and Discussion

4.1 Participant Backgrounds

A total of 113 valid responses were collected in this survey, wherein 45 responses were from female participants (39.8%) and 68 responses were from female participants (60.2%). Ages of respondents are mainly distributed between 30 and 50 (84.1%), and nearly half of the respondents have 4-6 years of experience (46.9%) in using smartphones, followed by more than 7 years (36.2%); while

most respondents use their smartphones for 3-6 hours every day (43.3%), followed by 6 hours (30.9%), and this result is similar to the survey result of time spent by users in using mobile phones every day announced by Counterpoint Research in 2017. It can be confirmed from the above that the respondents of this study are familiar with using computers and smartphones.

4.2 Analysis of Familiarity for Technology and Security Knowledge

From the analysis with respect to the familiarity of male and female respondents with technology shown in Table 2, more than half (53%) of overall respondents are familiar or very familiar with computer and smartphones technology, while the proportion of males (68%) is higher than that of females (32%). Particularly, for the male and female respondents who are very familiar with technology, the proportion of males (82%) is much higher than that of females (18%). Regarding technology familiarity calculated by converting Likert scale replies into scores 1-5: the overall average of technology familiarity was 3.65 with a standard deviation of 0.896; the average is 3.79 and the standard deviation is 0.907 for males as well as the average is 3.42 and the standard deviation is 0.839 for females respectively; with a difference of 0.05 in terms of the t-test it is clear male respondents are more familiar with technology than their female peers in this study.

Table 2: Analysis of Gender and Familiarity with Technology

	Male	Female	Total
Very Familiar	18(82%)	4(18%)	22(100%)
Familiar	23(60.5%)	15(39.5%)	38(100%)
Neutral	24(50%)	24(50%)	48(100%)
Unfamiliar	2(100%)	0(0%)	2(100%)
Very Unfamiliar	1(33.3%)	2(66.7%)	3(100%)
Total	68(60%)	45(40%)	113(100%)

In this study, there are 54 Android users (47.8%), 42 iOS users (37.2%), and 17 users who have both Android and iOS operating systems (15%). These three user groups have familiarities with technology as shown in Table 3. Android users have an average familiarity with technology of 3.41 with a standard deviation of 0.901. For iOS users, the average is 3.83 with a standard deviation of 0.853. Respondents having both Android and iOS have higher familiarity with technology and have an average score of 3.94 and a standard deviation of 0.827. This group is familiar with the usage and knowledge of the two operating systems, so that there is a higher familiarity with technology. More than half of the respondents who are quite familiar with technology use iOS, which is consistent with the research results conducted by Benenson (2013). Those who are more interested in technology tend to use iOS.

Table 3: Analysis of Mobile Phone Operating System and Familiarity with Technology

	Android	iOS	Mixed	Total
Very Familiar	5(23.8%)	11(52.4%)	5(23.8%)	21(100%)
Familiar	19(48.7%)	14(35.9%)	6(15.4%)	39(100%)
Neutral	26(54.2%)	16(33.3%)	6(12.5%)	48(100%)
Unfamiliar	1(50%)	1(50%)	0(0%)	2(100%)
Very Unfamiliar	3(100%)	0(0%)	0(0%)	3(100%)
Total	54(47.8%)	42(37.2%)	17(15%)	113(100%)

From Table 4, the proportion of respondents who can handle smartphone technical problems alone (76%) is higher than that of the respondents who can handle computer technical problems alone (66%), wherein the proportion of male respondents who handle computer technical problems alone is higher than that of female respondents with a very significant difference ($P=0.017<0.05$). However, generally people rely very much on smartphones in their daily life. The familiarity and mastery with smartphones are higher compared to computers. Furthermore, smartphones are more personal, and which issues are handled with less reliance on others. Although the proportion of males who handle issues alone is higher compared to females (82%>67%), the significance of difference is little higher than the level of 0.05 ($P=0.056>0.05$).

Table 4: Analysis of Gender and Handling Problems with Respect to Use of Computers and Smartphones

	Device	Handling Alone	Handling by Others	Total
Male	Computer	51(75%)	17(25%)	68(100%)
	Mobile Phone	56(82%)	12(18%)	68(100%)
Female	Computer	24(53%)	21(47%)	45(100%)
	Mobile Phone	30(67%)	15(33%)	45(100%)
Total	Computer	75(66%)	38(37%)	113(100%)
	Mobile Phone	86(76%)	27(24%)	113(100%)

74% of the respondents know MSA, and their understanding levels for and familiarities with infection channels of mobile threats are as following in order:

1) Unknown or fraudulent calls (85.8%)
2) Unknown or fraudulent messages (77.9%)
3) Malicious websites or programs (70.8%)
4) Application vulnerabilities (64.6%)
5) Spam (59.3%)

Possible consequences of thinking that smartphones are attacked by hackers are as follows in order:

1) Privacy such as account password, Email and contact data etc. will be stolen by hackers (92%)
2) Photos and files will be stolen (73.5%)
3) Emails with malicious attachment are sent automatically by smartphone (61.9%),
4) Phone call will be eavesdropped (59.3%),
5) Expensive SMS is sent and geographic location of mobile phone is monitored (51.3%)

It can be seen from the above that respondents are more familiar with infection channel such as unknown calls and messages, followed by malicious websites and applications. According to the categories of malware attacks set forth by Polla (2013), SMS or message is indeed one of the major channels by which hackers used to attack against mobile security.

4.3 Analysis Attitude for Mobile Security

Table 5 shows that most respondents (73.5%) believe that mobile security risk are a serious or very serious issue. There is a clear difference between gender and severity of mobile security risk. The proportion of females who think that the mobile security risk is very serious (57.1%) is much higher than that of males (42.9%). The overall average is 3.939 with a standard deviation of 0.8893. The average for opinions of males with respect to mobile security risk is 3.765 with a standard deviation of 0.9482; the average for females is 4.2 with a standard deviation of 0.7261. The t-test also shows a significant difference between the two cases ($P=0.01<0.05$). This shows that females pay more attention to mobile security issues than males.

Table 5: Analysis of Gender and Opinions for Severity of Mobile Security Risk

	Male	Female	Total
Very Serious	14(45.2%)	17(54.8%)	31(100%)
Serious	33(60%)	20(40%)	55(100%)
Neutral	16(66.7%)	8(33.3%)	24(100%)
Not Serious	4(100%)	0(0%)	4(100%)
Very Not Serious	2(3%)	0(0%)	2(100%)
Total	68(60%)	45(40%)	113(100%)

Table 6 shows that the average for Android respondents is 4.019 with a standard deviation of 0.8576, the average for iOS respondents is 3.833 with a standard deviation of 0.9606, the average score for users having both operating systems is 3.941 with a standard deviation of 0.8269. Compared to iOS respondents, Android respondents believe that the mobile security risk is serious, which is similar to the research result from Benenson (2013). Android users are more concerned with privacy security issues than iOS users.

Table 6: Analysis of Smartphone Operating Systems and Opinions for Severity of Mobile Security Risk

	Android	iOS	Mixed	Total
Very Serious	17(54.8%)	9(29%)	5(16.2%)	31(100%)
Serious	23(44.2%)	23(44.2%)	6(11.6%)	52(100%)
Neutral	13(54.2%)	5(20.8%)	6(25%)	24(100%)
Not Serious	0(0%)	4(100%)	0(0%)	4(100%)
Very Not Serious	1(50%)	1(50%)	0(0%)	2(100%)
Total	54(47.8%)	42(37.2%)	17(15%)	113(100%)

From Table 7, 67% of people think that MSA is important or very important. The proportion of female respondents who believe that MSA is important or very important (77%) is higher than that of male respondents (58%). The overall average is 3.912 with a standard deviation of 0.996. The mean value for opinions of females with respect to importance of MSA is 4.244 with a standard deviation of 0.9572, and that of males is 3.691 with a standard deviation of 0.9659. The t-test shows that the difference between both cases is at a level of 0.05 ($P=0.15<0.05$), which indicates that female respondents pay more attention to MSA than male respondents. Although most people think that MSA is very important, only 29.2% of the respondents actually install MSA, and it is worth exploring potential causes.

Table 7: Analysis of Gender and Opinions for Importance of MSA

	Male	Female	Total
Very Important	15(38.5%)	24(61.5%)	39(100%)
Important	25(69%)	11(31%)	36(100%)
Neutral	21(75%)	7(25%)	28(100%)
Unimportant	6(66.7%)	3(33.3%)	9(100%)
Very unimportant	1(100%)	0(0%)	1(100%)
Total	68(60%)	45(40%)	113(100%)

With analysis from the perspectives of different smartphone operating system (Table 8), the average for Android is 4.074 with a standard deviation of 0.9877, the average for iOS is 3.690 with a standard deviation of 0.9497, and the average score for users having both operating systems is 3.941 with a standard deviation of 1.088. Compared to iOS respondents, Android respondents think that MSA is more important.

Table 8: Analysis of Smartphone Operating System and Opinions for Importance of MSA

	Android	iOS	Mixed	Total
Very Important	25(64%)	8(20.5%)	6(15.4%)	39(100%)
Important	11(30.5%)	18(50%)	7(19.5%)	36(100%)
Neutral	15(50.6%)	12(42.8%)	1(3.6%)	28(100%)
Unimportant	3(33.3%)	3(33.3%)	3(33.3%)	9(100%)
Very unimportant	0(0%)	1(100%)	0(0%)	1(100%)
Total	54(47.8%)	42(37.2%)	17(15%)	113(100%)

With respect to users having different familiarities with technology, the results for opinions on mobile security risks are shown in Table 9. The average for users who are very familiar with technology is 3.762 with a standard deviation of 1.0443; the average for users who are familiar with technology is 3.923 with a standard deviation of 0.9565; the average for users having neutral familiarity with technology is 4.021 with a standard deviation of 0.7852; the average for users who are unfamiliar with technology is 3.5 with a standard deviation of 0.7071; and the average for users who are very unfamiliar with technology is 4.333 with a standard deviation of 0.5774. Due to an excessively small number of people who are very unfamiliar with technology, the result impact is ignored. It can be seen that those with neutral familiarity with technology believe there is a higher severity for mobile security risks than those are familiar with technology.

Table 9: Analysis for Severity of Mobile Security Risk Based on Familiarity with Technology

	Very Serious	Serious	Neutral	Not Serious	Very Serious	Not total
Very Familiar	4(19%)	12(57%)	2(9.5%)	2(9.5%)	1(5%)	21(100%)
Familiar	12(30.8%)	15(38.5%)	10(25.5%)	1(2.6%)	1(2.6%)	39(100%)
Neutral	14(29.2%)	22(45.8%)	11(23%)	1(2%)	0(0%)	48(100%)
Unfamiliar	0(0%)	1(50%)	1(50%)	0(0%)	0(0%)	2(100%)
Very Unfamiliar	1(33.3%)	2(66.7%)	0(0%)	0(0%)	0(0%)	3(100%)
Total	31(27.4%)	52(46%)	24(21.2%)	4(3.5%)	2(1.9%)	113(100%)

For the survey with respect to intention about recommending MSA to friends or family, the main value for overall respondents is 3.65 with a standard deviation of 1.085, the main value for female respondents is 3.91 with a standard deviation of 1.062, the main value for male respondents is 3.47 with a standard deviation of 1.072, and females have higher intention than males for recommending installation of MSA to friends and family.

4.4 Analysis of Behavior

51% of the respondents have installed Apps downloaded from non-Apple App Stores or non-Google Play stores. Even the respondents who believe that mobile security risk is very serious will still download Apps from non-Apple and non-Google official app stores. 35.4% of the respondents never click on the advertisement links in mobile applications or website; 80% of the respondents who never click on links or files in unknown messages or mails. With comparison to both cases, the respondents are more aware of risks of links or files in unknown messages or mail. Regardless of the respondent's familiarities with technology, their awareness of advertisement links in applications or websites is relatively low. Accordingly, users would be subject to mobile security risk more easily when being infected with malicious programs via advertisement links from hackers.

Table 10: Analysis of Opinions on Severity of Mobile Security Risk and MSA Installation

	Having MSA installed	Having no MSA installed	Total
Very Serious	13(46%)	15(54%)	28(100%)
Serious	15(27%)	40(73%)	55(100%)
Neutral	5(20.8%)	19(79.2%)	24(100%)
Not Serious	0(0%)	4(100%)	4(100%)
Very Not Serious	0(0%)	2(100%)	2(100%)
Total	33(29%)	80(71%)	113(100%)

From Table 10, 33 respondents among the 113 respondents install MSA (29%), wherein only 1 respondent uses a paid version which is a bundle when purchasing computer antivirus software, while the others use free versions. The average score of the respondents who install MSA with respect to opinions on the severity of mobile security risk is 4.27 with a standard deviation of 0.719; the average score of the respondents who do not install MSA respondents respect to opinions on severity of mobile security issues is 3.8 with a standard deviation of 0.919; there is no significant difference between both cases ($P=0.454>0.05$). That is, the respondents who regard mobile security risk as being serious may not install MSA necessarily. In fact, only 34% of the respondents who think that mobile security risks are very serious will have MSA installed. This phenomenon deserves further investigation to understand the actual needs of users for mobile security and their thoughts on the current MSA.

From Table 11, 46.3% of the 54 Android respondents have installed MSA, 24.1% of them consider installation in half a year, and 29.6% of them do not consider installation; while 7.1% of the 42 iOS

respondents have installed MSA, 40.5% of them consider installation in half a year, and 52.4% of them do not consider installation. 29.4% of the 17 respondents who have both iOS and Android have installed MSA, 29.4% of them consider installation in half a year, and 39.9% of them do not consider installation. Obviously, the proportion of Android respondents who install MSA is higher than that of iOS respondents; regardless of the lower proportion of installation compared to iOS respondents, the Chi-square test also shows a significant level of 0.05 for the difference. Because Android is an open operating system with more serious security risks, MSA in the market focuses more on solving security issues of Android. iOS is a closed operating system with a more rigorous App review mechanism. Therefore, most mobile security products for iOS are featured of MDM (Mobile Device Management), privacy, safe browsing or related functions, rather than malicious program detection etc. There is less of a necessity for the installation of MSA, which is installed by fewer users. Although iOS platform is more secure, there are still 40.5% of iOS users who consider installing MSA, indicating that they are also very concerned about mobile security, and need to ensure their smartphones are secure. Understanding the mobile security concerns and needs of iOS users is an issue worthy of further study.

Table 11: Analysis of Smartphone Operating Systems and Installation of MSA

Installation Intention	Android	iOS	Mixed	Total
MSA has been installed	25(75.8%)	3(9%)	5(15.2%)	33(100%)
Having no MSA installed	29(36%)	39(49%)	12(15%)	80(100%)
Consideration in half a year	13(37.1%)	17(48.6%)	5(14.3%)	35(100%)
No consideration	16(35.6%)	22(48.9%)	7(15.5%)	45(100%)
Total	54(47.8%)	42(37.2%)	17(15%)	113(100%)

The proportion of females who install MSA (38%) is slightly higher than that of males (26%). This result is consistent with the opinion that females think that the mobile security risk is serious, and MSA is important, so that there is higher installation intention for MSA. 31% of the respondents who install computer antivirus software have MSA installed. This proportion is slightly higher than the proportion of the respondents who do not install computer antivirus software (21%), but the difference is not significant ($P=0.392>0.05$). That is, people who install computer antivirus software may not install MSA necessarily, and vice versa. This result shows that users do not transfer the experience for computer antivirus software to MSA clearly and will ignore the severity of mobile security risks.

Table 12: Analysis of Existence for Installation of Computer And Smartphone Antivirus Software

	Having MSA installed	Having no MSA installed	Total
Having Computer antivirus installed	29(31%)	65(69%)	94 (100%)
Having no computer antivirus installed	4(21%)	15(79%)	19(100%)
Total	33(29%)	80 (71%)	113 (100%)

4.5 Use Experience of MSA

The main factors with which the respondents choose MSA are as follows in order:

1) Reference to user reviews and recommendations (51.5%)
2) Search in App stores (39.4%)
3) Recommendation from and installation by family or friends (36.3%)
4) Attached to computer antivirus software (9.1%)

From the above, the user reviews and recommendations in the App stores are an important promotion channel for MSA. The main causes due to which MSA is not installed are as follows in order:

1) No knowledge about where to download or install (46.3%)
2) No impact from malware. (25%)
3) No data theft or files infected on mobile. (23.8%)
4) No knowledge about benefits and values of MSA (15%)
5) Waiting for attacks against smartphones prior to handling (12.5%)
6) No knowledge about existence of MSA (12.5%)

Most people who do not install MSA do not know how to download or perform the installation. This result shows that users are still unfamiliar with the impact of malware attacks on smartphones, and their security awareness is insufficient, so that they do not search for or download MSA in the App stores actively.

The top major MSA used by the respondents are as follows in order: Clean Master Security, 360 Security, Trend Micro and AVAST. 12.1% of the respondents do not remember what brands are used. Clean Master Security of Cheetah Mobile accounts for 42.4% of the users who join the survey, which is much higher compared to other brands. It is a China mobile App developer with the fastest overseas market expansion. Its products include Clean Master, PhotoGrid etc. According to statistics from App Annie, a market analysis company, Cheetah Mobile ranks second for global

non-game developers in Google Play and is surpassed only by Facebook. By September 2017, Cheetah Mobile has more than 600 million mobile users worldwide. Cheetah Mobile attaches great importance to the user experience. Issues feedbacks by users around the world are usually replied to within about 5 minutes to help customers solve the issues quickly. It is not difficult to understand why its market share is much higher compared to other MSA brands.

Among 33 respondents who have installed MSA, 45.5% of them have 1-2 years of experience and 27.3% of them have 3-4 years of experience in using MSA. 36.4% of the users use it once a week, 24.2% of them use it once every day, and 18.2% of them do not have a certain frequency of use. Most MSAs provide very diverse features, but users usually don't use or appreciate all features. The top 5 features of MSA which have been used by users are: 1) malware prevention (81.8%), 2) safe browsing (69.7%), 3) garbage file cleanup (66.7%), 4) call and message filter (36.4%), and 5) privacy protection (36.4%).

Whether or not MSA can provide users with perception of being protected is a very important key factor for good user experience. In this survey, most of the 33 MSA users (73%) are perceptive of being protected, 15% of them do not have an opinion, and 12% of them are not perceptive of being protected. Which interaction designs provide users with perception of being protected? 72.7% of users identify showing alerts proactively when threat is detected. 60.6% of users identify display of current security status and all security conditions listed after performing scan; 33.3% of users identify recommendation of configuring security settings; only 15.2% of users identify regularly provided security reports which allow them to be perceptive of being protected. Overall, showing alerts proactively and the display for current security status may provide users with stronger perception of being protected, while users are less perceptive of security reports provided regularly. 39.4% of users regard that MSA makes them perceptive of being disturbed, 36.4% of users have no opinion, and 24.2% of users are not perceptive of being disturbed. 75.8% of users who are perceptive of being disturbed believe that advertisement is the main cause of disturbance, followed by slower speed, power consumption, falsely blocking websites or applications, App recommendations, and inability to completely block threats. Advertisements are one of the revenue sources of many Freemium MSA and seem to be a necessary evil. How to utilize advertisement into MSA for better user experience, reduce interference with users, or create other revenue models without using excessive advertisements which reduce user satisfaction, is one of the topics that is worthy of consideration by developers.

5. Conclusions and Recommendations

This study tries to explore knowledge, attitudes, and behaviors of users regarding mobile security and MSA. From research results, more than half of the respondents are either familiar or very familiar with computer and smartphone technology, and most of them believe that mobile security risk is a serious issue. Compared to iOS respondents, Android respondents believe further that mobile security risk is more serious. Those having lower familiarity with technology believe in a higher risk of mobile security. Overall, MSA is important, but the proportion of MSA installation is not high due mainly to no knowledge about where to download or install or lower awareness of possible impacts resulted from mobile malwares. It is obvious that both marketing and usability designs of MSA need improvement. Males are more familiar with technology about computers and smartphones compared to females, but females pay more attention to mobile security and account for higher proportion of MSA installation compared to males. Fewer iOS users install MSA compared to Android users, but nearly half of iOS users have also considered installing MSA, showing that iOS users also care about mobile security and the risks. The technology familiarity level about computers and smartphones of respondents will not affect their attitude towards mobile security risk significantly, and their attitude towards mobile security risk will not affect their installation of MSA significantly. It seems that computer antivirus software installation experience would not affect installation intention of MSA significantly. The most commonly used MSA features are: Malware prevention, safe browsing, garbage file cleanup, call and message filter, and privacy protection. Proactive alerts for intercepting threats and current security status for smartphones could better provide users with perception of being protected, while providing regular security reports is less effective. Advertisement is the main reason for users to feel that they are interfered by MSA. These can provide references for MSA vendors to design a better MSA user experience. In the future, we may further study the difference between actual user behaviors and needs for different user groups with respect to mobile security and MSA, identify possible improvement areas for MSA, and help users have higher awareness about mobile security risks and prevent attacks by malwares and cyber hackers.

Literature References

[1] Amit, Y. “No iOS zone” – a new vulnerability allows DoS attacks on iOS devices. Retrieved from, 2015 https://www.skycure.com/blog/ios-shield-allows-dos-attacks-on-iosdevices/ (accessed on 2017 Mar 15)

[2] Benenson, Z, Gassmann F, Reinfelder, L. Android and iOS Users; Differences concerning Security and Privacy. CHI 2013 Extended Abstracts, April 27{May 2, 2013, Paris, France. ACM 978-1-4503-1952-2/13/04.

[3] Bonnington C, First Instance of iOS App Store Malware Detected. www.wired.com May 7, 2012. (accessed on 2017 Mar 20)

[4] Botha R. A., Furnell S. M., and Clarke N. L., From desktop to mobile: Examining the security experience, Computers & Security, vol. 28, no. 34, pp. 130-137, May 2009.

[5] Check point, How The CopyCat Malware Infected Android Devices Around The World https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/, 2017 (accessed on 2017 Mar 15)

[6] Chin, E., Felt, A. P., Wagner, D., Sekar, V., Measuring User Confidence in Smartphone Security and Privacy.

[7] Counterpoint, Almost Half Of Smartphone Users Spend More Than 5 Hours A Day on Their Mobile Device, 2017 https://www.counterpointresearch.com/almost-half-of-smartphone-users-spend-more-than-5-hours-a-day-on-their-mobile-device/ (accessed on 2017 Mar 15)

[8] Felt A, Finifter M, Chin E, Hanna S, Wagner D. A Survey of Mobile Malware in the Wild. PSM'11, Chicago, Illinois, USA, October 17, 2011.

[9] Furnell S., Securing mobile devices: technology and attitude, Network Security, vol. 2006, no. 8, pp. 9-13, Aug. 2006.

[10] Harbach M, Hetting M, Weber A, Smith M, Using Personal Examples to Improve Risj Communication for Security and Privacy Decisions, CHI 2014, April 26-May 01, 2014

[11] Jorgensen Z, Chen J, Gates C, Li N, Proctor R, Yu T. Dimensions of Risk in Mobile Applications: A User Study, CODASPY '15: Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, March 2015

[12] Kelley P, Consolvo S, Cranor L, Jung J, Sadeh N, Wetherall D. A conundrum of permissions: installing applications on an android smartphone. FC 2012 Workshops, LNCS 7398, 2012, p. 68–79.

[13] King J, How Come I'm allowing Strangers to Go through My Phone? Smart Phones and Privacy Expectations, 2012.

[14] Kruger, H., and Kearney, W. Consensus ranking – An ICT security awareness case study. Computers & Security, 254–259.,2008

[15] Landman M., Managing smart phone security risks, in 2010 Information Security Curriculum Development Conference, ser. InfoSecCD '10. New York, NY, USA: ACM, 2010, p. 145-155.

[16] Mansfield-Devine S., Paranoid android: just how insecure is the most popular mobile platform? Network Security, vol. 2012, no. 9, pp. 5-10, Sep. 2012.

[17] Ophoff J., Robinson M., Exploring End-User Smartphone Security Awareness within a South African context, 978-1-4799-3384-6/14/, 2014 IEEE

[18] PANG Jian Hao Jeffrey, CHUA Chee Leong, CHAN Guan Huat, LIM Seh Leng, Challenges in Mobile Security, DSTA HORIZONS, 2016

[19] Panko R., Corporate Computer and Network Security, 2nd ed. Boston: Prentice Hall, Jul. 2009.

[20] Percoco N J, Schulte S, Adventures in bouncerland. In Black Hat USA, 2012.

[21] Polla M. L., Martinelli F., Sgandurra D., A Survey on Security for Mobile Devices, IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter, 2013

[22] Quora, Can the WannaCry Ransomware Affect Phones? https://www.quora.com/Can-the-WannaCry-ransomware-affect-phones, 2017 (accessed on 2017 Mar 15)

[23] Sumita U., Yoshii J., Enhancement of e-commerce via mobile accesses to the internet, Electronic Commerce Research and Applications, vol. 9, no. 3, pp. 217-227, May 2010.

[24] Theoharidou M., Mylonas A., Gritzalis D., A risk assessment method for smartphones, Gritzails D; Furnell S; Theoharidou M.. 27th Information Security and Privacy Conference (SEC), Jun 2012

[25] Trend Micro, Seven Kinds of Malware on Android Devices and its Ranking, 2012 https://blog.trendmicro.com.tw/?p=2164(accessed on 2017 Mar 18)

[26] Urban J. M., Hoornagle C. J., Li S., "Mobile phones and privacy, Social Science Research Network, Rochester, NY, SSRN Scholarly Paper 1D 2103405, Jul. 2012.

[27] Zafar H., Clark J., Current state of information security research in IS, Communications of the Association for Information Systems, vol. 24, no. 1, Jun. 2009.

[28] Clean Master invest AI, 2017 https://meet.bnext.com.tw/articles/view/42051(accessed on 2017 Mar 15)